Evaluation of a Threat of Terrorist Attack on a Selected Soft Target

Bc. Jakub Smolan

Master's thesis
2023

Tomas Bata University in Zlín
Faculty of Logistics and Crisis Management

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav krizového řízení

Akademický rok: 2022/2023

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Jakub Smolan**
Osobní číslo:	**L22649**
Studijní program:	**N1032A020002 Bezpečnost společnosti**
Specializace:	**Rizikové inženýrství**
Forma studia:	**Kombinovaná**
Téma práce:	**Posouzení rizik teroristického útoku na vybraný měkký cíl**

Zásady pro vypracování

1. Vymezte měkké cíle a doporučená bezpečnostní opatření pro jejich ochranu na základě relevantních strategických a metodických dokumentů.
2. Zpracujte přehled metod posuzování rizik měkkých cílů ve vztahu k hrozbě teroristického nebo jiného násilného útoku v souladu s aktuální odbornou literaturou a relevantními metodickými dokumenty.
3. Popište současný stav zabezpečení vybraného měkkého cíle.
4. Proveďte posouzení rizik teroristického útoku na vybraný měkký cíl.

Forma zpracování diplomové práce: **tištěná/elektronická**
Jazyk zpracování: **Angličtina**

Seznam doporučené literatury:

1. APELTAUER, Tomáš, Zdeněk DUFEK, Benedikt VANGELI, et al. *Ochrana měkkých cílů*. Praha: Leges, 2019. ISBN 978-80-7502-427-5.
2. BENNETT, Brian T. *Understanding, assessing, and responding to terrorism: protecting critical infrastructure and personnel*. Second edition. Hoboken: Wiley, 2018, xiv, 487 s. ISBN 978-1-119-23778-5.
3. HESTERMAN, Jennifer L. *Soft target hardening: protecting people from attack*. Second Edition. London: Routledge, Taylor & Francis Group, 2019, xxvi, 460 s. ISBN 9781138391109.

Další odborná literatura dle doporučení vedoucího diplomové práce.

Vedoucí diplomové práce: **doc. Mgr. Tomáš Zeman, Ph.D. et Ph.D.**
Ústav krizového řízení

Datum zadání diplomové práce: **1. prosince 2022**
Termín odevzdání diplomové práce: **28. dubna 2023**

L.S.

doc. Ing. Zuzana Tučková, Ph.D.
děkanka

Ing. et Ing. Jiří Konečný, Ph.D.
ředitel ústavu

V Uherském Hradišti dne 2. prosince 2022

PROHLÁŠENÍ AUTORA DIPLOMOVÉ PRÁCE

Beru na vědomí, že:

- diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem diplomovou práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne: 28.9.2023

Jméno a příjmení studenta: Bc. Jakub Smolan

.....
podpis studenta

ABSTRAKT

Diplomová práce rozebírá možnosti ochrany a zodolnění vybraného měkkého cíle před teroristickými útoky a násilnými činy. Diplomová práce je rozdělena na teoretickou a praktickou část.

V teoretické části se práce zabývá vymezením pojmu měkkého cíle a popisem zodpovědnosti za jeho ochranu, popisuje stručně historii terorismu, hlavní teroristické aktivity a rovněž rozebírá příčiny radikalizace, taktiku a fáze teroristického útoku. Teoretická práce rovněž nabízí srovnání světových pohledů a přístupů k ochraně měkkého cíle.

Praktická část nabízí aplikaci zjištěných poznatků na vybraném měkkém cíli, zobrazuje možnosti vymezení problematiky řízení bezpečnosntích rizik měkkého cíle, analýzy současného stavu a návrh preventivního opatření na mitigaci rizik za účelem zvýšení bezpečnosti měkkého cíle.

Klíčová slova: BOZP, terorismus, bezpečnost, zbraň, invakuace, vnitřní hrozba

ABSTRACT

The thesis analyses the possibilities of protection and hardening of a selected soft target against terrorist attacks and acts of violence. The thesis is divided into theoretical and practical parts.

In the theoretical part, the thesis defines the concept of a soft target and describes the responsibility for its protection, briefly describes the history of terrorism, the main terrorist activities and also discusses the causes of radicalization, tactics and phases of a terrorist attack. The theoretical work also offers a comparison of world views and approaches to soft target protection.

The practical part offers the application of the findings to a selected soft target, shows the possibilities of defining the issue of soft target security risk management, analysis of the current state and proposal of preventive measures to mitigate risks to increase soft target security.

Keywords: Occupational safety and health, terrorism, security, weapon, invacuation, inner threat

ACKNOWLEDGEMENT

I would like to thank Mr. Ing. Vít Hofman and Mr. Tomáš Gawron for providing me with excellent feedback and valuable suggestions for the research and development of this work.

I hereby declare that the print version of my Bachelor's/Master's thesis and the electronic version of my thesis deposited in the IS/STAG system are identical.

CONTENTS

INTRODUCTION

Terrorism, whose name is derived from the Latin word “terror” is frequently understood as a criminal act of violence against people (soft target) or things (hard target). It is an attack that is meant to achieve political, religious or ideological goals. Terrorism is the perpetration and spreading of the word terror. It serves as mean of spreading insecurity and terror or to generate a sympathy or force the willingness to cooperate. Due to the vast globalization efforts our society is undertaking, the acts of terror are usually well coordinated throughout the society, and they often connect various criminals with similar beliefs and goals.

Protecting soft targets, such as public spaces or events, from potential attacks requires a comprehensive approach that includes physical security measures, staff training, and emergency preparedness plans. Here are some general steps that can be taken to protect soft targets:

Conduct a risk assessment: Conduct a comprehensive risk assessment to identify potential threats and vulnerabilities. The assessment should consider factors such as the location, the nature of the event or activity, and the potential impact of an attack.

Implement physical security measures: Physical security measures such as access control, perimeter security, and video surveillance can help deter potential attackers and provide early warning of an attack. The measures should be designed to be scalable and adaptable to changing threat conditions.

Train staff and stakeholders: Staff and stakeholders should be trained to recognize and respond to potential threats. This includes training on emergency response procedures, identifying suspicious behavior, and reporting potential threats.

Establish emergency response plans: Emergency response plans should be established that include procedures for responding to potential attacks. This includes evacuation plans, communication plans, and procedures for coordinating with first responders.

Implement technology solutions: Technology solutions such as facial recognition systems, license plate readers, and other sensor-based technologies can provide additional layers of security and early warning.

Engage with the community: Engaging with the community can help build trust and awareness and may provide early warning of potential threats. This includes partnering with local law enforcement, community leaders, and stakeholders to develop and implement security plans.

Overall, protecting soft targets requires a holistic and multi-layered approach that includes physical security measures, staff training, and emergency preparedness plans.

THE AIM OF THE WORK AND THE METHODS USED

This thesis deals with the protection of a soft target from a terrorist attack. The main stated objective of the thesis is to identify, analyze the risks threatening the soft target, and then propose treatments and mitigate the risks.

The thesis seeks answers to these stated sub-objectives:

- to conduct a literature search in the field.
- to identify the technical documents and publications and procedures used in the world for the protection of soft targets

For the preparation of the thesis, I used a multi-source method of gathering information from professional literature and internet sources. Input data for assessing the frequency of each type of threat, I obtained from the Global Terrorist Database and at the local level from publicly available police databases. (1) (2)

To establish a framework for the risk management process, I used the Vyhodnocení ohroženosti měkkého cíle. (3)

The Crowded Place Security Audit method was used to assess current security measures.

I consulted with experts in the field of occupational health and safety and legal possession of firearms, Mr. Ing. Vít Hofman and Master Tomas Gawron, the attorney-at-law behind the project "zbrojnice.com". (4)

Observation, multi-source information gathering, application of experience and practice, modelling, synthesis, questioning, identification, evaluation, and analysis methods were used to develop the thesis.

I. THEORY

1 DEFINITION OF A SOFT TARGET

A soft target is a thing, person or group of people that is usually easily accessible by a perpetrator. Soft targets are relatively scarcely protected, as almost every location in our cities fits in the definition of being a soft target. In general, soft targets (unlike hard targets) are vulnerable to a military or terrorist attack. Hard target is in contrary defended (protected against attacks until some extent) and is generally inaccessible to general public. Hard target could be a subject of crisis infrastructure (gas, oil or water supply pipelines, reservoirs, dams, redistribution centres, energetic infrastructure, power plants etc.).The topic of soft target protection is a relatively young discipline in the Czech Republic. Unfortunately, it is not very widespread in the public awareness, even though the current terrorism threat level in the Czech Republic is at level 1, i.e. a general threat resulting from the situation abroad, where there is no known specific threat of terrorist activities on the territory of the Czech Republic, but it is necessary to pay attention to general awareness. This is a long-standing standard state of the lowest, but not zero, threat of terrorism. The term soft target has typically been used to describe a public spaces or other locations that are easily accessible, predominantly civilian, and often have limited security measures in place. Those locations are numerous and have been a preferred target by attackers. Soft targets are places (objects, premises or events) with a high concentration of people and a low level of security against violent attacks. These are open spaces or enclosed areas accessible to the public where there is an increased presence of people, making them potentially suitable targets for armed attackers or terrorists.

- Bars, nightclubs, discos, restaurants, hotels,
- open space locations like parks, squares, demonstrations, fairs,
- tourist sites and attractions, museums, galleries,
- shopping malls, marketplaces, business complexes (opened and closed to pedestrians),
- schools,
- sports halls and stadiums,
- cinemas, theatres, concert halls, entertainment centers,
- hospitals, clinics, educational establishments, libraries,
- religious monuments and places of worship,

- airports, transport hubs, railway stations, bus stops.[1] (1)

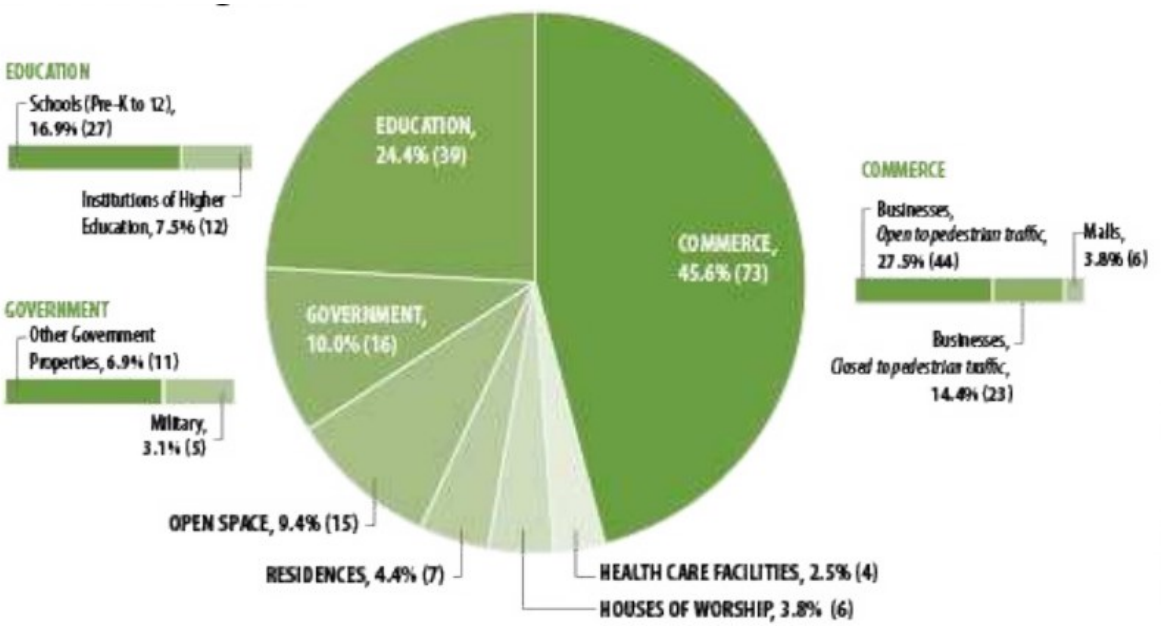

Figure 1 – Soft target locations in the USA where between 2000 and 2013 happened the active shooter incidents the most. Source: (2)

A stakeholder is any individual, group, or organization that has an interest or concern in a particular business or project. This can include shareholders, employees, customers, suppliers, partners, creditors, government agencies, and the community in which the business operates.

Stakeholders are generally interested in mitigating the threat of a terrorist attack due to its clearly negative effects on their safety, security, financial stability, or reputation.

[1] According to the Tony Blair's Institute for Global Change that as of the year 2017, an average 17 civilians were killed per day, often as a result of terrorist campaigns targeting public spaces like bus stops, town squares, marketplaces or places of worship. (77)

Figure 2 – Soft target security is at the heart of stakeholder concerns. Available from: author's collection. Source: Author's own collection.

1.1.1 Governments

Since it is the duty of governments to maintain the security and safety of their citizens, they have a keen interest in reducing the threat of terrorism. To stop terrorist operations, governments can put laws and programs into place that boost security precautions, intelligence collecting, and law enforcement.

1.1.2 Businesses

Terrorist attacks may have a direct impact on businesses, causing bodily harm, asset loss, operational interruption, and unfavourable publicity. By implementing security measures, engaging in contingency planning, and working with governmental organizations and other stakeholders, businesses have a role in reducing the threat of terrorism.

1.1.3 Communities

Terrorist attacks, which can cause fatalities, property damage, and social and economic upheaval, can have a significant impact on communities. By assisting local law enforcement, increasing public knowledge of potential threats, and fostering resilience to survive the impacts of a terrorist strike, communities can lessen the threat of terrorism.

1.1.4 Individuals

Terrorist attacks can have a direct impact on people, causing them to suffer bodily pain, mental distress, and financial losses. By staying alert, reporting suspicious activity, and supporting initiatives to stop terrorist operations, individuals can help reduce the threat of terrorism. The most common threats are mentioned in the official guidelines issued by the Ministry of Interior of the Czech Republic (name of the document Vyhodnocení ohroženosti měkkého cíle – which could be translated as the Evaluation of exposure the soft target's vulnerability). (3)

This document from the year 2017 lists these threats as relevant to soft targets:

- cold weapon attack,
- shooting,
- arson,
- taking of hostages, barricade incidents,
- explosives in the mailbox,
- crowd attack,
- poisoned pen letter,
- fake bomb planting,
- fake bomb threat reports. (3)

2 TERRORISM

Terrorism as a powerful military strategy has been known since the period of the Roman Empire. Its first use in the modern history is traceable to the French revolution and it's "reign of terror" or "La Terreur". (4)

In the 19th century was the term terrorism used to justify extremist political deeds, such as assassinations etc. A good example of the unprecedented upheaval that was caused by assassination of the Austrian Empress Sissi, and the new security threats it brought to daylight was the international conference of 21 nations where the rise of anarchism and terrorism was discussed. According to the Karl Pacner (Czech novelist) was the modern terrorism born in the modern Russia. This opinion could be observed quite in contrary, but it is imperative to understand that the early terrorists of the late 19th century and the early 20th century were predominantly anarchists with leftist beliefs whose main goals was the spread of communism. (5) (6)

Nowadays, terrorism is mostly connected to the Muslim radicals. Numerous Muslim terrorist groups and movements have been present since the so called "year zero". The exact number of officially recognized groups remains uncertain but to the most important movements belong Afghan Taliban, Al-Nusrah, Hamas, Hizballah, Boko Haram or the so-called Islamic State of Iraq and the Levant. (7)

A common unification element is the ability to spread the terror with a clear intention to achieve a political goal.

Not only terrorism with religious background exists. According to the Gemeinsames Extremismus- und Terrorismusabwwehrzentrum (GETZ) we can observe official governmental initiatives that aim to fight against various faces of radical terrorism, such are:

-left wing radicals,

-right wing radicals,

-international terrorism (supported by a government of another country). (8)[2]

[2] Such governmental approaches span throughout the entire society and the law-enforcing system and they associate single units into integrated system. In the case of Germany, the system covers the entire country on the federal level. The biggest advantages of this unified system are shorter lines of communication, improved interagency collaboration, timely compression, better evaluation of information, strengthened analytical capability and easier coordination of operations. (8)

According to the Global Terrorist Database, in the Europe between the years 1970 and 2020 12212 terrorist attacks occurred. To classify the attacks, they must correspond with selected criteria:

- the attack aims to reach a political, economic, social, or religious goal,
- the attack aims to spread a message to a larger audience,
- the attack is outside of the context of legitimate warfare activities.

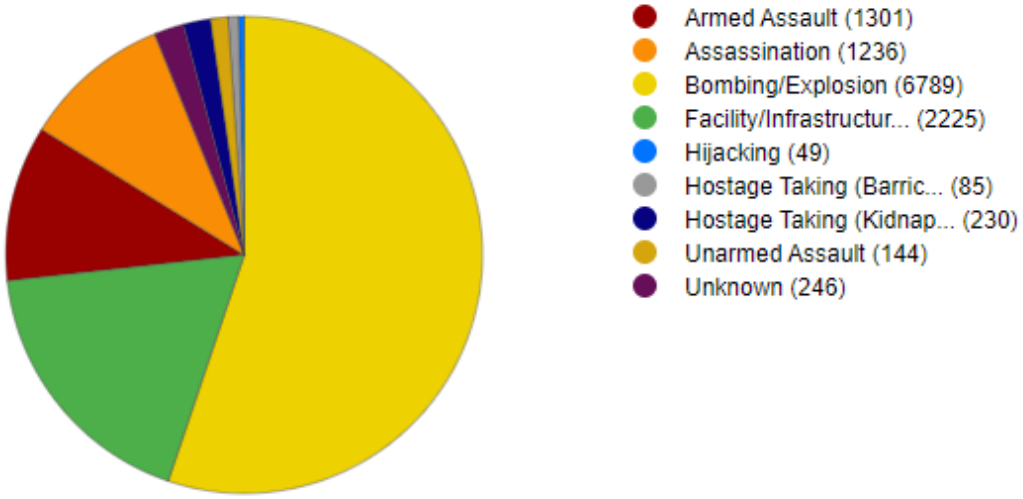

Figure 3 – Terrorist attacks by the attack type. Source: (9)

The Global Terrorist Database shows (Figure 3), that the most frequent type of an attack is the bomb attack. On the second place, the facility and infrastructure were labeled as the second most vulnerable target. Armed assault and assassination are likewise frequent ways how to hit the soft target.

