

Soukromé bezpečnostní služby v ČR při ochraně měkkých cílů

**Private Security Services in the Czech Republic
for the Protection of Soft Targets**

Disertační práce

Ing. Petr Mirovský, LL.M.

Kladno 2025

Doktorský studijní program: Civilní nouzová připravenost

Studijní obor: Civilní nouzové plánování

Školitel: doc. PhDr. Barbora Vegrichtová, Ph.D., MBA

Školitel specialista: Ing. Michael Somr, Ph.D.

PROHLÁŠENÍ

Prohlašuji, že jsem disertační práci s názvem Soukromé bezpečnostní služby v ČR při ochraně měkkých cílů vypracoval samostatně pouze s použitím pramenů, které uvádím v seznamu bibliografických odkazů.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu § 60 zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.

V Kladně dne 25.08.2025

Podpis

PODĚKOVÁNÍ

Rád bych poděkoval především rodině a nejbližším přátelům za podporu a trpělivost, kterou mi během celého doktorského studia prokazovali, a také kolegům, bez kterých by práce nemohla vzniknout. Díky patří taktéž celé Fakultě biomedicínského inženýrství ČVUT, jakožto domovskému prostředí v celé době mého vysokoškolského studia.

ABSTRAKT

Disertační práce je zaměřena na problematiku komerční bezpečnosti v České republice s důrazem na ochranu měkkých cílů. Jedná se o oblasti, které jsou v bezpečnostním prostředí úzce propojené. Vzhledem k absenci konkrétní legislativy upravující postavení a činnost soukromého bezpečnostního sektoru v České republice se práce věnuje i možnostem systémového ukotvení tohoto sektoru, a to jako výstupu analytické a komparační části práce po vzoru jiných států. Součástí výzkumu je rovněž analýza možností větší participace bezpečnostních agentur nejen při ochraně měkkých cílů, ale i v rámci bezpečnostního systému jako celku, což je předmětem návrhové části tohoto dokumentu.

Teoretická část disertační práce se zaměřuje na definici a typologii měkkých cílů, legislativní status soukromých bezpečnostních služeb v České republice a současným možnostem spolupráce právě v oblasti bezpečnosti a zapojení komerčního bezpečnostního sektoru do státních struktur s cílem ochrany měkkých cílů. Teoretická, analytická část práce je podkladem k následnému rozpracování a plnění vytyčených cílů.

Praktická a návrhová část práce představuje primárně vytvořenou metodiku pro hodnocení rizikovosti měkkých cílů. Navržená metodika vychází z principů rizikové analýzy a využívá kontrolní seznamy, skórovací tabulky a multikriteriální hodnocení. Zásadním přínosem je ranking TRS (total risk score) daného měkkého cíle s konkrétními návrhy na navýšení bezpečnosti za využití soukromých bezpečnostních služeb.

Primárním cílem disertace je navrhnout komplexní model systémového zakotvení soukromých bezpečnostních služeb do rámce národní bezpečnosti, s důrazem na jejich specifické schopnosti v ochraně veřejného prostoru a měkkých cílů. Výsledky práce mohou přispět k odborné diskusi o reformě komerční bezpečnostní politiky České republiky a nabídnout inspiraci pro legislativní úpravy i praktická bezpečnostní opatření.

KLÍČOVÁ SLOVA

Měkký cíl, soukromá bezpečnostní služba, fyzická bezpečnost, Total Risk Score (TRS).

ABSTRACT

This dissertation focuses on the issue of commercial security in the Czech Republic, with a particular emphasis on the protection of soft targets. These two areas are closely interconnected within the broader security framework. Given the absence of specific legislation regulating the status and operations of the private security sector in the Czech Republic, the work also explores potential models for its systemic integration, inspired by international practices. The research further analyzes the possibilities for broader participation of private security companies not only in the protection of soft targets, but also within the national security system as a whole, which underpins the thesis proposal section.

