Problematika terorismu a její souvislosti

Bc. Vojtěch Kolář

Diplomová práce
2023

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

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

Akademický rok: 2023/2024

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Vojtěch Kolář**
Osobní číslo:	**L21742**
Studijní program:	**N1032A020002 Bezpečnost společnosti**
Specializace:	**Rizikové inženýrství**
Forma studia:	**Kombinovaná**
Téma práce:	**Problematika terorismu a její souvislosti**

Zásady pro vypracování

1. Dle dostupných zdrojů vypracujte teoretickou část o problematice terorismu a jejích souvislostech.
2. Vyhodnoťte současná preventivní opatření problematiky.
3. Proveďte analýzu rizik pro vybraný měkký cíl.
4. Zhodnoťte současná rizika a následně navrhněte možná řešení.

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

Seznam doporučené literatury:

1. JELÍNEK, Jiří. *Terorismus – základní otázky trestního práva a kriminologie*. Praha: Leges, 2017. ISBN 978-80-7502-256--1.
2. MAKARIUSOVÁ, Radana. *Terorismus, globální terorismus a éra al-Káidy*. Praha: Metropolitan University Prague Press, 2013. ISBN 978-80-86855-95-0.
3. PRIYA, Dixit and Jacob L. STUMP. *Critical Terrorism Studies: An Introduction to Research Methods*. 2013. ISBN 9780415620468

Další odborná literatura dle doporučení vedoucího diplomové práce.

Vedoucí diplomové práce: **doc. Ing. Jaromír Novák, CSc.**
Ústav krizového řízení

Datum zadání diplomové práce: **4. září 2023**
Termín odevzdání diplomové práce: **19. září 2023**

L.S.

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

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

V Uherském Hradišti dne 4. září 2023

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 diplomové 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: 19. 9. 2023

Jméno a příjmení studenta: Bc. Vojtěch Kolář

…….
podpis studenta

ABSTRAKT

Tato diplomová práce se zaměřuje na problematiku terorismu a její souvislosti. Teoretická část je zaměřena na seznámení se se základními pojmy, definicí terorismu, jeho dělením podle druhů a forem a rovněž s teroristickými organizacemi. Popsána je také psychologie terorismu a bezpečnostní politika České republiky společně s bezpečnostní strategií, zájmy a hrozbami pro Českou republiku. Zmíněna je také prevence hrozeb a strategie státu pro boj s terorismem. Závěr teoretické části je věnován definici měkkého cíle, seznámení s dokumenty a systémem pro jeho ochranu a vyjmenovány jsou některé útoku provedené na měkké cíle. Počátek praktické části je věnován seznámení se se současnou situací, jenž je přehledně zpracován do SWOT analýzy. Následně jsou sepsány modelové situace teroristických útoků na měkké cíle. Nalezená rizika jsou ohodnocena pomocí metody PNH, která obsahuje zhodnocení odborníky zabývajícími se danou problematikou. Výstupem práce je návrh opatření za účelem zlepšit prevenci vzniku hrozby a reakci na ni.

Klíčová slova: terorismus, analýza rizik, SWOT analýza, metoda PNH, teroristický útok, riziko, hrozba, bezpečnost.

ABSTRACT

This thesis focuses on the issue of terrorism and its connections. The theoretical part is focused on getting to know the basic concepts, the definition of terrorism, its division according to types and forms, as well as terrorist organizations. The psychology of terrorism and the security policy of the Czech Republic are also described together with the security strategy, interests and threats to the Czech Republic. The prevention of threats and the state's strategy for combating terrorism are also mentioned. The conclusion of the theoretical part is devoted to the definition of a soft target, familiarization with the documents and the system for its protection, and some attacks carried out on soft targets are listed. The beginning of the practical part is dedicated to getting to know the current situation, which is clearly processed into a SWOT analysis. Model situations of terrorist attacks on soft targets are then written. The risks found are evaluated using the PNH method, which includes evaluation by

people dealing with the given issue. The output of the work is a proposal for measures to improve the prevention of threats and the response to them.

Keywords: terrorism, risk analysis, SWOT analysis, PNH method, terrorist attack, risk, threat, security.

Rád bych poděkoval rodině, kolegům a známým za podporu během tvorby této diplomové práce. Také bych chtěl poděkovat mému vedoucímu práce za ochotu, věcné připomínky a pevné nervy při vzájemných konzultacích.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Terorismus je v současnosti dynamicky se rozvíjející problém, který v našich podmínkách nebyl dlouho považován za skutečnou hrozbu. Až události několika posledních let ukázaly, že se jedná o skutečně globální hrozbu.

Tato diplomová práce je zaměřena na vyhodnocení současných preventivních opatření problematiky, provedení analýzy rizik měkkého cíle a jejího vyhodnocení. Jelikož je nutné, aby při vzniklé krizové situaci spojené s teroristickým útokem uměly složky IZS efektivně a koordinovaně spolupracovat, je důležité jim poskytnout dokumenty, které jim umožní se na tyto situace připravit.

Cílem této práce je zhodnotit současný stav ochrany měkkých cílů, poznat slabé stránky a hrozby a navrhnout opatření, která by zvýšila schopnost prevence a reakce systému na vzniklé krizové situace. Navrhnutá opatření jsou prodiskutována s krizovým manažerem města a zaměstnanci jednotek integrovaného záchranného systému.

Díky ohodnocení odborníky, kteří jsou součástí ochrany měkkých cílů, mohou výsledky této práce přinést relevantní návrh opatření vhodný pro implementaci do současného systému a tím zvýšit bezpečnost měkkých cílů vůči teroristickému útoku.

CÍLE A METODY ZPRACOVÁNÍ

Cílem této diplomové práce je zhodnotit současný stav ochrany měkkých cílů, provést analýzu rizik vybraného měkkého cíle a návrh opatření pro jejich lepší zabezpečení. Ačkoli se může zdát, že se jedná o problém určitých zemí, ukázalo se, že terorismus je v současnosti velmi rozvíjející se bezpečnostní hrozba, na kterou je potřeba reagovat. Jelikož cílem útoku se může stát kdokoliv, popřípadě jakýkoliv objekt, je nutné se na danou problematiku zaměřit komplexně.

V praktické části této diplomové práce jsou použity obvyklé metody jako analýza, syntéza, indukce a dedukce. Další metody jsou hodnoceny níže. Je provedena analýza SWOT, která slouží k zhodnocení současného stavu ochrany měkkých cílů a metoda PNH, která slouží k zhodnocení rizik. Dle výsledků těchto analýz je v závěru vypracován návrh opatření, který by měl současnou schopnost předvídat a bránit se útokům na měkké cíle zlepšit.

SWOT analýza

SWOT analýza je analýza a zhodnocení interních a externích faktorů působících na daný projekt. Mezi interní faktory se řadí silné a slabé stránky projektu, zatímco příležitosti a hrozby jsou vnější podmínky působící na daný projekt. Tyto podmínky mohou mít na budoucí fungování projektu kladné i negativní dopady. SWOT analýza navíc umožňuje po jejím zhodnocení zvolení optimální strategie fungování projektu (Srpová et al., 2011; Od SWOT analýzy k tvorbě firemní strategie, 2019):

SO strategie – využití interních silných stránek k těžení z externích příležitostí

WO strategie – minimalizace nebo odstranění slabých míst za pomocí vnějších příležitostí

ST strategie – slouží k omezení nebo potlačení vnějších hrozeb pomocí silných stránek projektu

WT strategie – takzvaná strategie úniku, kdy se jedná o snahu zmírnit dopad hrozeb

Metoda PNH

Je to polokvantitativní metoda k ohodnocení rizik s ohledem na pravděpodobnost vzniku rizika (P), jeho následky (N) a názor hodnotitele (H). Bodové ohodnocení a stupnice se volí individuálně. Výslednou míru rizika pak získáme vzájemným vynásobením daných hodnot, čili R = P x N x H, a následně je pak můžeme rozdělit do několika kategorií. (Koudelka a Vrána, 2006)

Polostrukturovaný rozhovor

Jedná se o formu interview, kde si tazatel vytvoří schéma rozhovoru neboli takové jádro, které je pro něj zásadní, a dle průběhu rozhovoru a reakcí dotazovaných může reagovat a podávat doplňující otázky nebo požadovat vysvětlení odpovědi dotazovaných lidí. Díky těmto možnostem je možné pochopit dané téma do hloubky. (Miovský, 2006)

I. TEORETICKÁ ČÁST

1 ZÁKLADNÍ POJMY

V rámci úvodní kapitoly teoretické části diplomové práce je nezbytné shrnout základní pojmy a nastínit tak problematiku terorismu.

Mimořádná událost (dále jen MU)

Dle zákona č. 239/2000 Sb. o integrovaném záchranném systému je MU definována jako škodlivé působení sil a jevů vyvolaných činností člověka, přírodními vlivy, a také havárie, které jsou život, zdraví, majetek nebo pro životní prostředí ohrožující a vyžadují provedení záchranných a likvidačních prací (Zákon č. 239/2000 Sb. Zákon o integrovaném záchranném systému a o změně některých zákonů, 2023).

Také ji lze definovat jako nenadálou, neočekávanou, časově a prostorově omezenou událost vzniklou v souvislosti s provozem technických zařízení, neodborným nebo neopatrným zacházením s chemickými a jinými nebezpečnými látkami nebo jiným nebezpečím způsobeným lidskou nebo technickou chybou. Často je spojena s bezpečností, ochranou zdraví při práci nebo požární ochranou. (BOZP, 2022)

Je možné tedy hovořit o události s negativním charakterem doprovázené řadou nepříznivých následků, které na sebe mohou navazovat. Tyto události je možné dle příčiny vzniku rozdělit do několika skupin, a to na MU události způsobené činností člověka, přírodními vlivy a vzniklé technickým problémem (BOZP, 2022):

MU způsobené činností člověka:

- Hromadná dopravní havárie
- Sabotáž
- Teroristický útok
- Válka
- Přepadení
- Vloupání
- Nepokoje
- Letecká katastrofa
- Železniční neštěstí

MU způsobené přírodními vlivy:

- Záplava
- Lesní požár
- Zemětřesení
- Lavina
- Tornádo/orkán
- Sesuv půdy
- Krupobití
- Sněhové kalamity
- Erupce vulkánu
- Extrémní vedro/sucho
- Epidemie/pandemie (onemocnění lidí)
- Epizootie (onemocnění zvířat)
- Epifytie (onemocnění rostlin)
- Přemnožení parazitů a škůdců

MU způsobené technickou chybou:

- Požár
- Výbuch
- Radiační havárie
- Ropná havárie
- Zřícení domu
- Únik čpavku z chladícího zařízení
- Únik chloru z úpravny vody
- Letecká katastrofa
- Železniční neštěstí

Krizová situace

Krizová situace je podle zákona 240/2000 Sb. definována jako událost, kdy je vyhlášen jeden z krizových stavů, a to stav nebezpečí, nouzový stav, stav ohrožení státu či válečný stav. Krizová situace může být svým vlivem vyhodnocena jako mimořádná událost, například v případě ohrožení či zasažení chodu subjektů kritické infastruktury. Ovšem tento pojem není v zákoně vymezen (ČESKO, 2000).

„Krizovou situací tedy rozumíme nepředvídatelný nebo těžko očekávatelný průběh událostí po narušení rovnováhy stavů přírodních, ekologických, ekonomických, technických, technologických nebo společenských systémů, což má za důsledek ohrožení životů, zdraví, životního prostředí, vnitřní nebo vnější bezpečnosti státu. Pro řešení těchto vzniklých situací nestačí využití běžných disponibilních zdrojů nebo pouze běžných kompetencí.“ (Antušák, 2013).

Nebezpečí

Nebezpečí jako pojem je velmi náročné definovat, obecně lze říci, že stav či pocit nebezpečí je možné vyhodnotit jako jakýkoliv zdroj ohrožení vedoucí k potenciální škodě, úrazu či poškození zdraví, života a majetku. (Šenovský, Šenovský a Oravec, 2020).

Ohrožení

Ohrožením jsou označeny potenciálně nebezpečné fyzické události, jevy nebo lidská činnost, která může zapříčinit ztrátu života nebo zranění. Dále škodu na majetku, sociální a ekonomické narušení nebo zhoršení životního prostředí, které mohou představovat budoucí hrozby. V základu jsou děleny na přírodní nebo vyvolané lidskými procesy. (Terminologický slovník pojmů, 2016)

Hrozba

„Je přírodní nebo člověkem podmíněný proces představující potenciál, tj. schopnost zdroje hrozby být aktivován a způsobit škodu. Tento potenciál může být spuštěn záměrně nebo náhodně. Využit může být pro atakování specifických zranitelností aktiva. Hrozba bývá zdrojem rizika.“ Mezi přírodní hrozby jsou řazeny geologická, hydrometeorologická a biologická rizika, zatímco do druhé skupiny je zařazeno zhoršování životního prostředí a technologická rizika. Z kybernetického hlediska je hrozba dále dělena na aktivní a bezpečnostní. (Terminologický slovník pojmů, 2016).

Aktivní hrozbu lze chápat jako záměrnou změnu stavu systému zpracování dat nebo používání počítačových sítí, jehož následkem je modifikace zpráv, vložení falešných zpráv či vydávání se za jinou identitu. (Terminologický slovník pojmů, 2016).

Bezpečnostní hrozba představuje potenciální příčinu nežádoucí události, která může potenciálně vyústit v poškození systému a jeho aktiv, čímž je myšleno zničení, nežádoucí zpřístupnění (kompromitaci), modifikaci dat nebo nedostupnost služeb. (Terminologický slovník pojmů, 2016).

Riziko

Riziko představuje určitou pravděpodobnost vzniku události, jenž je z hlediska bezpečnosti nežádoucí, vždy je odvoditelné z konkrétní hrozby. Pravděpodobnost škodlivých následků vyplývajících z hrozby a rizika, je možné určit pomocí analýzy rizik, která vychází z posouzení připravenosti hrozbám čelit. Riziko také může představovat nejistotu k dosažení cílů nebo pravděpodobnost výskytu nežádoucí události s následky, což je jakákoliv odchylka od normálního stavu. (Terminologický slovník pojmů, 2016)

Narušení či výskyt hrozby je ovlivňující pro různé oblasti, kterými jsou například ekonomika, bezpečnost, zajištění zdravotní péče nebo dopad na enviromentální prostředí či jejich kombinace. (Terminologický slovník pojmů, 2016)

Krize

Krize je stav, kdy nastane výrazné narušení fungování určitého systému nebo jeho části. Tento stav vyžaduje rychlé a účinné rozhodování a řešení. Řešení musí být přizpůsobeno jak časovým, tak systémovým potřebám. (Terminologický slovník pojmů, 2016)

Psychickou krizi je možné definovat jako narušení či ztrátu duševní rovnováhy, která nastane u člověka po prožití mimořádné události během posttraumatického šoku, který není schopen sám zpracovat v krátké době, proto je často nezbytné vyhledat odbornou pomoc. Takovou krizi dělíme na akutní a chronickou. Akutní krize vzniká náhle, zatímco chronická je provázena dlouhodobě zatěžující stresovou situaci. (Terminologický slovník pojmů, 2016)

Bezpečnost

Schopnost systému odolávat všem známým, předvídatelným i nenadálým vnitřním i vnějším hrozbám, které mohou negativně působit proti jednotlivým prvkům systému, popřípadě proti systému celému. Je třeba jim odolat takovým způsobem, aby byla zachována jeho struktura,

stabilita, spolehlivost a chování. Jde tedy především o míru stability systému a jeho primární a sekundární adaptace. (Terminologický slovník pojmů, 2016).

Z hlediska kybernetické bezpečnosti jde o ochranu důvěrnosti, integrity a dostupnosti informací při jejich zpracování, úschově, distribuci a prezentaci. Důvěrností je rozuměna vlastnost informace, která má vypovídající hodnotu a není dostupná neoprávněným osobám nebo procesům. Ochranou integrity je docíleno přesnosti a úplnosti, kdy data nebyla neoprávněně změněna, a jsou i nadále důvěryhodná. Dostupností informací se rozumí možnost jejich využití na základě oprávnění jejich použití vybranými osobami. (Terminologický slovník pojmů, 2016).

Bezpečnostní prostředí

Bezpečnost je prioritním požadavkem společnosti. Bezpečnostní hrozby mohou být z vnějšího i vnitřního prostředí. Je však nezbytné se zaobírat také ekonomickými a energetickými riziky, které mohou mít zásadní vliv v oblasti životního prostředí. Zdroje hrozeb mohou mít státní, nestátní, tak i nadnárodní význam. (Krásný a Socha, 2006)

Bezpečnostní prostředí lze chápat jako pojem, který zahrnuje jak přírodní, tak i společenskou stránku. Popisuje možné ohrožení a zranitelnost zkoumaného prostředí. Je to prostor, kde dochází ke střetu zájmů se zájmy jiných aktérů systému a odehrávají se zde procesy ohrožující bezpečnost státu (Frank, 2003).

Kritická infrastruktura (dále jen KI)

Prvek nebo systém KI představuje klíčovou součást infrastruktury, jejíž nefunkčnost nebo narušení by měla závažný vliv na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob a ekonomiku sátu (Terminologický slovník pojmů, 2016).

Prvkem KI rozumíme stavbu, prostředek, zařízení nebo veřejnou infrastrukturu určenou podle stanovených kritérií. Také zde můžeme zahrnout prvky v odvětví komunikačních a informačních systémů v oblasti kybernetické bezpečnosti (Ochrana kritické infrastruktury, 2023).

Subjekt KI je provozovatel, odpovídá za ochranu prvku KI a musí určit bezpečnostního zaměstnance, který odpovídá za součinnost při plnění úkolů podle krizového zákona. Pro potřeby ochrany zpracovává plán krizové připravenosti, kde jsou definována možná bezpečnostní rizika a ohrožení funkce prvku KI a zároveň jsou zde stanovena opatření na jeho ochranu (Kritická infrastruktura, 2023).

Měkký cíl

Jedná se o místa s vysokou koncentrací osob, symbolickým, kulturním nebo náboženským významem, která tvoří součást infrastruktury státu, jejíž narušení by mělo negativní vliv na fungování státu a společnosti. Tato místa nejsou střežena ozbrojenými složkami nebo jiným způsobem, potažmo nejsou střežena vůbec, jelikož jde o veřejně frekventovaná místa, snadno napadnutelné objekty nebo místa nevojenského charakteru. (Terminologický slovník pojmů, 2016)

Kyberterorismus

Kyberterorismus představuje úmyslný útok s politickými motivy, který je zaměřen proti počítačovým systémům, programům a uživatelům v rámci kyberprostoru. Tento typ terorismu využívá moderních technologií a může mít vážné dopady na společnost, ekonomiku a bezpečnost země. Jeho cílem je získat nezákonně citlivé informace, zničit data nebo sabotovat činnost počítačových systémů. Tito zločinci, známí jako crackerové, využívají různé techniky útoku. Kyberterorismus může mít vážné následky, včetně ztráty na lidských životech, zejména pokud se útoky zaměřují na bankovní, státní nebo vojenskou infrastrukturu (Co je kyberterorismus, 2022).

Aktivní střelec

Aktivní střelci jsou osoby s vysokou úrovní agresivity, jsou schopni během krátkého časového období spáchat například masovou střelbu, při které často používají nástražné a výbušné zařízení. Jejich činy jsou předem naplánovány a promyšleny. Často jsou smířeni s vlastní smrtí nebo jejich útok končí zabitím nebo sebevraždou. Cílem útočníků je usmrcení co největšího počtu obětí, proto jsou vybírány místa s vysokou koncentrací pohybu osob. Těmito místy mohou být sportovní stadiony, kulturní akce, nákupní centra, školy, nemocnice apod. (Agh, 2011).

2 TERORISMUS

Terorismus je brán jako hrozba od poloviny 90. let 20. století. Do té doby o něm bylo hovořeno jako o riziku. V současné době je řazen mezi nejvíce rostoucí a zásadní hrozbu společnosti. Mezi další taková rizika je možno zařadit organizovaný zločin, extremismus, migrační vlny a začleňování migrantů do společnosti, a mimo to další sociální, hospodářská či ekologická rizika. Zvratovou událostí této problematiky bylo 11. září 2001 tedy útoky ve Spojených státech. Tato událost byla spouštěč diskuzí, jakou váhu má terorismus, jaká je jeho míra ohrožení společnosti a jaké jsou jeho příčiny. Dále se začaly rozvíjet strategie, jak se s takovými událostmi vypořádat a jaké kroky je nezbytné učinit. (Janošec, 2010; Chailand a Biln, 2007)

Podle Priyi a Stumpa (2013) není možné terorismus jednoduše definovat. Nicméně lze jej vysvětlit jako formu politicky, ideologicky nebo nábožensky motivovaného násilného jednání za účelem vyvolat u lidstva obavy, strach nebo pocit nebezpečí. Hrozby mohou být kategorizovány podle několika faktorů, mezi které lze zařadit původce hrozby, cíle útoku a použité nástroje. Útoky a pokusy o ně by měly být vnímány jako varování a měli bychom přijmout preventivní opatření, která by minimalizovala jejich dopad na společnost. (Audit národní bezpečnosti, 2016; Jelínek, 2017)

Pachatelé teroristických útoků mají často společné charakteristické rysy, které mohou zahrnovat (Mareš, 2005):

- Oddanost svým vůdcům a idejím
- Nedostatek projevů lidských emocí, jako je slitování nebo výčitky
- Vysokou inteligenci a schopnost strategického myšlení
- Dobré schopnosti rozhodování a uvážlivosti
- Vzdělání a široké obecné znalosti

2.1 Právní úprava pojmu terorismus

Alternativní formulace trestněprávní definice pojmu terorismu v české legislativě lze nalézt v zákoně č. 40/2009 Sb., trestní zákoník ve znění následných předpisů. Tato definice vymezuje termín terorismus, jakož i pojmy "teroristický útok" a "teror". Konkrétně se tato definice nachází ve dvou paragrafech, a to v § 311 a § 312.