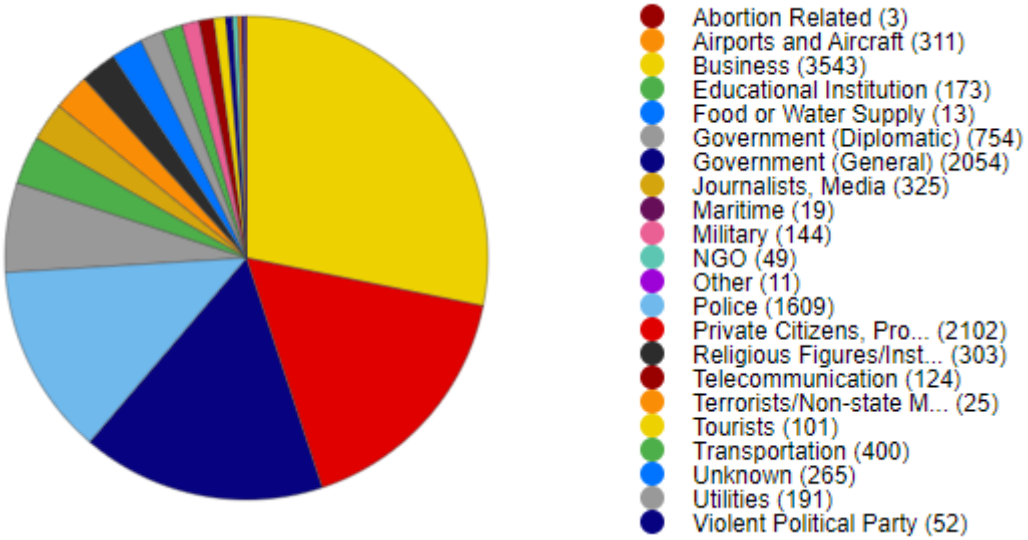

Figure 4 – The most common types of targets of terrorist attacks. Source: (9)

The Figure 4 describes the most common targets of a terrorist attack. Unsurprisingly, the business premises are on the first place, closely followed by private citizens, government targets and police.

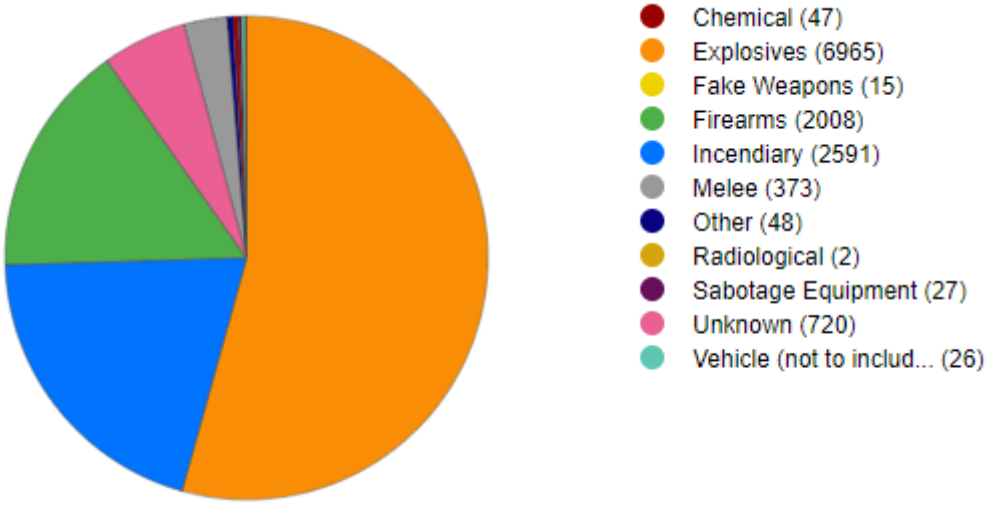

Figure 5 – The most used weapon types. Source: (9)

From the Figure 5 we understand that the most popular way of hitting a soft target is the explosive. Incendiary weapon is probably due to its easy manufacture on the second place. Firearms, both legally or illegally held, come on the third place.

2.1 Phases of Terrorist Attack

Every terrorist attack shows similarities and patterns, that describe the phases of selecting the target, the planning itself that describes how the attack should be conducted and final deployment on the location of the attack. Those steps could be also described as the pre-attack phase. Following this phase, the attack itself happens. When successfully conducted, and if the perpetrator managed to escape the scene, the post-attack stage of direct / non-direct exploitation sets in. (10)

Figure 6 – stages of the terrorist atack. Sourcs: (11)

2.1.1 Target Selection

Stage of preselection of the final target that will be attacked. The targets are usually chosen upon the criteria of the "biggest vulnerability". The most vulnerable target is usually the most desirable, tempting object of a terrorist attack. During the stage of target selection, the attackers may consider using all information sources possible. The most vulnerable and therefore welcome targets are usually those, where the police presence is not expected or where the attack could cause the biggest harm with the minimum effort. Attacker is always choosing the target according to what the options of hitting the target are. Significant role

also plays the range of weapons that are at the attacker's disposal (truck, firearm, chemical agents, explosives etc.) (10)

2.1.2 Planning

During the phase of planning, the terrorists may visit the location in person. Deliberate terrorist attack that is meant to be successful needs excessive preparations and many of them could not be done online. The mode of attack depends on many variables, such is the density of population, building construction, significance for the society or even daytime. (10)

2.1.3 Deployment

Is the phase when the attacker(s) move into the default positions from which is the attack later launched. (10)

2.1.4 Attack

Usually very hard to detect before occurring. This phase describes the entire duration of the attack, the longer it takes, the more casualties it produces. The final number of casualties is also dependent on the ability of attacker to move freely on the scene of attack. (10)

2.1.5 Escape

After a successfully conducted attack, the assailant tries to escape to be able to either fight another day or to exploit the consequences of the attack. The perpetrator will usually try to escape unseen, using various fewer known routes of potential escape. (10)

2.1.6 Exploitation

Act of terror could be promoted by surviving attacker himself or by other members of the terrorist organization. The main goal of exploitation is to spread the fear of future attacks and to recruit new members. (10)

2.2 Threat of Radicalization

Radicalization refers to the process by which an individual or group adopts extreme beliefs and ideologies that reject or undermine the values of mainstream society. The threat of radicalization is that individuals who become radicalized may turn to violence or other forms of extremism to achieve their goals. This can pose a serious risk to public safety and security,

as well as to the well-being of individuals who are targeted by extremist groups or individuals. (12)

Radicalization can take many forms, and it can occur within a wide range of ideological and religious contexts. Some of the factors that can contribute to radicalization include a sense of social isolation, a desire for belonging and purpose, exposure to extremist propaganda, and experiences of discrimination or marginalization. (13)

Radicalization is one of the biggest security problems; it is the strategy of a terrorist organization that mobilizes individuals to support the tactics and goals of the terrorist organization. The process of radicalization is highly individual and can be described as a multidimensional process in which an individual adopts distinct views and attitudes towards accepting, endorsing, supporting, and implementing violence based on an accepted ideology or belief. (14) (15)[3]

The transformation of an individual into the role of a terrorist is a long-term process that exhibits typical characteristics such as pathways and stages. The common features of radicalization are a section of the population suffering from a sense of injustice and unfair treatment, and this section of the population is unable to deal with such situations without resorting to aggression. This segment of the population uses all available legitimate means to correct perceived injustices. If these means fail, the individual is placed in a difficult social and psychological situation, becomes frustrated and accumulates anger and aggression. It is at this stage that the individual is most vulnerable to radicalization. Terrorist organizations therefore often attack feelings of despair, unhappiness and hopelessness and use them to start recruitment. The next step is gradual indoctrination into the ideology or beliefs held, which may be paralleled by intensive physical training and increasing psychological stress. The individual is tested for his or her reliability by being put through simple tasks. The individual's identity is reinforced in the new group and contacts with the original society are muted, with emphasis on concealing ties to the terrorist organization and reinforcing the us-versus-them viewpoint. (16) (13)

[3] Radiaclization could be also described as a psychological process when an individual accepts extremist manifestations, opinions and ideas. (82)

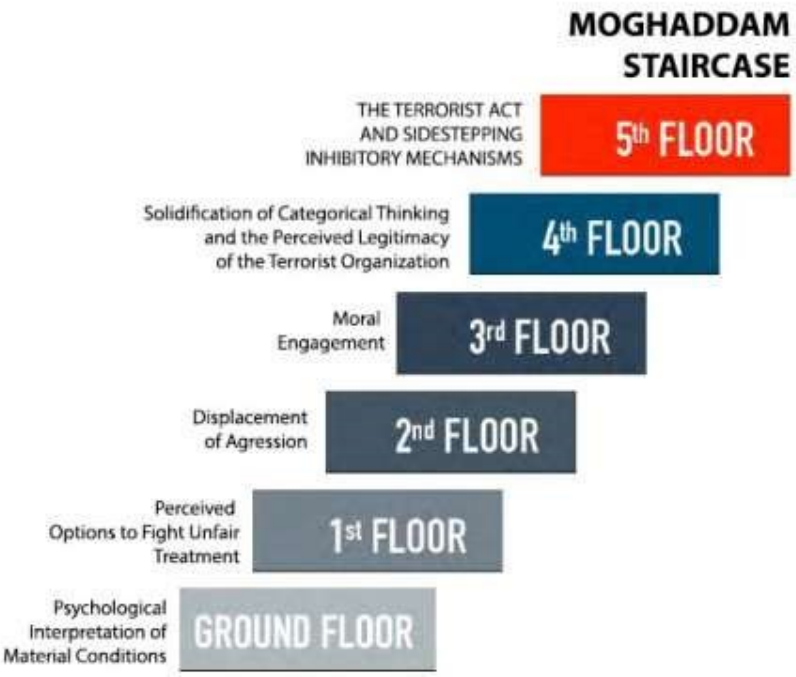

Figure 7 – Model of radicalization according to MOGHADDAM – staircase to terrorism. Sourcs: (17)

The basic common elements showed in the Figure 7 describe the mind-set justifying terrorism have the following basic elements: a sense of injustice (wrong) felt by a part of society towards the majority (national, religious, ethnic, political, etc.)[4], a clearly identified culprit – a common enemy (Jews, Christians, Americans, Europeans...) and the choice of a method to remove the cause of the injustice. (13) (18) (19)

2.3 Detection of Radicalization

One of the most important foundations for early detection of dangerous behavior is the ability and opportunity to identify radicalizing symptoms. These symptoms indicate that an individual is being radicalized, is in the process of radicalization or is directly radicalizing others. Planning or preparation for an act of violence can be inferred from these signs. A common problem is the lack of awareness of this issue. Indicators of radicalization can often be downplayed or overlooked, mainly due to fear of ridicule or fear of being labelled as an "informer" in society. [5] (13)

[4] A clear example is the Orland gay nightclub shooting. The perpetrator pledged allegiance to the ISIS, but one of the possible motives could be his own hidden sexual orientation. (83)

[5] In terms of early detection and identification, we speak of so-called warning signs or radicalization indicators. (13)

The basic prerequisite is a functioning community - a system of community policing. It is a greater degree of integration of the police into the civic community.

The basic features are:

- -being visible and accessible to citizens,
- to be knowledgeable,
- responsiveness to the needs of the community,
- listening to concerns and fears. (20) (21)

Radicalization can be detected in the soft targets themselves. According to the manual issued by the Ministry of the Interior of the Czech Republic, these objects can be soft targets as well (a complete description of soft targets and their detailed enumeration is given in the preceding chapter):

- -school facilities, dormitories, canteens, libraries,
- -church monuments and places of worship,
- shopping malls, marketplaces, and commercial complexes,
- -cinemas, theatres, concert halls, entertainment centers,
- rallies, parades, demonstrations,
- bars, clubs, hotels, discos, restaurants,
- parks, squares, tourist sights, places of interest, museums, galleries,
- -sports halls and stadiums,
- major transport hubs, train and bus stations, airport terminals, metro,
- hospitals, polyclinics, and other medical facilities,
- public gatherings, parades, pilgrimages,
- cultural, sporting, religious events,
- community centers. (13) (22)

2.4 Signs of a Terrorist Behavior

Terrorist attacks, like any other kinds of planned, deliberate violence, could be recognized with help of some unifying elements of suspicious behavior. Among the most frequent kinds of a suspicious behavior belong:

- surveillance – observation of the target during the planning phase,
- inquiries – attempts to gain information about a place, person, procedure, or security level of the target,
- testing the security – attempts to gather data by observing the target's or law enforcement's response to a security event (how long does it take to arrive to the location of the security breech etc.),
- fundraising – efforts to gain financial means like credit card frauds, defrauding the elderly, donations to legitimate organizations by peculiar ways or money laundry,
- acquiring supplies – piling up of purchased, counterfeit or stolen weapons, ammunition, explosives or harmful chemical equipment, uniforms, or identification of first respondents, military or police uniforms, ID cards,
- out-of-place / suspicious behavior – people who just "don't belong" to the place, a person that does not fit into the environment due to language used, unusual questions asked or their demeanor,
- dry run,
- deployment to the position,

And in the social media sector – those indicators could be discovered by using the OSINT, IMINT, SOCMINT, HUMINT techniques:

- changing your name, choosing a nickname,
- changing the style of dress,
- change of appearance, tattoos, and body modifications,
- trying to contact the leaders of the movement,
- ownership of propaganda books and magazines.
- ownership of promotional items,

- change in religious practice,
- monitoring information sources with extremist content,
- glorification of violence and martyrdom, (23) (13)

Signs of radicalization in prisons:

- intensive writing and correspondence about extremist ideologies,
- intensive reading about extremist ideologies,
- forming or joining a group,
- public speaking, presentation of views,
- isolating oneself from others,
- getting a new tattoo with a link to an ideology,
- aggression,
- intensive prayer and religious practice,
- stigmatization of other inmates,
- change in diet,
- increased frequency of correspondence with new contacts,
- refusal of contact with family,
- listening to characteristic music,
- drug use. (24)

2.5 Tactics of Terrorist Attack

Soft targets face a wide range of threats of different types from individuals and groups with different motivations. The current trend is to target public places with weak security. The link to religion or nationality is playing less and less of a role. clearly the most common type of terrorist attack globally is the bombing.

Element of unification for all the basic threats is a regular criminal activity, usually mixed with common acts of violence. In addition to the basic list of threats, few specific ways of attack could be added.

2.6 Armed Assault

An armed assault is a violent attack committed by one or more people using firearms, knives or other weapons to inflict physical harm or injury to other people. This kind of assault usually occurs on public places, private residences, business premises and other locations generally accessible by the public. The use of appropriate weapons could significantly enhance the number of killed or injured people. An armed assault is a serious offense resulting in penalties like imprisonment and other repercussions from the law.

2.6.1 Assassination

Assassination, in other words, deliberate act of killing, is according to the Czech penal code and act that results in death of human being. It is an act that could not be legally or ethically justified, therefore is usually punished with the most severe sentences possible. A person that deliberately kills another person, is called a murder, to the person killed is usually referred as to the victim. Act of killing has usually direct or indirect motive. Assassination as an act of terrorism is in the Czech penal code anchored in the paragraph 311. Most common weapons used in assassinations are firearms in general, but also cold weapon attacks or bombing. Assassination is mainly used against an individual (usually a high-positioned person) that is somehow significant in the relation to the targeted audience or plays an important role in the community the terrorist wants to intimidate. (25)

2.6.2 Cold Weapon Attack

This is one of the most unpredictable terrorist attacks that could be done with every sharp or blunt object. Cold weapon attacks are usually committed by so-called “lone-wolfs” who are individuals, on many occasions, immigrants, or drug addicts etc. Although it is exceedingly difficult to say, whether the knife attack is or isn’t an act of terror. In many cases, the knife attacks are usually undertaken spontaneously, without prior elaborate planning. Cold weapon attacks are an important source of threats, as they are usually committed spontaneously and are hard to predict. The motives are often unclear, as many countries remain on high-alert status after series of deadly attacks by Islamist radicals since 2015. (26)

One of the “most-spread” cold weapons is the knife causing the stab or cut wound. (27)[6]

[6] For instance, in the USA between the years 1965 and 2012, knife was the „most popular“ cold weapon to commit homicide with. (78)

A stab wound is a type of injury that occurs when a sharp object, such as a knife, scissors, or a broken bottle, penetrates the skin and enters the body. Stab wounds can cause damage to internal organs, blood vessels, and nerves, and can be life-threatening depending on their location and severity. (28)

Stab wounds can vary in depth and size, and their severity depends on the force of the object that caused them, as well as the location of the wound. A superficial stab wound may only affect the skin and underlying tissues, while a deep stab wound may penetrate vital organs and cause significant bleeding. (28)

Symptoms of a stab wound may include pain, bleeding, swelling, and difficulty breathing or moving. In some cases, symptoms may not be immediately apparent, and the severity of the injury may become more apparent over time. A cut wound is a type of injury that occurs when a sharp object, such as a knife, razor, or broken glass, cuts through the skin and into the tissues below. Cut wounds can vary in severity, depending on the depth and location of the cut, as well as the type of object that caused the injury. (29)

Like stab wounds, cut wounds can cause bleeding, pain, and swelling. The severity of the injury will depend on the depth of the cut, whether it has damaged underlying structures such as muscles, tendons or nerves, and how quickly medical attention is sought. If the wound is deep, bleeding profusely or has affected any important structures, it is important to seek medical attention as soon as possible. In some cases, stitches or other medical procedures may be required to close the wound and prevent further complications such as infection or excessive bleeding. (29)

One of the best tactics how to respond to a knife stabbing attack as a civilian bystander is to bring a gun to a knife fight. Physically confronting a furious attacker could be very difficult and could lead to severe injury or death. Also, the use of overpowering force is necessary (more than one person) to neutralize the assailant. Neutralizing the attacker with a more potent weapon like a firearm might be a good tactic. (30)

2.6.3 Shooting

Since the beginning of their existence, firearms have been designed primarily to destroy living things, and most of them are still used today to shoot against living creatures. Gunshot wounds caused by small-caliber or micro-caliber projectiles fired from small arms and shrapnel injuries are the dominant group among conventional weapons in terms of relative frequency. The fact that they are much more serious than mechanical injuries (stab wounds, cuts, lacerations) from a health point of view contributes to their importance. Gunshot and

shrapnel injuries are life-threatening and leave permanent effects on the victim. The branch of science that deals with gunshot injuries of this type is called wound ballistics and is part of so-called transitional ballistics (31).