The theoretical part of the dissertation addresses the definition and typology of soft targets, the legislative status of private security services in the Czech Republic, and current options for public-private cooperation in the field of security. Particular attention is paid to the integration of the private security sector into state structures for the purpose of soft target protection. This theoretical foundation serves as a basis for the subsequent development and achievement of the thesis objectives.

The empirical part of the dissertation introduces an original methodology for assessing the risk exposure of soft targets. The method is based on principles of risk analysis and employs checklists, scoring tables, and multicriteria evaluation. A key contribution is the development of a Total Risk Score (TRS) ranking system for individual soft targets, accompanied by concrete recommendations for enhancing their security through the deployment of private security services.

The primary aim of the dissertation is to propose a comprehensive model for the systematic integration of private security services into the national security framework, emphasizing their unique capabilities in protecting public spaces and soft targets. The outcomes of this research may contribute to professional discourse on the reform of commercial security policy in the Czech Republic and offer inspiration for both legislative changes and practical security measures.

KEYWORDS

Soft target, private security agency, physical security, Total Risk Score (TRS).

OBSAH

1	Úvod.....	10
2	Přehled současného poznání.....	12
2.1	Komerční bezpečnostní sektor v České republice.....	14
2.1.1	Současné legislativní ukotvení komerční bezpečnosti v České republice ...	14
2.1.2	Profesní sdružení soukromé bezpečnosti v České republice.....	17
2.1.3	Historický exkurz a geneze návrhů zákona o soukromých bezpečnostních službách.....	18
2.1.3.1	Návrh zákona o soukromých bezpečnostních službách z roku 2012/2013.....	19
2.1.3.2	Návrh zákona o soukromých bezpečnostních službách z roku 2015	19
2.1.3.3	Návrh zákona o soukromých bezpečnostních službách z roku 2020	20
2.1.3.4	Návrh zákona o soukromých bezpečnostních službách z roku 2024	20
2.2	Charakteristika měkkých cílů.....	22
2.2.1	Kategorizace typů útoků na měkké cíle	24
2.2.2	Strategické a metodické rámce ochrany měkkých cílů v České republice...	25
2.2.3	Modely ochrany měkkých cílů ve světě ve veřejně-soukromé spolupráci...	27
2.2.3.1	Veřejno–soukromé partnerství	27
2.2.3.2	Horizontální spolupráce mezi subjekty měkkých cílů	29
2.2.3.3	Asociativní a sektorové platformy	29
2.2.3.4	Multilaterální partnerství.....	29
2.2.3.5	Peer-to-peer spolupráce a benchmarking	30
2.2.3.6	Komunitně řízená bezpečnost	30
2.2.4	Trendy v ochraně měkkých cílů a inovace pomocí nestandardních prostředků.....	31
2.2.4.1	Zpevňování lokalit (Site Hardening).....	31
2.2.4.2	Technologie pro detekci a reakci	32
2.2.4.3	Ochrana proti výbuchům a útokům s vysokým dopadem	32

2.2.4.4	Zaměření na otevřené prostory	33
3	Cíle práce.....	34
4	Analytická část	36
4.1	Analýza využití bezpečnostních agentur v České republice	36
4.2	Případové analýzy komerční bezpečnosti vybraných evropských států	42
4.2.1	Soukromá bezpečnostní činnost v Německu.....	43
4.2.2	Soukromá bezpečnostní činnost ve Francii	43
4.2.3	Soukromá bezpečnostní činnost v Itálii	44
4.2.4	Soukromá bezpečnostní činnost v Nizozemsku	45
4.2.5	Soukromá bezpečnostní činnost na Slovensku.....	46
4.2.6	Soukromá bezpečnostní činnost ve Finsku	47
4.2.7	Vlastní závěry případových analýz	48
4.3	Komparace vybraných evropských modelů komerční bezpečnosti	50
4.4	Statistická analýza útoků na měkké cíle ve světě a v České republice	52
4.4.1	Útoky na měkké cíle ve světě.....	53
4.4.2	Útoky na měkké cíle v Evropské unii a Velké Británii.....	56
4.4.3	Útoky na měkké cíle v České republice	58
4.4.4	Případová studie útoku aktivního střelce na Karlově univerzitě s vlastními náměty na možnosti zlepšení řešení situace.....	59
4.4.5	Možnosti zlepšení bezpečnostního rámce a možná role komerční bezpečnosti v řešení modelové situace útoku na Filosofické fakultě Univerzity Karlovy	60
4.5	SWOT analýza možností využití soukromých bezpečnostních služeb k ochraně měkkých cílů v současných legislativních podmínkách České republiky.....	61
5	Použitá metodika	66
6	Syntetická – návrhová část	67
6.1	Návrh a uplatnění semikvantitativní metody Total Risk Score.....	67
6.1.1	Struktura a princip metody Total Risk Score	68