Podle tohoto zákona je "teroristický útok" definován jako soubor opatření prováděných jednotlivcem či skupinou lidí, kteří si kladou za cíl poškodit ústavní zřízení nebo obranyschopnost České republiky. Tímto jednáním je usilováno o narušení či zničení politické, hospodářské a sociální struktury země. Záměrem je vytvořit vážné zastrašení obyvatelstva a nátlak na vládu či jiné veřejné orgány, aby podnikaly, ustupovaly nebo utrpěly významné ztráty ve své moci. (Zákon č. 40/2009 Sb., 2023)

Součástí je seznam konkrétních akcí, které mohou být považovány za teroristický útok. To zahrnuje například útoky s cílem ohrozit životy a zdraví jednotlivců za účelem způsobit smrt či vážné zranění. Dále sem patří i činy jako únos rukojmích nebo uskutečnění únosu, spolu s dalšími možnými formami útoků, které mají za cíl narušit, zmocnit se, poškodit nebo vykonat jiné nepřijatelné činy ze strany potenciálních teroristů. (Zákon č. 40/2009 Sb., 2023)

Pokud je pachatel shledán vinným dle tohoto paragrafu, může být potrestán trestem odnětí svobody až na patnáct let, přičemž tento trest může být doprovázen ztrátou veškerého majetku. (Zákon č. 40/2009 Sb., 2023)

Dle § 312 zákona č. 40/2009 Sb., trestní zákoník ve znění pozdějších předpisů, označuje "teror" jako jednání osoby nebo skupiny lidí, kteří směřují své kroky k úmyslnému poškození ústavního zřízení České republiky nebo mají záměr usmrtit někoho jiného, v případě že bude tento záměr prokázán. V těchto situacích se může vynést rozsudek na odnětí svobody v rozmezí od patnácti do dvaceti let, případně může být uložen výjimečný trest, pokud jsou splněny příslušné podmínky. (Zákon č. 40/2009 Sb., 2023)

2.2 Formy a druhy terorismu

Ve světě je možné nalézt opravdu mnoho teroristických skupin, které se odlišují svou strukturou, motivací a cíli. Je možné jej rozdělit dle určitých kritérií do několika kategorií. Nejvíce se liší v cíli, kterého chtějí dosáhnout, nikoliv však použitými prostředky. Terorismus podle použitých metod se dělí:

- **Klasický terorismus** využívá tradiční metody, jako jsou střelba, výbuchy a únosy letadel, což ho činí více viditelným než ostatní typy. (Typologie terorismu, 2023)
- **CBRN terorismus** se zaměřuje na použití jaderných, biologických a chemických zbraní. Zatímco jaderné zbraně jsou příliš drahé a složité na výrobu, biologické zbraně využívají viry, bakterie a toxiny, které mohou způsobit smrtelné nemoci.

Teroristé také mohou použít chemické látky, které jsou snadno dostupné a levné. (Vičar, 2017)

- **Kybernetický terorismus** je způsob vedení boje skrze počítačové sítě, které mohou vést k paralyzování automatizovaných systémů pro rozvod vody, plynu a energie, a také k útokům na leteckou dopravu a komunikační sítě vládních orgánů a armád. (Brzybohatý, 2001)

Teroristé také využívají internetu k propagaci svých ideologií, rekrutaci, plánování útoků, zastrašování a získávání nových prostředků.

Podle použité motivace lze útoky dělit na následující:

1. **Ultralevicový terorismus** – forma politického násilí, která se snaží prosazovat své cíle prostřednictvím použití násilí a teroru. Využívá různých prostředků – bomby, únosy, vraždy, aby vyvolal strach a chaos v politickém životě. Často reaguje na společenské změny a opírá se o ideologie anarchismu a komunismu. Nejvíce rozšířen je v latinskoamerických zemích, kde se snaží o změnu politického systému a sociálních struktur. (Sedláková, 2017)
2. **Ultrapravicový terorismus** – prosazuje národnostní a rasovou nadřazenost a klade důraz na konzervativní hodnoty. Pilířem tohoto typu terorismu je xenofobie, tedy strach z neznámého a cizího, ale také rasismus spočívající v přesvědčení o nadřazenosti jedné rasy nad druhou a s tím související nenávisti. Vyskytuje se po celém světě, ačkoliv v různé míře a pod různými názvy. (Co je rasismus, homofobie, extremismus..., n.d.; Sedláková, 2017)
3. **Single-issue terorismus** – nesnaží se transformovat celou politickou agendu, ale bojuje proti jedinému tématu nebo problému. Často se vyskytuje u tematických otázek – životní prostředí, práva zvířat, potraty, náboženské nebo etnické nesnáze apod. Vidí použití násilí jako jedinou možnost na upoutání pozornosti a dosažení změn. (Chenoweth, English a Gofas, 2019)
4. **Terorismus osamělých vlků** – jedná se o jedince, kteří jsou radikalizováni sami a používají násilí nebo hrozbu násilí k prosazení svých zájmů. Nelze je spojovat s žádnou organizací, ani s žádným hnutím, protože jednají samostatně. (Bates, 2012; Nosál, 2012)

5. **Náboženský terorismus** – je využíván pro dosažení náboženských cílů a je ovlivněn náboženskými přesvědčeními. Typickými zástupci tohoto terorismu jsou islámský stát a křesťanský terorismus. Pojí se s dalšími faktory, jako jsou etnické nebo teritoriální ambice a politické ideologie. (Svoboda, 2021)
6. **Etnický terorismus** – na rozdíl od útoků motivovaných ideologií, náboženstvím nebo finančními zájmy, je tento typ zaměřen na prosazování zájmů konkrétní etnické skupiny a často se snaží ovlivnit spíše oblast, kde členové skupiny žijí, než celý stát. (Svoboda, 2021; Byman, 1998)
7. **Teritoriální terorismus** – je zaměřen na získání nezávislosti pro určité území. Pojmy etnický a teritoriální terorismus se vzájemně prolínají a jsou často spojovány. (Svoboda, 2021)
8. **Kriminální terorismus** – teroristické akce provedeny za účelem získání osobních i materiálních výhod. Jsou zaměřeny na finanční zisk a jeho pachatelé jsou často organizovanými zločineckými skupinami. (Typologie terorismu, 2023)
9. **Patologický terorismus** – pachatelé často trpí psychickými poruchami, které se svými činy snaží uspokojit. Mohou být společensky vyloučeni a v páchaní teroristických akcí vidí způsob, jak se zviditelnit. (Typologie terorismu, 2023)

Další možné dělení je podle původce:

1. **Státní terorismus** – použití síly nebo hrozby násilí ze strany státních orgánů nebo vlády proti obyvatelům svého vlastního území s cílem vyvolat strach a zastrašování. Rozlišuje se mezi tajným státním terorismem a terorismem podporovaným státem. (Breen-Smyth, 2016; Makariusová, 2013)
2. **Nestátní terorismus** – Jsou zde zahrnuty aktivity teroristických skupin nebo jednotlivců, kteří nejsou součástí státních orgánů. Tyto skupiny nebo jednotlivci mají omezené zdroje a členů ve skupině není mnoho. Mají za cíl upoutat pozornost a vyvolat strach mezi veřejností pomocí násilných útoků a psychologického tlaku. (Bahenský, 2016)
3. **Individuální terorismus** – Je páchán jednotlivci, kteří páchají své činy jednotlivě, bez příslušnosti v nějaké organizované skupině a bez vlivu vůdce či hierarchie. Metodu, jakou provedou svůj čin a taktiku si volí jedinec sám. (Heide, 2011)

Dále lze dělit terorismus podle použitých typů zbraní na letální (smrtící) a neletální.

Letální formy terorismu

Letální formy terorismu se vyznačují se použitím základních nástrojů násilí nebo donucování. Tyto formy terorismu lze podrobněji rozdělit do dvou kategorií v závislosti na použitých prostředcích. Konkrétně se jedná o konvenční a nekonvenční terorismus. Tyto formy terorismu jsou nebezpečné a mohou mít vážné důsledky pro společnost.

Konvenční a nekonvenční terorismus (Lesser, 1999):

1) Sečné a bodné zbraně
2) Střelné zbraně
3) Hořlavé látky
4) Výbušné zbraně
5) Zbraně hromadného ničení

Neletální formy terorismu

Moderní terorismus se vyznačuje použitím nových nebo inovativních způsobů teroristických útoků, včetně kombinace moderních nástrojů a neletálních prostředků. Tato forma terorismu je také označována jako sofistikovaný terorismus. Pro snazší kategorizaci je možné tuto formu terorismu rozdělit do dvou podskupin na základě použitých prostředků při teroristickém útoku. První podskupina zahrnuje běžné prostředky pro teroristické útoky (neozbrojený terorismus), zatímco druhá podskupina zahrnuje nekonvenční prostředky. Do této kategorie je tedy možné zařadit:

- Dopravní prostředky (auta, letadla, vlaky, lodě) (Terrorist attacks in the U.S. or against americans, 2022)
- Kyberterorismus
- Mediální (psychologický) terorismus
- Zbraně využívající principy akustiky, optiky, elektromagnetického pulsu (Brzybohatý, 2002)

Tyto prostředky mají za úkol vyřazení protivníka z boje na určitou dobu, aniž by byl přímo ohrožen jeho život. Při jejich použití může také dojít k psychologickému účinku. Tyto zbraňové prostředky jsou stále vývojově vylepšovány, ale zatím nejsou příliš rozšířené. To

je způsobeno absencí smrtícího nebo těžce zraňujícího účinku a vysokými finančními náklady.

2.3 Stupně ohrožení

Dne 25.5.2016 bylo vládou rozhodnuto usnesení č. 63 o Systému vyhlašování ohrožení terorismem. Pro vyhlášení určitých mimořádných opatření není podmínkou stanovení určitého stupně ohrožení terorismem, nýbrž je nutno zohlednit právní podmínky a posoudit vhodnost, přínosnost, nezbytnost a přiměřenost daných opatření pro řešení konkrétní bezpečnostní situace. Bez ohledu na zachování stejného stupně ohrožení terorismem může být přijato nebo zrušeno různé opatření v závislosti na charakteru a intenzitě hrozby. Změna aktuální bezpečnostní situace také nemusí nutně vést ke změně vyhlášeného stupně, ale může vést pouze k úpravě opatření. (Stupně ohrožení terorismem, 2023)

Tento systém definuje stupně ohrožení terorismem do čtyř kategorií. **Nulový stav** je situace, kdy není známa žádná konkrétní ani obecná hrozba teroristického či podobného útoku na území ČR. Ačkoliv se jedná o ideální stav, je vzhledem k obecné bezpečnostní situaci ve světě těžko dosažitelný. V takovéto situaci by nebyla vydána žádná zvláštní doporučení, varování pro veřejnost ani přijímána žádná protiteroristická opatření bezpečnostních složek. Tento stav není nevyhlašován vládou. (Stupně ohrožení terorismem, 2023)

První stupeň je ohrožení terorismem signalizující obecné ohrožení terorismem v zahraničí, ale není známa konkrétní hrozba teroristických aktivit na území ČR. V této situaci jsou zavedena dlouhodobě vytipovaná zvýšená bezpečnostní opatření v rozsahu, v jakém rozhodne vláda. (Stupně ohrožení terorismem, 2023)

Druhý stupeň signalizuje, že se zvyšuje riziko vystavení teroristické hrozbě, ale není možné přesně určit podrobnosti ohledně času či povahy hrozby. Tento stupeň je vyhlášen po předchozích událostech, nebo pokud jsou k dispozici informace naznačující možné teroristické aktivity. (Stupně ohrožení terorismem, 2023)

Třetí stupeň ohrožení terorismem zavádí vysoký stupeň bdělosti a pohotovosti, kdy je teroristický útok na cíl zájmů ČR očekáván s vysokou pravděpodobností nebo již proběhl a je třeba přijmout opatření k zamezení pokračování či opakování útoku a minimalizování následných škod. (Stupně ohrožení terorismem, 2023)

3 PSYCHOLOGIE TERORISMU

Terorismus je psychosociální logikou, která se zakládá na působení sociálních a psychologických faktorů. Každý jedinec, který se rozhodne stát teroristou, má své vlastní důvody a pohnutky nebo je dlouhodobě ovlivňováno jeho jednání a empatie, která má návaznost na plánování teroristických činů.

Motivaci jedince je možno chápat i jako psychické narušení, které souvisí s životní nespokojeností, nedostatečným vzděláním či působení nevhodného společenského prostředí. To může osobu natolik ovlivnit, že jakékoliv jiné chování či poměry mimo tuto skupinu osob se stejným teroristickým smýšlením vede k předsudkům, zaujatosti a touze po likvidaci cíle. (Ibañez, 2009)

Teroristé mají většinou sklony k samotářství a jsou přesvědčeni, že mají vždy pravdu. Tito jedinci obvykle nesouhlasí se společenskými a politickými normami, proto je chtějí změnit pomocí teroristických činů. Často mají své následovníky, kteří sdílejí jejich názory. Teroristé jsou ochotni se obětovat pro své cíle a často hledají mediální pozornost. Jsou většinou nadprůměrně inteligentní, dominantní a dokáží sofistikovaně připravit teroristické útoky. (Smolík, 2015)

Získávání ucelené definice psychologického modelu teroristy je obtížné, protože teroristé často zemřou během útoku, což znemožňuje podrobné psychologické posouzení. Navíc mnoho teroristů odmítá spolupracovat s psychologem nebo psychiatrem, což dále komplikuje jakékoliv snahy o identifikaci jejich motivace a chování. (Smolík, 2015)

Přesto je možné jejich motivaci rozdělit dle motivu pro jejich činy (Smolík, 2015):

1. Politická ideologie, která může být založena na různých faktorech, jako jsou politické postoje, rasová, národnostní či etnická příslušnost.
2. Náboženský fanatismus může hrát klíčovou roli v motivaci teroristů k násilným činům.
3. Někteří teroristé mohou mít touhu po negativní seberealizaci, což zahrnuje pomstu a způsobení utrpení druhým.
4. Patologická touha ničit může být faktorem, který motivuje teroristy k útokům na ostatní.
5. Finanční zisk může být důležitým motivem organizovaného trestného činu a kriminálního terorismu.

6. Afekt může hrát roli u teroristů, kteří jednají samostatně a bez organizované skupiny.
7. Potřeba uznání skupinou a širším okolím může být motivací pro teroristy, kteří se chtějí stát součástí určitého hnutí nebo skupiny.

První skupina psychologů, kteří se věnovali výzkumu terorismu, zaměřovala svou pozornost na psychoanalytické aspekty této problematiky. Dle jejich interpretace byl terorismus považován za patologický jev, který se objevoval u jednotlivců s psychologickými odchylkami nebo s poruchou chování, jež se projevovaly již v raném dětství. Z prvních analýz vyplývalo, že motivací pro teroristické činy bylo nepřátelství vůči rodičům, přičemž tyto pohnutky byly nevědomé. Z dalších studií vyplývalo, že mezi teroristy byla častěji zastoupena skupina jedinců, kteří byli v dětství vystaveni šikaně či týrání. (Smolík, 2015)

V současnosti se většinou spojují tři hypotézy s terorismem Smolík, 2015):

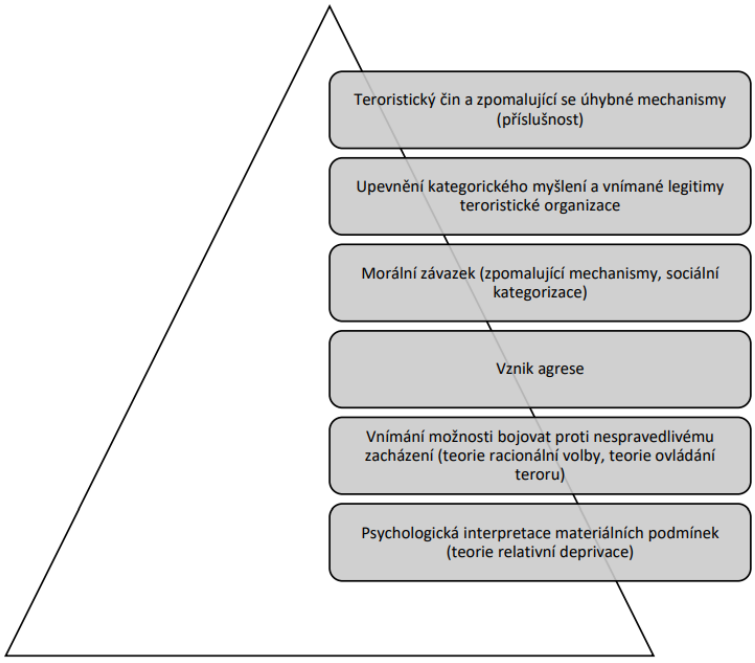
- **Hypotéza frustrace neboli agrese**. Ta vysvětluje terorismus jako reakci na nespokojenost jedinců s jejich situací, která je často spojena s chudobou, nespravedlností a diskriminací.
- **Hypotéza narcistického hněvu**, která zdůrazňuje roli narcistického sebevědomí a pýchy u jedinců, kteří se stávají teroristy. Ti pociťují urážku a ztrátu svého statusu v různých oblastech života a touží po pomstě.
- **Hypotéza negativní identity** a vysvětluje, že terorismus může být pro jedince způsobem, jak si vybudovat pozitivní identitu v rámci své skupiny. Tento proces může být zvláště důležitý pro jedince, kteří se cítí okrajoví nebo vyloučení ze společnosti.

3.1 Metafora schodiště

Myšlenkovou koncepci lze přirovnat k budově s pěti patry a schodištěm, kde každé patro představuje určitý psychologický proces, který je spojen s terorismem. Na přízemí se nachází pocit nespravedlnosti, který může být veden do prvního patra, kde jedinec hledá způsoby, jak zlepšit svoji životní situaci. Pokud se situace nelepší, může se jedinec dostat do dalšího patra, kde se frustrace prohlubuje a zvyšuje se vliv sociálně-ekonomických faktorů. V této fázi mohou teroristické organizace zneužívat zlost a frustraci a přesvědčovat jedince o ospravedlnitelnosti terorismu. Další patra jsou zaměřena na přesvědčování jedinců o zákonnosti terorismu a přípravu na provádění teroristických činů. (Smolík, 2015)

První stupeň lze přirovnat k úvodnímu kroku na schodišti, kde osoba může zažívat pocit nespravedlnosti a ztráty. V prvním patře se jedinec snaží najít způsob, jak zlepšit svou situaci a nalézt větší spravedlnost. Je důležité, aby jedinec měl k dispozici podporující prostředí a příležitosti pro sociální integraci. Pokud se situace nevyvíjí příznivě, frustrace se prohlubuje a osoba postupuje do dalšího patra, kde socioekonomické faktory mají větší vliv, než faktory politicko-psychologické. Zde se objevuje zlost a frustrace, které mohou být zneužity radikálními teroristickými organizacemi, aby osoby postupovaly do dalších pater. V těchto patrech se jedinci seznamují s myšlenkami a taktikami teroristických organizací, vznikají rekruti, kteří jsou podrobeni psychickému tlaku a jsou přesvědčováni o ospravedlnitelnosti terorismu. Tito jedinci vedou tajné životy a jsou vystavováni nátlaku, aby drželi své členství v teroristické organizaci v tajnosti. (Smolík, 2015)

V poslední fázi se jedinci dostávají k rozhodnutí, zda se stanou aktivními členy teroristických organizací. Někteří se rozhodnou stát se plnohodnotnými členy, kteří se podílejí na plánování a provádění teroristických akcí. Druhá skupina se skládá z tzv. "pěšáků" nebo "foot soldierů", kteří jsou využíváni k provedení sebevražedných útoků nebo rychlých násilných akcí. V této fázi jsou členové organizace připravováni a motivováni k páchání teroristických útoků. Všichni lidé, kteří nejsou součástí organizace, jsou vnímáni jako nepřátelé. (Smolík, 2015)



Obrázek 1 Metafora schodiště Zdroj: Sojková, 2018

3.2 Dynamika teroristických skupin

Teroristická skupina je strukturovaný kolektiv, složený z řady jednotlivců, kteří se dobrovolně spojují za účelem provádění teroristických aktivit. Pro každou takovou skupinu je klíčové k samostatné existenci, což často vyžaduje provádění teroristických akcí, aby skupina získala další podporu a legitimizaci v médiích. (Smolík, 2015)

Podle psychologických analýz není většina teroristů duševně nemocná, psychopatická nebo násilnická, vyskytují se u nich stejné psychologické prvky jako u běžných lidí. V teroristických skupinách bývají často formální struktury, které odpovídají specializacím a rolím jednotlivých teroristů, ale také se mohou vyskytovat neformální vztahy a organizace bez jasného vůdce, které se řídí taktikou odporu. (Smolík, 2015)

Pro teroristické organizace jsou klíčové normy, tedy soubor pravidel ovlivňujících chování jednotlivých teroristů při provádění teroristických útoků. Tyto organizace jsou většinou složeny z jedinců, kteří se snaží dosáhnout pro svou skupinu tzv. "vyšších cílů" a měnit tak společenské a politické prostředí. (Smolík, 2015)

3.3 Nejvýznamnější teroristické organizace

Islámský stát je znám také pod zkratkou ISIS (Islámský stát od Iráku a Šímu). Tato organizace ovládá severní část Iráku a západní část Sýrie a uvnitř těchto oblastí si vytvořila vlastní vládu s velmi krutými praktikami, které přijímají právo šaría. Zakladatelem islámského státu byl Abú Bakr al-Baghdádí, který stojí za některými z nejbrutálnějších teroristických útoků, včetně některých, které byly odsouzeny i Al-Káidou. ISIS přijímá bojovníky z celého světa a povzbuzuje je, aby emigrovali do tzv. „nebe na zemi“. (Šmíd, n.d.)