A shooting attack, also known as a mass shooting, is an incident in which one or more individuals use firearms to shoot and kill or injure several people in a public or private location. It is an incident of violence "using firearms" where many victims are involved. Shooting attacks can occur in a variety of settings, such as schools, workplaces, places of worship, shopping malls, and public spaces.[7] (32)

Shooting attacks can be planned or may occur spontaneously. The motives behind such attacks can also vary, including revenge, terrorism, mental illness, or other reasons. (8)

Shooting attacks can cause significant physical and emotional harm to the victims, their families, and the community at large. Survivors of shooting attacks may experience long-term physical injuries and psychological trauma. (31)

In the event of a shooting attack, it is important to prioritize safety and take necessary precautions, such as running away, hiding, or fighting back if necessary. Seeking medical attention as soon as possible and reporting any suspicious behavior to authorities can also help prevent future attacks. (8)

Majority of the active shooters would want to cause the greatest harm in the shortest possible period. Most of the individuals use handguns and assault rifles. Some of the individuals purchase the guns legally, however, it is not rare that those attacks are also committed with a gun stolen from a family member. (33)

Elements, that are making a gun “more dangerous” are:

- firing mode,
- magazine capacity,
- barrel length.

Firing mode describes the “number of bullets” the shooter can fire upon pressing the trigger. Currently, we recognize between **manual**, **semi-automatic**, **fully automatic** and /or **burst-firing** mode firearm. Single modes of fire are adjusted by a **selector** switch. Usually, weapons available to civilians operate in manual or semi-automatic firing mode. (34)

Fully automatic weapons are restricted for civilian use and therefore are available to military or law enforcement units only. Civilian shooters, who possess a firearm, have to go through

[7] Soft targets as defined in the beginning of this thesis.

a relatively complicated process of gun ownership. This process consists of medical examination, and they must pass an exam. Sometimes, additional psychological examination of candidate is needed. Fully automatic gun could be entrusted to soldiers, reservists, police force without the need of having to pass the forementioned procedure.

Selector switch firing modes that enable to operate the gun in single, burst and full auto mode are depicted in the Figure 8. (35)

Fig 8 - Selector switch firing modes.

Magazine capacity is another factor that affects the ultimate use of the firearm. Bigger the magazine, higher the magazine capacity and higher the amount of ammunition the shooter can fire on one loading of the firearm. Most of the firearms are so designed, that they will not operate without the magazine attached. Guns like shotguns have built-in magazine, but most firearms do not. Currently, there are several sizes of magazines. In the Czech Republic, their ownership is restricted by the size of the magazine. Below-limit magazines for rifles firing the classical central-fired round is a magazine with capacity of 10 rounds. Anything else that has the capacity to carry more than 10 rounds is an over-size magazine and thus falls to obligation to hold an exemption to own an over-size magazine. For small firearms (pistols) the same principle is applied, whereas the oversize limit lies at 20 rounds of capacity of a magazine. (38)

Figure 9 – Rifle magazine size comparison. Source: (36)

Barrel length is a crucial factor that allows or in contrary does not allow concealed carry of weapon. Smaller guns (small arms, handguns with short barrel length or just saw offs) are easier to hide under the clothes or in the luggage and therefore harder to detect by law enforcement, security employees or civilians. Timely disclosure of an armed perpetrator helps reduce number of casualties or can lead to stop the attack before it happens.[8] Specific attention requires smuggled military weapons. A country where the war is going on, is always a significant and easily accessible source of military-grade weapons to the illegal market. So far, there has not been any major incident where the smuggled weapons would be found but that could change anytime. The volume of weapons sent to Ukraine in form of international help raises alarm. Donated weapons, especially small weapon systems are extremely hard to find. [9] (36)

2.6.4 Active shooter

An active shooter is an individual who is actively engaged in killing or attempting to kill people in a populated area, typically using firearms. Active shooters may target specific

[88] According to research posted in The New York times, 64 attacks out of 433 were thwarted by a bystander, 42 times the attacker was subdued and 22 times even shot beforehand. (88)

[9] Smuggled weapons captured in the Gulf of Oman could be sent to Ukraine in form of international military aid. (89)

individuals, groups of people, or may simply shoot indiscriminately. Active shooter situations are typically fast-moving and unpredictable, and can occur in a variety of settings, such as schools, workplaces, and public spaces. The goal of an active shooter is to inflict as much harm as possible in a short amount of time, often causing mass casualties and widespread panic. (37) (38)

Number of active shooter incidents since the year 2000 is at least in the United States of America on the rise.

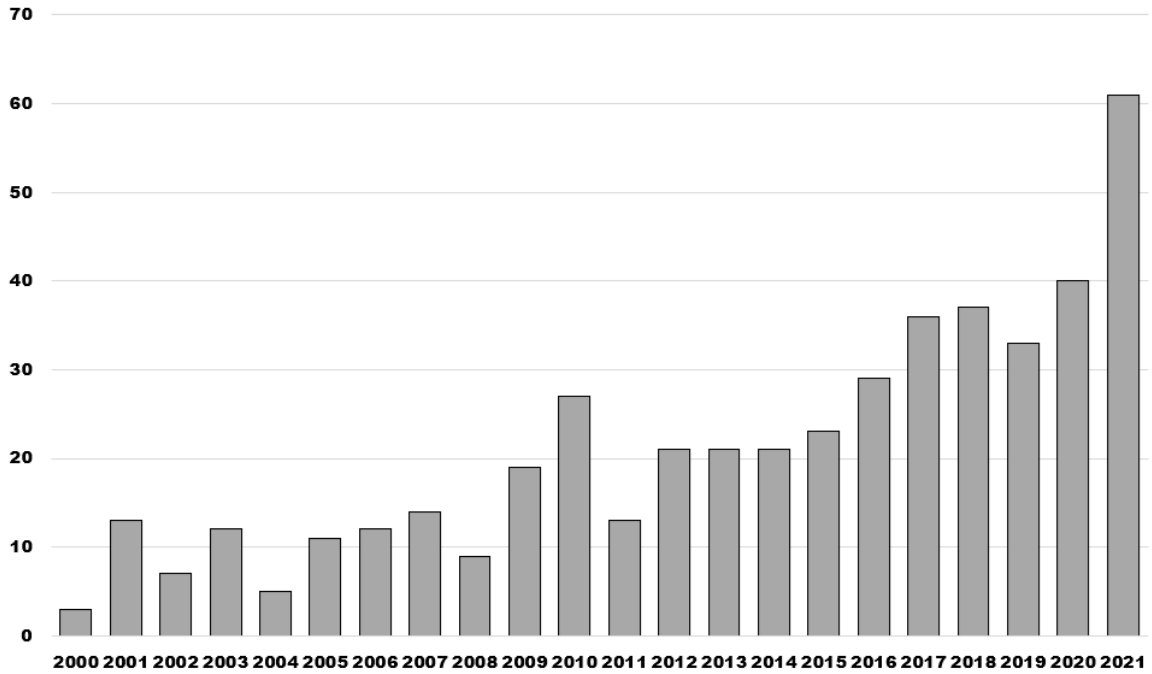

Figure 10 – Active shooter attack frequency in the USA shows for the period 2000 – 2021 a clear upward trend. Source: (39)

The fastest increases in the frequency of active shooter attacks are between the years 2019 and 2021 and are demonstrated in the Figure 11.

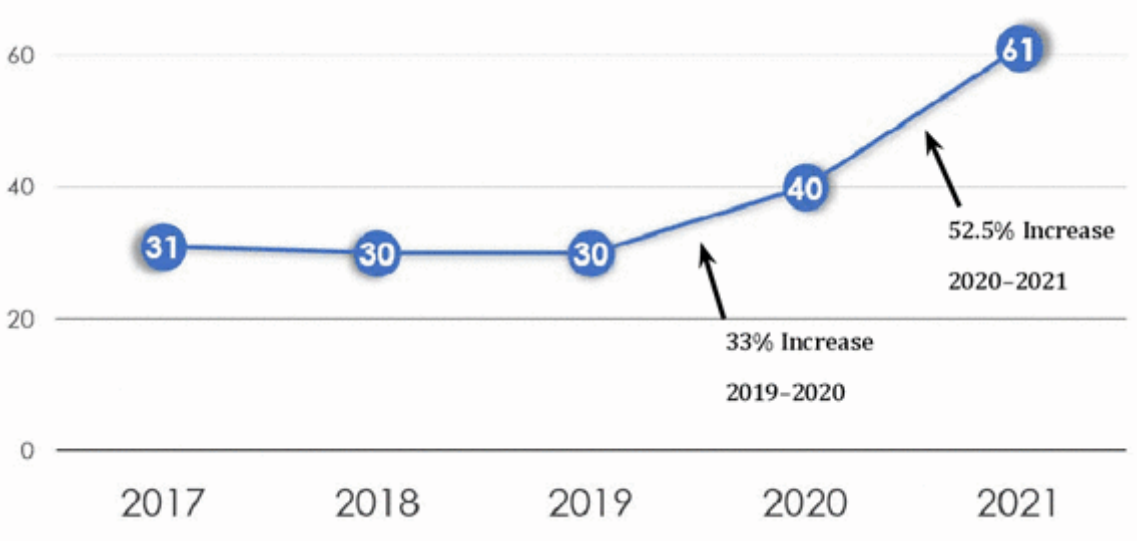

Figure 11 Active shooter incidents in the USA in the years 2017 to 2021. Source: (40)

Most of the active shooter incidents happens in June, as the Figure 12 indicates.

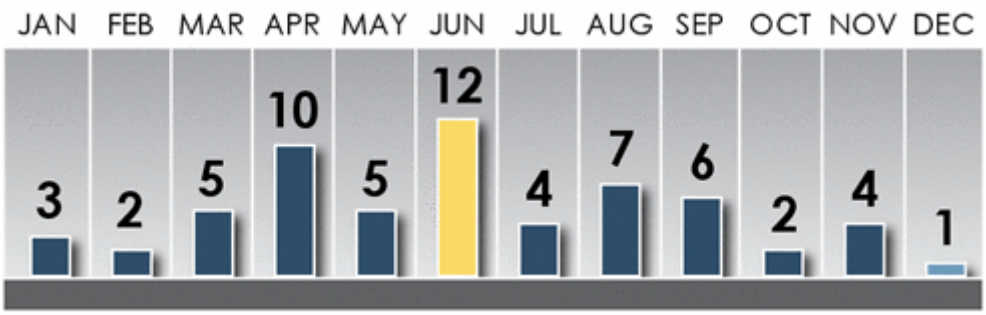

Figure 12 – Active shooter incidents by month. Source: (40)

As shown in the Figure 13, out of seven weekdays, Tuesday, Thursday and Saturday were the days when the most attacks happened.

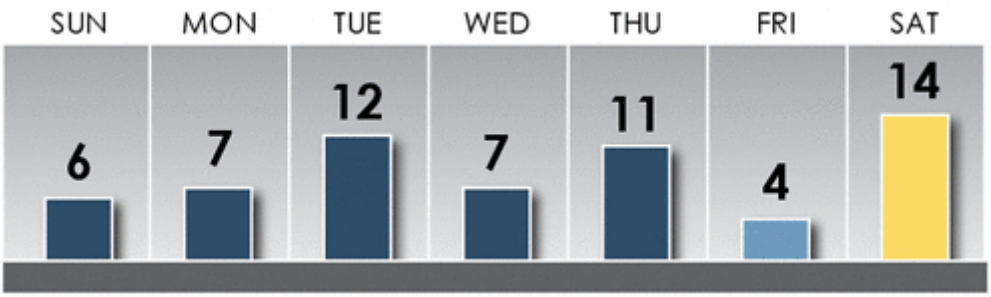

Figure 13 – Active shooter incidents by Day of the Week. Source: (40)

Most of an active shooting incident is likely to occur between 6 a.m. and 5 p.m. with isolated increase around 6 p.m. states the Figure14.

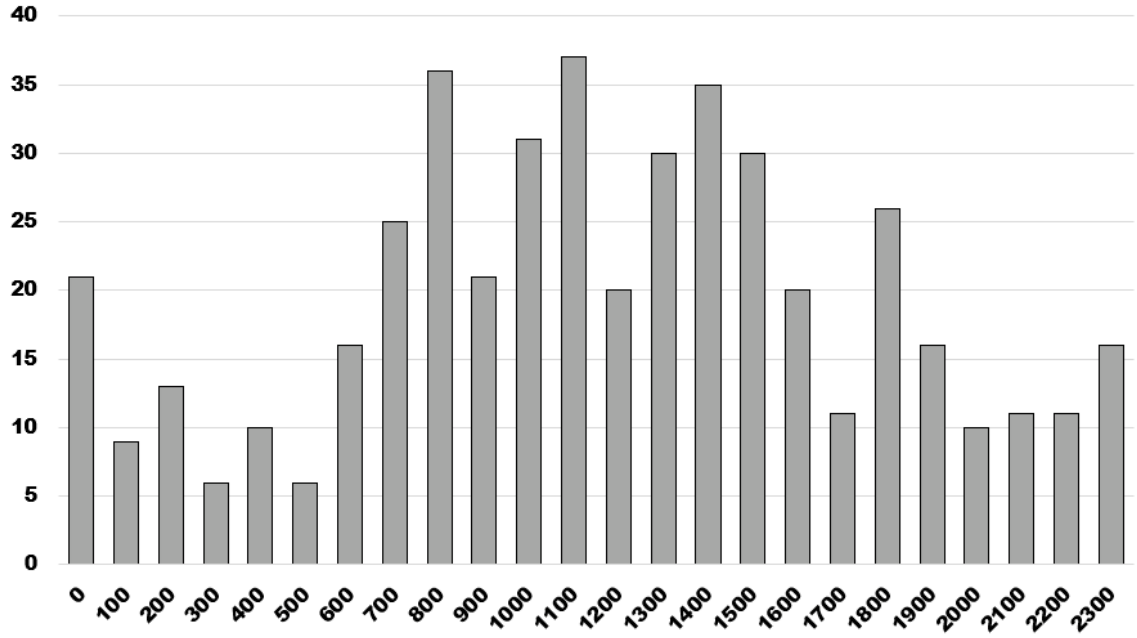

Figure 14 – Numbers of active shooter incidents by Time of Day. Source: (41)

According to the Figure 15, many attacks happens in places of business (more than 50% of attacks). Those places include warehouses, factories, retail locations or office space. The second most frequent location to suffer from an active shooter attack is the public space followed by schools and other locations (military bases, places of worship etc.)

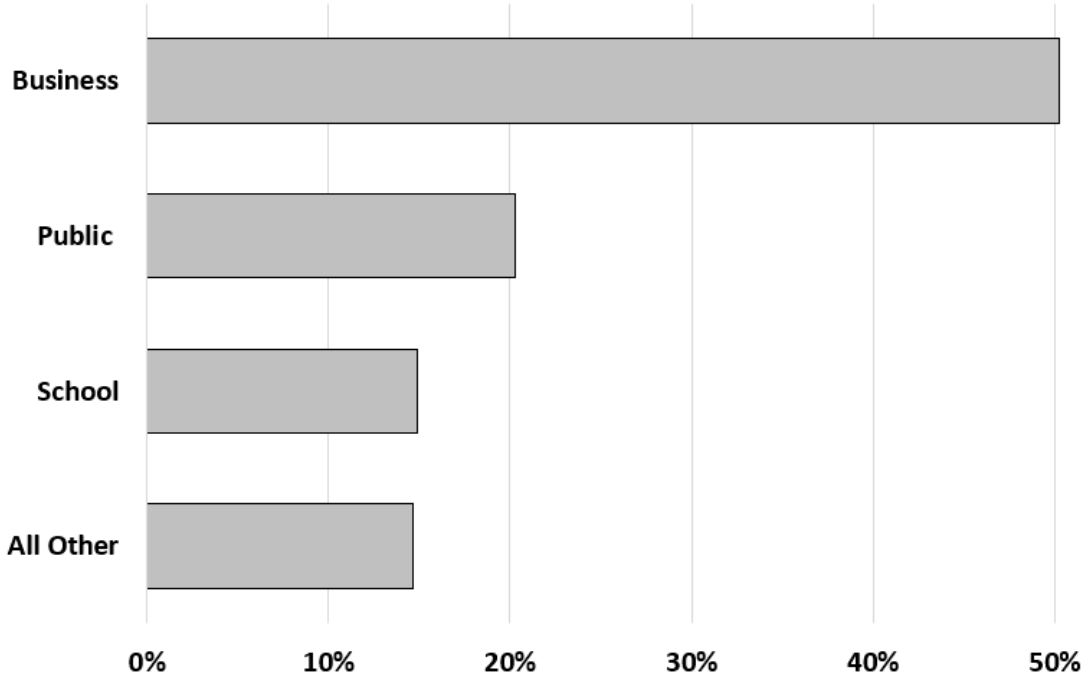

Figure 15 – Most frequent locations where the active shooter attacks usually occur. Source: (39)

Majority of active shooter attacks are small scale situations and not mass casualty incidents, as the Figure 16 indicates.

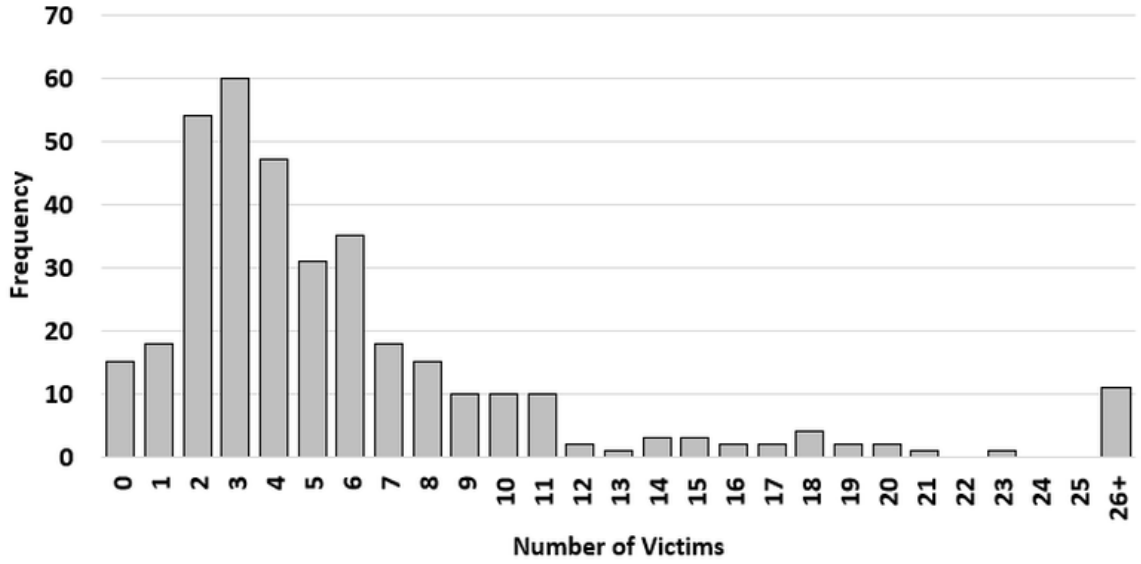

Figure 16 – Average number of victims per attack. Source: (39)

The most used weapon for such attack according to the Figure 17 is a firearm, mostly due to its absolute destructive power and capability to easily kill and hurt. Handling of most of the firearms does not require special training. When an oversize magazine is attached to the gun, the intensity of an attack increases.