6.1.2	Kategorizace a využití soukromých bezpečnostních služeb v metodice Total Risk Score.....	70
6.1.3	Výsledné Total Risk Score a interpretace rizikové úrovně	72
6.1.4	Aplikace metodiky TRS a závěry.....	74
6.2	Návrh optimálního modelu komerční bezpečnosti v České republice	76
6.2.1	Tří úrovněová kvalifikace pracovníků	77
6.2.2	Efektivní spolupráce s veřejnými orgány	79
6.3	Inovace v ochraně měkkých cílů a možná nová technologická řešení.....	80
6.3.1	Technologická výbava pracovníků soukromých bezpečnostních služeb	80
6.3.2	Technologická řešení po vzoru společnosti Genasys	81
6.3.3	Funkce reverzní 112	82
6.3.4	Neletální zbraňové systémy a jejich možnosti využití v komerční bezpečnosti.....	84
6.3.5	Letální prostředky ochrany.....	85
6.4	Pohled do blízké budoucnosti a vize soukromých bezpečnostních služeb	85
6.4.1	Využití personálu a civilního obyvatelstva ke zvýšení bezpečnosti	85
6.4.2	Návrh možných forem zapojení soukromých bezpečnostních služeb v integrovaném záchranném systému České republiky	87
6.4.3	Role First Responders v rámci soukromých bezpečnostních služeb při ochraně měkkých cílů.....	89
6.4.4	Možné zapojení zaměstnanců soukromých bezpečnostních služeb do třídění raněných při mimořádných událostech měkkých cílů	90
6.4.5	Možnosti zapojení soukromých bezpečnostních služeb k ochraně kritické infrastruktury.....	90
7	Diskuse.....	93
8	Závěr.....	102
9	Seznam publikací disertanta vztahujících se k disertační práci	104
10	Seznam použitých zkratk.....	106

11 Seznam použité literatury	107
12 Seznam použitých obrázků.....	119
13 Seznam použitých tabulek.....	120
14 Seznam použitých příloh	121
15 Přílohy	122

1 ÚVOD

Bezpečnostní situace v Evropě i ve světě prochází dynamickými proměnami. Společnost čelí vzrůstajícím hybridním hrozbám, změnám v migračních tocích, geopolitickým napětím a rostoucí aktivitě jednotlivců i skupin motivovaných různými ideologiemi. Tyto okolnosti kladou nové nároky na způsoby zajišťování ochrany osob, majetku, kritické infrastruktury i veřejného pořádku.

Předložená disertační práce se věnuje tématu komerční bezpečnosti v České republice (dále ČR), se zvláštním důrazem na ochranu tzv. měkkých cílů (dále jen MC). Obě oblasti spolu úzce souvisejí a jejich význam neustále roste, jednak v reakci na aktuální bezpečnostní hrozby, jednak kvůli dlouhodobě chybějící komplexní legislativní úpravě, která by jasně vymezovala postavení a činnost soukromého bezpečnostního sektoru. Hlavní motivací práce je proto snaha nabídnout návrh systémového ukotvení tohoto sektoru a hledat inspiraci v zahraničních přístupech, které by mohly být aplikovatelné v českém prostředí.