Al-Káida je jedním z nejznámějších jmen spojených s terorismem. Proslavila se hlavně kvůli útokům 11. září 2001 v New Yorku. Tato extremistická islámská organizace byla založena v roce 1989 Usámou Bin Ládinem a pod jeho vedením provedla několik velkých útoků na Spojené státy, což vyvrcholilo afghánskou válkou. V květnu 2012 byl Bin Ládin zabit v Pákistánu. Tato organizace je známá svou integrovanou sítí, výkonnou strategií a několika tisíci členy, kteří absolvovali řádný vojenský výcvik. (Al-Káida, 2003-2023)

Hamás, neboli Harakat Al-Muqawama Al-Islamia je teroristická organizace původem z Palestiny, která vznikla jako odnož Muslimského bratrstva v roce 1987. Hlavním cílem této sociopolitické skupiny bylo uskutečnit džihád, což je náboženská povinnost muslimů

bojovat za obranu a rozšíření islámu, zejména vůči Izraeli a zajistit tak svobodu Palestiny. Skupina je známá pro své sebevražedné atentáty a je aktivně podporována Hizballáhem v boji proti izraelské vládě a civilistům. (Nejnebezpečnější teroristické organizace na světě, © 2018; Hamas: Definition, History, Ideology and Facts, 2023)

Hizballáh byl založen během libanonské občanské války v roce 1982. Patří mezi největší nepřátele Izraele a sunnitských arabských zemí. Podle zpráv CIA se těší podpoře až 41% libanonské populace a organizace se také angažuje v několika humanitárních a společenských akcích v celé zemi. (Libanonský Hizbulláh: vznik a transformace hnutí 1982-2000, 2019)

Taliban se proslavil svým působením v Afghánistánu v letech 1996-2001, kdy měla jako jedna z mála organizací na starosti správu této země. Jejím zakladatelem byl Mullah Mohammed Omar a během své vlády v Afghánistánu zavedla přísnou interpretaci islámských zákonů a práva šaría, čemuž se země vrátila do středověku. Kromě toho organizace odstraňovala starobylé artefakty a sochy a nutila ženy, aby chodily zahalené. Organizace také získala aktivní podporu Al-Káidy, ale následně byla svržena během invaze USA. (Taliban Fast Facts, 2023)

Óm šinrikjó byl spolek založen roku 1984, který se zaměřoval na meditaci a jógu pod vedením Šókó Asahary. O tři roky později byl tento spolek přeměněn na náboženskou organizace Óm šinrikjó, což znamená „Nejvyšší pravdu“. Tato sekta hlásala katastrofický a progresivní milenialismus a Asahara varoval před možností třetí světové války. Následně však došlo k několika vraždám členů sekty, kteří se nechtěli podřídit jejím pravidlům, nebo ji opustit. Toto vedlo k tomu, že Asahara začal více inklinovat ke katastrofickému milenialismu a začal shromažďovat střelné, biologické a chemické zbraně. (Srbová, 2016)

4 BEZPEČNOSTNÍ POLITIKA

Bezpečnostní politika státu se opírá o soubor klíčových cílů a prostředků, které jsou zaměřeny na ochranu suverenity a celistvosti státu a jeho demokratických principů. Dále na podporu činnosti demokratických institucí, na podporu ekonomického a sociálního rozvoje, na ochranu zdraví a života občanů, majetku, kulturních statků, životního prostředí a plnění mezinárodních bezpečnostních závazků.

Bezpečnostní politika státu se skládá z pěti základních částí (Bezpečnostní politika, 2023):

- „zahraniční politika“,
- „obranná politika“,
- „politika v oblasti vnitřní bezpečnosti“,
- „hospodářská politika v oblasti bezpečnosti státu“
- „politika veřejné informovanosti v oblasti bezpečnosti státu“.

Bezpečnostní strategie je základním koncepčním dokumentem, který definuje bezpečnostní hrozby a způsoby, jak jim čelit. Tento dokument byl přijat jako odpověď na zhoršující se bezpečnostní prostředí ve světě, které má výrazný vliv na bezpečnost euroatlantického prostoru a vyžaduje, aby NATO, EU a jednotlivé členské státy účinně reagovaly na nové bezpečnostní hrozby a výzvy. Dokument zároveň klade větší důraz na plnění spojeneckých závazků a posiluje otázku zajištění vnitřní bezpečnosti. (Bezpečnostní politika, 2023)

Bezpečnostní strategie je důležitým dokumentem, který poskytuje jasný rámec pro řešení bezpečnostních výzev, kterým čelíme. Jeho přijetí reflektuje narůstající nebezpečí, které vzniká v souvislosti se změnami v mezinárodním prostředí a zvyšující se komplexitou bezpečnostních hrozeb. Strategie zahrnuje široké spektrum oblastí, včetně obrany, bezpečnosti, hospodářství, energetiky a technologií. Jejím cílem je zajistit efektivní koordinaci mezi jednotlivými subjekty a zvýšit úroveň bezpečnosti pro všechny občany. (Bezpečnostní politika, 2023)

4.1 Bezpečnostní strategie ČR

Bezpečnostní strategie České republiky (dále jen Bezpečnostní strategie ČR) představuje základní dokument, který určuje směřování bezpečnostní politiky ČR a slouží jako východisko pro další strategické dokumenty. Tento dokument je výsledkem spolupráce vlády, Kanceláře prezidenta republiky a Parlamentu ČR s cílem najít nadstranické přístupy

k otázkám bezpečnosti. Při tvorbě strategie se zapojila i široká bezpečnostní komunita zahrnující zástupce jak ze státní, tak i nestátní sféry. Bezpečnost ČR je zajištěna právním rámcem, který se skládá nejen z Ústavy ČR, ale také z dalších zákonů a mezinárodních závazků vyplývajících z členství v organizacích jako NATO, EU, OSN a OBSE. Tyto zákony a závazky jsou nedílnou součástí bezpečnostního systému zajišťujícího ochranu zájmů ČR.

Aktuálně se řídíme podle Bezpečnostní strategie z roku 2015, která vychází z bezpečnostní strategie z roku 2003 a aktualizuje její upravené vydání v roce 2011. Bezpečnostní strategie ČR analyzuje a popisuje vývoj bezpečnostního prostředí v euroatlantickém prostoru a klíčové bezpečnostní hrozby. Jejím hlavním cílem je zajistit koordinovaný a systémový rámec pro prosazování bezpečnostních zájmů ČR a efektivní využívání multilaterálních, bilaterálních a národních nástrojů a stručně popisuje bezpečnostní systém ČR. V dokumentu jsou definovány bezpečnostní zájmy ČR, konkrétní hrozby a přístupy k bezpečnosti. (Bezpečnostní strategie České republiky, 2009-2023)

Východiska bezpečnostní politiky ČR

Vláda ČR a orgány územní samosprávy mají za úkol chránit obyvatele, suverenitu, celistvost země a zajistit zachování demokratického právního státu. Pro dosažení těchto cílů slouží komplexní a funkční bezpečnostní systém, který se průběžně přizpůsobuje aktuální bezpečnostní situaci v ČR i v zahraničí. Bezpečnost v ČR je založena na principu ochrany jednotlivce a jeho života, zdraví, svobody, lidské důstojnosti a majetku, k tomu je nezbytné zajistit bezpečnost státních institucí a rozvíjet procesy a nástroje, které posilují bezpečnost a ochranu obyvatelstva. Ačkoli je zodpovědnost zajištění bezpečnosti především na vládě, je žádoucí aktivní spolupráce občanů, organizací a veřejné správy pro snižování rizik a posilování celkové odolnosti společnosti proti bezpečnostním hrozbám. (Bezpečnostní strategie České republiky, 2009-2023)

Bezpečnostní strategie ČR vychází z aktivního přístupu, který se snaží včas odhalit bezpečnostní hrozby a přijmout účinná opatření, zaměřuje se na aktivní prevenci ozbrojených konfliktů a diplomacii. Nedělitelnost bezpečnosti znamená, že bezpečnost ČR a euroatlantického prostoru je propojena s globální bezpečnostní situací. Ochrana občanů a území není omezena na hranice státu, jelikož bezpečnostní zájmy ČR je třeba často chránit i mimo hranice spojeneckých zemí. (Bezpečnostní strategie České republiky, 2009-2023)

ČR se zavázala k posílení svých obranných schopností a postupnému vytvoření moderní a profesionální armády, která bude schopna účastnit se aliančních a mezinárodních operací v různých částech světa. ČR také aktivně spolupracuje v rámci SZBP (Společná zahraniční a bezpečnostní politika) EU a ESDP (Evropská bezpečnostní a obranná politika), aby posílila své bezpečnostní zájmy a přispěla k mezinárodní stabilitě. (Bezpečnostní strategie České republiky, 2003)

4.2 Bezpečnostní zájmy ČR

Jsou klasifikovány dle jejich významu a důležitosti. Jsou rozděleny do tří kategorií, a to životní, strategické a další významné.

Životní zájmy

Cílem je zajištění suverénnosti, územní integrity, politické nezávislosti a dodržování prvků demokratického právního státu, včetně ochrany základních lidských práv a svobod občanů. Vláda a veřejné orgány mají povinnost chránit životní zájmy státu a jeho občanů, a jsou připraveny využít všech legitimních prostředků a zdrojů k tomuto účelu. (Bezpečnostní politika, 2023)

Strategické zájmy

Podpora strategických zájmů má za cíl chránit životní zájmy a zároveň podpořit společenský rozvoj a prosperitu ČR. Pro dosažení těchto cílů jsou zvoleny přístupy a prostředky odpovídající dané situaci. Strategickými zájmy pro ČR mohou být například (Bezpečnostní strategie České republiky, 2003):

- Bezpečnost a stabilita, především v euroatlantickém prostoru.
- Aktivity zaměřené na zabránění a řešení místních a regionálních konfliktů a minimalizování jejich dopadů.
- Posilování spolupráce, rozvíjení strategického partnerství a rozvoj obranných a bezpečnostních schopností s NATO a EU.
- Utužování důvěry a bezpečnosti v rámci OBSE, stejně jako i prevence proti ozbrojeným konfliktům a podpora demokracie a lidských práv.
- Zajištění ekonomické, vnitřní, energetické, surovinové a potravinové bezpečnosti.

- Rozvoj regionální spolupráce a podpora mezinárodní stability, demokracie a základních svobod a principů právního státu.

Další významné zájmy

Cílem podporování dalších důležitých zájmů je poskytnutí ochrany životních a strategických zájmů a zvýšit odolnost společnosti vůči bezpečnostním rizikům. Můžeme sem zařadit například (Bezpečnostní strategie České republiky, 2009-2023):

- Snižování kriminality, potlačování extremismu.
- Zlepšování zpravodajské ochrany.
- Rozvoj efektivity a profesionality soudnictví a státních institucí.
- Vylepšování nevládních organizací a občanských sdružení zabývajících se bezpečností a zvýšení informovanosti obyvatelstva a jejich zapojení.
- Inovace při zpracování a přenosu utajovaných informací, obzvláště v oblasti ochrany a dostupnosti.

4.3 Bezpečnostní hrozby

Na základě analýzy bezpečnostního prostředí, v němž se ČR nachází, je možné identifikovat konkrétní hrozby. ČR, jako odpovědný člen mezinárodních organizací, zahrnuje mezi relevantní bezpečnostní hrozby i ty, které nemají přímý dopad na její bezpečnost, ale mohou ohrozit spojence.

Terorismus

Neustálá hrozba terorismu jako prostředku násilného prosazování politických cílů přetrvává. Významným prvkem této hrozby je přítomnost nadnárodních sítí, které spojují skupiny i jednotlivce. Tyto sítě jsou schopné přímo ohrozit lidské životy, zdraví a životní prostředí, stejně jako kritickou infrastrukturu. (Bezpečnostní strategie České republiky, 2009-2023)

Šíření zbraní hromadného ničení

Existují státní i nestátní subjekty, které se snaží získat zbraně hromadného ničení. Šíření těchto prostředků může mít závažné dopady na bezpečnost v euroatlantickém prostoru. Zvláštní hrozbou je použití balistických řízených střel a střel s plochou dráhou letu, které mohou nést konvenční nebo nekonvenční nálože. (Bezpečnostní strategie České republiky, 2009-2023)

Kybernetické útoky

Kybernetický prostor je velmi specifický, jelikož nemá geografickou hranici, díky tomu mohou státní i nestátní aktéři poškodit strategické a významné zájmy ČR bez použití konvenčních prostředků. Počet a sofistikovanost kybernetických útoků na veřejnou i soukromou sféru neustále roste. Tyto útoky mohou vést k selhání komunikačních, energetických a dopravních sítí, průmyslových nebo finančních systémů a způsobit významné materiální škody. (Bezpečnostní strategie České republiky, 2009-2023)

Extremismus a nárůst interetnického a sociálního napětí

Existence opuštěných oblastí a sociálně marginalizovaných skupin přispívá k vzniku prostředí, které podporuje kriminalitu a vyvolává napětí mezi různými etnickými a sociálními skupinami. Tyto problémy jsou často využívány extremistickými organizacemi. (Bezpečnostní strategie České republiky, 2009-2023)

Organizovaný zločin

Organizovaný zločin, především prostřednictvím těžké hospodářské a finanční kriminality, korupce, obchodování s lidmi a drogové kriminality, je stále větší hrozbou. Tyto kriminální sítě často překračují hranice států a jsou schopny narušovat instituce, ale i hodnoty právního státu, infiltrovat orgány státní správy a ohrožovat bezpečnost občanů. (Bezpečnostní strategie České republiky, 2009-2023)

Ohrožení kritické infrastruktury

Kritická infrastruktura je klíčový systém prvků, jejichž porušení nebo nefunkčnost by vážně ohrozila bezpečnost státu, zabezpečení základních potřeb obyvatelstva nebo hospodářství státu. Kvůli silnému propojení jednotlivých odvětví může být kritická infrastruktura ohrožena hrozbami různého charakteru. To může zahrnovat manipulaci s dodávkami strategických surovin z politických důvodů, vstup cizího kapitálu s rizikovým původem a cíli do kritické infrastruktury v ČR, sabotáže, kybernetické útoky nebo hospodářskou kriminalitu. (Bezpečnostní strategie České republiky, 2009-2023)

4.4 Institucionální a ekonomický rámec zajištění bezpečnosti

Instituce, které se starají o bezpečnost

Aby stát mohl zajistit svou bezpečnostní politiku, využívá institucionální nástroje, z nichž nejdůležitějším je bezpečnostní systém. Ten integruje, koordinuje a řídí jednotlivé složky,

aby pružně reagoval na vznikající hrozby. Hlavním nástrojem obranné politiky jsou ozbrojené síly, zejména Armáda ČR. Kromě toho existují i další instituce státní správy, samosprávy a právnické a fyzické osoby, které patří mezi nástroje obranné politiky. ČR systematicky pracuje na koordinaci svých obranných nástrojů jak na národní, tak mezinárodní úrovni. (Bezpečnostní strategie České republiky, 2009-2023)

Při zajišťování vnitřní bezpečnosti a ochrany obyvatelstva zaujímají klíčové místo bezpečnostní sbory, především Policie ČR a Hasičský záchranný sbor ČR. V případě, že síly Policie ČR a integrovaného záchranného systému nejsou dostatečné, může být využita i Armáda ČR s jejími silami a prostředky. Tyto bezpečnostní sbory hrají důležitou úlohu při zajišťování vnitřní bezpečnosti a ochraně obyvatelstva, společně pracují na minimalizaci rizik a zajištění bezpečnosti. (Bezpečnostní strategie České republiky, 2009-2023)

Národní bezpečnostní úřad je klíčovým hráčem v oblasti kybernetické bezpečnosti, zodpovědným za řešení této problematiky a funguje jako národní autorita v této oblasti. Jeho hlavním úkolem je účinně předcházet, řešit kybernetické útoky a přijímat nezbytná opatření. (Bezpečnostní strategie České republiky, 2009-2023)

Ekonomický rámec

Hospodářská politika hraje významnou roli při zajišťování bezpečnosti a obrany ČR, a to prostřednictvím vytváření vhodných podmínek. Příznivé ekonomické a právní prostředí spolu s makroekonomickou stabilitou jsou klíčovými faktory pro získávání lidských, materiálních a finančních zdrojů, které jsou nezbytné pro zajištění bezpečnosti a obrany státu. Zdrojem jsou převážně veřejné rozpočty s důslednou fiskální konsolidací.

Jako opatření vedoucí k udržení hospodářského růstu a příznivých ekonomických podmínek slouží například (Bezpečnostní strategie České republiky, 2009-2023):

- Podpora inovací, výzkumu a vývoje k posílení konkurenceschopnosti ČR
- Prevence možného zneužití tržního postavení ekonomickými subjekty
- Optimalizace ochranných mechanismů
- Minimalizace dopadů negativních jevů
- Eliminace mezinárodních arbitráží vůči ČR
- Omezení závislosti na nestabilních zemích

- Zajišťování bezpečného kyberprostoru a ochrana informační a komunikační infrastruktury.

4.5 Strategie prevence hrozeb

Mezi hlavní priority v oblasti boje proti terorismu patří přijímání opatření zaměřených na zabránění financování teroristických aktivit, prevenci radikalizace a rekrutování, a zajištění ochrany obyvatelstva a klíčových infrastruktur, které mohou být potenciálně napadeny teroristickými skupinami. ČR v rámci NATO aktivně podporuje boj proti terorismu prostřednictvím sdílení zpravodajských informací, rozvoje odpovídajících schopností, intenzivnější spolupráce s ostatními partnery a aktivní účasti v aliančních operacích a misích. (Bezpečnostní strategie České republiky, 2009-2023)

ČR aktivně pracuje na prohlubování a efektivnějším provádění procesů a mechanismů odzbrojení, kontroly zbrojení a nešíření zbraní hromadného ničení a jejich nosičů. S ohledem na novou Strategickou koncepci NATO a opatření směřující k posílení článku 5 Washingtonské smlouvy podporuje aktivně rozvoj a budování územní protiraketové obrany NATO a zkoumá možnosti konkrétního zapojení do tohoto systému. Dále se zaměřuje na rozvoj schopností v boji proti hrozbě chemických, biologických, radiologických a jaderných zbraní hromadného ničení. V souladu se sdílením společných rizik a odpovědnosti v NATO, ČR nadále specializuje své ozbrojené síly v oblasti ochrany proti zbraním hromadného ničení. ČR plně podporuje všechny ustanovení Smlouvy o nešíření jaderných zbraní, včetně článku VI, který vyzývá k uzavření smlouvy o všeobecném a úplném jaderném odzbrojení za přísných a efektivních mezinárodních kontrol. Avšak úplná eliminace jaderných zbraní je cílem dlouhodobým a vyžaduje splnění mnoha podmínek, zejména v oblasti nešíření. V oblasti mírového využití jaderné energie, ČR aktivně podporuje aktivity Mezinárodní agentury pro atomovou energii, směřující k posílení jejího systému záruk. (Bezpečnostní strategie České republiky, 2009-2023)

Bezpečnost kritické informační infrastruktury a významných informačních systémů je pro vládu prioritou vzhledem k neustále rostoucímu ohrožení kybernetickými útoky, proto je zřízeno vládní koordinační místo, které umožňuje okamžitou reakci na kybernetické bezpečnostní incidenty. ČR podporuje budování systémů, které umožňují spolupráci všech aktérů a výměnu zkušeností při řešení kybernetických incidentů. Při budování systémů pružné odolnosti je kladen důraz na minimalizaci dopadů kybernetického útoku a rychlé navrácení systému do funkčního stavu. (Bezpečnostní strategie České republiky, 2009-2023)

Vláda se zaměřuje na boj proti korupci, daňovým únikům a závažné hospodářské kriminalitě, které jsou klíčovými faktory pro průnik organizovaného zločinu do veřejné sféry a ohrožují hospodářskou soutěž a zásady demokratického uspořádání. (Bezpečnostní strategie České republiky, 2009-2023)

4.6 Strategie ČR pro boj proti terorismu

Strategie České republiky v boji proti terorismu, navazující na předešlou strategii z období 2010-2012, je založena na principu "Bezpečnostní strategie České republiky" (Bezpečnostní strategie České republiky, 2015) a byla naposledy aktualizována v roce 2013. Tato strategie se zaměřuje na zásadní prvky boje proti terorismu v rámci České republiky a na identifikaci klíčových oblastí, které jsou s touto problematikou úzce spojeny. Zároveň upozorňuje na aktuální nedostatky v bezpečnostním systému ČR, které je třeba řešit.