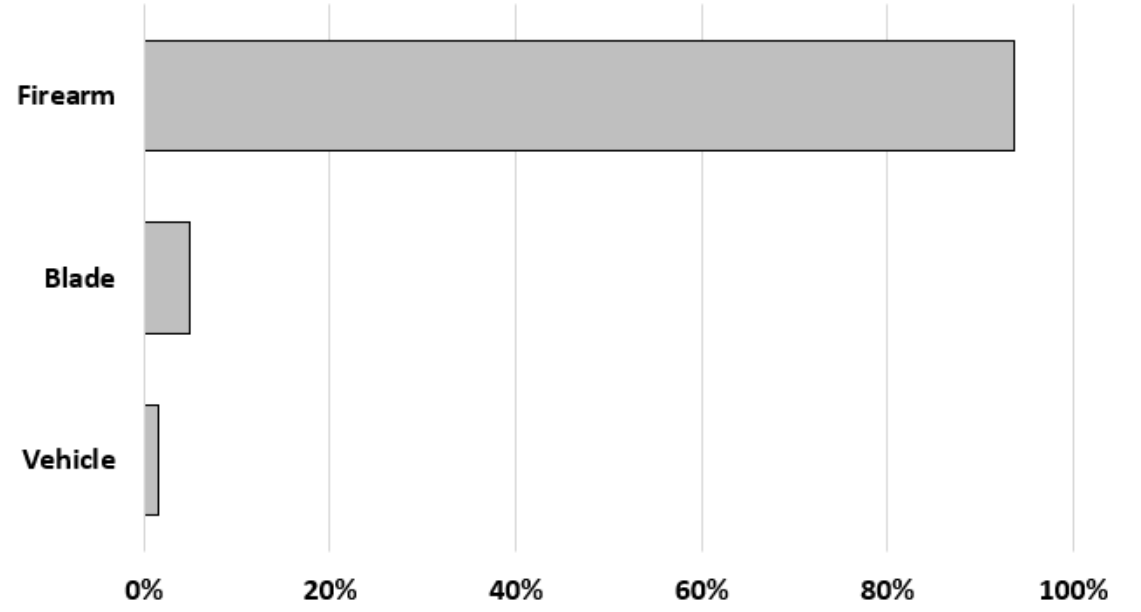

Figure 17 – Most used firearms by active shooters. Source: (41)

In most cases, (Figure 17) the attacker does not have any relationship to the victims. The second most common case is that the perpetrator is a former coworker (business premise) or student (high school, university). (41)

2.6.5 Amok Shooter

The difference between an active shooter and the amok shooter is simple. Active shooter deliberately chooses his target and plans the action of killing ahead. Whereas an amok shooter is a person in grip of sudden negative emotions that result in violent actions like spontaneous shooting, stabbing, arson, vehicle ramming etc. This condition is also called a running amok. (42) (43)

2.6.6 Rampage Shooting

A rampage shooting, also known as a mass shooting, is a violent attack in which an individual or group of individuals deliberately target and kill multiple people in a public area, such as a school, workplace, or other gathering place. Unlike an active shooter situation, which typically involves a single shooter targeting people at random, a rampage shooting usually involves a premeditated plan and may have specific targets in mind. The shooter may use a variety of weapons, such as firearms, knives, or explosives, to inflict as much damage as possible in a short amount of time. Rampage shootings can be particularly deadly and have a significant impact on communities and society. They are often motivated by a variety of factors, including mental illness, extremist beliefs, and personal grievances, and can occur in a variety of settings. (37)

2.7 Suicidal Bomb Attack

Explosives that are illegally prepared by both amateur chemists and persons with the aim of misusing them are called improvised explosives (homemade explosives). The range of substances covered by improvised explosives can be wide. Information on the manufacture and preparation of these explosives can be drawn from available sources of information, including specialist literature, which may enable such persons to attain an appropriate level of knowledge. The problem is that this knowledge can then be shared on the internet and, although this group of people do not primarily manufacture explosives for the purpose of misuse, the results of their work can be a valuable source of information for potential attackers. The explosives produced are mainly those with good availability of raw materials, easy preparation procedures and available know-how. A major risk of improvised explosive

devices is their instability. The creation of a perfect final product by the attacker is not one of his priorities, so the risk of self-ignition or explosion must be assumed for these explosives. (44)

Brisance – Brisance is a term used to describe the shattering or fragmentation power of an explosive material. It refers to the ability of an explosive to break or shatter materials and structures upon detonation. Explosives with high brisance can produce a large amount of energy in a very short time, resulting in a shockwave that can break or rupture materials nearby. [10] (45)

An **explosive** is a material or substance that can rapidly release energy in the form of heat, light, sound, and pressure when it undergoes a chemical reaction, usually accompanied by a sudden release of gas. Explosives are typically used in various industrial, military, and mining applications for their ability to create controlled and powerful explosions that can perform a range of functions. (45)

Explosives can be classified into two categories: **low explosives** and **high explosives**. Low explosives, such as gunpowder[11] and some types of fireworks, burn slowly and steadily, producing a flame that can be used to propel a projectile. High explosives, on the other hand, detonate instantaneously, producing a rapid and powerful release of energy that can cause massive destruction. High explosives can further be categorized into primary explosives, which are extremely sensitive and used to trigger other explosives, and secondary explosives, which are less sensitive and used for actual blasting or other applications. (45)

An improvised explosive device (IED) is a homemade or improvised bomb that is constructed and deployed by non-state actors such as terrorists, insurgents, or criminals. IEDs can be made from a wide variety of materials, including commercial and military explosives, fertilizers, gas cylinders, and other readily available components. (46)

The design and construction of an IED can vary depending on the intent and expertise of the individual or group building it. Some IEDs are designed to be hidden in public places and

[10] Brisance is often measured by the velocity of detonation, or VOD, which is the speed at which the detonation wave travels through the explosive material. Higher VOD means greater brisance, and therefore greater destructive power. Other factors that affect the brisance of an explosive include its chemical composition, density, and confinement. (45)

[11] Gunpowder is a mixture of saltpeter (potassium nitrate), sulfur and charcoal. It was discovered in the 9th century in China and its mass usage was seen during 14th century in medieval Europe. Another significant revolution of explosives in the late 19th century brought us the smokeless gunpowder (Poudre Blanche). (85) Smokeless powder is further divided by the number of propellants it consists of – therefore we speak about single base, double base and triple base powder. (85)

detonated remotely or by a timer, while others are carried and planted by a suicide bomber. (47) (48)

IEDs have been used extensively in conflicts around the world, particularly in Iraq and Afghanistan. They have also been used in acts of terrorism and violence outside of war zones. The use of IEDs poses a significant threat to civilians and military personnel alike, as they are often difficult to detect and can cause indiscriminate and devastating damage. Counter-IED measures, including detection technologies, training, and equipment, have become a major focus of military and law enforcement operations in recent years. **Detonation velocity** is the speed at which the chemical reaction front (also known as the detonation wave) propagates through an explosive material. It represents the rate at which the explosive energy is released. [12]Detonation velocity is typically measured in meters per second (m/s) or feet per second (ft/s), and it can vary depending on the type of explosive and the conditions under which it is detonated. The detonation velocity is an important parameter for assessing the potential destructive power of an explosive device, and it is often used in the design and testing of explosive materials and devices. (45)

Acetone peroxide TATP

Acetone peroxide forms snow-white powder or colorless crystals. It is insoluble in water with a characteristic pleasant odor. It is a physically unstable substance with a high vapor pressure and sublimates at normal temperatures. A major risk is the subsequent desublimation, in which TATP in the form of crystals is deposited on the surrounding material (e.g., the cap of the container) and there is an elevated risk of explosion if the container is opened. During storage there is a risk of spontaneous explosion due to thermal instability of the substance. The substance is extremely sensitive to mechanical stimuli. IF a substance in a large quantity in a closed container is initiated by flame, it will explode. TATP is prepared by reacting acetone with hydrogen peroxide in an acidic environment. One of the most used explosives worldwide, especially in Palestine. (44)

[12] For example, the detonation velocity of TNT (trinitrotoluene) is approximately 6900 m/s (22,600 ft/s), while the detonation velocity of C4 (a plastic explosive) is approximately 8000 m/s (26,200 ft/s). (86)

Hexamethylene Triperoxide Diamine HMTD

Hexamethylene Triperoxide Diamine is white powder, odorless in fresh state. It does not melt on heating and goes into explosion. It is chemically unstable, decomposing over several years with loss of its explosive properties. Decomposition is manifested by the smell of rotting fish. Overly sensitive to mechanical stimuli, especially friction. Explodes when ignited by flame in massive quantities when sealed. (44)

Erythritol tetranitrate ETN

Erythritol tetranitrate is a colorless crystalline substance, white powder in the fine state. Its low melting point allows it to be cast. It is insoluble in water, soluble in acetone. A new explosive, it is more sensitive in the cast state than in the powder state. (44)[13]

Nitromethane NM

Is a colorless liquid with a characteristic odour of organic solvent. Sparingly soluble in water. Detonation parameters are comparable to TNT. Available as a fuel for aeromodellers. (44)

Urea nitrate

Urea nitrate is a colorless crystalline substance, in the fine state it forms a white powder. Slightly soluble in cold water, freely soluble when hot. Quite acidic, corrodes in contact with metals, especially when wet. Not sensitive to mechanical stimuli, prepared by reacting urea with nitric acid. (44)

A suicide bombing, often referred to as a suicidal bombing, is a sort of terrorist assault in which a person detonates an explosive device that is strapped to their body, hidden in a car, or somewhere else. The assailant frequently targets busy public areas, such as marketplaces, mosques, or transit hubs, to increase deaths. The attacker usually seeks to cause as much death and destruction as possible. Suicide bomb assaults are a particularly severe and damaging form of terrorism since they not only harm the local community physically but also instill dread, worry, and trauma. The assailants may consider themselves martyrs or heroes of a cause and are frequently driven by extreme ideologies or political grudges.

[13] A proof that it is relatively easy to produce such an explosive is a recent case from Japan. In 2019, a high school student with developed passion for chemistry tried to produce this explosive. As the police found out, he became acquainted with another adult student, who was sentenced to prison for producing the TATP explosive. (84)

2.8 Arson

Intentionally setting fire to property, such as a vehicle, building, or other structure, is known as arson. Arson is a serious crime since it puts the public's safety in danger and has the potential to result in significant property damage, harm, or even death. Vandalism, retaliation, insurance fraud, and other crimes can all be covered up by arson, among other motives. Depending on the motive and the extent of the damage caused by the fire, the seriousness of the offense can vary. A Molotov cocktail is a home-made incendiary weapon constructed of a glass bottle filled with a flammable substance like gasoline, alcohol, or kerosene and a cloth wick that is lit before being thrown at a target. The combustible liquid ignites when the bottle breaks on impact, producing a fireball that may result in property damage and personal harm.[14] (49)

2.9 Hostage Taking

In a hostage situation, one or more people are being held against their will by a person or group in exchange for demands or concessions from the government or other parties. It is possible for hostages to be seized for a variety of purposes, such as political, criminal, or personal ones, and the situation can be very risky and explosive. The outcome of a hostage crisis depends on a variety of variables, including the quantity and location of the hostages, the hostage-motivation, taker's and the tools at the disposal of the police. Successful outcomes could include the negotiation of the hostages' release, the use of force to free the hostages, or the hostage-surrender. (1)

2.10 Barricade Situation

In a barricade situation, a person or group barricades themselves inside a building or another enclosed area, typically with the goal of resisting police enforcement or other authorities. In addition to threats of violence or harm to others, the barricade may be constructed out of furniture, vehicles, or other items. Situations involving a barricade can be particularly risky since the participants may be armed and holding hostages or other innocent people. Negotiation strategies and tactical operations, such the deployment of SWAT teams or other specialist units, are frequently used by law enforcement organizations to deal with barricade

[14] The Molotov cocktail is named after Vyacheslav Molotov, a Soviet politician, who signed a non-aggression pact with Nazi Germany in 1939.

situations. In a barricade situation, law enforcement's main objective is to end the crisis with as little harm to all parties as possible. When people are barricaded, negotiation strategies are frequently utilized to open lines of contact and defuse the situation. Loudspeakers or flashbang grenades are only two examples of the diversionary techniques that law enforcement may employ to confuse the people being besieged and open a window for negotiation or tactical action. When all other options have been exhausted, tactical actions are often undertaken as a final resort. The safety of everyone involved is always the top priority, even when using force to free hostages or other people who are in danger. Situations involving barricades are distressing for all parties involved and may have long-term psychological repercussions. Those affected by the crisis are frequently given access to support services including counseling and medical care. (30)

2.11 Poisoned Pen Letter

A poisoned pen letter is a form of malevolent writing that is often sent anonymously and contains unfounded charges, insulting comments, or other offensive content with the intention of intimidating or harming the receiver. The phrase "poisoned pen" refers to the writer's malicious motives, who is using the letter as a weapon to strike their intended recipient. From ancient times, poisoned pen letters have been used to propagate falsehoods, damage reputations, and stir fear and anxiety. They may be transmitted for political or personal purposes and can have major repercussions for the recipient, including reputational injury, loss of job opportunities or relationships, and in some cases, physical harm. (50)

2.12 Vehicle Ramming Attack

Vehicle ramming into the crowd, also known as vehicular assault or car-ramming attack, is a type of attack in which a vehicle is intentionally driven into a crowd of people with the intention of causing harm or death. The vehicle can be a car, truck, van, or any other type of motorized vehicle. (51)

These types of attacks have been used in acts of terrorism, as well as in cases of deliberate criminal behavior. They can cause considerable damage and injuries, and in some cases, fatalities. The motive behind these attacks can vary, but they are often intended to create chaos, instill fear, and cause harm to a specific group of people. Perpetrators are deliberately choosing pedestrian areas as location where they could cause the most harm in the easiest way. (52)

A vehicle attack is often conducted in combination with another method of attack - shooting, using a cold weapon or explosives. Ramming attacks could be caused not only by the so called “lone wolfs” but also by stray dogs” who are seeking relief from anger by a spontaneous deadly action. (53)

2.13 Threads of Intimidation

Statements or actions that are intended to scare, frighten, or coerce someone into doing something or refraining from doing something. This type of behavior is often used as a tactic to gain power or control over others, and can take many forms, such as physical threats, verbal abuse, stalking, or cyberbullying. Threats of intimidation can have a significant impact on the well-being and mental health of those targeted, leading to feelings of fear, anxiety, and vulnerability. In some cases, they may even lead to physical harm or violence. (54)

2.13.1 Blackmailing

Extortion (Blackmailing) is a form of extortion in which someone threatens to reveal embarrassing, damaging, or incriminating information about another person unless a demand is met. The demand may involve money, property, or some other type of benefit. Extortion is illegal and can have serious consequences for both the blackmailer and the victim. The information that is used in extortion can be true or false and can be obtained through various means such as hacking, spying, or social engineering. Blackmailers may use this information to coerce their victims into doing something they would not otherwise do, such as giving them money or performing an illegal act. Blackmail can be a very stressful and traumatic experience for the victim and can have long-lasting consequences on their personal and professional life. If you are being blackmailed, it is important to seek help from a trusted friend or family member, and to report the incident to the authorities. (54) (55)

2.13.2 Sabotage

Sabotage refers to the deliberate and malicious destruction, damage, or obstruction of something, often for political or ideological reasons. Sabotage can take many forms, including physical damage to property or equipment, disruption of services, or interference with communication and information systems. It can also involve the theft or manipulation of information, the spreading of false rumors or propaganda, or the infiltration of an organization to disrupt its operations. Sabotage is often conducted as a form of protest or

resistance against a perceived injustice, or as a means of advancing a political or social agenda. It can also be used as a tactic in warfare or espionage to weaken or disable an opponent. Sabotage can have serious consequences, both for the individuals or groups involved and for the wider society. It can lead to economic loss, endangerment of human life, and disruption of critical services. Sabotage is considered to be illegal and is punishable by law. A typical example of sabotage is a cybernetical attack. (54)

2.13.3 Disinformation

Disinformation refers to false or misleading information that is deliberately spread to misinform, deceive, or manipulate people. It is a type of propaganda that is used to influence public opinion, create confusion, or sow discord. Disinformation can take many forms, including fake news, rumors, conspiracy theories, and propaganda. It can be spread through traditional media channels such as television, radio, and newspapers, as well as through social media platforms and other online forums. The spread of disinformation is often carried out by individuals or groups with a specific agenda or motive, such as political organizations, governments, or malicious actors. Disinformation campaigns can be used to influence elections, discredit opponents, or create chaos and division within a society. Disinformation can have profound consequences for individuals and societies, as it can lead to the spread of misinformation and undermine trust in institutions and the media. It is important to be critical of information sources and to verify information before sharing it with others. (54)

2.13.4 Fake Bomb Planting

A fake bomb threat is a false report of an explosive device or other dangerous substance or device that is intended to create fear or panic. The threat may be made in a phone call, email, letter, or other form of communication, and can be made by an individual or group for several reasons, such as seeking attention, causing disruption, or as a malicious act. Fake bomb threats are illegal and can have grave consequences, as they divert resources from legitimate emergency response efforts and can cause significant disruption to businesses, transportation, and public services. They can also result in criminal charges, fines, and imprisonment for those responsible. In some cases, fake bomb threats are part of a larger pattern of harassment or intimidation and may be investigated as acts of terrorism or other forms of criminal behavior. It is important to take all bomb threats seriously and to follow established protocols for responding to such threats, even if they are suspected to be fake. (45)

2.14 Drone Strike

An unmanned aerial vehicle, or drone, is used in a drone strike to conduct targeted attacks against people or targets that are threats. A pilot on the ground or in a control room normally controls the drone remotely. It can be armed with a variety of weaponry, such as missiles, bombs, and precision-guided projectiles. Targeting high-value persons, such as terrorist organization leaders or those involved in attack planning or execution, is a common tactic utilized in counterterrorism operations. When compared to conventional air attacks, the deployment of drones by armed forces can lower the danger of civilian casualties by allowing them to target people in distant or inhospitable locations. (56)

An unmanned aerial vehicle, or drone, is used in a terrorist drone strike to conduct a targeted strike against a civilian or military target with the goal of causing harm or inciting fear. Drones are becoming increasingly popular among terrorist organizations as a means of carrying out operations because they can be inexpensive, simple to procure, hard to detect, and tough to fight against. Many methods, such as the use of explosives, chemical or biological substances, or small arms fire, may be employed in terrorist drone attacks. Whether human populations, vital infrastructure, or military installations are the intended targets, the attack may be planned to cause the most destruction and disruption. (56) (30)

2.15 CBRN Threat

Chemical, biological, radiological, and nuclear (CBRN) hazards are the intentional or unintentional leakages of potentially dangerous materials that threaten both human health and the environment.