Původní motivací vzniku soukromých bezpečnostních služeb (dále jen SBS), tak jak je známe dnes, byla potřeba doplnit nebo částečně nahradit státní složky při ochraně osob a majetku tam, kde kapacity státu nestačily na zajištění veřejného pořádku a bezpečnosti. Za pozornost stojí i sílící role SBS v Evropě. Již v roce 2006 dosahoval počet personálu v řadách SBS ve státech EU přibližně 1,1 milionu, zatímco počet policistů činil zhruba 1,5 milionu. Tento poměr se i nadále proměňuje ve prospěch komerční bezpečnosti, v některých oblastech začínají tyto subjekty stále častěji doplňovat, a někdy i částečně nahrazovat, státní bezpečnostní složky samotné [1].

Tento početní růst poukazuje na jasnou vysokou potenciální využitelnost zaměstnanců SBS k bezpečnostním účelům. Předpokladem je však efektivní a funkční nastavení možností ze strany státu.

Dále je nutno zmínit, že se zvyšuje význam soukromého sektoru v ochraně před tzv. hybridními hrozbami – tedy komplexními a těžko identifikovatelnými formami útoku, které kombinují fyzické, informační a kybernetické prvky nátlaku. Těmto typům útoků jsou MC často vystaveny, a právě zde by mohla komerční bezpečnost sehrát klíčovou úlohu. Tuto skutečnost podporuje zpráva Evropské komise bezpečnosti, která dne 1. dubna 2025 představila strategii ProtectEU, která klade důraz na budování odolnosti proti hybridním hrozbám, včetně kybernetických útoků a taktéž vyzdvihuje kritický nedostatek odborně způsobilých personálních zdrojů v této oblasti. Mimo to, že zpráva opomíjí významný

nedostatek policejního personálu, otevírá tato skutečnost další možnost realizace pro komerční bezpečnost [2,3].

Předmětem výzkumu této disertační práce je soukromý bezpečnostní sektor v ČR, a to z hlediska jeho potenciální role v ochraně MC. Výzkum se zaměřuje na konkrétní nástroje, přístupy a modely, které mohou přispět ke zvýšení účinnosti ochrany veřejně přístupných prostor, přičemž zohledňuje i legislativní a systémové možnosti začlenění těchto subjektů do národní bezpečnostní architektury. Klíčovou otázkou, kterou si práce klade, je, jak lze SBS efektivně zapojit do ochrany MC, právě tímto směrem se ubírá jak analytická, tak návrhová část disertace.

Stávající systém ochrany MC v ČR vykazuje řadu nedostatků. Ačkoli již existují určité strategické dokumenty a doporučení, chybí ucelená metodika pro posouzení rizikovosti konkrétních lokalit v kombinaci s návrhem vhodného zapojení komerčních bezpečnostních subjektů. Tato mezera významně oslabuje efektivitu celkového bezpečnostního systému. Jedním z hlavních výstupů práce je proto návrh nové metodiky hodnocení rizikovosti, která by měla být prakticky využitelná v prostředí MC a zároveň přispět k efektivnímu zavádění odpovídajících bezpečnostních opatření. Jedná se o nové unikátní řešení určení rizikovosti jakéhokoliv MC. Zásadní přínos této metody je, že dle úrovně rizika nabízí konkrétní zapojení SBS k navýšení bezpečnosti. Navržená metoda je tak všeobecně využitelnou platformou přímo propojující SBS při ochraně MC, její ojedinělost tkví v možném spektru využití, jak ze strany provozovatelů MC, tak zaměstnanců SBS či jiného bezpečnostního managementu včetně státních bezpečnostních struktur. Současně jsou přínosem nové možnosti vývoje SBS v ČR, které jsou obsahem návrhové části práce. Zde definované návrhy jsou novým, vizionářským pohledem na využití komerční bezpečnosti a jejího propojení se státním bezpečnostním sektorem.