Hlavními body strategie je spolupráce, ochrana, výzkum, prevence a legislativa (Bezpečnostní strategie České republiky, 2015).

- Strategie zdůrazňuje význam úzké **spolupráce** mezi různými subjekty jak na národní, tak mezinárodní úrovni.
- Prioritou je **ochrana obyvatelstva a kritické infrastruktury** před teroristickými hrozbami a útoky. To zahrnuje opatření pro zvýšení bezpečnosti veřejných míst a klíčových objektů.
- Strategie klade důraz na podporu **výzkumu a vývoje** v oblasti bezpečnosti, který je klíčový pro inovace v metodách boje proti terorismu.
- Část strategie je věnována prevenci radikalizace a následného rekrutování jednotlivců do teroristických skupin.
- Strategie zahrnuje také posouzení právního rámce týkajícího se terorismu a navrhuje případné změny, aby byl systém co nejefektivnější a přizpůsobitelný rychlému vývoji teroristických taktik a technologií.

Strategie uznává, že metody boje proti terorismu se neustále vyvíjejí, proto je důležité, aby strategické dokumenty byly dynamicky upravovány a bylo díky nim možné rychle a flexibilně reagovat na vývoj v oblasti terorismu. (Strategie České republiky pro boj proti terorismu**,** 2013)

5 MĚKKÝ CÍL

Definice vycházející z institucí zabývajících se bezpečností zní: "Měkký cíl je termín, který používáme pro objekty, prostory nebo události, které jsou často navštěvovány větším počtem osob a zároveň mají nedostatečnou nebo minimální úroveň bezpečnostního zabezpečení proti násilným útokům." (Koncepce ochrany měkkých cílů pro 2017-2020, 2018)

Další definice, kterou lze nalézt v strategických dokumentech, zní: "Měkkými cíli jsou označována místa s vysokou koncentrací lidí a s nízkou úrovní zabezpečení proti násilným útokům, která jsou vybírána jako cíle pro takovéto útoky, typicky teroristické útoky, kvůli své charakteristice, která spočívá v otevřenosti a nedostatečné obraně, kterou je snadné překonat při vnějším útoku." (Metodika základy ochrany měkkých cílů, 2018)

Z těchto definic vyplývá, že měkké cíle jsou místem, kde se běžní lidé volně pohybují, a mají nízkou úroveň zabezpečení, což je činí atraktivními pro potenciální teroristické útoky.

Měkké cíle můžeme dělit podle více kritérií, jedním z těchto kritérií je rozdělení měkkých cílů na trvalé a dočasné. Trvalé měkké cíle lze dále rozdělit na venkovní prostory (stadiony, sportovní komplexy, tržiště) a vnitřní prostory (nemocnice, kina). Mezi dočasné měkké cíle patří shromáždění, venkovní akce s placeným nebo volným vstupem (festivaly, demonstrace, trhy). (Koncepce ochrany měkkých cílů pro 2017-2020, 2018)

Další možné dělení měkkých cílů je z hlediska zdroje nebezpečí (Koncepce ochrany měkkých cílů pro 2017-2020, 2018):

- Ohrožení samotným aktivním útočníkem bez ohledu na motivaci
- Ohrožení teroristickou skupinou
- Ohrožení jinou specifickou skupinou

Tato koncepce také popisuje faktory zvyšující atraktivitu daného cíle pro útočníky. Patří sem otevřenost pro veřejnost, symboličnost cíle, přítomnost médií, Policie ČR a kvalita bezpečnostního personálu. (Koncepce ochrany měkkých cílů pro 2017-2020, 2018)

5.1 Koncepce ochrany měkkých cílů

Koncept ochrany měkkých cílů vychází z úkolu, který byl stanoven na základě Usnesení vlády č. 711 ze dne 27. července 2016 v rámci Protiteroristického balíčku. Tato koncepce se celistvě zaobírá otázkami spojenými s měkkými cíli a poskytuje základy pro zavedení funkčního systému jejich ochrany. (Koncepce ochrany měkkých cílů pro 2017-2020, 2018)

I když v době, kdy byla tato koncepce vypracována, v České republice nebyl nikdo odsouzen za teroristický čin, nyní máme příklad jednoho občana, který byl odsouzen za teroristický útok a za hrozbu teroristickým útokem. Tato koncepce byla vyvinuta s ohledem na prevenci potenciálních teroristických útoků, což bylo způsobeno zvýšeným rizikem terorismu v Evropě, včetně důsledků migrační krize. (Koncepce ochrany měkkých cílů pro 2017-2020, 2018)

Cílem Koncepce ochrany měkkých cílů je vytvoření komplexního národního systému. Tento systém umožňuje efektivní, integrovanou a rychlou reakci na hrozby vůči měkkým cílům. Díky tomu je možné předejít nejen ztrátám na lidských životech, ale také ekonomickým ztrátám. (Koncepce ochrany měkkých cílů pro 2017-2020, 2018)

Principy ochrany měkkých cílů

Z Koncepce ochrany měkkých cílů vyplývá, že máme čtyři základní principy, jimiž je bezpečnost měkkého cíle, proaktivní přístup, spolupráce, kooperace, nastavení komunikačních spolu s koordinační činností. (Koncepce ochrany měkkých cílů pro 2017-2020, 2018).

- **Bezpečnost měkkého cíle je věcí všech dotčených subjektů:** Bezpečnost měkkých cílů není pouze povinností státu, ale společným zájmem všech zúčastněných subjektů, včetně vlastníků a provozovatelů.
- **Proaktivní přístup:** Čekání na násilné útoky není efektivní. Musíme systematicky a dlouhodobě pracovat na jejich předcházení a připravenosti.
- **Spolupráce a kooperace:** Úspěšné řešení krizových situací vyžaduje úzkou spolupráci mezi měkkým cílem, bezpečnostními složkami a okolními subjekty.
- **Komunikační procesy a organizace a koordinace činností**: Zvýšení odolnosti měkkých cílů často závisí na správném nastavení komunikačních procesů, organizaci práce a připravenosti personálu na mimořádné události.

Pro dosažení účinných opatření v této oblasti je nevyhnutelná úzká spolupráce s řadou soukromých subjektů a jejich sdílená odpovědnost. Evropská unie a další orgány zdůrazňují potřebu uplatňovat koncept "veřejně-soukromého partnerství". V tomto směru má Česká republika zlepšovací potenciál. (Koncepce ochrany měkkých cílů pro 2017-2020, 2018)

Zásadní je si uvědomit, že ochrana měkkých cílů je pro ně samotné klíčová, neboť spočívá v jejich vlastním zájmu. Je však důležité si uvědomit, že rozsah potenciálních měkkých cílů,

které by mohly být terčem závažných násilných útoků, je tak obrovský, že stát nemá dostatečné kapacity na jejich fyzické zabezpečení, a to ani ve velkém rozsahu. Jediným směrem k efektivnímu zvýšení bezpečnosti měkkých cílů obecně je spolupráce a spoluodpovědnost veřejného a soukromého sektoru. (Koncepce ochrany měkkých cílů pro 2017-2020, 2018)

5.2 Základy ochrany měkkých cílů

Dokument s názvem "Základy ochrany měkkých cílů" představuje metodiku, která je navržena s cílem chránit fyzické osoby, zejména jednotlivce, před vážnými násilnými útoky. Tato metodika je vypracována tak, aby byla použitelná pro útoky provedené různými subjekty, včetně teroristů, násilných extremistů, osob s kriminálními sklony, a dokonce i lidí, kteří útočí z osobních důvodů nebo kvůli duševním poruchám. (Metodika základy ochrany měkkých cílů, 2018)

Hlavním záměrem této metodiky je především prevence útoků namířených proti měkkým cílům a minimalizace jejich následků. Bezpečnostní opatření, která jsou v tomto dokumentu uvedena, jsou prezentována jako doporučení pro provozovatele a vlastníky měkkých cílů. Tato doporučení jsou formulována tak, aby byla jejich implementace dobrovolná a v souladu s právními předpisy České republiky. (Metodika základy ochrany měkkých cílů, 2018)

Tato metodika také povzbuzuje provozovatele měkkých cílů k tomu, aby vytvořili své vlastní postupy a pravidla pro zvládání mimořádných situací různého rozsahu v prostředích, které spravují. Tímto způsobem se měkké cíle stávají více připravenými na reakci v případě nečekaných událostí. (Metodika základy ochrany měkkých cílů, 2018)

5.3 Útoky na měkké cíle

Od roku 1998 do současnosti se nejčastěji objevují útoky sebevražedných aktivních útočníků na veřejných místech, kteří používají ruční zbraně. Tento způsob útoku se ukazuje jako efektivní v počtu obětí, než dříve oblíbené výbušniny a improvizované nástražné výbušné systémy, přestože jejich příprava je relativně snadná. Rovněž jsou stále častější mnohonásobné současné útoky, jak se stalo nedávno v Paříži a Bruselu. Tyto útoky vyžadují vyšší úsilí a prostředky, ale také lepší koordinaci bezpečnostních složek, komunikaci s "měkkými" cíli a rychlé varování obyvatelstva. (Koncepce ochrany měkkých cílů pro 2017-2020, 2018)

V nedávné době jsme byli svědky nárůstu útoků typu "car-ram", což znamená nájezd automobilu do většího počtu osob, příkladem podobných situací jsou události v Nice a Berlíně v roce 2016. Tato forma útoku se ukázala jako mimořádně efektivní, pokud jde o počet obětí, v porovnání s útoky střelnými zbraněmi. Navíc, v porovnání s útoky střelnými zbraněmi, je útok vozidlem mnohem rychlejší. Tuto informaci získáváme z analýzy teroristických útoků v Evropě prováděné Soft Targets Protection Institute v roce 2017 a metodiky ochrany "měkkých" cílů z roku 2016. (Koncepce ochrany měkkých cílů pro 2017-2020, 2018)

Útoky na měkké cíle nejsou výjimkou ani v České republice, což dokládají incidenty jako útok ve škole ve Žďáru nad Sázavou nebo útok v restauraci v Uherském Brodě, byť nešlo o teroristické činy. Přesto, pokud by k takovému incidentu došlo na českém území, lze s velkou pravděpodobností předpokládat, že měkké cíle by mohly být terčem teroristického útoku, stejně jako to vidíme ve světě. (Koncepce ochrany měkkých cílů pro 2017-2020, 2018)

6 SYSTÉM OCHRANY MĚKKÝCH CÍLŮ V ČR

V současné době si Česká republika uvědomuje důležitost ochrany měkkých cílů a neustále pracuje na jejím vylepšení. Danou problematikou se zabývalo již mnoho odborníků z řad akademické sféry i praxe. Existuje již několik dokumentů, jako například Strategie České republiky pro boj proti terorismu, Audit národní bezpečnosti z roku 2016 a vláda také schválila Protiteroristický balíček, kde je ochrana měkkých cílů jako jedna z priorit. Nesmíme opomenout také Hasičský záchranný sbor, který pohlíží na ochranu měkkých cílů komplexně z pohledu ochrany obyvatelstva a zpracoval dokument Koncepce ochrany obyvatelstva. (Koncepce ochrany měkkých cílů pro 2017-2020, 2018)

Na přelomu roku 2016 a 2017 byla publikována česká technická norma ČSN 73 4400, která se zabývá problematikou Prevence kriminality - řízení bezpečnosti při plánování, realizaci a užívání škol a školských zařízení. Ministerstvo vnitra vytvořilo metodiku nazvanou „Základy ochrany měkkých cílů," která je volně dostupná ke stažení na jejich webových stránkách. Tato metodika je nezaměřena na obvyklou ochranu majetku jednotlivců a organizací. Současně se zaměřuje na ochranu před závažnými násilnými útoky, a to zejména na ochranu samotných fyzických osob. (Koncepce ochrany měkkých cílů pro 2017-2020, 2018)

Tato metodika je široce uplatnitelná v rámci různých subjektů, které mohou být vystaveny různým druhům útoků. Využitelná je pro ochranu proti teroristům, násilným extrémistům, jednotlivcům s čistě kriminální motivací, a dokonce i proti lidem, kteří mohou útočit z osobních důvodů, kterými mohou být bývalí zaměstnanci či jedinci s duševními problémy. (Koncepce ochrany měkkých cílů pro 2017-2020, 2018)

Tato metodika klade důraz na zásadní principy, které lze aplikovat na různé typy organizací, včetně firem, škol, neziskových organizací, veřejných institucí nebo rodiny. Je vhodná pro ochranu soukromých i komerčních budov a různé společenské události. (Koncepce ochrany měkkých cílů pro 2017-2020, 2018)

Cílem metodiky je preventivní přínos a omezení dopadů, jelikož je vyčleněno málo finančních prostředků na přímou obranu měkkých cílů. Samotný zásah proti útočníkovi je většinou ponechán na profesionálních státních, městských či výjimečně soukromých bezpečnostních složkách. Pro koordinaci jejich akcí při společných zásazích existují standardy, jako například STČ 09/IZS pro zásahy integrovaných záchranných složek při

mimořádných událostech s velkým počtem zraněných osob nebo STČ 14/IZS pro situace amok-útoků aktivního střelce. (Koncepce ochrany měkkých cílů pro 2017-2020, 2018)

6.1 Hlavní body systému ochrany měkkých cílů

Dle Koncepce ochrany měkkých cílů jsou čtyři hlavní body v tomto systému. Jedná se o metodické vzdělávání a vedení, u něhož jde o zaměření se na analýzu hrozeb pro daný měkký cíl, detekci podezřelého chování a plánování reakce na útok, způsob komunikace a podobně. Toto vedení je pod záštitou Ministerstva vnitra, které má za úkol vytvořit sérii kurzů pro vzdělávání odborné veřejnosti. (Koncepce ochrany měkkých cílů pro 2017-2020, 2018)

Dalším bodem je dotační podpora. Zvýšení zabezpečení vyžaduje finanční prostředky, které jsou přidělovány ministerstvy. (Koncepce ochrany měkkých cílů pro 2017-2020, 2018)

Třetím bodem je komunikace, spolupráce, výměna informací a sdílení praxe. Za tímto účelem bude vytvořen poradní sbor Ministerstva vnitra pro ochranu měkkých cílů, kde bude hlavním cílem sdílení informací a dobré praxe, standardizace bezpečnostních plánů a vytvoření systému zasílání varování o bezpečnostní situaci nebo bezpečnostních incidentech vybraným subjektům. (Koncepce ochrany měkkých cílů pro 2017-2020, 2018)

Posledním bodem je aktivní přístup Policie České republiky, jejíž role spočívá v samotné ochraně měkkého cíle. V případě, že není možné dále kapacitně zvládnout situace je k těmto účelům je přizvána také Armáda ČR. (Koncepce ochrany měkkých cílů pro 2017-2020, 2018)

6.2 Instituce spojené s bojem proti terorismu

V současné době je boj proti terorismu v kompetenci Ministerstva vnitra, Policie ČR a Bezpečnostní informační služby (dále jen BIS). V případech, kdy samotné organizace nejsou schopné zajistit bezpečnost, je navázána spolupráce s Ministerstvem obrany, zdravotnictví a zahraničních věcí. Dále je pro získání informací využíván Úřad pro zahraniční styky a informace a také Vojenské zpravodajství. Po vzniklé bezpečnostní situaci, na návrhy Bezpečnostní rady státu (dále BRS) jsou přijímána nezbytná opatření, která jsou následně vyhodnocována a Vláda ČR spolupracuje s orgány NATO a EU určenými pro boj s terorismem. BRS neustále vyhodnocuje bezpečnostní opatření, v ČR i v zahraničí, spojena s terorismem. Ústřední krizový štáb a Bezpečnostní rady krajů se také podílejí na zajištění bezpečnosti na našem území. (Národní akční plán boje proti terorismu, 2012)

7 DÍLČÍ ZÁVĚR

Teoretická část této diplomové práce je zaměřena na seznámí s problematikou terorismu. Je zmíněna jeho definice, jeho dělení dle použité metody, motivace a původu, psychologické aspekty teroristických útoků a bezpečnostní politika státu.

V kapitole o psychologii terorismu jsou zmíněny motivace útočníků, na které lze navázat tvorbou vhodných opatření a tím snížit hrozbu vzniku teroristického útoku. U bezpečnostní politiky jsou zmíněny i hrozby identifikované státem, strategie jejich prevence a popsána je také strategie boje proti terorismu.

Závěr teoretické části je věnován měkkým cílům. Je zde sepsána definice, co to je měkký cíl, jaké dokumenty se starají o jejich ochranu a zmíněny jsou i některé útoky na měkké cíle. V samotném závěru jsou sepsány hlavní body systému ochrany měkkých cílů a instituce starající se o tuto ochranu.

II. PRAKTICKÁ ČÁST

8 SOUČASNÁ SITUACE

S každým rokem se počet teroristických útoků různého charakteru neúměrně zvyšuje. Od roku 2010 se jich uskutečnilo více než 2000, některé z nich se dotýkali i ČR a bylo nutné zvýšit ochranu bezpečnosti republiky. Mimo to se řada z nich stala přímo v České republice a zapsala se tak do smutné historie českých občanů. Z čísel, které jsou sesbírány agenturami a speciálními skupinami bojující s různými druhy terorismu, je možné vyhodnotit, že od standartních a nejstarších forem terorismu, kterými je střelba či útok bodnou nebo sečnou zbraní, je postupně využíváno efektivnějších útoků pomocí výbušnin či car-ram. Často dochází ke kombinaci různých forem útoku. Možnou malou nadějí a pozitivní zprávou pro společnost by mohl být pokles separatisticky a nacionalisticky motivovaných útoků o 30%, v současnosti se uskutečňují nejvíce útoky levicovou a náboženskou motivací.

9 SWOT ANALÝZA OHROŽENÍ

Jedná se o analýzu silných a slabých stránek, příležitostí a hrozeb zaměřenou na současný stav, schopnost včasného rozpoznání a reakce na vznik krizové situace (dále jen KS) spojené s měkkými cíli. Na této analýze a jejím vyhodnocení se podílelo 5 zaměstnanců kritické infrastruktury, zastupující policii ČR, městskou policii, hasičský záchranný sbor, zdravotnickou záchranou službu a pozici krizového manažera obce s rozšířenou působností. Přínos zaměstnanců spočíval v číselném ohodnocení této analýzy a tedy získání reálnějšího pohledu do problematiky.

Tabulka 1 SWOT analýza ohrožení (vlastní zpracování)

SILNÉ STRÁNKY	SLABÉ STRÁNKY
• Systém kontroly ze strany PČR • Spolupráce IZS • Kontroly zabezpečovacího personálu soukromých prostorů • Systém evakuačních plánů • Zpracována analýza rizik • Kamerový systém	• Nedostatečné obvodové zabezpečení prostoru vyhrazených pro veřejné akce či pro širokou veřejnost • Zabezpečovací security personál bez výcviku • Nedostatečné vybavení security personálu • Nemožnost detekce zbraní na veřejných akcích či komerčních prostor • Nedostatečná ochrana kritických míst • Nedostatek financí a dokumentů k ochraně měkkých cílů
PŘÍLEŽITOSTI	**HROZBY**
• Vzdělávání veřejnosti • Osvěta a prevence • Cvičení jednotek IZS	• Neočekávanost útoku • Nezpracované plány postupu při KS způsobené teroristy

• Vzdělávání pro veřejný sektor • Rozšíření personálu a jeho vybavení • Spolupráce veřejnosti a veřejného sektoru	• Napadení internetové či mobilní sítě • Získání citlivých údajů

Z provedené SWOT analýzy je možné vyhodnotit, že zabezpečení měkkého cíle je komplexní. Za silné stránky je považován systém pravidelných kontrol ze strany PČR, ale i spolupráce celého IZS při vzniklém nebezpečí, rovněž i kontroly zabezpečovacího personálu daného měkkého cíle. Pro prevenci vzniku KS je nezbytné zpracovaní analýzy rizik, evakuační plán a minimálně kamerové zabezpečení objektu.

Naopak za slabé stránky systému se považováno nedostatečné obvodové zabezpečení prostoru, například proti vjezdu vozidel do prostoru, nemožnost detekce zbraní. To by bylo možné zajistit detektoru kovu u vstupu na veřejnou akci či při vstupu do areálu určeného pro širokou veřejnost. Je možné říci, že nedostatečná ochrana měkkých cílů je zapříčiněna nedostatečnou ochranou kritických míst měkkého cíle, nedostatkem financí a dokumentů poskytnutých k lepšímu zabezpečení, tak i vybavením zabezpečovacího personálu a jeho úrovní výcviku.

Příležitostí by mohla být širší možnost vzdělávání veřejnosti, jak postupovat při vzniklé KS, osvětě a prevenci a vzdělávání veřejného sektoru. Pro lepší koordinaci jednotek IZS zasahujících na místě je nezbytná příprava, společný výcvik při modelových situacích. K lepšímu bezpečnostnímu zabezpečení by také mohlo dojít díky posílení počtu osob pracujících v zabezpečovacích security firmách, které jsou najímány v rámci akcí pro dohled nad bezpečností, nepochybně by bylo možné odvrátit některé situace

Za hrozby je možné považovat nepředvídatelnost či nezpracované plány postupu při KS, kdy bohužel dochází k určitým prodlevám při rozhodovacím procesu. V kyberprostoru je ohrožující napadení internetové sítě a získání citlivých údajů, které by mohly být zneužity.