Chemical hazards involve the usage of poisonous chemicals that can be harmful when inhaled, come into touch with the skin, or are swallowed. Examples include choking, blistering, and nerve agents.

When a chemical substance interacts with an organism, it passes through four processes:

-absorption,

-transport,

-metabolic effect,

-toxic effect.

The term "toxic" describes something that is poisonous or poisonous to living things.

Exposure is the period when an individual is exposed to a chemical substance in the body. Poisoning can be identified based on the duration of exposure:

-acute,

-chronic.

They are categorized into poisons with effects based on how they affect the human organism:

-non-specific (damaging basic life functions),

-specific (damages some organs),

-systemic (damages systems and organs),

-allergenic (producing hypersensitivity),

-carcinogenic (induces malignancy).

According to their predominant effects at the systemic level, toxic substances can be divided into:

- nerve paralytic,

-suffocating,

-poisonous,

-incapacitating,

-irritants.

Toxic properties of poisons are characterized by constants. Their mean threshold concentration (concentration which in 50% of affected individuals will induce symptoms of poisoning after a certain time) while medium incapacitating concentration (the concentration that causes incapacitation in 50% of affected individuals after a certain time) whereas intermediate lethal concentration (a concentration that kills 50% of affected individuals after a certain time). (57)

The usage of **biological agents** including viruses, bacteria, and toxins (pathogen) that can sicken or kill people, animals, or plants constitutes a biological hazard. The basic characteristics of a successful pathogen are:

- the ability to survive and spread in the environment,

- the ability to attach to the surface of the target cell,

- the ability to breach the defensive barriers of the human body,

- the ability to damage target cells, for example by producing toxins.

Pathogens can enter the cannon in the following ways:

- by inhalation,

- by ingestion,

- through the skin,

- surface contamination of the skin.

They are usually recognized by fever, inflammation, rash, immune system reaction. (57)

Using **radioactive materials** that can harm people through radiation exposure is a radiological threat. The ionizing radiation that an unstable atomic core emits is known as radioactivity. For living things, including people, this radiation may be seriously harmful. Ionizing radiation exposure has the potential to harm or even kill body cells, resulting in radiation sickness, cancer, and in severe circumstances, even death. Nuclear accidents, nuclear weapons testing, and the disposal of nuclear waste are just a few of the ways radioactivity can be discharged into the environment. When radioactive substances are released, they can contaminate the air, water, soil, and food, which causes radiation to spread over wide areas and over extended periods of time. Radiation sickness, cancer, and genetic damage are just a few of the acute and chronic health effects that high radiation exposure can have. When a person is exposed to significant doses of ionizing radiation, a group of symptoms known as **radiation sickness** develop. There may be burns on the skin, nausea, vomiting, diarrhea, and central nervous system injury among the symptoms. In extreme circumstances, radiation illness can be lethal. Ionizing radiation exposure can harm cells' DNA, which can result in the emergence of **cancer**. The kind of radiation, the amount absorbed, and the length of exposure all affect the kinds of cancer that might develop because of radiation exposure. Leukemia, thyroid cancer, and lung cancer are a few cancers that have been linked to radiation exposure. High doses of ionizing radiation can damage the DNA in sperm or eggs, altering the genetic makeup that can be passed down to subsequent generations. Birth abnormalities or genetic diseases may be the result of this kind of damage. (58)

Nuclear weapons or other mechanisms that have the potential to injure or destroy large areas of land or people are called the nuclear threats. A **dirty bomb**, often referred to as a radiological dispersal device (RDD), is a form of explosive that combines radioactive material like cesium-137 or cobalt-60 with conventional explosives like dynamite or C-4. A dirty bomb's objective is to disperse radioactive material over a large region, poisoning people, buildings, and infrastructure with radioactive particles. A dirty bomb does not result in a nuclear explosion or chain reaction, in contrast to a nuclear weapon. Nevertheless, radiation illness, cancer, and other long-term health problems may result from the radioactive material that the explosion releases into the environment. Urban centres, transportation hubs, and other congested regions could be at risk from dirty bombs. The aftermath of a dirty bomb assault can be difficult to clean up, expensive, and have a profound psychological impact on the people who were there. But it is crucial to remember that

compared to other terrorist attacks, a dirty bomb's actual risk is quite low, and there have only been a very small number of cases of this kind of attack in history. (59)

3 ASSESING THE RISKS OF A TERRORIST ATTACK

Assessing the risk of a terrorist attack involves evaluating the likelihood[15] and potential impact[16] of an attack occurring. While it is impossible to predict the exact time and location of a terrorist attack, there are several factors that can be considered to scale the risk:

- threat intelligence: Gathering information on terrorist groups and their activities, including their intentions, capabilities, and potential targets, can help assess the likelihood of an attack occurring. (60)[17]
- vulnerability assessment: Identifying and assessing potential targets, including critical infrastructure, government buildings, public events, and transportation hubs, can help identify areas that may be at higher risk of attack. (61)
- historical analysis: Examining past terrorist attacks, including their methods, targets, and impacts, can help identify patterns and trends that may indicate areas of higher risk. (62)
- geopolitical context: Examining the current geopolitical climate and ongoing conflicts can help assess the potential for terrorist groups to expand their operations or launch attacks in new locations.
- societal factors: Examining social and economic factors, including political tensions, social unrest, and economic inequality, can help assess the potential for terrorist groups to gain support or recruit new members.

Once these factors have been considered, a risk assessment can be conducted to prioritize resources and develop mitigation strategies to reduce the likelihood and impact of a terrorist attack. Effective risk management requires ongoing monitoring and reassessment, as the Metodika koordinace měkkého cíle pro fázi po bezpečnostním incident. Following methods are suitable for detection of potential "weak spots" in the soft target's defense. Impact of the attack on the soft target - it is about the functionality of the soft target even after it is attacked, what effect it leaves on the primary activity of the soft target and its surrounding area. **Location of the soft target** - one of the most important criteria, it depends on whether the soft target is located directly in the centre of a city, an industrial estate, a large housing estate,

[15] Likelihood – sources of threats of terrorist attack.
[16] Potential impact – the severity of an attack. Different severity will have a cold weapon attack or bombing / mass shooting spree.
[17] So called TCPED cycle – Tasking, Collection (IMINT, HUMINT, OSINT) Processing, Exploitation and Dissemination of an intelligence product. (79)

etc. **Availability of information** - the quality of the attack directly corresponds to the availability of information on the soft target. The more detailed information the perpetrators can obtain, the greater the effect the attack will have. This criterion is also related to the reliability of the personnel (possibility of leakage of sensitive information) and related to this the screening and delegation of authority according to the hierarchy. **The current state of security** - a critical criterion that can mostly only be corrected by attack with greater or lesser effectiveness. Of course, the higher the level of security, the more likely it is that dilettante groups or individuals will be less likely to attack. In each category, security will be considered from several levels as follows: **mechanical** means, **technical** means, **physical security,** access road for the integrated rescue system units and **escape** routes. **Importance of soft target** - this criterion describes the possibility of crippling functionality of the soft target in the system (e.g., a transportation hub). **Number of people in the soft target** - a key factor that determines the possibility of an attack. One of the main motives of terrorist attack is to create psychological pressure on the population. This effect is easily achieved by making people feel threatened and thus creating a more suitable environment for demanding a successful societal change (or whatever the motive for a terrorist attack may be). The speed of response of the first responder forces in each soft target. **Vehicle accessibility** - this refers to the accessibility of vehicles to the facility or to its access to the vicinity where there is a risk of attack by ramming into a cluster of vehicles or crowd of people in the area.[18] As we have recently seen an increase in the number of attacks of this style, there is a need to increase attention to measures that can be very easily built. **Chemical weapons proliferation options** - the most common will be accessibility to the building's ventilation system, which the perpetrators can use as an easy means to attack without rapid detection. Unguarded access to the facility's maintenance hub – unguarded switches, electricity, water, and gas distribution centers and or data storage etc. is always a big weakness. A perpetrator could deliberately aim on turning off the supply of energy what can cause first problem, and later attack the responders or the maintenance stuff.[19] (63)

Further attractive elements may be a crucial factor among the secondary, potentially. There is a risk with owners of soft targets who also have interests in risky areas. Structure and building materials of the property - another factor in deciding on which soft target to attack.

[18] There is a big potential to suffer from a secondary attack on the first responders or gathered survivors or evacuees.

[19] Such a case happened recently in the Czech Republic where an unknown perpetrator disabled the energy and water supply to a local business premise, causing it financial harm. This clearly demonstrates how easy i tis to wreak chaos and use it later for potential attack against a soft target. (93)

It may also play a role in the structural layout or materials of the facility, of which it was constructed. Detached objects of the primary soft target - this is a factor that may 'sound' like an attractive target for attack, due to the lower level of protection but approximately equal impact on the primary soft target. Unemployment - the higher the unemployment rate, the higher the likelihood of a propensity for crime. This factor depends heavily on the industry in certain areas. Perhaps also consider the salary level, where a large number of the population with a minimum wage, the risk of crime is closer to areas with unemployed people. Foreigners, a factor increasing the likelihood of crime, and especially residents coming from outside the European Union, are a much higher risk group for religious fanaticism. Width of escape routes - when an unwanted event occurs, this factor decides the speed of escape method from the premises. The minimum escape route width is set at one escape lane, which shall be 550 mm wide. Grouping of persons in one space - in large buildings there is a large number of sub-areas in which a relatively large number of persons may be trapped in relation to the layout of the whole space (e.g. a cinema in a shopping center). In such segregated areas, the risk of an adverse event is increased. (63)

3.1 The Czech Republic's response to Terrorism

The most common threats are mentioned in the official guidelines issued by the Ministry of Interior of the Czech Republic (name of the document Vyhodnocení ohroženosti měkkého cíle – which could be translated as the Evaluation of exposure the soft target's vulnerability). This document from the year 2017 lists these threats as relevant to soft targets:

- cold weapon attack,
- shooting,
- arson,
- taking of hostages, barricade incidents,
- explosives in the mailbox,
- crowd attack,
- poisoned pen letter,
- fake bomb planting,
- fake bomb threat reports. (3)

There are four levels of terrorist threat, one of which is the basic (so-called "zero") state, which has no graphical representation and is not separately declared. Elevated terrorism threat levels - elevated terrorism threat levels are referred to as levels one, two and three. (64)

Figure 18 – Levels of terrorist threat. Source: (65)

According to the approved system, a **zero state** is a situation in which there is no known specific or general threat of a terrorist or similar attack on the territory of the Czech Republic. Given the general security situation in the world, especially in Europe, and the Czech Republic's membership in Euro-Atlantic structures, this state is quite ideal and therefore difficult to achieve in the foreseeable future, as zero risk of terrorist threat does not currently exist in most countries of the world. In this theoretical state, no special recommendations or warnings would be issued to the public, nor would any anti-terrorist measures be taken by the security forces. This state is not independently declared. The first level of the terrorist threat (yellow-colored triangle) draws attention to the existence of a general terrorist threat arising from the situation abroad and from the Czech Republic's membership of Euro-Atlantic structures as well as from the Czech Republic's international activities, but at the same time there is no known specific threat of terrorist activities on the territory of the Czech Republic. In this state, general vigilance is required. In this situation, some of the long-established increased security measures are in force to the extent decided by the Government. From this point of view, therefore, it is a long-standing standard state of lowest, but not zero, threat of terrorism. (64)

Terrorism Threat Level 2 (orange-colored triangle) highlights the existence of an increased likelihood of a terrorist threat, and the specific circumstances of the threat, including its precise timing, cannot be predicted. It is declared in response to previous events or following information about the threat of terrorism. (64)

The third terrorism threat level (red-colored triangle) establishes a high level of vigilance and alertness when a terrorist attack on a Czech target (in Czech territory or abroad) is

expected with a high probability or has already taken place and measures must be taken to prevent a continuation or repetition of the attack and to minimize consequential damage. (64)

A characteristic feature of this system is that the condition for declaring an emergency measure is not the declaration of a certain terror threat level, but rather a consideration of whether the necessary legal conditions under the relevant legislation are met for the measures in question and whether the adoption of such measures is at all beneficial, appropriate, necessary, and proportionate to address the security situation. The system allows the government to apply sensitive measures 'tailored' to a given security situation. Even while maintaining the same degree, different measures can be adopted, cancelled depending on the nature and intensity of the threat. A change in the current security situation, either positive or negative, does not necessarily automatically trigger a change in the declared level, but may also lead to a change in the measure. Soft target protection became an imminent threat after the series of terrorist attacks in Europe in 2015. (64)

3.2 The United States of America

The approach covered by the Cybersecurity and Infrastructure Security Agency outlines the importance of cooperation between the public and the private sectors in enhancing the resilience of soft targets. Soft targets (crowd places) are here defined usually as public areas such are parks, shopping centers, special event venues etc. The recommended attitude to secure such places is well described and divided into four sectors – the public, the businesses, the government and the first responders. Resources mention several fact sheets, guides, trainings or other study materials that covers the most significant threats like the active assailant situation, unmanned aircraft systems or the identification of suspicious behavior. (61)

3.2.1 Developing and Maintaining Emergency Operations Plans

In this guide an emergency operations planning advice is provided. Its primary goal is to assist planners in analyzing a risk of threat and creating integrated, coordinated and synchronized plans as well as developing a shared understanding of risk-informed planning and decision making. (66)

3.2.2 Active Shooter – How to Respond Booklet

This document offers guidance on how to respond to on-the-scene active shooter, what to do when law enforcement arrives, how to train the personnel and how to get ready for an active shooter scenario, including roles and duties. (67)

3.2.3 Emergency Action Plan Guide

In this document summarizes various approaches to the soft target hardening problematics. It covers steps, which are recommended to undertake in the pre-planning phase (prior to the attack). Its uses of collaborative planning team, that integrates various stakeholders within the organization itself. Such a team usually consists of representatives from following departments:

- Human resources,
- Security, risk, and safety managers,
- Facility managers or engineers,
- First responders,
- Information technology managers,
- Legal advisors,
- Persons with disabilities or functional needs,
- Communication managers. (68)

The outcome of this guide is an Active Shooter Prevention Plan, that clearly defines roles, positions, and responsibilities (in the form of Threat Management Team). A risk assessment is also included. (68)

3.3 Australia and New Zealand

The issue of soft target protection (crowded place) is covered by joint effort of the Australian-New Zealand Counter-Terrorism Committee. This strategy defines the soft targets as places with high number of people (visitors, residents, tourists etc.). The threat that can affect them is represented by a five-point scale, starting from certain, expected, possible, probable, and unexpected. The framework for protecting high-density places (crowded places, soft targets) contains four steps, emphasizing the development and building of cooperation, distributing and accessibility of information and increasing the resilience of the

soft target. Primarily, this approach defines the crowded places as locations, which are easily approachable by higher amounts of people. Second condition is that the accessibility of such place should be easily predicted, the density of crowd may be different, depending on the season, day and night or temporary events like sporting matches, festivals etc. According to this approach, terrorists choose soft targets due to their vulnerability, being predictably available and easily accessible to hitting with simple weapons and simple tactics. Other significant factor that makes crowded places a lucrative target is that by hitting them, certain level of media attention will be aroused, enabling further spreading of fear and intimidation. Besides that, the crowd places are complicated targets to secure. The responsibility for protection of crowded places lies clearly on the shoulders of crowded places' owners and operators. One of the methods how the owners and operators could assess the vulnerability of their crowd place is an official document (The Crowded Places Self-Assessment Tool). This document itself should not be used as the risk assessment tool. Primarily it is meant to help understanding the attractiveness of the site and could be therefore used as a baseline for further security planning. In this approach, the private security providers play key role in protecting the soft targets. Governments and local authorities often see the private security providers as the first responders to the terrorist incident. However, strict regulations are applied on the security providers that contains employment, training, registration, and cooperation with law enforcement forces. The communities itself could help immensely in protecting the crowded places. It is encouraged to keep situational awareness and to report any signs of suspect or unusual behavior. Australian-New Zealand approach relies on the concept of layered security, which is based on four principles of deterring, detecting, delaying, and responding to the threat. (69)

The Australian-New Zealand attitude uses those three documents as backbone for crowded place security:

3.3.1 Crowded Place Security Audit

This is a basic document that is meant to reveal potential threats and security gaps. In form of a checklist, various problematics, such the security governance, plans, policies and procedures, physical security or access control are reviewed. (70)

3.3.2 Active Armed Offender Guidelines for Crowded Places

It is a guideline that's purpose is to raise the level of awareness of stakeholders (owners, operators etc.) in protecting the crowded places against armed attacks. It generally considers

the usage of firearms, prohibited weapons or improvised weapons, which could be used to strike the soft targets. Their primary objective is to help the law enforcement (police etc.) to carry out response to the attack, to minimize the duration of the attack itself, to restrict the attacker's movement and to help people escape from the place of attack as well as to provide them with a warning to avoid entering the area. This document mentions the connection between the duration of the attack and the freedom of unrestricted movement of the attacker. This document mentions the preparedness, prevention, response, and recovery as the four main pillars of risk treatment. (71)

3.3.3 Improvised Explosive Device (IED) Guidelines for Crowded Places

The third and last major significant document referring about the soft target's protection. In similar four pillars (prevention, preparedness, response, and recovery) inform the stakeholders of ways of dealing with explosive devises on the premise of the crowded place. (72)

3.4 Risk Treatment – Hardening the Soft Target

Soft target hardening refers to measures taken to increase the security of vulnerable targets that may be at risk of attack, such as schools, shopping malls, and public events. These targets are often referred to as "soft" because they are easily accessible and may not have the same level of security as other high-value targets, such as government buildings or military installations. Soft target hardening can involve a range of physical and procedural security measures, such as:

- installing physical barriers, such as bollards or concrete planters, to prevent vehicle-borne attacks.
- conducting vulnerability assessments to identify areas of weakness and developing security plans to address those weaknesses.
- training staff and employees to recognize and respond to potential threats, including active shooter situations.
- implementing access control measures, such as ID checks or bag inspections, to prevent unauthorized entry.
- deploying security personnel, such as guards or police officers, to deter and respond to potential threats.