Ústřední metodou disertační práce je metoda analýzy a syntézy, která umožňuje komplexně nahlížet na problematiku regulace soukromého bezpečnostního sektoru a MC. Analýza slouží k podrobnému rozboru teoretických, legislativních a praktických aspektů dané problematiky, zatímco syntéza propojuje zjištěné poznatky do návrhů nových řešení. Tyto výše zmíněné vizionářské návrhy reflektují reálné i potenciální podmínky SBS v právním prostředí ČR.

2 PŘEHLED SOUČASNÉHO POZNÁNÍ

SBS nejsou v historii ničím novým, už v dávných dobách si lidé najímali ozbrojené profesionály, žoldněře, kteří je chránili před nebezpečím nebo dohlíželi na jejich majetek. Postupem času si stát začal upevňovat kontrolu nad používáním síly a bezpečnost se stala hlavně státní záležitostí. Tento monopol ale začal od 70. let minulého století postupně oslabovat a na scénu se znovu začaly vracet soukromé bezpečnostní firmy. Definice komerční bezpečnosti v dnešní době tak reflektuje tuto historickou evoluci: "Jde o poskytování služeb komerční bezpečnosti na základě koncesní listiny, která má za cíl zajistit ochranu osob, majetku a dalších bezpečnostních zájmů. Tyto služby jsou poskytovány na obchodním a smluvním základě [4,5,6,7]".

Pojem komerční bezpečnosti poskytuje rámcový pohled na využití fyzické síly k ochraně života nebo majetku prostřednictvím nasmlouvané úplaty a koncese, což je projev ze strany státu, že daný subjekt může provozovat činnosti spojené s bezpečností. Cílem komerční bezpečnosti je vytvářet nadstandardní služby, které překračují běžné možnosti státních orgánů, a to za účelem dosažení zisku. Avšak, vzhledem k charakteru této činnosti jako soukromé podnikatelské aktivity, se poskytovaná služba stává obchodní komoditou, zbožím, které podléhá poptávce a nabídce na otevřeném trhu. Zákazník má tak možnost volby v souladu s kategorií nejnižší ceny, čímž vytváří prostor pro nabídku zjevně nekvalitních služeb, které odpovídají této nízké cenové hladině [4].

Jejich rozmach byl zvlášť výrazný po roce 1989 ve státech střední a východní Evropy, kde se stal součástí širších společenských a ekonomických změn. V období Československé socialistické republiky nelze plnohodnotně mluvit o formě komerční bezpečnosti tak, jak ji známe dnes (jedná se o soukromé podnikání, které tehdy nebylo možné). Určitým zástupcem v hlídání objektů byli vlastní zaměstnanci jednotlivých podniků (vrátní), kteří plnili funkci fyzické ochrany a režimových opatření na nižší úrovni. S nástupem tržní ekonomiky a otevřeného trhu se však scénérie komerční bezpečnosti dramaticky mění. Nyní se stává klíčovým faktorem kvalita poskytovaných služeb a konkurenceschopnost firem působících na tomto poli. Trendy v oblasti technologie, školení personálu a inovace služeb hrají klíčovou roli v přetrvávajícím vývoji komerční bezpečnosti, kde kvalitní a efektivní ochrana majetku získává na významu v dynamickém prostředí moderní doby [5,7].

Existuje zde však rozpor s jednou ze základních definic Policie ČR (dále PČR), tedy zachovávání, ochrana a obnova vnitřní bezpečnosti státu a veřejného pořádku je úkolem

policie, a též znakem každého demokratického státu. Tato skutečnost je pak předpokladem pro efektivní návaznost ostatních státních složek bezpečnostního charakteru a taktéž běžného bezpečného každodenního života obyvatel. Naneštěstí zmíněná definice vymezující legislativní ukotvení policie značně oslabuje postavení SBS, která je ukotvena primárně v živnostenském zákoně bez vazeb a dělby kompetencí s policií. Nicméně po listopadu 1989 v ČR však dochází k nárůstu poskytování služeb tohoto charakteru i ze strany soukromých subjektů, které nazýváme právě SBS [8,9].