9.1 Číselné ohodnocení SWOT analýzy

Číselné ohodnocení SWOT analýzy nám ukáže, jak na tom v současné době systém je. Každému bodu v předchozí analýze bude přidělena určitá váha (V) a hodnota (H). U váhy

se budou čísla pohybovat v rozmezí od 0 do 1, přičemž jejich výsledný součet musí být právě 1. Hodnota bude vyjádřena pomocí čísel 1 až 5 (silné stránky a příležitosti), popřípadě -1 až -5 (slabé stránky a hrozby). Hodnoty 1 (nespokojenost) až 5 (spokojenost) slouží k vyjádření spokojenosti, zatímco hodnoty -1 (nejnižší nespokojenost) až -5 (nejvyšší nespokojenost) představují míru nespokojenosti. Součin hodnot V a H tvoří výslednou hodnotu (VH).

Tabulka 2 Číselné ohodnocení SWOT analýzy – část A (vlastní zpracování)

SILNÉ STRÁNKY				**SLABÉ STRÁNKY**			
Název	**V**	**H**	**VH**	**Název**	**V**	**H**	**VH**
Systém kontroly ze strany Policie ČR	0,2	4	0,8	Nedostatečné obvodové zabezpečení prostoru vyhrazených pro veřejné akce či pro širokou veřejnost	0,1	-3	-0,3
Spolupráce IZS	0,2	4	0,8	Zabezpečovací security personál bez výcviku	0,2	-4	-0,8
Kontroly zabezpečovacího personálu soukromých prostorů	0,15	2	0,3	Nedostatečné vybavení security personálu	0,2	-4	-0,8
Systém evakuačních plánů	0,2	3	0,6	Nemožnost detekce zbraní na veřejných akcích či komerčních prostorech	0,1	-2	-0,2

Zpracována analýza rizik	0,2	3	0,6	Nedostatečná ochrana kritických míst	0,2	-3	-0,6
Kamerový systém	0,05	2	0,1	Nedostatek financí a dokumentů k ochraně měkkých cílů	0,2	-4	-0,8
CELKEM	**1**		**3,2**	**CELKEM**	**1**		**-3,3**

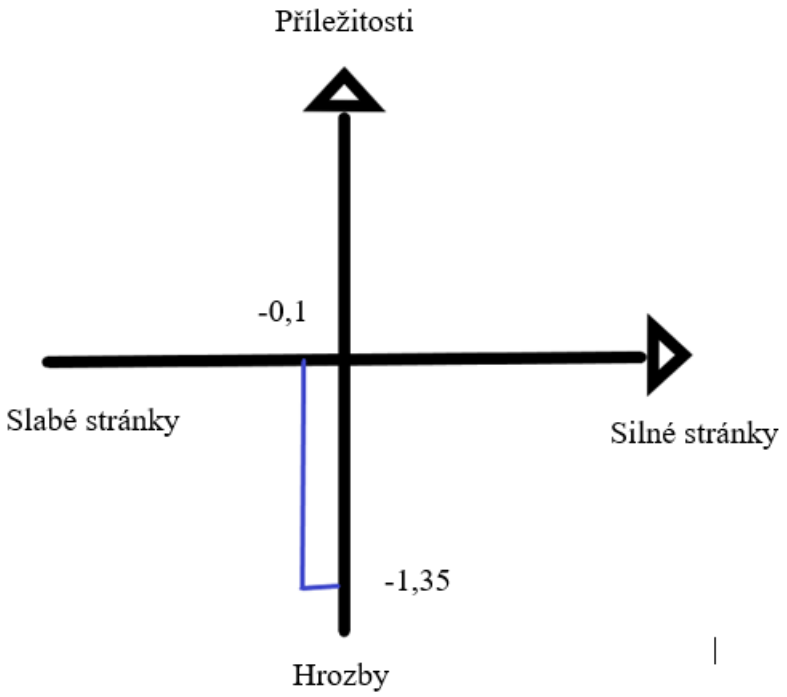
Tabulka 3 Číselné ohodnocení SWOT analýzy – část B (vlastní zpracování)

PŘÍLEŽITOSTI				**HROZBY**			
Název	**V**	**H**	**VH**	**Název**	**V**	**H**	**VH**
Vzdělávání veřejnosti	0,2	2	0,4	Neočekávanost útoku	0,3	-4	-1,2
Osvěta a prevence	0,1	1	0,1	Nezpracované plány postupu při KS způsobených teroristy	0,4	-5	-2
Cvičení jednotek IZS	0,2	4	0,8				
Vzdělávání pro veřejný sektor	0,15	3	0,45	Napadení internetové či mobilní sítě	0,1	-2	-0,2
Rozšíření personálu a jeho vybavení	0,15	2	0,3	Získání citlivých údajů	0,2	-2	-0,4

Spolupráce veřejnosti a veřejného sektoru	0,2	2	0,4				
CELKEM	**1**		**2,45**	**CELKEM**	**1**		**-3,8**
Silné a slabé stránky							**-0,1**
Příležitosti a hrozby							**-1,35**

Číselné ohodnocení provedené SWOT analýzy ozřejmilo, že situace týkající se zabezpečení ochrany měkkých cílů není přívětivá. Systém má mnoho mezer a jejich odstranění by usnadnilo samotný zásah jednotek i předcházení vzniku takových situací. Tuto skutečnost nezmírní ani fakt, že zasahující jednotky jsou podrobeny výcviku, jsou vybaveni kvalitním vybavením a jsou vedeni k efektivní spolupráci.

9.2 Diagram a vyhodnocení



Obrázek 2 Diagram SWOT analýzy (vlastní zpracování)

Výsledná strategie zaznačená v diagramu je defenzivní. Z toho vyplývá, že převažují slabé stránky a hrozby. Je možno zhodnotit, že i přes snahu zasahujících jednotek při výcviku a vzájemné spolupráci nalezneme řadu faktorů, které veškeré úsilí kazí. Dále je možné zhodnotit, že největší pozitiva shledávají členové zapojených složek právě ve výcviku a kooperaci jednotek IZS i provádění kontrol Policií ČR. Kladně jsou hodnoceny možnosti vzdělávání veřejnosti a veřejného sektoru, zpracování analýz rizik a evakuačních plánů. Naopak za slabé stránky je považována absence plánu postupu při KS, neočekávanost útoku a nízká úroveň výcviku případně vzniknutých situací a materiálního zabezpečení zabezpečovacího security personálu. Není možné také opomenout, že nedostatek financí, jednoduché obvodové zabezpečení prostoru a množství dokumentů věnovaných k ochraně měkkých cílů je klíčovým faktorem ovlivňující zvládnutí KS.

10 MODELOVÉ SITUACE

Pro přehlednost budou zpracovány dvě modelové situace, které nastíní problematiku v praxi. Cílem je poskytnout ucelený náhled na skutečnou funkčnost systému a odhalení nedostatků.

Postup jednotek IZS při amoku aktivního střelce v nákupním centru

Každá mimořádná událost počíná prvním ohlášením na tísňovou linku, kdy dojde k aktivaci jednotek IZS. V rámci hovoru má operátor za úkol zjistit prvotní informace, kterými jsou:

- Jméno volajícího
- Příčina jeho hovoru
- Místo konání
- Popis situace
- Naléhavost hovoru

Po získání informací je důležité, aby vyškolený operátor krizového operačního střediska tísňové linky vyhodnotil závažnost situace a zaktivoval potřebné složky IZS. Jeho úkolem je zjistit stav volajícího a v případě zraněných osob na místě, navigovat volajícího k úspěšnému zvládnutí poskytnutí první pomoci.

Jakmile se na místo dostaví policejní hlídka, stává se automaticky velitelem zásahu. Prvním úkolem je zhodnotit vážnost situace a komunikovat s operačním střediskem, aby vyslala další jednotky, případně další členy IZS. Následně je nezbytné vyhodnotit postup v situaci a případně jej komunikovat s operačním střediskem.

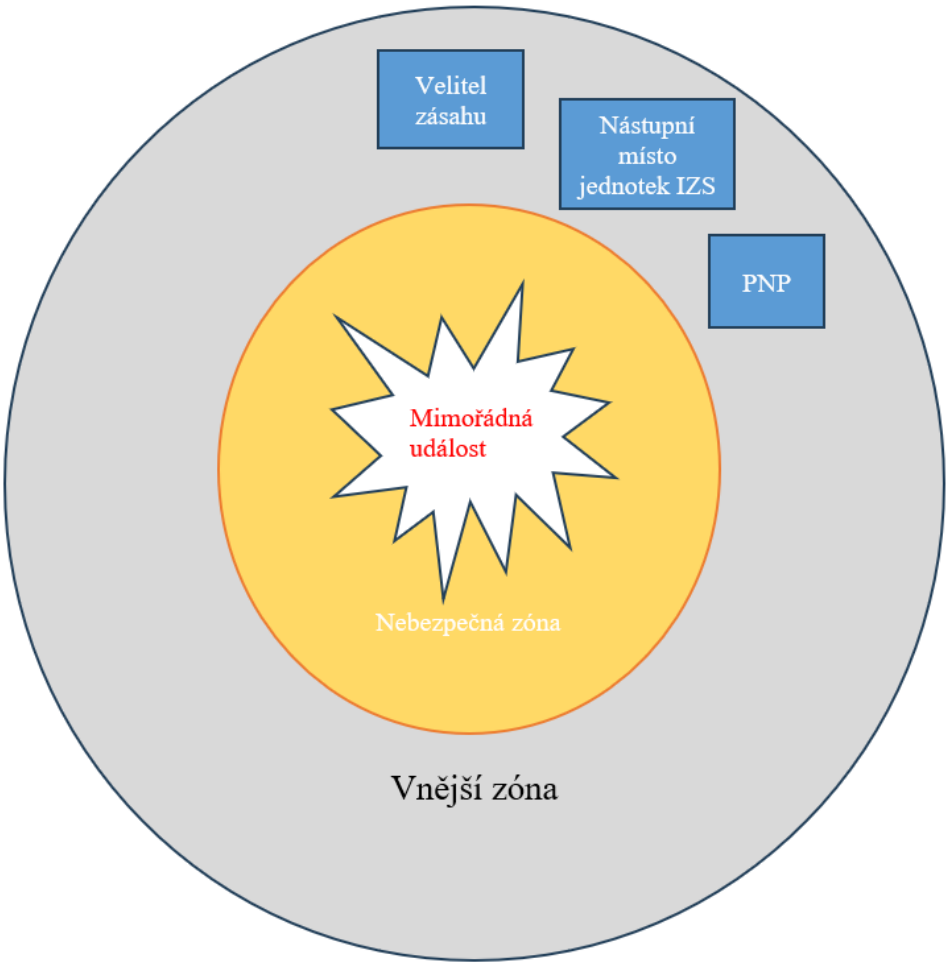
Postup při zásahu je možné rozdělit do několika etap, a to:

- Eliminace aktivního střelce (s možností vyžádání pomoci dalších složek IZS)
- Poskytnutí přednemocniční neodkladné péče
- Záchranné a likvidační práce
- Psychosociální pomoc lidem zasažených mimořádnou událostí
- Předání místa zásahu orgánům činným v trestním řízení

Eliminace aktivního střelce spadá výhradně do kompetence Policie ČR. Postup policistů by měl být proti směru postupu aktivního střelce. Jelikož se předpokládá použití jejich služební zbraně, je nezbytné s ní zacházet velmi obezřetně a dávat pozor, aby nebyli zraněni nebo

zabiti ještě další lidé. Jestliže si policisté vyžádají pomoc dalších složek IZS, jako třeba přistavení výškové plošiny pro odstřelovače, osvětlení místa mimořádné události, do nebezpečné oblasti, jsou jim policisté povinni zajistit bezpečnost. Stejně tak mají jednotky IZS možnost zapůjčení balistické ochrany při vstupu do této zóny. Na taktické úrovni řízení zásahu by měl velitel zásahu úzce spolupracovat se zdravotní záchrannou službou a velitelem hasičského záchranného sboru. Velitel zásahu by měl složkám IZS dávat jasné informace o aktuální bezpečnostní situaci a dalších důležitých okolnostech na místě zásahu.

Dalším úkolem Policie ČR je vyznačit vnější a nebezpečnou zónu. Nebezpečnou zónou se rozumí místo, kde se očekává útok aktivního střelce. Ve vnější zóně, která by měla být dostatečně daleko od nebezpečné zóny, se zřizuje nástupní místo pro přijíždějící složky IZS. Dále se ve vnější zóně zřizuje stanoviště velitele zásahu, stanoviště pro poskytování přednemocniční neodkladné péče, ztotožnění a kontrolu zdravotního stavu evakuovaných osob, poskytnutí psychosociální pomoci. Také by se na přelomu vnější a nebezpečné zóny měl zřídit kontrolní bod pro vstup a bezpečnostní uzávěry.



Obrázek 3 Vytyčení zón (vlastní zpracování)

Zaměstnanci zdravotnické záchranné služby mají na místě za povinnost poskytovat neodkladnou přednemocniční péči, a to ve vnější zóně před eliminací aktivního střelce. Při větším množství postižených osob se dělí do tří skupin (třídící skupina, skupina poskytování přednemocniční péče a skupina odsunu), kdy každá skupina má svého vedoucího. Jestliže je postižená osoba uniklá z nebezpečné zóny schopna komunikovat, mohou jí být během zdravotnického vyšetření položeny otázky k situaci probíhající uvnitř, případně může být požádán o předložení totožnosti.

Městská (obecní) policie může pomoci Policii ČR při eliminaci aktivního střelce, podávání informací o místě zásahu, vytváření zón a organizaci dopravy. Hasičský záchranný sbor je až do eliminace aktivního střelce ve vnější zóně a poskytuje výškovou techniku pro odstřelovače a osvětluje místo zásahu.

Po celou dobu velitel zásahu spolupracuje s integrovaným operačním střediskem, které má údaje o místu posledního známého výskytu útočníka, jejich počtu, popisu, směru postupu a způsobu útoku.

Metodika postupu velitele sil a prostředků Policie ČR

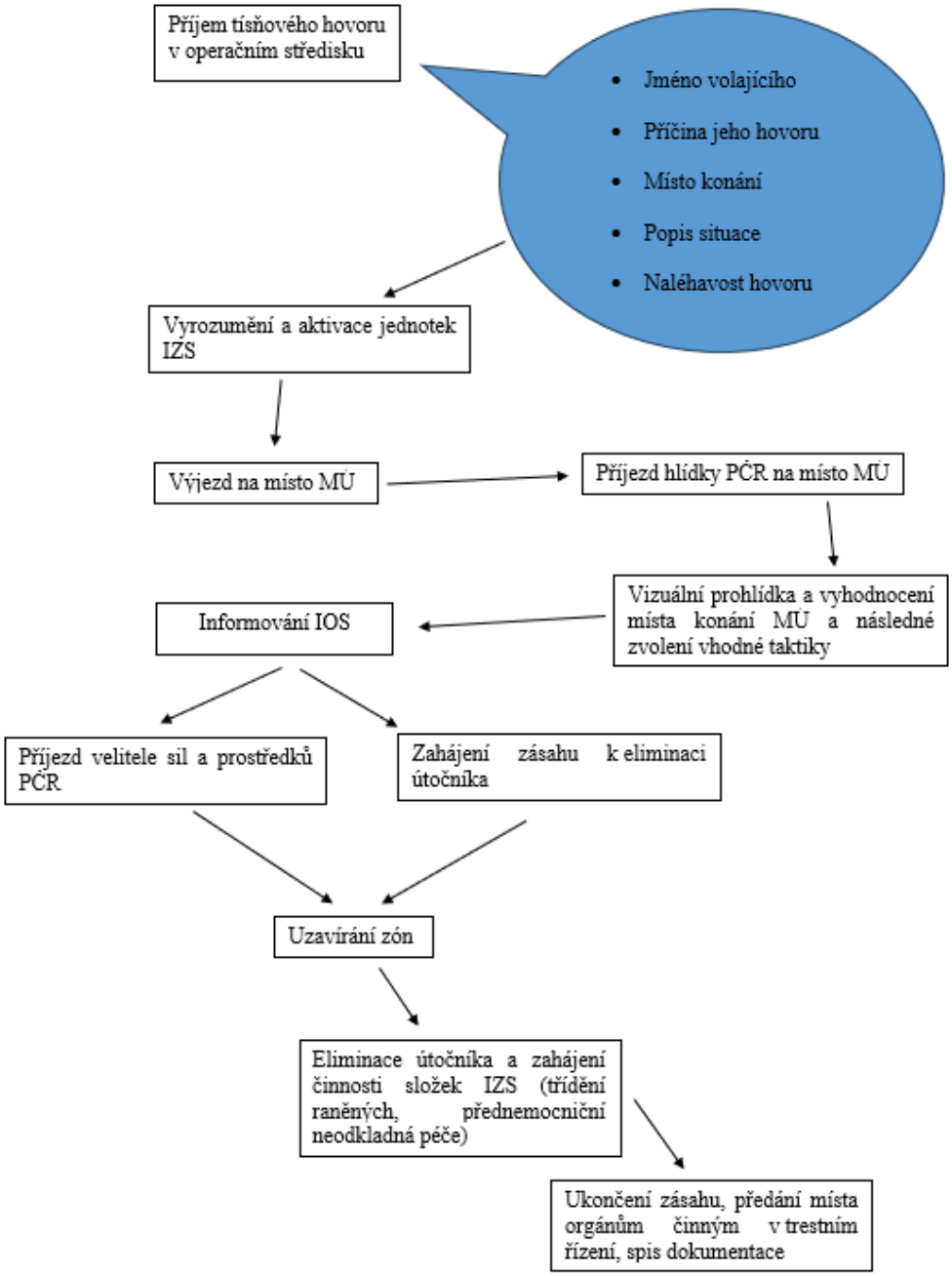
- Po příjezdu na místo vizuálně provádí průzkum, komunikuje s integrovaným operačním střediskem, získává upřesňující informace
- Vydá pokyn k zahájení zákroku
- Pro koordinaci s policisty spolupracujícími při zásahu zřídí radiový kanál
- Řídí prvosledové hlídky dle stanovených taktik, které udávají počet policistů, vykrývání prostorů, kdy střílet, kam posílat ohrožené osoby, jak postupovat a možnost požádat o spolupráci vyjednavače či v případě zřízených barikád zažádat o specialisty
- Získávat informace od integrovaného operačního střediska
- Ověří, že je útočník eliminován a zkontaktuje se s vedoucími a veliteli složek IZS

Metodika postupu velitele zásahu složek IZS:

- Označí se jako velitel zásahu a s veliteli složek IZS provede prohlídku dosavadní vnější a nebezpečné zóny a popřípadě je upraví
- Stanoví místo pro shromažďování a třídění raněných

- Vytvoří z řad policistů a hasičů dvojice, které slouží k transportu raněných do shromaždiště a případně jim poskytnou první pomoc
- Požádá o poskytování psychosociální pomoci obětem i zasahujícím
- V případě velkého počtu obětí zavolá soudního lékaře
- Určí, co zřídit ve vnější zóně
- Vyčká do příjezdu orgánů činných v trestním řízení, předá informace a poskytne pomoc při vyšetřování
- Dohodne se způsob a rozsah informování veřejnosti a médií
- Organizuje odvoz obětí
- Ukončí zásah a předá místo zásahu orgánům činným v trestním řízení

Po ukončení zásahu dojede na místo skupina pracovníků určená k identifikaci obětí, tzv. Disaster Victim Identification (DVI). V závěru je sepsán protokol o zásahu všemi složkami IZS.



Obrázek 4 Logické fáze při zásahu (vlastní zpracování)

Útok car-ram během konání vánočních trhů na náměstí

Car-ram, neboli nájezd vozidlem do osob je v poslední době využíván teroristy vzhledem k jeho rychlosti a účinnosti. Ve většině případů posléze dochází k sebevraždě útočníka.

Tato nebezpečná situace vyžaduje postup jednotek Integrovaného záchranného systému (IZS), který bude zahrnovat několik kroků:

Rychlá odezva: Jakmile je nahlášen útok car-ram, je třeba reagovat co nejrychleji, protože každá sekunda může znamenat rozdíl v ochraně životů.

Ochrana veřejnosti: Prvním cílem je chránit bezpečnost veřejnosti. Pokud je možné, je nezbytné rychle vytvořit bezpečnou zónu kolem místa incidentu a evakuovat ohrožené osoby. Policisté mohou použít zátarasy, bariéry a další prostředky k omezení pohybu vozidel.

Zasahování policií: Policie by měla zasáhnout a pokusit se zastavit útočníka. To může zahrnovat vystřelení na vozidlo, pokus o zastavení vozidla, nebo v nejhorším případě použití střelné síly, pokud je to nezbytné pro ochranu veřejnosti.

Zabezpečení místa činu: Po zastavení útočníka je třeba zajistit místo činu a předejít přístupu k němu. Policisté budou zkoumat vozidlo a provádět další bezpečnostní opatření, jako například prohledávání okolí na případné další hrozby.

První pomoc a záchranářské operace: Zdravotnické jednotky by měly být poslány do postižené oblasti co nejrychleji, aby poskytly první pomoc zraněným. Mohou být také třeba záchranářské operace a evakuace zraněných na bezpečná místa.

Koordinace: Koordinace mezi různými složkami IZS (policie, hasiči, zdravotnický personál atd.) je klíčová. Musí být jasně definovány role a odpovědnosti jednotlivých týmů a zajištěna efektivní a rychlá komunikace.

Vyšetřování: Po zajištění situace je nezbytné zahájit vyšetřování útoku a shromáždit důkazy pro trestní stíhání pachatele.