Overall, soft target hardening aims to make vulnerable targets less attractive to attackers by increasing the difficulty and risk associated with an attack. To set up a functional security system, it is necessary to clarify the areas of protected interests and define sources of danger or threats to the protected interests, on the basis of which the threatening methods of attack can then be specified. The specified threats need to be subjected to a risk analysis, which will determine the priority areas of the security system and the subsequent security measures and strategies. People who are inside the attacked grounds and call an emergency number at one of the operations centers for the IZS's core components:

1. Stay away from the shooter and, if you can, get away.
2. Shut off the sound of the cell phone, lock the room, and barricade the entrance if possible.
3. Seek refuge in a space far from the entryway and away from the door.
4. Keep the door closed, wait for assistance, and refuse to open it until you have proofed the police is trying to open the door.
5. Obey to the instructions of the intervening officers, keep empty hands clearly visible away from the body.
6. If the contact with an active shooter is inevitable, try to aggressively fend off his assault. (73)

II. ANALYSIS

4 CHARACTERIZATION OF THE SELECTED SOFT TARGET

The selected soft target for the purposes of this analysis is the restaurant and adjacent supermarket. The location is significantly crowded in peak times during the morning and evening rush hours. The site is a favorite and well-known meeting place for the entire neighborhood. High retention of people is therefore highly possible.

4.1 Soft Target and its Surroundings

In the immediate vicinity of the destination lies road. The soft target itself is located at the intersection of two streets. Near in an easterly direction is a supermarket, which is separated from the restaurant by a parking lot that primarily serves both restaurant visitors and visitors of the supermarket. Other significant soft targets that are relevant to the safety assessment are the Jehovah's Witnesses Religious Society community site, located to the north of the assessed soft target, approximately one hundred meters on adjacent street. This site is separated from the soft target site by road and the railway tracks connecting the towns of Otrokovice and Zlín. The railway station is also located at this site. To the south, 100 m away, on an uphill street, there are two accommodation facilities, which are used by foreign workers from Eastern Europe. In the current geopolitical situation, these hostels, which accommodate foreign workers, may be the target of an attack motivated by right-wing extremism. They are relevant to the soft target threat assessment because the guests staying there enter the soft target area to buy food or eat. In a south - southwest direction, within four hundred meters of the assessed site lies a primary school. This school has an average of nine primary grades with two classes in each grade. In the past, there was an incident between disgruntled parents and the school, which allowed children to create pictures with themes depicting Islam as part of their lessons, which aroused a wave of resentment and disgust among several people. The whole affair was publicized and had a social media backlash. To the south-west, within one kilometer lies a catholic church. To the west, at five hundred meters as the crow flies, on a town square, we can find the post office building, a branch of the Zlín Municipal Police, the community sports and recreation center and a building housing another supermarket. This building is mentioned here because the Asian secondhand store shares its premises with the above-mentioned supermarket. In a purely westerly direction, there is also a public transport and long-distance bus stop. This bus stop is located approximately two hundred meters to the west of the application site and serves as

a frequented point which must be walked through to reach each site. It is therefore a junction point where people waiting for the bus congregate.

4.2 Security

According to police statistics, there were 186 and 168 violent incidents reported in the immediate vicinity of the assessment site between 16/04/2022 and 16/04/2023, the vast majority of which were misdemeanors. (74)

The reported incidents (total 1008 incidents in the police database) were activities:

- violent 4
- fires, explosions 1
- burglaries 14
- theft 19
- fraud 21
- other property 19
- generally dangerous 3
- traffic accidents 1
- toxic addiction 13
- misdemeanors 913 (74)

Using the crime database created by the Open Society Project o.p.s., we find that for the last available time interval November 2019 to November 2020, the crime index was 121, measured in the police municipality in which the assessed locality falls. (75)

4.3 Soft Target Description

The first of the soft targets is a restaurant. The restaurant contains a food court, an outdoor garden, and a drive-in. The daily number of visitors is around 500 to 600 people. The restaurant is open every day of the week from 7 a.m. to 10 p.m. The capacity of the restaurant is up to one hundred visitors plus approximately 10 – 15 staff members. (76)

There are three entrances to the building - the main entrance (for customers), the north entrance and the east entrance. Another possible point of entry to the restaurant space is the windows on the south side near the drive-in dispensing locations.

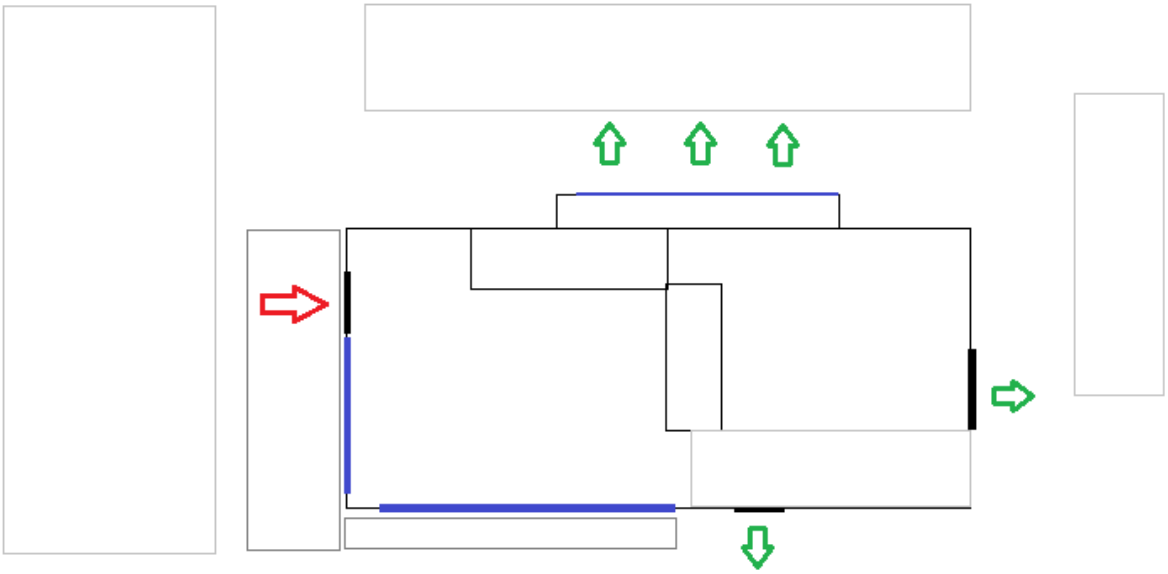

Figure 19 – Soft target situational plan. Source: Author's own collection.

The main potential way of entering the building is marked with red arrow. This is the main entrance door, connecting the outside part of the restaurant (here is permanently placed the exterior furniture – tables, chairs, and benches). Visitors sparsely use this exterior area, predominantly in warmer months. A potential commence of an armed attack in this part of the restaurant is therefore not excluded. The exterior next to the restaurant is an open space location, which is not concealed from the bypassing traffic, therefore the chance of spotting the attacker prior to the attack is significantly higher. This fact is leaving more space for reaction and response, depending on the spot from which was the attacker spotted. Some possible options for mitigating an armed attacker, who is spotted on the open space before the restaurant (on the premises of the parking lot) could be neutralized by other visitors with use of vehicles (ramming over the attacker) or by a person that carries a legal firearm. Due to significant complexity of input data, it is very problematic to define all the scenarios that may or may not occur. The attack itself and the way in which it is made is always dependent on the environmental factors. From the sources analyzed in the theoretical part we know that the attacker (more likely a determined one, motivated by hate) is going to strike the soft target on the least problematic way – which also means the attacker's intention to remain unrecognized for longest time possible. This allows him to launch the attack from the best

moment possible (a knife attack – when standing directly at the unsuspecting victim etc. or a firearm attack – when the people are static targets). A mentally ill attacker (like the "amok shooter" style described in the theoretical part) is going to strike immediately upon sighting the chosen soft target.

5 ASSESMENT OF THE CURRENT SECURITY MEASURES OF THE SELECTED SOFT TARGET

Using the method shown in the approach from Australia – New Zealand, the current security measures with the help of the checklist could be identified. For maximum authenticity, this chapter will be divided parts, each of the parts covers one of the sections mentioned in the Crowded Places Security Audit. The suggested actions, which arise from each topic, will be answered in the chapter 7 of this thesis. To answer this questionnaire, an interview was conducted with a former employee who worked in the company for which this evaluation is being processed. Due to the nature of the soft target, some questions used in the Security Audit were irrelevant. Those questions were not considered, because they were not matching with the primary purpose of the soft target.

Clearly visible weak spots are those questions, which were answered as Negative or Not Aware.

5.1 Security Governance

Security governance was checked in the Table 1, and we can see many security issues on the place. The most important one is the lack of a general Risk Management Plan, that could be rehearsed and constantly improved to reflect or the imminent, possible, or theoretical threats, that could affect the soft target and its function in the society. One of the biggest flaws is, that there is no distinguished area for evacuation in the shooter scenario. This could lead to accumulation of people on a spot, that is clearly visible, easily approachable, and therefore significantly vulnerable to second wave of attack.

Table 1 – Selected questions relevant to the soft target. Source: (70)

	Plans, Policies and Procedures	Yes	No	N/A
1.	Do you have a Risk Management Plan for your site?		No	
2.	Do you have a specific site or event Emergency Response Plan?	Yes		
3.	Do you practice or exercise your Plan?		No	
4.	Do you have a person responsible for security at your site or event?	Yes		
5.	Are they aware of the current security environment?			N/A
6.	Do you have nominated evacuation and lockdown officials?	Yes		

7.	Do you have a Security Policy for your site or event that covers physical information and personnel security?			N/A
8.	Does your Security Policy include screening of bags, mail and vehicles?		No	
9.	Do you have Evacuation and Lockdown procedures, including a protected space/s, factored into your planning?	Yes		
10.	If so, are they practiced or exercised?		No	
11.	If your site or event is located within precinct of similar businesses, are there precinct-wide plans?	Yes		
12.	Have you created secure incident assembly areas distinct from fire assembly areas in your planning?		No	
13.	Do you regularly review and update your plans?	Yes		
14.	Are staff trained in activation and operation of relevant plans?			N/A
15.	Do you have a Business Continuity plan in the event of disruption to power, telecommunications, water, or key equipment?	Yes		
16.	Do you regularly meet with staff to discuss security issues?		No	
17.	Do you maintain regular liaison with local police, emergency services and neighboring businesses?		No	
18.	Do your plans address active armed offender, hostile vehicles, trusted insider and improvised explosive device threats?		No	
19.	Do you encourage all staff to raise their concerns about security and incidents?	Yes		
20.	If so, do you have a formal mechanism to support these concerns and report incidents?	Yes		
21.	Do staff receive training that includes risk of terrorism-related and other security-related threats and hoaxes?			N/A
22.	Are staff aware of what to do should a threat be received?		No	
23.	Do you consider security penetration testing t your site?			N/A
24.	Are your staff and supervisors trained in managing telephone bomb threats?		No	
25.	Do you have a bomb threat checklist?		No	

.

5.2 Physical Security

This part is focused on describing the current security mechanisms in case of an armed attack, stabbing attack or vehicle ramming. As the biggest weakness we could label the non-existent parallel network of communication. Furthermore, the Table 2 shows, that the risk of poisoning the food and waterways is not mitigated.

Table 2 – Selected physical security criteria. Source: (70)

	General	Yes	No	N/A
1.	Do you regularly keep external areas, entrances, exits, stairs, and toilets clean and tidy?	Yes		
2.	Do you keep furniture to a minimum to provide little opportunity to hide devices?	Yes		
3.	Can items/equipment at your site be used as weapons?	Yes		
4.	Are unused offices, rooms and function suites locked?	Yes		
5.	Do you have reliable, tested communication in the event of an incident at your site?		No	
6.	Do your public communication messaging for evacuations in response to a serious incident include a direction to disperse rather than congregate?	Yes		
7.	Do you have pre-existing communication arrangements in place with neighboring businesses or crowded places in the event of a serious incident?			N/A
8.	If you have a police force, or other emergency response presence, are they familiar with the site's emergency response plans?			N/A
9.	Do you monitor social media?	Yes		
10.	Do you have easily identifiable security officers?	Yes		
11.	Do you have a procedure in the place to manage and store unattended baggage at your site or event?	Yes		
12.	Does your site provide opportunity for food or waterways to be contaminated?		No	

13.	Are air conditioning inlet ducts and other access points to your building appropriately secure from both persons and foreign objects/substances?	Yes		
14.	Do you conduct a systematic search of your site that includes toilets, lifts, restricted areas, car parks, service areas?	Yes		
15.	Do you have tested barriers around your site that are tested against vehicle crash?			N/A
16.	Are your CCTV cameras regularly maintained?			N/A
17.	Do you have CCTV cameras covering critical areas, such as IT equipment, back-up generators, cash offices, restricted areas, exits?	Yes		

5.3 Explosive Devices Blast Mitigation

The main goal of this section is to reveal possible weak spots in the field of explosive devices preparedness. According to the results summarized in the Table 3, there are no procedures for checking the waste receptacles on the site. The windows and door lack fragment mitigation installations.

Table 3 – Selected procedures of explosive device blast mitigation. Source: (70)

	Explosive Device Blast Mitigation	Yes	No	N/A
1.	Does the design and layout of your site enable easy concealment of explosive devices?	Yes		
2.	Do you review the use and location of all waste receptacles?		No	
3.	Could an explosive device be easily smuggled onto your site?	Yes		
4.	Do you use flammable materials and are they appropriately secured?	Yes		
5.	Does your location have fixtures or fittings that could become shrapnel?	Yes		
6.	Have fragment mitigation measures been installed on windows and other glass?		No	

5.4 Information Security

Information security is generally perfectly processed topic, as the Table 4 indicates. Insufficiently mastered level of cybernetical protection could lead to serious data leaks and information exposure. Any easily approachable data is another "unguarded door" the attacker may use as a point of penetration.

Table 4 – Selected information security procedures. Source: (70)

	Information security	Yes	No	N/A
1.	Do you have information security plans and procedures?			N/A
2.	Does your site have a website or otherwise release information which might assist terrorists or other offenders in planning the attack?	Yes		
3.	Do you lock away all business documents at the close of the business day?	Yes		
4.	Do you have a clear-desk policy at the close of the business day?		No	
5.	Are all your computers password protected?			N/A
6.	Do you log off and close down all computers at the close of the business day?	Yes		
7.	Do you have computer firewall and antivirus software on your computer systems?	Yes		
8.	Is information discussed and distributed on "need-to-know" basis?	Yes		
9.	Do you have a back-up of critical information contained securely at a different location from where you operate your business?	Yes		
10.	Do monitors, screens, whiteboards face away from windows in order to prevent oversight?		No	

5.5 Personnel Security

Personnel (or the peopleware) is an important security factor that presents very high risk. The system is only as good as its weakest member is. According to the Table 5, few security problems could be spotted.

Table 5 – Relevant personnel security topics. Source: (70)

	Personnel security	Yes	No	N/A
1.	Do you have Personnel Security policies and procedures?	Yes		
2.	Do they cover following things:			
3.	Code of conduct	Yes		
4.	Information and personal privacy	Yes		
5.	Notification of personal overseas travel		No	
6.	Workplace prohibited items	Yes		
7.	Security awareness and training	Yes		
8.	Are staff pre-employment checked?	Yes		
9.	Do staff pre-employment check include:			
10.	Identity checks	Yes		
11.	Qualification checks	Yes		
12.	Employment checks	Yes		
13.	Criminal history checks	Yes		
14.	Financial background checks			N/A
15.	Is ongoing sustainability for employment managed?	Yes		
16.	Are security breaches reported and investigated by trained personnel?	Yes		
17.	Are exit interviews conducted?		No	
18.	Is there a checklist for staff leaving that includes:			
	Return of all keys	Yes		
	Return of uniforms and official identification		No	
	Return of official information (documents, files)	Yes		
	Return and deactivate access passes			N/A

6 ASSESMENT OF THE RISK OF A TERRORIST ATTACK ON THE SELECTED SOFT TARGET

Risk register of threats assembled from various approaches researched in the theoretical part. To determine the probability, the frequency with which each attack occurs per unit of time will be determined. For the purposes of this paper, this is one calendar year. In this place we need to mention, that the source data was collected mainly from two different sources – The Global Terrorism Database and the Police crime database.

Evaluation of the vulnerability of a soft target using the method used in the methodology "Evaluation of the vulnerability of a soft target" prepared by the Ministry of the Interior of the Czech Republic in 2018. This methodology is used to validate the soft target. It seeks answers to three interrelated questions - what are we protecting (i.e., what values), against what threat, and how are these values vulnerable. Using a three-step procedure, we define what we protect, against whom we protect it, how we expect an attack, in which places and with what probability. This methodology also includes the determination of impacts and the determination of the overall degree of vulnerability of a soft target.

6.1 Framework of Protection

We protect the human lives in the first place, the economic and commercial interests, good name of the owners and the preservation of a safe neighborhood. The main assets we therefore need to protect in the first place are the visitors and the employees working in both institutions.

6.2 Sources of Threats

According to the police databases and the respective methodology used, we can establish direct sources of threats for this location as following:

- classical criminal activity – thugs,
- mentally ill persons,
- vengeful employees or customers,
- organized crime groups,
- extremists, attacks motivated by hatred,
- terrorists. (3)

6.3 Ways of Attack

Because the selected soft target does not inherently appear to be lucrative for terrorism, racially, ethnically, or religiously motivated crimes, the range of potential threats is thus reduced. However, the nature of a soft target means that soft targets (persons, groups of persons) who will meet any of the above-mentioned conditions (minorities, religious groups, etc.) may be present on its premises. Potentially 'interesting' locations in the vicinity of the soft target under consideration also play a key role. Indeed, it is possible that if the attacker is not apprehended or neutralized in an attack on the first target, an attack on other soft targets in the vicinity is not excluded. By its nature, the soft target under consideration is seen as a place frequented for the purpose of fulfilling more basic human needs, such as grocery shopping, eating, etc. It will therefore always be likely that there will be 'enough' people in the immediate vicinity of the soft target to become secondary targets of attack. This fact is also facilitated by the very location of the soft target - at the intersection of a main and a secondary traffic route.

The source of the basic attack patterns relevant to all soft targets is usually classic violent crime-related activity, attacks by mentally disturbed persons or attacks by workers, former employees, or customers. They can be covered by the following list:

- assault with a cold weapon,
- assault with a firearm,
- arson attack,
- hostage-taking, barricade situations,
- attacking a soft target with a crowd,
- explosives in the mail,
- poisonous substance in a mail piece,
- planted imitation explosive,
- false notification of the location of an explosive,
- explosive in a parked vehicle,
- planting an explosive,
- ramming a vehicle into people.

Due to the targets location and the minimum occurrence of attack types (according to the police crime databases in the vicinity of the soft target), the only relative threats to the soft target are an armed assault, melee assault, bomb planting or an incendiary attack.