Tento vzestup měl za následek vznik Asociace bezpečnostních a detektivních služeb Čech, Moravy a Slezska, což bylo první uskupení bezpečnostně-soukromého charakteru v ČR. Nicméně se tato asociace posléze rozpadá. Tento rozpad byl výsledkem názorového nesouladu zejména ohledně vstupu zahraničního kapitálu do oboru a koncepce fungování sektoru soukromé bezpečnosti v ČR. Následně vzniká několik dalších na sobě nezávislých sdružení. Sdružení měly vesměs snahu o vymezení komerční bezpečnosti nejen v legislativním řádu ČR, jelikož soukromé bezpečnostní služby fungovaly na základě zákona 1/1988 Sb., o podpoře drobného podnikání. Toto řekneme volné pole působnosti pro působení soukromých bezpečnostních služeb v ČR mělo za následek vznik velkého počtu bezpečnostních agentur včetně přílivu zahraničních zaběhnutých organizací. Značná volnost a neznalost v oboru ze strany nových českých agentur vedla ke vzniku konkrétních stanov, na kterých se shodli nejvýznamnější tuzemské bezpečnostní agentury té doby. Jako hlavní sdružující orgán vzniká i Komora soukromých bezpečnostních služeb, a to v roce 1993 [10,11].

Snahy o sjednocování postupů, navyšování odbornosti, získávání zahraniční praxe a sdílení informací mezi členskými organizacemi pod taktovkou jednotného sdružení či asociace zlepšují celkový pohled na domácí formu komerční bezpečnosti. Jednotné standardy a stanovy by měly být zájmem všech členů a poskytovatelů služeb v oblasti bezpečnosti za současné legislativní absence [12].

Problém jednotlivých asociací, leč s dobrým úmyslem, lze spatřit v jejich decentralizaci a také absenci podřízení vyššímu státnímu institutu. Řád, stanovy, snahy a přístup se liší dle jednotlivých členů v konkrétních asociacích a spolcích a též dle zájmů jejich vedení (viz 2.1.2.).

Činnost bezpečnostních agentur je členěna a plněna mnohdy dle právních předpisů, které se jí primárně netýkají. Zásadním zákonem pro tuto oblast je stále zákon 455/1991 Sb., o živnostenském podnikání. Z tohoto zákona primárně vyplývá, jaké služby agentury poskytují a jaké je jejich oprávnění. Samotný výčet poskytovaných služeb je pak konkrétněji uveden

v nařízení vlády č. 278/2008 Sb., o obsahových náplních jednotlivých živností, bude rozebráno dále v samostatné kapitole [10].

Místní působnost bezpečnostních agentur není taxativně vymezena. Můžeme na našem území shledat i zahraniční podnikatelské subjekty. Místní příslušnost je vždy řádně vymezena ve smlouvě mezi zákazníkem a poskytovatelem bezpečnostních služeb a liší se u každého případu dle jeho požadavků a možností [13].

Některé státy mají přísné zákony a dohled, jiné téměř žádnou speciální úpravu. Chybějící harmonizace na úrovni EU, tedy neexistuje jednotný evropský předpis pro SBS. Významným trendem je růst sektoru (v některých zemích více pracovníků v SBS než u policie) a s tím spojené problémy jako infiltrace zločinem či nadměrné používání síly. Studie doporučuje posílení dohledu a sdílení osvědčených postupů mezi státy [14].

Z výše uvedeného vyplývají základní problémy v sektoru komerční bezpečnosti, tedy rozsah a kompetence k jejich činnosti a nedořešená právní úprava.

2.1 Komerční bezpečnostní sektor v České republice

2.1.1 Současné legislativní ukotvení komerční bezpečnosti v České republice

Pro další postupy disertační práce je nezbytné analyzovat současné právní předpisy, kterými se SBS v ČR řídí. Zásadní problém je neexistence konkrétního právního dokumentu a tím vzniklá roztržičnost, která sebou nese riziko neprofesionality.