Psychologická podpora: V takových situacích může být poskytována psychologická podpora jak obětem, tak i záchranářským týmům, které mohou být vystaveny traumatickým událostem.

Zjištění motivace: Po útoku je důležité zjistit motivaci a pozadí pachatele. To může pomoci předejít podobným útokům v budoucnu.

Likvidační práce: Po všech úkonech zasahujících jednotek a zajištění důkazů orgány činnými v trestním řízení musí být provedeny likvidační práce k odstranění následků mimořádné události.

Je třeba poznamenat, že reakce na takový incident je obtížná a vyžaduje spolupráci mezi všemi složkami IZS a dalšími bezpečnostními orgány. Rychlá a koordinovaná reakce je klíčová pro minimalizaci škod a zachování bezpečnosti veřejnosti.

10.1 Zhodnocení současného stavu

V dnešním světě se již potýkáme s terorismem jako s globální hrozbou. Z výše uvedených modelových situací je jednoznačně viditelné, že Česká republika si uvědomuje hrozby a s tím spojená rizika teroristických útoků. Můžeme si povšimnout, že aktuální navržený systém se snaží z předchozích útoků poučit a ze získaných informací předejít a zabránit následujícím útokům. Mezi kladné body současného stavu se může řadit snaha jednotek o plynulou a efektivní spolupráci dosaženou díky společným cvičením. Jisté pozitiva lze shledat také v úrovni vycvičenosti jednotek samotných. Jelikož je každá mimořádná situace jedinečná, nelze se na ně dokonale připravit. Proto je nutné, aby na ně zasahující jednotky dokázaly pružně reagovat. V tom spočívá i největší negativum této problematiky. I přes snahu velitelství nelze sepsat metodické plány pro postup zásahu, a proto se velitelé a jednotlivce musí řídit obecnými postupy, které zpracované jsou a jejich zkušenostmi. Dalším záporným bodem je nenaplněnost stavů jednotlivých složek IZS a jejich vybavení, což je dost limitující ve snaze posunout se dále k úspěšnějšímu detekování útoků, respektive v reakci na již vzniklé mimořádné události. S tím souvisí i nedostatečná finanční podpora ze stran ministerstvem daných složek. Optimální také není spolupráce veřejnosti se zasahujícími jednotkami ať už při příjezdu těchto jednotek na místo mimořádné události, nebo při zásahu samotném. Příčinou tohoto negativa je jednoznačně panika postižených lidí touto mimořádnou událostí a také to, že neprobíhá žádné obecné školení pro veřejnost, jak v dané situaci postupovat. Existuje však několik civilních firem sloužících pro veřejnost, kteří provádí kurzy na dané situace. Většinou v těchto firmách, dle mých zkušeností, pracují bývalí policisté a vojáci, kteří jsou schopni podat věcné rady.

11 OHODNOCENÍ RIZIK POMOCÍ METODY PNH

V této kapitole diplomové práce jsem využil polokvalitativní metodu výzkumu, která zahrnovala řadu rozhovorů se zaměstnanci složek působících při mimořádné události a krizovým manažerem města. Jejich odpovědi jsem analyzoval a zpracoval metodou PNH (Pravděpodobnost-Následky-Hodnotitelé), což mi umožnilo definovat míru rizika. Odpovědi zaměstnanců byly zprůměrovány, aby bylo možné lépe kvantifikovat riziko.

Dalším krokem bylo určení pravděpodobnosti vzniku rizika (P), pravděpodobnost následků (N) a názor hodnotitelů (H), které jsou vyjádřeny hodnotami od 1 do 5. Pravděpodobnost (P) nám umožnila odhadnout, zda daná situace může nastat, a jaká je její pravděpodobnost. Pomocí následků (N) jsme mohli zhodnotit, jak závažné by byly následky dané situace, pokud by se vyskytla. Názor hodnotitelů (H) zahrnuje hodnocení závažnosti a rizika.

Tato kombinace prvků metodiky PNH nám umožnila komplexně analyzovat a vyhodnotit riziko a závažnost situace, kterou jsme zkoumali, s pomocí pohledu a zkušeností již zmíněných zaměstnanců.

Tabulka 4 Pravděpodobnost vzniku daného rizika (vlastní zpracování)

Mizivá	1
Málo pravděpodobná	2
Střední	3
Pravděpodobná	4
Jistá	5

Tabulka 5 Pravděpodobnost následků (vlastní zpracování)

Minimální	1
Nízká	2
Střední	3
Vysoká	4
Zásadní	5

Tabulka 6 Názor hodnotitelů (vlastní zpracování)

Minimální	1
Nízká	2
Střední	3
Vysoká	4
Zásadní	5

Výslednou hodnotu míry rizika (R) získám vynásobením hodnot P, N, H. Tímto součinem lze vyhodnotit závažnost tohoto rizika a dle toho také můžeme určit prioritu přijmutí opatření, aby bylo dané riziko sníženo na přijatelnou hodnotu nebo zcela eliminováno. Maximální hodnotu, kterou můžeme získat, je 125.

Tabulka 7 Stupně míry rizika (vlastní zpracování)

Stupeň rizika	**Hodnota**	**Míra rizika**
I.	>63	Nepřijatelná
II.	43-63	Vysoce ohrožující
III.	25-42	Střední
IV.	10-24	Mírná
V.	<10	Přijatelná

Tabulka 8 Hodnocení rizik (vlastní zpracování)

Riziko	**P**	**N**	**H**	**R**	**Stupeň rizika**
Útok sečnou a bodnou zbraní	4	4	3	48	II.
Útok střelnou zbraní	4	4	4	64	I.
Útok hořlavými látkami	2	3	2	12	IV.
Nastražení výbušnin	3	5	4	60	II.
Útok bombovou vestou	3	5	4	48	II.
Útok chemickými zbraněmi	2	4	2	16	IV.

Útok biologickou zbraní	1	4	1	4	V.
Útok nukleární zbraní	1	4	1	4	V.
Útok dopravním prostředkem	4	4	4	64	I.
Útok na zabezpečení v kyberprostoru	3	4	4	48	II.
Krádež osobních dat v počítačové a mobilní síti	3	3	4	36	III.
Únos	4	4	3	36	III.
Falešné šíření poplašných zpráv	4	2	2	16	IV.
Podstav jednotek IZS	4	3	3	36	III.
Nezkontrolované vybavení na začátku směny	2	3	3	18	IV.
Nehoda při cestě na zásah	1	4	3	12	IV.
Selhání lidského faktoru při akci	3	4	4	48	II.
Závada materiálu při akci	3	4	3	36	III.
Nesprávné vytyčení zón	2	3	2	12	IV.
Nesprávné rozhodnutí velitele	3	3	2	18	IV.
Zničení materiálu při výcviku	4	2	1	8	V.
Zničení výcvikových prostor	2	2	1	4	V.

Na základě zanalyzovaných odpovědí je nyní možné vyhodnotit, která rizika jsou pro společnost přijatelná a která jsou naopak nejvíce ohrožující. Výsledky jsou získané z rozhovoru s lidmi zaměstnanými u bezpečnostních složek, zasahujících při mimořádné události a krizovým manažerem města.

Rizika nepřijatelná

Rizika nepřijatelná by měla být systémem řešena akutně a mělo by co nejdříve dojít k jejich maximálnímu snížení. Mezi tato rizika, po provedené analýze a jejich hodnocení, patří útok střelnou zbraní a útok dopravním prostředkem.

- **Útok střelnou zbraní**

  Útok střelnou zbraní je v minulosti nejvíce používanou formou teroristického útoku. Hlavně v zemích, kde nákup zbraní není přísně hlídán, je velké riziko tohoto typu útoku. To ovšem neznamená, že se to netýká i zemí dalších. Například v ČR, kde je podmínkou pro vlastnictví zbraně mít zbrojní průkaz, což znamená splnit psychologické testy a řadu dalších podmínek, mít zbraň přihlášenou na Policii ČR, se už stalo více útoků tohoto typu. Jde však většinou o ojedinělé útoky, které končí buď sebevraždou pachatele nebo jeho brzkým zadržením.

- **Útok dopravním prostředkem**

  Právě útok dopravním prostředkem vystřídal útok střelnou zbraní na pomyslné první příčce, co se oblíbenosti týče. Do popředí se dostal díky jeho jednoduchosti a efektivnosti. Můžeme sem zařadit auta, letadla, lodě, vlaky. Právě letadlo bylo použito při největším a nejslavnějším teroristickém útoku na světě, tedy 11. září 2001. Navíc není moc možností, jak takovému útoku předejít, jelikož se tento útok používá hlavně na veřejných místech a města nechtějí taková místa obestavovat ploty a různými barikádami. Mnohdy se vyskytuje v kombinaci s bombovým útokem, kdy se výbušnina nachází ve vozidle, což je extrémně ohrožující.

Rizika vysoce ohrožující

Následující skupina rizik rovněž představuje vysokou míru ohrožení a měla by být také řešena velice rychle. Patří sem útok bodnou a sečnou zbraní, nastražení výbušnin, útok bombovou vestou, útok na zabezpečení v kyberprostoru a selhání lidského faktoru.

- **Útok bodnou a sečnou zbraní**

  Útok bodnou a sečnou zbraní se dle hodnotitelů objevuje méně než v minulosti, ovšem jeho následky jsou z hlediska zasažených lidí stále velice vážné. Jedná se o útoky na vybrané osoby nebo ke zranění menších skupin. Převážně je útočník jeden a útok nemá dlouhého trvání.

- **Nastražení výbušnin**

  Jedná se opět o útok, který se v našem prostředí velmi nevyskytuje, jeho následky jsou ovšem zničující. Je velmi účinný, co se týče přímého zranění nebo usmrcení lidí, ovšem při instalaci na správné místo může vyřadit z provozu i důležité budovy nebo

cesty. Také se dá velice lehce uschovat do tašek, kufříků, což snižuje šanci na jeho detekci.

- **Útok bombovou vestou**

  Podobně jako u předchozí formy útoku se jedná o ne příliš využívaný druh teroristického útoku v našem prostředí. Navíc oproti nastražení výbušnin není tak efektivní, co se týče zranění lidí. Většinou se používá při útoku na jeden konkrétní cíl, popřípadě malou skupinku lidí.

- **Útok na zabezpečení v kyberprostoru**

  Digitální prostředí se stává čím dál víc nebezpečným, díky anonymitě útočníka a jeho těžšímu vypátrání. Cílem tohoto útoku se může stát kdokoli, od zabezpečovacího systému státu, firmy, tak i soukromých bezpečnostních agentur. Nejvíce se používá tento útok jako příprava a oslabení nepřítele před útokem hlavním. Může ovšem také sloužit k demonstraci síly útočníka a psychologickému boji s nepřítelem.

- **Selhání lidského faktoru**

  Selhání lidského faktoru je nejvíce ohrožující při zásahu při mimořádné události a může mít zásadní následky. Může tím ohrozit jak sebe, tak i své kolegy. Dochází k tomu díky zanedbání postupu, nedostatečné přípravě, stresu. I z pohledu hodnotících se jedná o zásadní riziko.

Rizika střední

Rizika střední představují rizika, která sice jsou ohrožující, nicméně jejich pravděpodobnost vzniku nebo následky nejsou tak vysoké. Ani tak se ale na tato rizika nesmí opomínat. Patří sem krádež osobních dat v počítačové a mobilní síti, podstav jednotek IZS, závada materiálu při akci a únos.

- **Krádež osobních dat v počítačové a mobilní síti**

  Jedná se o rozvíjející problém současnosti vzhledem k pokroku a vyspělosti v technologiích. Jde o útok na jednotlivé osoby nebo organizace přechovávající osobní údaje, s cílem získání osobních dat, které útočníci využívají k následnému vydírání, obohacení se nebo pod ukradenou identitou vystupují či s ní jinak nakládají.

- **Podstav jednotek IZS**

  Nenaplněnost stavů jednotek IZS je dlouhodobým problémem. I přes snahu státu zabezpečit pro tyto zaměstnance řadu benefitů a jistotu v dobách krize, nedaří se mu nalákat nové zájemce. Naplněnost stavů by zaručila možnost častějšího střídání pohotovostních jednotek, zároveň by se mohla zvýšit četnost výcviků.

- **Závada materiálu při akci**

  I když porouchání správné funkčnosti při akci je věc, se kterou se musí počítat, je to věc, která ohrožuje jak samotné zaměstnance, tak i lidi v ohrožení. Předejít tomuto riziku je velmi obtížné, nikoliv však nereálné. Chce to ovšem lepší výběrové řízení při vybírání výrobce materiálu, což vyžaduje zároveň větší dotační pomoc od státu.

- **Únos**

  Riziko únosu je v naší zemi z pohledu hodnotitelů na nízké úrovni, je to problém hlavně zemí blízkého východu. Metoda únosu se využívá hlavně k možnosti získání finančních prostředků jako výměnu za unesenou osobu.

Rizika mírná

Jsou to rizika, která jsou téměř na přijatelné hodnotě, nemělo by se na ně ovšem zapomínat, aby se systém dotáhl k dokonalosti. Jako mírné riziko se bere útok hořlavými látkami, útok chemickou zbraní, falešné šíření poplašných zpráv, nezkontrolované vybavení na začátku směny, nehoda při cestě na zásah, nesprávné vytyčení zón a nesprávné rozhodnutí velitele.

- **Útok hořlavými látkami**

  Pravděpodobnost útoku hořlavými látkami je malá, její následky však mohou být velké. Tento útok se ovšem moc nevyužívá a převážně se jedná o vandalismus, než o cílený útok.

- **Útok chemickou zbraní**

  Útok chemickou zbraní se používal hlavně za války, v současné době nemá oblibu. Při správném použití by ovšem mohl způsobit zranění velkému počtu osob.

- **Falešné šíření poplašných zpráv**

  Falešné šíření zpráv se c současnosti děje velmi často. Jeho následky ovšem nejsou nijak vážné. Každý si může pravdivost výroku ověřit na několika platformách.

- **Nezkontrolované vybavení na začátku směny**

  Kontrolu vybavení je povinen každý zaměstnanec na začátku směny. Jestli něco zapomene, nebo některé jeho vybavení nebude funkční, spadá všechna odpovědnost na něj samého. Může tím ohrozit nejen sebe, ale i kolegy nebo ohrožené osoby.

- **Nehoda při cestě na zásah**

  Riziko nehody při cestě na zásah je dlouhodobou otázkou a její řešení je pouze v pozornosti ostatních účastníků silničního provozu. Nehody, které způsobí zaměstnanci IZS se stávají velmi zřídka.

- **Nesprávné vytyčení zón**

  Zde velmi záleží na zkušenostech osoby, která vytyčuje nebezpečnou a vnější zónu. Dle počátečního hodnocení nemusí být správně určena. Výhodou ovšem je, že se rozložením zón může kdykoli hýbat. Otázkou ovšem zůstává, jak pružně dokáží reagovat na změnu tohoto rozložení ostatní jednotky, například konkrétně záchranná zdravotnická služba v případě, že už probíhá přednemocniční neodkladné péče.

- **Nesprávné rozhodnutí velitele**

  Nesprávné rozhodnutí velitele je vždy velmi těžké hodnotit. U jednotek se vždy s oblibou říká, že žádné rozhodnutí není špatné. Opět zde záleží jen na zkušenostech a schopnostech dané osoby. Ovšem v případě, že se rozhodne špatně, pozdě nebo nezváží všechna rizika, mohou na to doplatit jeho kolegové.

Rizika přijatelná

Tato rizika už jsou na přijatelné úrovni. Pro fungování systému nepředstavují žádné riziko, nikdy by ovšem ani tyhle rizika neměla být opomíjena. Řadí se sem útok biologickou a nukleární zbraní, zničení materiálu při výcviku a zničení výcvikových prostor.

- **Útok biologickou zbraní**

  Tento typ útoku se řadí mezi rizika přijatelná díky jeho nízké pravděpodobnosti použití, ikdyž jeho následky mohou být dosti zásadní. Při správném použití se dá vyřadit nebo zranit spoustu lidí.

- **Útok nukleární zbraní**

  Podobně jako u předchozího útoku se ani tady nepočítá s jeho použitím. Jeho výroba je pro spoustu teroristických organizací nad jejich možnosti a ani použití není příliš efektivní.

- **Zničení materiálu při výcviku**

  Jev, se kterým se zasahujíc jednotky potýkají velmi pravidelně. Jde však většinou o materiál určený pro výcvikové účely a s jeho poškozením se počítá. Jeho náhrada je také zabezpečena v co nejkratší době.

- **Zničení výcvikových prostor**

  Poškození výcvikových prostor je zcela běžnou věcí, ale výkon ani připravenost jednotek IZS to nijak nenarušuje.

Z celkového hlediska hodnotím připravenost jednotek IZS na zásah při mimořádné události i po vlastní zkušenosti jako velmi dobrou. Lze vidět, že stát si danou hrozbu uvědomuje a klade důraz na obce i organizace, aby dané riziko nepodceňovaly.

Kladně hodnotím snahu státu naplnit stavy jednotek IZS, zlepšovat jejich vybavení, zázemí a úroveň vycvičenosti těchto jednotek. Zároveň vidím velký prostor pro zlepšení v dokumentech zpracovaných pro ochranu měkkých cílů, dotační podpoře od státu, školení veřejnosti a security zabezpečovací dané akce a samozřejmě v oblasti nabírání zaměstnanců do složek IZS. Tyto body jsou ovšem natolik zásadní, že pro systém bylo mělo být prioritou je napravit.

12 PŘIPRAVENOST MĚSTA

Pro zhodnocení skutečného stavu připravenosti města je připraven rozhovor se zaměstnanci policie ČR, městské policie, zdravotnické záchranné služby a krizového manažera daného města. Rozhovor má za cíl zjistit, jestli:

- se město poučilo z proběhlých útoků
- na ně nějakým způsobem reaguje
- probíhá spolupráce jednotek IZS na cvičeních
- by sami rádi něco změnili v celé koncepci ochrany měkkých cílů.

Vybral jsem si malé město na jižní Moravě. Rozhovor obsahuje 16 otázek. Během rozhovoru došlo ke shodě, že město i zaměstnanci jednotlivých složek si přejí zůstat v anonymitě. Celý rozhovor je zpracován a probíhal s ohledem na nemožnost sdílet veškeré dokumenty a vědomosti kvůli ochraně měkkých cílů.

Rozhovor:

Na úvodní otázku, jestli **je dané město po smutné události v Uherském Brodu nějak připraveno na podobnou situaci**, zněla odpověď jednoznačně *„ano“*. Respondenti mi sdělili, že po tragické události byla provedena analýza daného útoku. Po jejím vyhodnocení, s přihlédnutím na rostoucí turistický zájem ve městě a růst počtu obyvatel, začali co nejdříve chystat plány pro prevenci a případný zásah. Po zjištění, že na danou situaci reagovali, jsem pokračoval s dotazem, **zda kontaktovali majitele restaurací a podobných zařízení za účelem zvýšení jejich připravenosti.** Opět odpověděli, že *„ano“*, jenže bez kladné odezvy. Donutilo mne se zamyslet, z jakého důvodu. *„Majitelé si jsou jistí, že se jednalo o ojedinělý případ a věří, že se nebude opakovat.“* Pokračoval jsem dotazem, zda **byly zavedeny nějaké opatření, i přes nesouhlas majitelů.** Bylo mi sděleno, že majitelé těchto zařízení byli seznámeni s možnostmi posílení připravenosti a jsou kdykoli vítáni, kdyby se nakonec rozhodli jinak. Zároveň ale s tím zařadily jednotky IZS několik společných cvičení do svých plánů, aby byly na případný vznik této události připraveni.

Předchozí otázky byly zaměřené na rizika v objektech, rozhovor poté směřoval k rizikům na venkovních akcích, které pořádá město. **Pokud je na území města pořádána akce externími organizacemi či agenturami, je s nimi probírána otázka bezpečnosti a má město dohled nad průběhem?** Na otázku bezpečnosti mi bylo příslušníky policie řečeno, že je snaha ze strany města seznámit pořadatele s možnými riziky, je jim nabídnuta pomoc

ze strany policie ČR i městské policie a také je probíráno, jak by případný zásah probíhal, jaká by byla role policie a pořadatelů a kde si můžou vzájemně pomoci. Oznámili mi, že organizátoři tuhle pomoc vždy rádi uvítají. Dohled nad průběhem akce je vždy samozřejmě podpořen místní policií formou hlídek a kontrol. **Je v rámci akcí pořádaných pro širokou veřejnost vytvořen bezpečností plán?** Odpovědí na tuto otázku bylo, že žádný konkrétní bezpečnostní plán na jednotlivé akce vytvořený není, ale jsou v pohotovosti jednotky IZS a při daných akcích jsou posíleny. Pokračoval jsem otázkou, **jak je tedy zajišťována ochrana osob účastnících se na akcích?** Rozvedla se diskuze na dané téma. V prvé řadě je důležité si uvědomit, že hrozba útoku v našich podmínkách je dosti malá, až mizivá. Jelikož se nejedná o akce, kde by se scházeli lidé s extremistickým myšlením, nejde ani o sportovní utkání, kde se sejdou dva znepřátelené tábory a ani se nejedná o demonstrace, kde se dá očekávat násilný střet, je posilování bezpečnosti zbytečné a mohlo by dokonce působit, pro běžné občany, až přehnaně kontrolované. Pro zajištění bezpečnosti tedy úplně stačí security personál pořadatelů a již zmíněné hlídky ze strany policie. Dalším faktorem je obvodová ochrana pořádaných akcí. Městu a externím organizátorům takových akcí jde hlavně o zachování nenásilné atmosféry, aby nedošlo k odlákání případných zájemců o tuto akci. Dotázaní si ovšem myslí, že tohle je problémem spíše událostí ve větších městech, popřípadě významnějších místech. Tímto jsme ukončili otázky zaměřené na veřejné akce a přesunuli jsme se k otázkám týkajících se hrozby teroristického útoku celkově.