Based on the data provided from the Global Terrorism Database, in the fifty-year period between 1970 to 2020 we can identify 666 relevant incidents.

Following charts show the incidents that were committed regardless of doubt. The target of those incidents was predominantly the business, local citizens and private property, religious institutions, or tourists. Countries, in which this data was collected, were the Czech Republic, Germany (West Germany and East Germany), Austria, Hungary, Poland and the former Czechoslovakia.

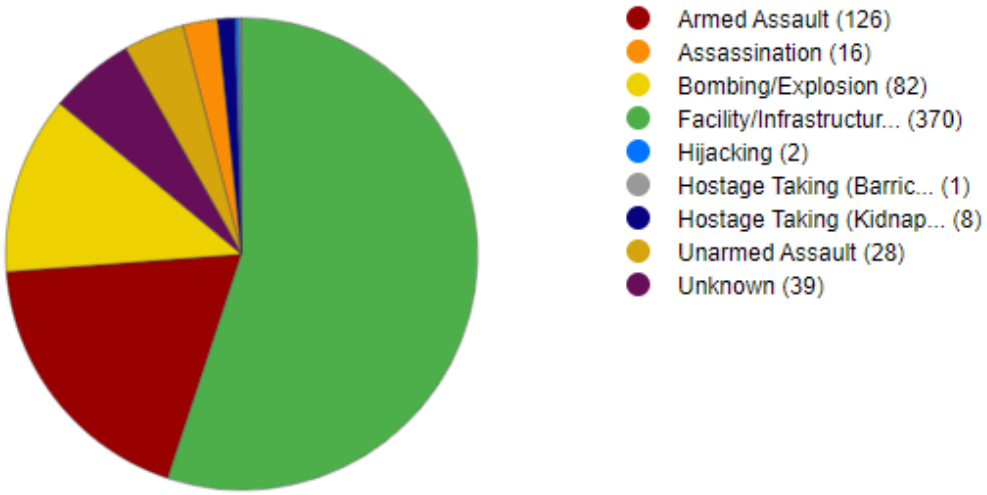

Figure 20 - Terrorist attack types in the selected region between 1970 and 2020. On the first place is the facility/infrastructure. Source: (9)

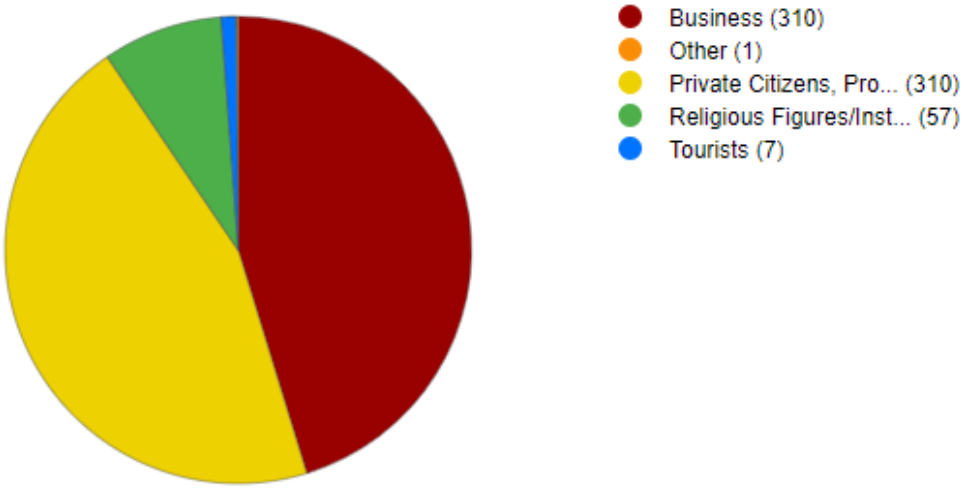

Figure 21 - The businesses (office buildings or places of commerce) were the primary target, being hit with the same frequency as private citizens or property. Source: (9)

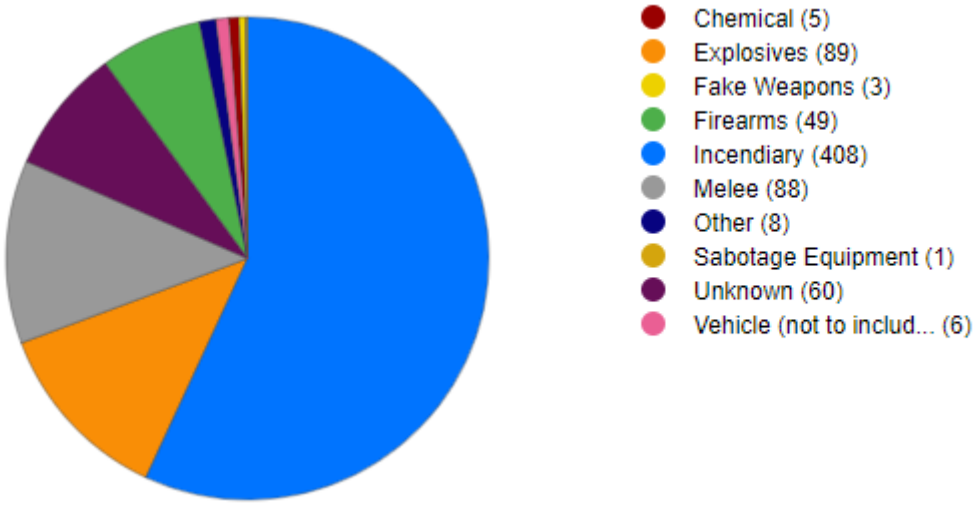

Figure 22 - The leading type of weapon used. Source: (9)

As the Figure 22 mentions, the leading type of the weapon used is the incendiary weapon (like the Molotov cocktail for instance). The biggest threat resolving from this mode of violence is therefore the arson. The second place is represented with the use of explosives. Melee or firearm attacks were “rather rare”.

6.4 Event Tree Analysis

Using the Event Tree Analysis method, we can predetermine the major decision points in the duration of an attack.

6.4.1 Analyzing the Melee / Firearm Threat

As we can see from this figure, the main decision points consider whether the attacker was or was not spotted in time. With timely disclosure of the attacker, the success rate of his attack decreases. From the risk management point of view, our primary goal is to keep the risk chance (represented by the "expected casualties" column in this chart) on the minimum.

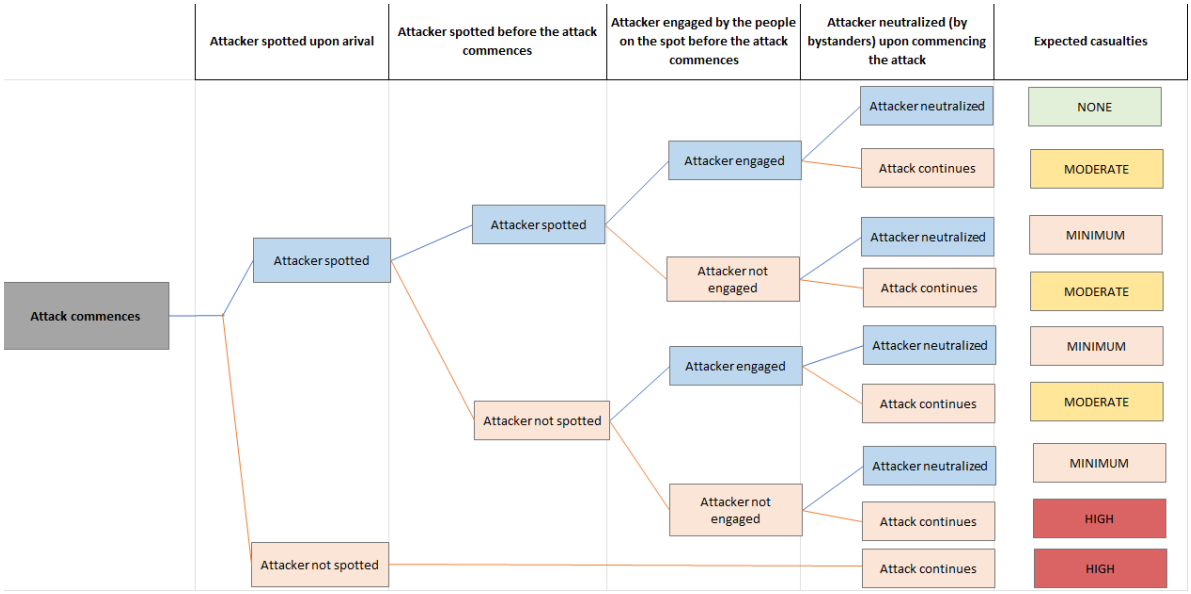

Figure 23 - Event Tree Analysis used for analyzing the threat of a melee or firearm attack. Source: Author's own collection.

This value is in the ETA analysis covered by the "NONE" result. This means, that there will not be any fatalities resulting from the attack. Injuries could not be excluded, because this model considers neutralizing the attacker either physically or with use of objects, weapons, or other emergency solutions. The number of casualties or the extent of injuries is therefore dependent on the martial skills of the people who are targeted (self-defense / deliberate engagement of the assailant) and on the collective and individual situational awareness (staying alert, observing the environment, trying to spot suspicious behavior).

In order to keep the risks on the minimum level acceptable, we need to focus on all the events that are marked with orange color. In the first decision knot, it is imperative that the staff / visitor spots the attacker. Should the attacker be unspotted / unrecognized before he launches the attack, the risk of the high number of casualties is the most probable outcome. Likewise,

shouldn't the attacker be spotted neither upon his arrival to the soft target, neither imminently before the attack commences, the chances for not sustaining casualties are very low. Once again, the success of the attack is dependent on many factors, one of the most important is the response of the target. The people, who are targeted by the attack, are the first responsive element on the site of attack. Therefore, it is a generally well-accepted opinion, that in the spite of increasing the soft target's resiliency, people, who are not killed or injured in the first seconds of an attack, should either run away (escape strategy), hide (survival strategy) or fight when the escape is not possible.

6.4.2 Analyzing the Threat of an Incendiary Attack / Explosive Planting

Event tree analysis cannot be performed on the selected soft target for the purpose of this research. This is mainly because there is a large amount of input data and variations of scenarios in which a given attack may unfold. Since the event tree method relies primarily on the use of probabilities to determine the magnitude of the impact of a given threat, it is not possible to analyze and statistically determine something that happens with an absolute minimum probability, if at all, in the Czech Republic. These are scenarios where an arson attack will be combined with a shooting attack or a cold gun attack, possibly combined with a vehicle ramming into a crowd of people who are evacuating the site or being evacuated from the site either spontaneously or in an organized manner. This research is extensive and cannot be summarized in one simplistic model. Moreover, as the questionnaire shows, the soft target has a fire evacuation plan to follow in the event of an arson attack. Whether an arson attack is supplemented by a secondary attack depends purely on the sophistication of the attacker. Since the data examined is silent on the possibility of a combination of attacks, this is not relevant to the intent of the paper. Thus, the goal of analyzing this situation remains only partially fulfilled.

7 SUGGESTION OF PREVENTIVE MEASURES TO MITIGATE THE RISK OF A TERRORIST ATTACK

In this concluding chapter, the discovered weak spots in the resilience of the soft target will be reviewed. As the method used mentions, every question could be answered in three ways – Yes, No or Not Aware. Every question, which was answered with Not Aware (N/A), should be discussed with the stakeholder of the soft target. Only after the discussion on the topic of security and crowded place's resilience, those measures could be re-evaluated and brought into praxis. For the purposes of this assessment, we will assume, that the respective security measures are either installed or operational and therefore have impact on the soft target's resiliency.

Out of this reason, we will concentrate on mitigating the threats that were answered with "No" response.

7.1 Security Governance

As can be seen from the analysis conducted, it is important to develop a soft target risk management plan around safety management. This plan will identify all important officials who have an impact on the operation of the company. The procedures set out in this plan should be rehearsed regularly. One important vulnerability that is not currently addressed is the possibility of items being smuggled into the facility, so the plan should focus on, for example, random checks of luggage, but also mail or vehicles that regularly come to the facility (contractors, etc.). One of the biggest weaknesses that is not addressed in the current state is the evacuation plan in the event of a shooting or attack. This plan should be developed and should also be different from the fire evacuation plan available to the public. If, in the event of an armed attack, the fire evacuation plan is used, it is possible that it will be known to the attacker (e.g., during reconnaissance of the site prior to the planned attack) and that the information contained therein (the assembly area, for example) may be used as a primary or secondary target of the attack. It is also advisable to set up regular all-staff meetings to discuss current security risks and to demonstrate appropriate approaches and measures to respond to or prevent these risks, it is also advisable to set up a telephone link to the local Metropolitan Police to deal with suspicious security incidents etc. Finally, the risk management plan should include information, guidance and procedures for staff explaining how to respond to telephone threats, threats or, for example, bomb notifications etc.

According to the outcomes revealed by the Event Tree Analysis, additional points could be added here. As the method itself revealed, the first "response" to the attack itself are the people, who are at the time of the attack present on the site of the attack. Here, the general what-to-do attitude could be applied (as mentioned in the Australia-New Zealand and in the strategy promoted in the USA). Such attitude suggests three possible ways of conduct in an armed attack scenario – run, hide, and fight. To increase their chances to run away (escape) safely, special staff training should be introduced. For purposes of hiding (survive strategy), it is recommended for staff to practice sports and martial arts. There is also a branch of Krav Maga (self-defense system for civilians) that is available for everyone. This technique shows methods of self-defense against an armed attacker carrying sharp or blunt weapon including a firearm. Martial arts do not only aim on defeating the attacker, but also on a general training in situational awareness. Another well encouraged attitude of mitigating the negative outcomes of an attack is the first aid training. Together with the knowledge of how to treat the wounds, first aid equipment should also be available on the site (generally available on the location mentioned in the risk and emergency plans and in the "safe room" as well). Safe room is a room, specially adjusted to offer a hiding place in the case of an armed attack during the "invacuation" process.

7.2 Physical Security

The evaluation of the physical security area is the second point to be worked on. The biggest weakness is the lack of a secondary, authenticated communication network (e.g. radios, chat channels, etc.) that can be used in the event of a security incident. At the same time, it is essential to secure water sources (toilets, etc.) from poisoning or setting a bait that could poison someone (see the chapter on CBRN risk). However, this solution is complicated and needs detailed consultation.

7.3 Explosive Devices Blast Mitigation

The deposition of an explosive device is a major hazard in this area. The interior and exterior around a soft target should be arranged to be clear. Any suspicious luggage without owners should be highly visible and conspicuous. At the same time, the interior and exterior should be constructed of materials that minimize the risk of secondary projectiles - shrapnel. A trash can is likely to be a potential place where a booby trap could be left. Trash cans and garbage cans should therefore be replaced by special security bins and containers such as those used, for example, in subways or public transport stops. An important safety feature is, in

particular, the installation of special glass that is fitted with protective elements that minimize the risk of the glass panel shattering to form shards - secondary projectiles. Glass shards are a frequent hazard accompanying explosions, causing life-threatening cutting injuries by bleeding, and posing a significant risk.

7.4 Information Security

In the area of information security policy, which was quite satisfactory, the only criticism is that there is no "clean desk" policy in the soft target. This may pose an information risk whereby an unauthorised person or, for example, an unauthorised employee may discover sensitive security information about the soft target. The deliberate misuse of this information is not the primary threat, but it is possible that inadvertently or by any other means this sensitive information could be leaked onto the Internet where it could be misused by a potential attacker. At the same time, to increase security, it is necessary to lay out furniture and equipment in the space so that monitors, whiteboards and screens cannot be seen from windows or doors. This is achieved by ensuring that monitors are not facing in this unwanted direction.

7.5 Personnel Security

People are always the weakest link in any security strategy. To strengthen soft target security and possibly prevent incidents, it is recommended to monitor employee travel to dangerous areas. For example, due to radicalization etc. A vengeful ex-employee is one of the most common causes of armed attacks on soft targets. This problem can be avoided, or at least minimized or detected, by introducing exit interviews. Hand in hand with this measure is the introduction of an obligation to return work clothes (clothing, uniform, etc.) after an employee stop working for the company. This will prevent infiltration, which may allow a vengeful employee to multiply the attack or overcome imaginary 'security' measures that would clearly reveal an attacker not wearing a work uniform.

CONCLUSION

The threat of terrorism refers to the risk of individuals or groups using violence or the threat of violence to intimidate or coerce a government, organization, or population to achieve a political or ideological goal. Acts of terrorism can take many forms, including bombings, shootings, hijackings, and cyber-attacks, among others.

Terrorism poses a significant threat to individuals, communities, and nations, as it can cause widespread fear, panic, and disruption. Terrorist attacks can result in loss of life, physical and psychological harm, economic damage, and social and political instability.

The motivations behind terrorist attacks can vary widely, ranging from ideological or political grievances to religious extremism, ethnic or nationalist separatism, or personal grievances. Terrorist groups may target specific individuals, organizations, or governments, or may seek to create chaos and disruption more broadly.

The threat of terrorism is a complex and evolving challenge that requires a multifaceted response, including intelligence gathering, law enforcement, diplomatic efforts, and community engagement. Effective counterterrorism efforts require a balance between protecting public safety and upholding individual rights and civil liberties.

This work presents an unusual and unique viewpoint on the issue of assessing the security of soft targets and crowded places. In the theoretical section of this thesis, significant phenomena are discussed, including terrorism, the concept of a soft target, risk factors, and dangers to which these soft targets are particularly vulnerable. The theoretical section is concluded with a study of the various methods employed in the Anglo-Saxon world for the analysis and management of security concerns associated with soft targets. The practical section includes a study of a chosen soft target, a description of its current security measures, a presentation of a potential attack scenario, and the actual design of security risk reduction and mitigation measures.

The thesis's major goal, which was to identify the best approach for assessing the threat to soft targets, has been accomplished. The search for a legal foundation upon which soft target security could be based was undertaken while this thesis was being developed. On this subject, experts in occupational health and safety as well as a lawyer who handles issues with the possession of firearms were contacted. There was no satisfactory answer to the question of which laws may cover the evaluation of soft target vulnerability after consultation and discussion with them. Therefore, the soft target protection continues to be

voluntary, at least in terms of civilian assets that do not meet the definition of critical infrastructure.

BIBLIOGRAPHY

1. **FOREST, J.F. James.** *Homeland Security: Protecting America's Targets.* s.l. : Praeger, 2006. 978-0275987688.
2. **A Study of Active Shooter Incidents in the United States Between 2000 and 2013.** ***FBI. Welcome to fbi.gov.*** **[Online] FBI. https://www.fbi.gov/file-repository/active-shooter-study-2000-2013-1.pdf/view.**
3. Kalvach, Zdeněk and Vangeli, Benedikt. ***Vyhodnocení ohroženosti měkkého cíle.*** **[Online] Praha : Ministerstvo vnitra, 2018.**
4. ***Reign of Terror.*** **[Onlne] s.l. : Encyclopædia Britannica, Inc., 2023.**
5. Aanmoen, Oskar. ***Murdered Royals: Empress Elisabeth of Austria.*** **[Online] s.l. : Royal Central, 2020.**
6. PACNER, Karel. ***Osudové okamžiky Československa.*** **Praha : Nakladatelství BRÁNA, 2012. 978-80-7243-597-5.**
7. Terrorist groups. ***Counter terrorism guide.*** **[Online] Office of the Director of National Intelligence. [Cited: January 30, 2023.] https://www.dni.gov/.**
8. ***Gemeinsames Extremismus- und Terrorismusabwehrzentrum (GETZ).*** **[Online] [Cited: January 30, 2023.] https://www.verfassungsschutz.de/.**
9. Global Terrorism Database. [Online] 2009 . [Cited: 4 19, 2023.] https://www.start.umd.edu/gtd/.
10. SAMPELS, Rick. ***A Police Officer's Guide to the Terrorist Attack Cycle.*** **[Online] s.l. : LEXIPOL, 2021.**
11. Defining the Terrorist Attack Cycle. [Online] Stratfor: The World's Leading Geopolitical Intelligence Platform [online]. https://worldview.stratfor.com.
12. Barbora, VEGRICHTOVÁ. ***Terorismus a radikalizace v České Republice - Možnosti detekce rizikových osob.*** **Praha : Grada, 2022. 978-80-271-3126-6.**
13. —. ***Hrozba radikalizace : terorismus, varovné signály a ochrana společnosti.*** **Praha : Grada, 2019. 9788027120314.**
14. P.A., SCHMID. ***Radicalisation, De-Radicalisation, Counter-Radicalisation: A Conceptual Discussion and Literature Review.*** **s.l. : The Hague: The international Centre for Counter-Terrorism, 2013.**
15. BORUM, R. ***Radicalization into Violent Extremism I. A Review of Social Science Theories.*** **s.l. : Journal of Strategic Security, 2011.**
16. MOGHADDAM, F. ***Staircase to terrorism.*** **s.l. : American Psychologist, 2005.**
17. MOGHADDAM, FATHALI M. ***The Staircase to Terrorism A psychological Exploration Vol. 60, No. 2,.*** **s.l. : American Psychologist, 2005.**
18. KRUGLANSKI, W. A., GELFAND, J. M., BÉLANGER, J. J. SHEVELAND, A., HETIARACHCHI, M. GUNARATNA, R. ***The Psychology of Radicalization and Deradicalization. How Significance Quest Impacts Violent Extremism.*** **s.l. : Advances in Political Psychology, 2014.**
19. VEGRICHTOVÁ, B. ***Extremismus a společnost.*** **Plzeň : Ales Čeněk, 2017.**
20. ***Co je to community policing?*** **[Online] s.l. : Policie.cz.**
21. ***Manual for Trainers: Community Policing Preventing Radicalisation and Terrorism.*** **s.l. : Prevention of and Fight against Crime., 2009.**
22. Soft Targets Protection Institute, z.ú. pod vedením Ing. Zdeňka Kalvacha. ***Základy ochrany měkkých cílů: Metodika.*** **Praha : MVČR, 2018.**
23. 8 Signs of Terrorism. ***Indiana Intelligence Fusion Center.*** **[Online] 2023. [Cited: February 1, 2023.] www.in.gov.**
24. Fighting against Inmates" Radicalization. Project Number: 763538 - FAIR - JUST - AG. [Online] 2016. [Cited: March 27, 2023.]

25. politiky, Odbor bezpečnostní. ***Typologie terorismu.*** **[Online] s.l. : Ministerstvo vnitra České republiky, 2009. https://www.mvcr.cz/.**
26. ***Paris attack: knife-wielding man injures six people at Gare du Nord.*** **[Online] s.l. : Guardian News & Media Limited , 2023. https://www.theguardian.com.**
27. infoplease. ***Murder Victims, by Weapons Used.*** **[Online] Sandbox Networks Inc., 2022. [Cited: March 26, 2023.] https://www.infoplease.com/.**
28. Stab Wounds. ***Mahoney Criminal Defense Group.*** **[Online] Mahoney Criminal Defense Group., 2023. [Cited: March 26, 2023.] https://www.relentlessdefense.com.**
29. Wounds, cuts and grazes. ***Healthdirect*** **. [Online] Healthdirect Australia , October 2021. [Cited: March 26, 2023.] https://www.healthdirect.gov.au/.**
30. HESTERMAN, Jennifer. ***Soft Target Hardening - Protecting People from Attack.*** **Abingdon, Oxon : Taylor and Francis, 2019. 9781138391109.**
31. kolektiv, JUŘÍČEK Ludvík a. ***Ranivá balistika.*** **Ostrava : Key Publishing s.r.o., 2017. 9788074182747.**
32. Weiss, Jeffrey. Mass shootings in the U.S. this year? 353 — or 4, depending on your definition. [Online] Dallas Morning News, December 5, 2015. [Cited: March 26, 2023.] https://www.dallasnews.com/.
33. Public Mass Shootings: Database Amasses Details of a Half Century of U.S. Mass Shootings with Firearms, Generating Psychosocial Histories. ***National Institute of Justice.*** **[Online] February 3, 2022. [Cited: March 29, 2023.] https://nij.ojp.gov/.**
34. Matt, ASPLAND. ***Switch Firing Modes | Full Auto, Burst And Single Fire - Unreal Engine 4 Tutorial.*** **[Online] s.l. : YouTube, 2021.**
35. ***Switch Firing Modes | Full Auto, Burst And Single Fire - Unreal Engine 4 Tutorial - YouTube.*** **[[online]] YouTube : Google LLC, 2023.**
36. Magazine recommendations? | Community for Kel-Tec Shooters. [Online] Community for Kel-Tec Shooters [online]. . https://www.thektog.org.
37. U.S. Department of Homeland Security. ***ACTIVE SHOOTER HOW TO RESPOND.*** **[Online] Washington : s.n., 2008.**
38. John, WILLIAMS. ***Active Shooter - Response & Tactics.*** **[Online] s.l. : Los Angeles County Sheriff's Department.**
39. ALERRT Active Attack Data. [Online] https://www.activeattackdata.org.
40. Active Shooter Incidents in the United States in 2021 — FBI. ***Welcome to fbi.gov.*** **[Online] https://www.fbi.gov.**
41. ALERRT Active Attack Data. [Online] [Cited: March 29, 2023.] https://www.activeattackdata.org/.
42. MURPHY, Dominic. ***Deviant Deviance": Cultural Diversity in DSM-5 - Philosophy and Theory of the Life Sciences, vol. 10.*** **Dordrecht : Springer Netherlands, 2015. 978-94-017-9764-1.**
43. Best models of interventions against amok shooters. ***CEPOL - European Union Agency for Law Enforcement Training.*** **[Online] CEPOL, October 17, 2022. [Cited: March 28, 2023.] https://www.cepol.europa.eu/.**
44. J., TUREČEK. ***Policejní pyrotechnika.*** **Plzeň : Aleš Čeněk s.r.o., 2014. 9788073805104.**
45. Explosives. ***GlobalSecurity.*** **[Online] GlobalSecurity.org. [Cited: March 27, 2023.] https://www.globalsecurity.org/.**
46. SINGER, W. Peter. The Evolution of Improvised Explosive Devices (IEDs). [Online] The Brookings Institution, February 7, 2012. [Cited: March 27, 2023.] https://www.brookings.edu/.
47. COMBS, C. Cynthia. ***Terrorism in the Twenty-First Century.*** **s.l. : Taylor and Francis, 2017. 9781317206798.**

48. Бастіон, Останній. Як зробити безпечний вибуховий пристрій із решток боєприпасів. s.l. : Youtube, 2022.
49. HOW TO COOK A MOLOTOV COCKTAIL. RECIPE. ***Lviv Now.*** **[Online] MEDIA-HUB "TVOE MISTO" ("CITY OF YOURS"), February 27, 2022. [Cited: March 29, 2023.] https://tvoemisto.tv/.**
50. E., STEPANOVA. ***Terrorism in Assymetrical Conflict - SIPRI Research Report 23.*** **Oxford : SIPRI, 2008. 978–0–19–953355–8.**
51. ERICSON, A., STANLEY-BECKER, I. How ramming cars into crowds became a major terror tactic. [Online] The Washington Post, March 22, 207. [Cited: March 27, 2023.] https://www.washingtonpost.com/.
52. Joshua, KEATING. Why Terrorists Use Vehicles as Weapons. [Online] The Slate Group LLC, November 5, 2014. [Cited: March 27, 2023.] https://slate.com/.
53. Jacob, SIEGEL. Lone Wolves, Terrorist Runts, and the Stray Dogs of ISIS. ***Why ISIS and al Qaeda rely on loners and losers to carry out their terrorist agenda in the West.*** **[Online] Daily Beast, July 12, 2017. [Cited: March 27, 2023.] https://www.thedailybeast.com/.**
54. MERRIAM, WEBSTER. ***Merriam-Webster's dictionary of law.*** **1996. 978-0-87779-604-6..**
55. Houghton, MIFFLIN. ***The American Heritage® Dictionary of the English Language, 4th edition.*** **s.l. : Harcourt Publishing Company, 2010. 978-0618701728.**
56. BOCIAGA Robert. Myanmar's Drone Wars. ***The Diplomat.*** **[Online] DIPLOMAT MEDIA INC, February 26, 2022. [Cited: March 29, 2023.] https://thediplomat.com.**
57. PRYMULA, Roman a kolektiv. ***Biologický a chemický terorismus - informaace pro každého.*** **s.l. : GRAD Publishing, spol. s.r.o., 2002. 8024702886.**
58. MATOUŠEK, Jiří, ÖSTERREICHER, Jan, LINHART, Petr. ***VBRN Jaderné zbraně a radiologické materiály.*** **s.l. : MATOUŠEK, Jiří, ÖSTERREICHER, Jan, LINHART, Petr., 2007. 9788073850296.**
59. kolektiv, KLEMENT Cyril a. ***Biologické a chemické zbraně - pripravenosť a odpoveď.*** **Banská Bystrica : Vydavateľsvo PRO, 2013. 9788089057436.**
60. HOLLYWOOD John S., SNYDER Diane, MCKAY Kenneth, BOON E. John Jr. ***"Connecting the Dots" in Intelligence Detecting Terrorist Threats in the Out-of-the-Ordinary.*** **[Online] s.l. : The RAND Corporation, 2004.**
61. Cybersecurity and Infrastructure Security Agency. ***Security of Soft Targets and Crowded Places–Resource Guide.*** **[Online] U.S. Department of Homeland Security, April 2019. [Cited: March 26, 2023.] https://www.fema.gov/.**
62. Edwin, BAKKER. ***Forecasting the Unpredictable: A Review of Forecasts on Terrorism 2000 - 2012*** **. [Online] s.l. : International Centre fo Counter-Terrorism - The Hague, 2012.**
63. Radoslav, ROJKO. Modelové hodnocení měkkých cílů pro Olomoucký a Zlínsky kraj. ***Diplomová práce.*** **Zlín : Univerzita Tomáše Bati ve Zlíně, 2018.**
64. STUPNĚ OHROŽENÍ TERORISMEM. ***Centrum proti hybridním hrozbám.*** **[Online] Ministerstvo vnitra České republiky, 2023. [Cited: March 26, 2023.] https://www.mvcr.cz/.**
65. Vyhlašování stupňů ohrožení terorismem. [Online] Ministerstvo vnitra České repubiky, 2023. https://www.mvcr.cz/.
66. ***Developing and Maintaining Emergency Operations Plans*** **. [Online] s.l. : Federal Emergency Management Agency, 2010.**
67. ***Active Shooter: How to Respond Booklet.*** **[Online] Washington : U.S. Department of Homeland Security.**

68. Emergency Action Plan Guide. ***Active Shooter Preparedness.*** **s.l. : Homeland Security.**
69. COMMITTEE, AUSTRALIA-NEW ZEALAND COUNTER-TERRORISM. ***AUSTRALIA'S STRATEGY FOR PROTECTING CROWDED PLACES FROM TERRORISM.*** **[Online] s.l. : Commonwealth of Australia, 2023. 978-1-925593-95-2.**
70. ***Crowded Places Security Audit.*** **[Online] s.l. : Australia-New Zealand Counter-Terrorism Committee.**
71. Committee, Australia-New Zealand Counter-Terrorism. ***Active Armed Offender Guidelines for Crowded Places*** **. [Online] s.l. : Commonwealth of Australia, 2017. 978-1-925593-95-2.**
72. —. ***Improvised Explosive Device (IED) Guidelines for Crowded Places.*** **[Online] s.l. : Commonwealth of Australia , 2017. 978-1-925593-95-2 .**
73. ***Amok – útok aktivního střelce.*** **[Online] 2014. STČ 14/IZS.**
74. Policie ČR. ***Mapa kriminality.*** **[Online] [Cited: April 16, 2023.] https://kriminalita.policie.cz/.**
75. Mapakriminality.cz. s.l. : Projekt Otevřené společnosti, o.p.s., 2020.
76. [Online] McDonald's Česká republika, 2022. [Cited: April 16, 2023.] https://www.mcdonalds.cz/.
77. (ICT), International Institute for Counter-Terrorism. ***Ms. Farah Kasim - Workshop: Protecting Soft Targets - Prevention, Preparedness & Recovery.*** **[Online] s.l. : ICT, 2019.**
78. Uniform Crime Reports for the United States, 1997, 2007 and 2008; Crime in the United States 2011. ***Federal Bureau of Investigation.*** **[Online] Department of Justice, 2012. [Cited: March 26, 2023.]**
79. J., HUGHBANK Richard. ***Intelligence and Its Role in Protecting Against Terrorism.*** **[Online] s.l. : Journal of Strategic Security, 2010. Number 1, Volume 3, No.1.**
80. SMEJKAL Vladimír, RAIS Karel. ***Řízení rizik ve firmách a jiných organizacích.*** **Praha : Grada Publishing, a.s., 2013. 9788024746449.**
81. Tom, KENDRICK. ***Identifying and Managing Project Risk: Essential Tools for Failure-Proofing Your Project.*** **s.l. : AMACOM, 2015. 9780814436097.**
82. FRAIHI, T. ***(De-) Escalating radicalization: The debate within Muslim and immigrant communutues. In Coolsaet, R. Jihadi terrorism and the radicalization challenge in Europe.*** **Hampshire : Ashgate, 2008.**
83. ELLIS, R.,FANTZ, A., KARIMI, F., MCLAUGHLIN, E.C. Orlando shooting: 49 killed, shooter pledged ISIS allegiance. [Online] June 13, 2016. [Cited: March 27, 2023.] https://edition.cnn.com/.
84. ***Japanese Student Accused of Making Lethal Explosive.*** **[Online] Tokyo : The Jiji Press, Ltd., 2019.**
85. Lyn, RAO Heidi. History of Cartridge Propellants - Without gunpowder there would be no guns! [Online] National Rifle Association, March 29, 2022. [Cited: March 27, 2023.] https://www.nrawomen.com/.
86. CYBULSKI, W.B., PAYMAN, W., WOODHEAD, W. D. Trinitrotoluene - TNT. [Online] [Cited: March 27, 2023.] https://www.ch.ic.ac.uk/.
87. International Assoc of Chiefs of Police . ***Terrorist Propaganda (From Clandestine Tactics and Technology A Technical and Background Intelligence Data Service.*** **Arlington : s.n., 1975.**
88. BUCHANAN, L., LEATHERBY, L. Who Stops a 'Bad Guy With a Gun'? [Online] The New York Times Company, June 22, 2022. [Cited: March 29, 2023.] https://www.nytimes.com/.

89. Jake, EPSTEIN. US military weighs sending Ukraine weapons and ammo seized from gunrunners in repeated raids on smuggling boats. [Online] Insider INc., February 14, 2023. [Cited: March 29, 2023.] https://www.businessinsider.com/.
90. ERICSON, C. A. ***Hazard Analysis Techniques for System Safety.*** **s.l. : Wiley, 2015. 978-1118940389.**
91. HESSING Tedd. What is Fault Tree Analysis. ***Fault Tree Analysis.*** **[Online] [Cited: March 30, 2023.] https://sixsigmastudyguide.com/.**
92. FAILURE MODE AND EFFECTS ANALYSIS (FMEA). [Online] American Society for Quality. [Cited: March 30, 2023.] https://asq.org/.
93. BROŽOVÁ Dagmar. Policisté pátrají po neznámém pachateli, který firmu v Plzni odpojil od elektřiny, plynu i vody. ***Týdeník policie.*** **[Online] Bc.Monika Jaňurková, March 29, 2023. [Cited: March 30, 2023.] https://tydenikpolicie.cz/.**
94. Tomáš, NEUGEBAUER. ***Vyhledání a vyhodnocení rizik v praxi. 2. vydání.*** **Praha : Wolters Kluwer, 2014. 9788074784583.**
95. Statistika střelných zbraní. [Online] Policie ČR, 4 20, 2020. [Cited: 4 16, 2023.] https://www.policie.cz/.
96. Věkové složení obyvatelstva - k 1.1. 2020. [Online] Český statitický úřad, 4 30, 2021. [Cited: 4 16, 2023.] https://www.czso.cz/.
98. kkg.

LIST OF ABBREVIATIONS

CBRN	Chemical Biological Radioactive Nuclear
CQB	Close Quarter Battle
ETN	Erythritol tetranitrate
HMTD	Hexamethylen Triperoxide Diamine
HUMINT	Human-source intelligence
IMINT	Imagery-source intelligence
NM	Nitromethane
OHS	Occupational Health and Safety
OSINT	Open-source intelligence
RDD	Radiological dispersive device
SOCINT	Social media intelligence
TATP	Triacetone Triperoxide
TNT	Trinitrotoluene

LIST OF FIGURES

LIST OF TABLES

APPENDICES

Appendix P I: List of threats

APPENDIX P I: LIST OF THREATS

ID	Threat Name
1	Assassination
2	Cold weapon attack
3	Shooting
4	Active shooter
5	Amok shooter
6	Rampage shooting
7	Bomb planting
8	Suicidal bomb attack
9	Arson
10	Taking of hostages
11	Barricade situation
12	Poisoned pen letter
13	Vehicle ramming attack
14	Threats of intimidation
15	Blackmailing
16	Sabotage
17	Disinformation
18	Fake bomb planting
19	Drone strike
20	CBRN Threat