Pokud je vytvořen bezpečnostní plán pro teroristický čin, jaký je postup při vzniku? *„Opět, žádný konkrétní plán pro postup při teroristickém útoku vytvořený není.“* Město vychází z obecných zásad pro postup při takové události a jednotky, které by tak zasahovaly, jsou na ně připravovány formou cvičení. Optal jsem se, **jak tedy vypadá takové cvičení?** Jedná se o komplexní společné cvičení jednotek IZS, jejichž součástí je i výměna zkušeností s jednotkami z jiných měst, a dokonce i zemí. Jsou připraveny různé modelové situace a jednotky si zde zkouší vzájemnou kooperaci a spolupráci. Hledají se optimální řešení a jde hlavně o získání zkušeností jak pro velitele, tak i samotné zasahující jedince. Jelikož se ale nikdy žádná akce neopakuje úplně stejně, jde i o individuální schopnosti pružně reagovat. Pokračoval jsem dotazem, zda **je policie schopna v takovém případě dostatečně a včas zasáhnout?** Bylo mi řečeno, že jelikož se v tomto městě nikdy žádný teroristický útok nestal, je velmi těžké odpovědět. Věří však, že i přes nedostatečný počet policistů jsou schopni zasáhnout. *„Faktem je, že když už se něco stane, policie vše vyřeší rychle a efektivně. Nejde však o žádné komplikované případy, spíše běžné prohřešky našich*

spoluobčanů.“ Na otázku, **jestli se už někdy setkali s jakoukoliv variantou teroristického útoku**, odpověděla většina respondentů *„ne“*, pouze krizový manažer odpověděl, že se stal obětí několika kybernetických útoků. Nejednalo se však nikdy o nic závažného a pokus o útok šlo lehce odhalit. **Jak jste postupoval?** Odpověděl, že jelikož šlo o útok na město, celou událost nahlásil lidem z kybernetické bezpečnosti, odevzdal jim počítač a incident ohlásil i na policii. Zopakoval však, že jelikož rozpoznal, že se jedná o podvodný email, na nic neklikal a tím bylo celé řešení jednodušší. **Myslíte si, že je v daném městě nějaký cíl, který by mohl být pro teroristy zajímavý?** Všichni se shodli, že v současné době ne. Jelikož se jedná o opravdu malé město, nenachází se zde žádný takový objekt. **Jak vnímáte riziko terorismu? Je třeba se ho obávat?** Krizový manažer i zástupci policie si jsou vědomi, že se tato problematika velice rozrůstá. Jsou pravidelně zpracovávány analýzy rizik pro dané město, zkoumány útoky ve světě a hledány různé souvislosti. Opět ale zopakovali, že se na dané situace připravují a věří, že jejich reakce by byla rychlá a funkční. Vzhledem k minulosti si uvědomují, že největší riziko pro ně představuje kybernetický útok. Jako preventivní opatření pro toto riziko jsou najímáni informatici a matematici, kteří se pokoušejí prolomit jejich zabezpečení a město poté na případné prolomení reaguje. **Je policie a Vy, jako krizový manažer, průběžně školen i na tuto problematiku?** *„Ano“*, školení probíhají pravidelně a veškerá data jsou průběžně aktualizována. Zároveň probíhá i sdílení vědomostí s okolními městy v rámci kraje. **Poskytuje město v rámci této problematiky občanům nějaký návod, jak postupovat?** Zde krizový manažer odpověděl, že ne. Je to hlavně díky minimální pravděpodobnosti vzniku jakéhokoli teroristického útoku, ale také, že žádný konkrétní návod neexistuje. Myslí si, že kdyby se lidé cítili nějak dlouhodobě ohrožení, určitě by si na internetu našli nějaké rady, jak postupovat. **Myslíte si, že by v daném městě mohl být nějaký měkký cíl terčem teroristického činu?** V úvahu všem respondentům připadaly pouze přístav, vánoční trhy, kulturní akce pořádané na náměstí města nebo sešlost v rámci kampaně nějakého politika. Za dob pandemie Covid-19 se obávali ohrožení lokální nemocnice, tato obava se však naštěstí nenaplnila.

Na závěrečnou otázku, **pokud byste mohl, změnil byste celkovou koncepci ochrany měkkých cílů**, odpověděl krizový manažer negativně. Současná koncepce je dle něj zpracována dobře, zahrnuje všechny logické základní principy ochrany měkkých cílů a díky složitosti problému je dle něj nesmyslné tuto koncepci více specifikovat a konkretizovat. Donutilo ho se ovšem zamyslet nad nějakým obecným návodem pro občany, jak se v případě nějakého teroristického útoku zachovat. Otázkou však zůstává, zda by se konaly nějaké

přednášky ze strany města pro občany, nebo by byl jen vypracován dokument, do které by všichni obyvatelé mohli kdykoli nahlédnout.

Po rozhovoru se zainteresovanými lidmi a vzájemnou diskusí nad riziky a jejich řešeními jsem nabyl dojmu, že město a příslušní pracovníci si tohle rostoucí globální riziko uvědomují a snaží se na něj efektivně připravovat. Zároveň jde vidět jejich snaha o rozšíření povědomí spoluobčanů v dané problematice. Smysl tohoto by však viděli ve větších městech nebo u měst, kde je velké riziko aktivace této hrozby. Zároveň si jsou ovšem vědomi, že i v poklidném malém městě se jednou může stát neštěstí, které bude mít velké následky, a proto nic nepodceňují. Bylo mi řečeno, že velkým přáním místního zastupitelstva je navázání spolupráce s cizími státy a vzájemně si vyměňovat znalosti a poznatky, provádět cvičení a osvojit si tak další dovednosti. Dalším jejich přáním je, aby se měkké cíle daly zabezpečit bez narušení jejich klidného a přátelského prostředí.

13 NÁVRH OPATŘENÍ

V závěrečné kapitole této diplomové práce jsou navrhnuta opatření, která by měla současný stav připravenosti systému předcházet a schopnost reagovat na mimořádné události související s ochranou měkkých cílů povýšit na vyšší úroveň.

Naplněnost stavů jednotek IZS

Jako nejzásadnější problém je všemi vnímán nedostatek pracovníků u policie ČR, zdravotnické záchranná služby, hasičského záchranného sboru a městské policie. Možným faktorem, proč lidé nechtějí do těchto složek nastoupit, může být stresové prostředí, náročné vstupní podmínky a nízké finanční ohodnocení.

Jako možné způsoby nápravy této situace shledávám v poskytnutí benefitů zaměstnancům od různých firem a společností, ale i státu samotného. Mohlo by se jednat například o navýšení fondu dovolené, příspěvky na dovolenou, kulturu, wellness a sport, ale také příspěvky na osobní a kariérní rozvoj zaměstnanců (škola, kurzy) a také samotné bonusové finanční ohodnocení. Motivační by také mohlo být navýšení finančního ohodnocení po předem stanovených odpracovaných letech.

Zpracování dokumentů pro ochranu měkkých cílů

Neméně důležité pro zlepšení situace je řádné zpracování bezpečnostních dokumentů, na které by mohly zasahující jednotky navázat nějakým cvičením a popřípadě navrhnout různé body pro zlepšení. Spolupráce mezi zasahujícími složkami a úředníky zpracovávajícími tyto dokumenty je velmi důležitá, jelikož musí navzájem vědět, co jsou schopni zabezpečit a v čem budou potřebovat pomoc. Jelikož bývají tyto dokumenty veřejnosti nepřístupné, umožňuje to organizacím se dopodrobna věnovat jednotlivým rizikům.

Dotační podpora od státu

Finanční podpora od státu je důležitou součástí ochrany měkkých cílů a celkového fungování systému. Přispěním většího počtu peněz by mohlo nejen přilákat nové zaměstnance, jak bylo zmíněno výše, ale mohlo by se z toho nakoupit lepší vybavení pro všechny složky, ať už vozy, součástí výzbroje a výstroje, tak i lepší zázemí pro dané složky, a i rozšíření jejich počtu stanic.

Materiální podpora a školení security

Lidé pracující v zabezpečení dané akce nebo objektu jsou mnohdy lidé, kteří se tímto druhem práce neživí. Proto jejich podpora k vystrojení, vyzbrojení a předání důležitých poznatků a zkušeností by mělo být prioritou. Zřízení určité formy školení pro takové lidi pořádané minimálně někým z řad policie a zdravotníků by mělo určitě velký přínos a zvýšily by úroveň zabezpečení. Dalším možným řešením je najímání na zabezpečení organizace, které se na to přímo specializují. Tyto firmy totiž většinou zaměstnávají bývalé policisty a vojáky.

Navýšení počtu security, ochrana vstupu

Zvýšení počtu security pracovníků s dostatečnou úrovní jejich vycvičenosti by určitě pomohlo zvýšit úroveň zabezpečení dané akce nebo vstupu a usnadnilo práci policii. Umožnilo by to hlídat přístupové cesty, skenovat přicházející lidi nebo auta a tím i možnost odhalit potencionální hrozbu. Uvažovat by se také dalo nad určitou formou obvodového zabezpečení prostor (plot, závora, detektor kovů, přístupové karty) posílené o kamerové systémy zaměřené na vstupy a důležitá místa.

Vzdělávání veřejnosti

Proces vzdělávání veřejnosti v oblasti bezpečnosti je důležitá věc, podobně jako je vyznačení únikových cest v případě požáru. Je důležité, aby měl stát nebo obec zpracovaný a volně přístupný dokument, ve kterém by se uvádělo, co dělat, jaký by byl postup a čísla, na které je třeba v případě potřeby zavolat. Zároveň je důležité, aby lidé věděli, že takový dokument existuje a stát se nespoléhal jen na sebevzdělávání občanů.

Také by bylo vhodné, aby stát upozornil obyvatelstvo na globální a lokální hrozby a rizika. Je důležité, aby je dokázal včas varovat co nedělat, jak se zachovat, co vůbec je terorismus a jaké může mít formy. V současné době plné technologií je snadné vypracovat dokument, který by toto všechno obsahoval a pomocí reklam, v médiích a na sociálních sítích upozornil na jeho existenci a předal ho veřejnosti.

Vzdělávání veřejného sektoru

Stejně jako u vzdělávání veřejnosti je důležité, aby se neustále vzdělával i veřejný sektor. Cílem je, aby byl neustále informovaný o současné situaci a vzdělával se v nových trendech terorismu. Zároveň je díky neustálému vzdělávání možnost se na tato rizika připravit.

Spolupráce veřejného sektoru s veřejností

Nakonec je neméně důležité, aby se veřejný sektor propletl s veřejností, protože jedině tak lze považovat připravenost za kompletní. Způsobem, jak dosáhnout spolupráce veřejnosti s veřejným sektorem je pořádání workshopů na veřejných akcích, přednášek a dne otevřených dveří, kde lidé mohou nahlídnout na vybavení a fungování dané instituce.

Cvičení jednotek IZS

Mimo navázání spolupráce s veřejností je důležité, aby uměly spolupracovat jednotky IZS mezi sebou. Efektivní a účinné spolupráce lze dosáhnout pouze opakovaným a usilovným cvičením, proto je důležité, aby se tyto jednotky pravidelně potkávali a cvičili různé modelové situace. Zároveň si mohou mezi sebou vyměňovat poznatky a vědomosti z proběhlých zásahů a stav jejich vybavení. Dalším možným způsobem, jak zlepšit jejich dovednosti je spolupráce s jednotkami ze zahraničí, které se už s nějakou takovou událostí setkaly.

Zabezpečení komunikace

V rámci ochrany měkkých cílů je potřeba zabezpečit všechny dokumenty specifikující tuto problematiku. Jelikož komunikace k vylepšení těchto dokumentů neprobíhá vždy ústně, je třeba zabezpečit elektronickou a telefonní síť, včetně šifrování e-mailové komunikace.

Sociální podpora a prevence

Sociální podpora jako nástroj prevence vzniku terorismu by se neměla opomínat. Můžeme sem zařadit podporu všech náboženství, ras a ekonomických tříd. Lze toho docílit tvořením komunitního ducha pomocí komunitních vzdělávacích programů a veřejných aktivit.

Aktualizace analýzy rizik, využití technologií

Neustálé sledování současných trendů terorismu je nezbytné pro udržení trvalé připravenosti. Je třeba sledovat dění ve světě, proběhlé teroristické útoky a hledání souvislostí. Detailní analýza provedených útoků a analýza současných hrozeb, hledání souvislostí mezi nimi, by měla probíhat pravidelně a detailně.

Díky moderním technologiím je možné sledovat sociální sítě a internet a hledat zde hrozby a znaky radikalizace. Zároveň by se moderní technologie mohly využít k zabezpečení, jako jsou vyjíždějící závory, kamery s detekcí obličeje, které by sloužily k identifikaci známých i neznámých útočníků a blokování útoků v kyberprostoru.

Systémy včasného varování

Systém včasného varování by umožnil zasahujícím jednotkám dojet na místo události rychleji a tím získat čas potřebný pro záchranu co největšího počtu obyvatel. Ideální variantou pro zabezpečení je napojení kamerových systému na jedno centrální pracoviště. Zdejší dispečer by mohl okamžitě zjišťovat informace o události a rychleji kontaktovat jednotky IZS.

13.1 Zhodnocení připravenosti po zavedení opatření

Po zpracovaných návrzích na opatření je pomocí již použité metody PNH zhodnocena míra jejich využitelnosti. Názor hodnotitelů bude opět od zaměstnanců jednotek IZS a krizového manažera města, jejichž jednotlivé názory vyjádřené čísly budou zprůměrovány. Metoda PNH bude pro tyto účely upravena. Hodnotou P bude vyjádřena pravděpodobnost využitelnosti návrhu a bude v rozmezí hodnot od 1 (mizivá) do 5 (velmi pravděpodobné). Míra účinnosti po zavedení opatření na následky (N) bude vyjádřena rovněž hodnotami od 1 (minimální) do 5 (zásadní) a názor na využití od hodnotitelů (H) s hodnotami od 1 (minimálně využitelné) do 5 (trvalé).

Tabulka 9 Pravděpodobnost využitelnosti návrhu (vlastní zpracování)

Mizivá	1
Málo pravděpodobná	2
Střední	3
Pravděpodobná	4
Velmi pravděpodobná	5

Tabulka 10 Pravděpodobnost následků (vlastní zpracování)

Minimální	1
Nízká	2
Střední	3
Vysoká	4
Zásadní	5

Tabulka 11 Názor na využití od hodnotitelů (vlastní zpracování)

Minimálně využitelné	1
Nízké	2
Střední	3
Vysoké	4
Trvalé	5

Pro vyhodnocení efektivnosti navržených opatření vynásobíme faktory P, N, H, čímž získáme výslednou míru využitelnosti opatření R (R=P x N x H). Výsledná míra využití opatření, jejíž maximální hodnota může být 125, nám ukáže možnost implementace navržených opatření za účelem minimalizace rizika.

Tabulka 12 Míra využitelnosti opatření (vlastní zpracování)

Stupeň využitelnosti	**Hodnota**	**Míra využitelnosti opatření**
I.	>63	Nejvyšší využitelnost
II.	43-63	Vysoce využitelné
III.	25-42	Využitelné
IV.	10-24	Málo využitelné
V.	<10	Zanedbatelné

Tabulka 13 Hodnocení využitelnosti návrhů (vlastní zpracování)

Návrh opatření	**P**	**N**	**H**	**R**	**Stupeň využitelnosti**
Naplněnost stavů jednotek IZS	2	4	4	32	III.
Zpracování dokumentů pro ochranu měkkých cílů	3	3	4	36	III.
Dotační podpora od státu	2	4	3	24	IV.
Materiální podpora a školení security	2	3	3	18	IV.

Navýšení počtu security, ochrana vstupu	4	3	3	36	III.
Vzdělávání veřejnosti	5	2	4	40	III.
Vzdělávání veřejného sektoru	5	3	5	75	I.
Spolupráce veřejného sektoru a veřejnosti	4	3	5	60	II.
Cvičení jednotek IZS	4	5	5	100	I.
Zabezpečení komunikace	3	3	3	27	III.
Sociální podpora a prevence	3	2	3	18	IV.
Aktualizace analýzy rizik, využití technologií	4	4	4	64	I.
Systémy včasného varování	3	5	3	45	II.

Zhodnocením využitelnosti návrhů, založeném na subjektivním názoru a zkušenostech zaměstnanců jednotek IZS a krizového manažera, jsme schopni vyselektovat opatření, která dokážou současná rizika snížit a která naopak prospěšná nejsou. Žádné opatření nebylo vyhodnocené jako zanedbatelné, neboli nevyužitelné.

Návrhy s nejvyšší mírou využitelnosti

Návrhy s nejvyšší mírou využitelnosti jsou návrhy, které by měly nejvíce snížit hodnotu rizika. Zároveň by tato opatření měla být lehce aplikovatelná do praxe. Jedná se o vzdělávání veřejného sektoru, cvičení jednotek IZS a aktualizace analýzy rizik společně s využitím technologií.

- **Cvičení jednotek IZS**

  Společné cvičení všech jednotek IZS je i z pohledu hodnotitelů naprosto zásadní pro efektivní řešení všech mimořádných událostí. Je důležité, aby si vzájemně uvědomovali, co je třeba udělat a při zásahu si nepřekáželi. Jednotliví zástupci těchto jednotek pozitivně ocenili návrh na cvičení s kolegy ze zahraničí nebo s kolegy, kteří už zasahovali při teroristickém útoku. Zároveň vidí tuto možnost opatření jako nejvíce účinnou a lehce proveditelnou.

- **Vzdělávání veřejného sektoru**

  Jako další možností, která by měla být snadná pro zavedení do praxe a dle názoru hodnotitelů i velmi účinná je vzdělávání veřejného sektoru. Státní zaměstnanci by měli být znalí současných hrozeb a měli by znát jejich gradaci. Také by si měli uvědomovat, jaký by byl postup v případě řešení KS a jak takovým situacím předcházet. Možnými způsoby, jak docílit této vzdělanosti, je pořádání konferencí a přednášek pro zaměstnance veřejného sektoru.

- **Aktualizace analýzy rizik, využití technologií**

  Provádění pravidelné analýzy rizik a její vyhodnocení by mělo být nedílnou součástí všech lidí starajících se o bezpečnost. Je důležité pochopit současná rizika a efektivně se na ně připravovat. S hodnotiteli jsme se shodli na návrzích opatření s využitím technologie. Spojení policejní databáze s kamerami rozpoznávajícími obličej poskytne výhodu v možnosti sledování známých teroristů. Je ale třeba si uvědomit, že spoléhání se na moderní technologii nestačí, jelikož se může kdykoli porouchat.

Návrhy s vysokou mírou využitelnosti

Návrhy s vysokou mírou využitelnosti mají oproti předchozí skupině menší hodnotu pravděpodobnosti začlenění do praxe, menší vliv na snížení rizika nebo se dle hodnotitelů nevyplatí zavádět. Patří sem spolupráce veřejného sektoru s veřejností a systémy včasného varování.

- **Spolupráce veřejného sektoru a veřejnosti**

  Toto opatření má za cíl připravit obyvatelstvo na případný útok a seznámit je s technikou a postupem jednotek IZS. Návrhy na pořádání workshopů, přednášek a dne otevření dveří všichni zaměstnanci IZS považovali za rozumné a proveditelné. Nemyslí si však, že zájem obyvatelstva by byl natolik velký, aby to vedlo ke zlepšení současné situace. Ze svých zkušeností ale zmiňují, že o tyto akce mají spíše zájem celé rodiny,

- **Systémy včasného varování**

  Díky včasnému varování by se zkrátil čas dojezdu zasahujících jednotek. To by umožnilo záchranu většího počtu postižených lidí. Lidé obsluhující dispečink by uvítali lepší pokrytí kamerovým systém, aby měli větší přehled o situaci a mohli tak zasahujícím jednotkám podat více přesnějších informací.

Návrhy opatření se střední mírou využitelnosti

Následující skupina opatření už dle subjektivního názoru i názoru hodnotitelů nemá vysokou pravděpodobnost využitelnost nebo jeho snížení následků není tak velké. Tato skupina opatření je nejpočetnější. Jedná se o vzdělávání veřejnosti, zpracování dokumentů pro ochranu měkkých cílů, navýšení počtu security a ochrana vstupu, naplněnost stavů jednotek IZS a zabezpečení komunikace.

- **Vzdělávání veřejnosti**

  Vzdělávání veřejnosti je nedílná součást pro navázání spolupráce s veřejným sektorem. Vzdělaná a uvědomělá veřejnost může být nápomocná díky zachování klidné hlavy a správnou reakcí může usnadnit práci zasahujícím jednotkám. Z navrhnutých opatření se krizovému manažerovi zdá jako nejvíce pravděpodobná možnost sepsání dokumentu, který by poskytoval rady občanům, jak postupovat při teroristickém útoku, kam v takovém případě zavolat, co to je terorismus a jaké má formy.

  Při debatě o možnosti rozšíření takového dokumentu mezi obyvatele jsme se shodli, že nejjednodušší a nejúčinnější bude jeho tištěnou formu vyvěsit v prostorech městského úřadu a elektronickou verzi dát na městský web. Informování obyvatelstva o tomto dokumentu by bylo prostřednictvím lokálního zpravodaje, televize a rozhlasu.

- **Zpracování dokumentů pro ochranu měkkých cílů**

  Nejdůležitějším základním kamenem pro lepší zabezpečení měkkých cílů je zpracování dokumentů na tuto ochranu. Ale podle hodnotících je malá pravděpodobnost, že vzniknou s detailnějším popisem, hlavně díky velké škále možností těchto útoků. S tímto závěrem jsem musel souhlasit. Shodli jsme se, že současné dokumenty poskytující obecné návody jsou dostatečně přehledné.

- **Navýšení počtu security, ochrana vstupu**

  Malý počet security je důsledkem nízké hrozby teroristického útoku. Navýšení jejich počtu by zajistilo zvýšit úroveň zabezpečení, díky možnosti pokrytí vstupních bodů na akci nebo do objektu a zároveň zabezpečit místo konání akce. Posílení zabezpečení vstupních bodů zajistí kamerový systém s rozpoznáváním obličejů, vyjíždějící bloky a závory.

- **Naplněnost stavů jednotek IZS**

  Naplněnost stavů jednotek IZS je dlouhodobý problém. Získat větší počet zaměstnanců by zajistilo navýšení jejich mzdy, možnost osobního rozvoje, náborový bonus, příspěvky na dovolenou, rekreaci a kulturu. Jistota stabilního zaměstnání je dalším faktorem, který je lákavý pro uchazeče. S hodnotiteli jsme se shodli, že naplnit stavy těchto jednotek je důležité pro stát celkově, ale díky malému zájmu veřejnosti je tento cíl těžce dosažitelný.

- **Zabezpečení komunikace**

  V době, kdy se nejvíce rozvíjí hrozby v kyberprostoru je zabezpečení komunikace velmi důležité. Předejít riziku krádeži informací a identity je lepší, než ji pak řešit. Možné řešení shledávám v najímání lidí, kteří by se pokoušeli prolomit tuto síť.

Návrhy s nízkou mírou využitelnosti

Závěrečná skupina opatření dle subjektivního názoru i názoru hodnotitelů nepřináší velké benefity v prevenci vzniku teroristického útoku nebo není reálné jejich zavedení, a proto nejsou prioritou pro zavedení. Patří sem dotační podpora od státu, materiální podpora a školení security, sociální podpora a prevence.

- **Dotační podpora od státu**

  Dotační podpora od státu by určitě pomohla zvýšit úroveň zabezpečení, ale vzhledem k aktuální ekonomické situaci to není možné. Za dotace poskytnuté státem lze nakoupit lepší výzbroj a výstroj pro jednotky IZS, zvýšit zájem o práci v těchto jednotkách a poskytnout lepší výcvikové podmínky.

- **Materiální podpora a školení security**

  Školení security personálu od příslušníku policie a zdravotníků by určitě pomohlo v zabezpečení akce a následnému případnému zásahu, jelikož by se zaručila efektivita a plynulost. Ovšem dle hodnotitelů nemají organizace starající se o zabezpečení o tyto služby zájem, proto je pravděpodobnost zavedení tohoto opatření tak nízká.

- **Sociální podpora a prevence**

  Vzhledem k současným podmínkám, kdy není společnost rozdělena na etnické a náboženské skupiny, jsme s hodnotiteli usoudili, že současná snaha státu v této problematice je dostačující.

14 DÍLČÍ ZÁVĚR

Praktická část měla za cíl zhodnotit současný stav připravenosti státu předcházet a reagovat na vznik KS, a to za použití SWOT analýzy, metody PNH a rozhovoru s vybranými odborníky. Pomocí SWOT analýzy byly odhaleny silné a slabé stránky současného stavy a tedy body, které potřebují zlepšit, aby se zvýšila bezpečnost. Výsledné ohodnocení této analýzy ukázalo, že je v současnosti je brána defenzivní strategie.

Následně jsou nastíněny modelové situace, které v současné době mohou nastat. Na těchto situacích byl popsán postup zasahujících jednotek a vyplývají z nich rizika pro měkké cíle a zasahující jednotky. Tato rizika jsou ohodnoceny metodou PNH, při které byly dotázány osoby z řad krizového manažera města a zaměstnanců jednotek IZS, aby ohodnotili daná rizika dle svých zkušeností. S těmito odborníky byl proveden i rozhovor, aby se zjistil reálný stav připravenosti města na prevenci vzniku a schopnost reagovat na vzniklé KS.

V závěru praktické části byl zpracován návrh opatření ke snížení daných rizik, který byl rovněž ohodnocen těmito odborníky, a tím se posoudila reálnost zavedení těchto opatření.

ZÁVĚR

Tato diplomová práce byla zaměřena na problematiku terorismu a její souvislosti. Hlavním cílem práce bylo zhodnotit současný stav připravenosti systému na ochranu měkkých cílů a pomocí nabytých vědomostí a poznatků identifikovat slabá místa a navrhnout opatření vhodná pro implementaci do současného stavu systému ochrany měkkých cílů.

Provedená analýza odhalila silné stránky připravenosti systému v hlídkách prováděných příslušníky policie ČR a členy security, schopnosti jednotek IZS efektivně a koordinovaně spolupracovat, zpracovaných evakuačních plánech a analýzy rizik pro danou oblast.

Naopak mezi slabé stránky systému ochrany patří nedostatečné obvodové zabezpečení prostoru vyhrazeného pro veřejnou akci, security personál bez dostatečného výcviku a vybavení, nedostatečné ochraně kritických míst, nedostatku financí a dokumentů pro ochranu měkkých cílů a nezabezpečení mobilní a internetové sítě. Závažnost rizik byla ohodnocena odborníky zapojenými do ochrany měkkých cílů.

Díky jejich zkušenostem bylo možné následně vyhodnotit reálnost zavedení navržených opatření do praktického použití. Mezi opatření, která by bylo nejvíce reálné zavést a nejvíce by snížily daná rizika patří zvýšení schopností a dovedností jednotek IZS jejich společným cvičením, vzděláváním veřejného sektoru a častější aktualizování analýzy rizik s přihlédnutím na využití moderních technologií.

Dle mého názoru je současný stav ochrany měkkých cílů na velmi vysoké úrovni. Je možné pozorovat snahu státu a organizací posilovat svoji obranyschopnost a jednotek IZS o plynulejší průběh při zásahu.

SEZNAM POUŽITÉ LITERATURY

AGH, Karel, 2011. *Aktivní střelec 2011, In: Sborník příspěvků 8. ročníku konference Medicína katastrof, zkušenosti, příprava, praxe.* Hradec Králové: Zdravotní a sociální akademie Hradec Králové. ISBN: 978-80—905089-0-3.

Al-Káida, 2003–2023. Novinky.cz ČR: Borgis. [online]. Dostupné z: https://www.novinky.cz/tag/al-kaida-880

ANTUŠÁK, Emil, 2013. *Krizová připravenost firmy*. Praha: Wolters Kluwer Česká republika, 184 s. ISBN 978-80-7357-983-8.

Audit národní bezpečnosti, 2016. Vláda České republiky. Praha: Vláda ČR. [online]. Dostupné z: https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf

BATES, Rodger, 2012. *Dancing With Wolves: Today's Lone Wolf Terrorists. The journal of public and professional sociology* [online]. USA: Kennesaw State University. Dostupné z: https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=1023&context=jpps

BAHENSKÝ, Vojtěch, 2016. *Komentář: Stručné dějiny terorismu. Dotyk* [online]. ČR: VLTAVA LABE MEDIA. Dostupné z: https://www.dotyk.cz/publicistika/komentar-strucne-dejiny-terorismu-20160804.html

Bezpečnostní politika, 2023. Ministerstvo zahraničních věcí ČR [online]. ČR: MZV ČR. Dostupné z: https://www.mzv.cz/jnp/cz/zahranicni_vztahy/bezpecnostni_politika/index.html

Bezpečnostní strategie České republiky, 2003. Ministerstvo obrany ČR [online]. ČR: Army.cz. Dostupné z: https://mocr.army.cz/images/Bilakniha/CSD/2003%20Bezpecnostni%20strategie%20CR.pdf

Bezpečnostní strategie České republiky, 2015. ČR: Vláda ČR [online]. Dostupné z: https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf

Bezpečnostní strategie České republiky, 2009-2023. Vláda České republiky [online]. ČR: Vláda ČR. Dostupné z: https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf

BOZP, 2022. *Mimořádná událost. Definice, druhy a řešení prostřednictvím IZS*. [online]. Dostupné z: https://www.bozp.cz/aktuality/mimoradna-udalost/

BREEN-SMYTH, Marie, 2016. *The Ashgate Research Companion to Political Violence. New York: Routledge Taylor & Francis Group*. ISBN 978-0-7546-9493-9

BRZYBOHATÝ, Marian, 2001. *Terorismus a my.* Praha: Computer Press. ISBN 80-7226-584-9

BRZYBOHATÝ, Marian, 2002. *Současný terorismus.* Vojenské rozhledy, Praha, č.2. ISSN 1210-3292.

BYMAN, Daniel, 1998. *The logic of ethnic terrorism, Studies in Conflict & Terrorism. Taylor and Francis online* [online]. UK: Informa UK Limited. Dostupné z: https://www.tandfonline.com/doi/abs/10.1080/10576109808436060

Co je kyberterorismus, 2022. Správa sítě: Slovník pojmů [online]. Praha: Aira GROUP. Dostupné z: https://www.sprava-site.eu/kyberterorismus/

CORTE BÁÑEZ, Luis de la, 2009. *Logika terorismu*. 1.vyd. Praha: Academia, 321 s. ISBN 978-80-200-1.

ČESKO, 2000. *Zákon č. 240/2000 Sb., o krizovém řízení, v aktuálním znění.* [online] Dostupné z: https://www.aspi.cz/

FRANK, Libor, 2003. *Bezpečnostní prostředí České republiky*. Obrana a strategie [online]. ČR: Ministerstvo kultury ČR. Dostupné z: https://www.obranaastrategie.cz/cs/archiv/rocnik-2003/1-2003/bezpecnostni-prostredi-ceske-republiky.html

Hamas: Definition, History, Ideology and Facts, 2023. Britannica [online]. USA: Encyclopædia Britannica. Dostupné z: https://www.britannica.com/topic/Hamas

HEIDE, Liesbeth van der, 2011. *Individual terrorism indicators of lone operators.* Utrecht. Master. University of Utrecht.

CHAILAND, Gerard a Arnaud BILN, 2007. *The history of terrorism: From antiquity to Al Queda.* 1. Berkley and Los Angeles, California: University of California Press. ISBN 978-0-520-24533-4.)

CHENOWETH, Erica, Richard ENGLISH a Andreas GOFAS, 2019. *The Oxford Handbook of Terrorism.* Oxford: Oxford University Press. ISBN 978-0-19-873291-4

JANOŠEC, Josef, 2010. *O terorismu: pro pracovníky bezpečnostního systému.* V Ostravě: Spektrum, Sdružení požárního a bezpečnostního inženýrství. ISBN: 978-80-7385-097-5.

JELÍNEK, Jiří, 2017. *Terorismus - základní otázky trestního práva a kriminologie.* Praha: Leges. Teoretik. ISBN 978-80-7502-256-1.

Koncepce ochrany měkkých cílů pro 2017-2020, 2018. Ministerstvo vnitra ČR [online]. Dostupné z: https://www.mvcr.cz/soubor/koncepce-ochrany-mekkych-cilupro-2017-2020-pdf.aspx)

KOUDELKA, Ctirad a Václav VRÁNA, 2006. *Rizika a jejich analýza* [online]. Dostupné z: https://fei1.vsb.cz/kat420/vyuka/Magisterske%20nav/prednasky/web/RIZIKA.pdf

KRÁSNÝ, Antonín a Oldřich SOCHA, 2006. *Možné vlivy bezpečnostního prostředí na Českou republiku a její ozbrojené síly*. Obrana a strategie [online]. ČR: Ministerstvo kultury ČR. Dostupné z: https://www.obranaastrategie.cz/cs/archiv/rocnik-2006/1-2006/mozne-vlivy-bezpecnostniho-prostredi-na-ceskou-republiku-a-jeji-ozbrojene-sily.html

Kritická infrastruktura, 2023. Hasičský záchranný sbor České republiky [online]. ČR: Generální ředitelství Hasičského záchranného sboru ČR. Dostupné z: https://www.hzscr.cz/clanek/web-krizove-rizeni-a-cnp-kriticka-infrastruktura-kriticka-infrastruktura.aspx

LESSER, I. O. et al., 1999. *Countering the New Terrorism*. RAND Corporation. ISBN 0-8330-2667-4

Libanonský Hizbulláh: vznik a transformace hnutí 1982-2000, 2019. Asociace pro mezinárodní otázky [online]. ČR: Moravio. Dostupné z: https://www.amo.cz/libanonsky-hizbullah-vznik-a-transformace-hnuti-1982-2000/

MAREŠ, Miroslav, 2005. *Terorismus v ČR*. 1.vyd. Brno: Centrum strategických studií. ISBN 80-903333-8-9

MAKARIUSOVÁ, Radana, 2013. *Terorismus, globální terorismus a éra al-Káidy*. Praha: Metropolitan University Prague Press. ISBN 978-80-86855-95-0.

Metodika základy ochrany měkkých cílů, 2018. Ministerstvo vnitra ČR [online]. Dostupné z: https://www.mvcr.cz/soubor/metodika-zaklady-ochrany-mekkychcilu-pdf.aspx

MIOVSKÝ, Michal, 2006. *Kvalitativní přístupy a metody v psychologickém výzkumu*. 3 vyd. Praha: Grada. ISBN 80-247-1362-4.

Národní akční plán boje proti terorismu, 2012. Ministerstvo vnitra ČR [online]. Dostupné z: file:///C:/Users/Admin/Downloads/NAP_2002_CZE_1.pdf)

Nejnebezpečnější teroristické organizace na světě, 2018. Lui body [online]. Praha: DIVERSITY MEDIA. Dostupné z: https://www.lui.cz/co-se-deje/13827-nejnebezpecnejsi-teroristicke-organizace-na-svete

NOSÁL, Juraj, 2012. *Terorismus osamělých vlků – útoky v Oslu*. Válka [online]. ČR: Válka.cz. Dostupné z: https://www.valka.cz/14654-Terorismus-osamelych-vlku-utokyv-Oslu#google_vignette

Ochrana kritické infrastruktury, 2023. MVČR [online]. ČR: Ministerstvo vnitra České republiky. Dostupné z: https://www.mvcr.cz/chh/clanek/ochrana-kriticke-infrastruktury-ochrana-kriticke-infrastruktury.aspx

PRIYA, Dixit a Jacob L. STUMP, 2013. *Critical Terrorism Studies: An Introduction to Research Methods* [online]. USA: Routledge. ISBN 978-0-415-62046-8. Dostupné z: https://books.google.cz/books?hl=cs&lr=&id=saoPmAtf08sC&oi=fnd&pg=PP1&dq=PRIYA,+Dixit+and+Jacob+L.+STUMP.+Critical+Terrorism+Studies:+An+Introduction+to+Research+Methods.+2013.+ISBN+9780415620468&ots=XpaWeYz3Qt&sig=_oD-gKSK644RTtUufw1GABPyZYo&redir_esc=y#v=onepage&q&f=false

SEDLÁKOVÁ, Monika, 2017. *Téma „terorismus“ ve výuce zeměpisu na ZŠ*. Brno. Diplomová. Masarykova univerzita. Vedoucí práce Libor Lněnička.

SMOLÍK, Josef, 2015. *Psychologie terorismu a metafora schodiště*. [online] ISSN 2336-2995. Dostupné z: www.vojenskerozhledy.cz/ kategorie/psychologie-terorismu-a-metafora-schodiste

SOJKOVÁ, Anna, 2018. *Problematika terorismu* [online]. Dostupné z: https://is.ambis.cz/th/sav5t/. Bakalářská práce. AMBIS vysoká škola, a.s. Vedoucí práce Věra KOSÍKOVÁ.

SRBOVÁ, Karolína, 2016. *Óm šinrikjó: anomálie, nebo logický důsledek neřešených problémů v japonské společnosti?* [online]. Praha. Bakalářská. Univerzita Karlova.

Srpová, J. et al., 2011. *Podnikatelský plán a strategie*. Expert (Grada), Praha. ISBN 978-80-247-4103-1.

Strategie České republiky pro boj proti terorismu, 2013. ČR: Vláda ČR [online]. Dostupné z:

https://www.mzv.cz/jnp/cz/zahranicni_vztahy/bezpecnostni_politika/boj_proti_terorismu/index.html

Stupně ohrožení terorismem, 2023. MVČR [online]. ČR: Ministerstvo vnitra České republiky. Dostupné z: https://www.mvcr.cz/chh/clanek/stupne-ohrozeni-terorismem.aspx

SVOBODA, Ivo, 2021. *Rizika terorismu jako nástroje projevů extrémismu*. Akadémia policajného zboru [online]. Bratislava: Akadémia policajného zboru v Bratislave. Dostupné z: https://www.akademiapz.sk/sites/default/files/Notitiae/1-2020/005%20%20SVOBODA%20Terorizmus_EDITED.pdf

ŠENOVSKÝ, Pavel, Michail ŠENOVSKÝ a Milan ORAVEC, 2020. *Teorie krizového managementu*. 2. rozšířené vydání. Ostrava: Sdružení požárního a bezpečnostního inženýrství, 138 s. ISBN 978-80-7385-231-3. S7.

ŠMÍD, Tomáš, n.d. *Základní fakta o Islámském státu v Iráku a Sýrii (ISIS).* Katedra politologie FFS MU [online]. Dostupné z: http://polit.fss.muni.cz/zakladni-fakta-o-islamskem-statu-v-iraku-a-syrii-isis/

Taliban Fast Facts, 2023. Edition.cnn.com [online]. USA: Cable News Network. Dostupné z: https://edition.cnn.com/2013/09/20/world/taliban-fast-facts/index.html

Terminologický slovník, 2016. Terminologický slovník pojmů z oblasti krizového řízení, ochrany obyvatelstva, enviromentální bezpečnosti a plánování obrany státu. [online] Dostupné z: https://www.mvcr.cz/clanek/terminologicky-slovnik-krizove-rizeni-a-planovani-obrany-statu.aspx

Terrorist attacks in the U.S. or against americans, 2022. Infoplease [online]. USA: Sandbox Networks. Dostupné z: https://www.infoplease.com/disasters/man-made/terrorist-attacks-in-the-us-or-against-americans

Typologie terorismu, 2023. MVČR [online]. Praha: Ministerstvo vnitra České republiky. Dostupné z: https://www.mvcr.cz/clanek/typologie-terorismu.aspx?q=Y2hudW09Mg%3D%3D

Od SWOT analýzy k tvorbě firemní strategie, 2019. [online]. Dostupné z: https://www.ustavprava.cz/blog/2019/10/od-swot-analyzy-ktvorbe-firemni-strategie

VIČAR, Dušan. 2017. *Ochrana proti zbraním hromadného ničení* [online]. Uherské Hradiště: Univerzita Tomáše Bati ve Zlíně.

Zákon č. 239/2000 Sb. Zákon o integrovaném záchranném systému a o změně některých zákonů, 2023. Zákony pro lidi [online]. ČR: AION CS. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-239

Zákon č. 40/2009 Sb., 2023. Zákony pro lidi [online]. AION CS. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

BIS Bezpečnostní informační služba

BRS Bezpečnostní rada státu

ČR Česká republika

ESDP Evropská bezpečnostní a obranná politika

EU Evropská unie

KI Kritická infrastruktura

KS Krizová situace

MU Mimořádná událost

NATO Severoatlantická aliance

OBSE Organizace pro bezpečnost a spolupráci v Evropě

OSN Organizace spojených národů

SZBP Společná zahraniční a bezpečnostní politika

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: ROZHOVOR

Je dané město po smutné události v Uherském brodu nějak připraveno na podobnou situaci?

Byli majitelé restaurací a podobných zařízení kontaktováni za účelem zvýšení jejich připravenosti?

Byly zavedeny nějaké opatření i přes nesouhlas majitelů?

Pokud je na území města pořádána akce externími organizacemi či agenturami, je s nimi probírána otázka bezpečnosti a má město dohled nad průběhem?

Je v rámci akcí pořádaných pro širokou veřejnost vytvořen bezpečností plán?

Jak je zajišťována ochrana osob účastnících se na akcích?

Pokud je vytvořen bezpečnostní plán pro teroristický čin, jaký je postup při vzniku?

Jak vypadá společné cvičení jednotek IZS?

Je policie schopna v takovém případě dostatečně a včas zasáhnout?

Setkali jste se s jakoukoliv variantou teroristického útoku?

Jak jste postupovali?

Myslíte si, že je v daném městě nějaký cíl, který by mohl být pro teroristy zajímavý?

Jak vnímáte riziko terorismu? Je třeba se ho obávat?

Je policie a Vy, jako krizový manažer, průběžně školen i na tuto problematiku?

Poskytuje město v rámci této problematiky občanům nějaký návod, jak postupovat?

Myslíte si, že byv daném městě mohl být nějaký měkký cíl terčem teroristického činu?

Pokud byste mohl, změnil byste celkovou koncepci ochrany měkkých cílů?