Určující legislativa pro komerční bezpečnostní sektor v ČR:

- Ústava ČR – formulují základní lidské hodnoty a nároky na svobodu a bezpečí jakožto znaku vyspělé demokratické evropské země [15].
- Listina základních práv a svobod – tento dokument si zpravidla bezpečnostní agentury vykládají po svém, jelikož garantuje svobodu, právo na soukromé vlastnictví a svobodu podnikání, tím pádem vzniká i nárok na jejich ochranu [16].
- Živnostenský zákon – primární právní dokument pro činnost SBS. Zákon definuje nejen oblasti činností těchto organizací či fyzických osob, ale klade i podmínky pro jejich naplnění. V zákoně a jeho přílohách se přímo hovoří o komerční bezpečnostní činnosti jako o službě prováděné na základě koncese a za úplatu. Nároky kladené na provozovatele a zaměstnance jsou dle příloh následující: bezúhonnost, dovršení 18 let, svéprávnost [17].

Živnostenský zákon uvádí tři základní kategorie působnosti SBS v ČR. Tyto oblasti zájmů jsou pak konkretizovány v nařízení vlády o obsahových náplních jednotlivých živností (viz níže):

- Ostraha majetku a osob – poskytování služeb spojených s ostrahou a ochranou nemovitého a movitého majetku, ostrahou při přepravě peněz a při jejich zpracování, cenností nebo jiného majetku, ochranou osob, zajišťováním pořádku v místech konání veřejných shromáždění, slavností, sportovních podniků nebo lidových zábav podle pokynů objednatele, vyhodnocováním bezpečnostních rizik a provozováním centrálních pultů ochrany (PCO).
- Služby soukromých detektivů – služby spojené s hledáním majetku a osob, se zjišťováním skutečností, které mohou sloužit jako důkazní prostředky, získáváním informací týkajících se fyzických nebo právnických osob nebo jejich majetkových poměrů, získáváním informací v souvislosti s vymáháním pohledávek, vyhledáváním protiprávních jednání ohrožujících obchodní tajemství, a s tím související sběr dat a jejich vyhodnocování.
- Poskytování technických služeb k ochraně majetku a osob – projektování, montáž, kontrola, údržba a opravy elektronických poplachových systémů (zejména systémů zabezpečovacích, tísňových, protipožárních, kontroly vstupu, přivolání pomoci, dále systémů integrovaných a kamerových), určených k ochraně majetku a osob před neoprávněnými zásahy, včetně poplachových systémů a zařízení umožňujících sledování pohybu osob v objektech a jejich okolí. Taktéž montáž, opravy, údržba, revize a správa mechanických zábranných systémů.

Tento výčet konkrétních pracovních náplní bezpečnostních agentur lze doplnit ještě o jednu kategorii, která rozhodně není zanedbatelná, ba naopak je její poptávka na vzestupu. Jedná se o kategorii bezpečnostního vzdělávání, do které spadá i bezpečnostní poradenství a vývoj pomůcek pro vykonávání činností komerční bezpečnosti včetně jejich výroby a distribuce [4,18].

Další právní dokumenty, kterými se SBS v současné době řídí, jsou následující:

➤ Nařízení vlády (NV) o obsahových náplních jednotlivých živností – požadavky na kvalifikaci pracovníků v oblasti soukromé bezpečnosti se liší podle konkrétní profese, přičemž právní předpisy stanovují několik možných kvalifikačních cest. Mezi uznávané varianty patří vysokoškolské vzdělání, vyšší odborné vzdělání v oblasti práva, bezpečnosti nebo příbuzných oborů. Dále střední vzdělání s maturitní

zkouškou v bezpečnostním či právním oboru a alespoň tříletá praxe. Střední vzdělání s maturitou, doplněné tříletou praxí v oboru a osvědčením o rekvalifikaci nebo jiným dokladem o odborné způsobilosti. Tento doklad musí být vydán zařízením akreditovaným podle příslušných právních předpisů, Ministerstvem školství, mládeže a tělovýchovy, nebo resortním ministerstvem podle oblasti činnosti. A nakonec případně také střední vzdělání s maturitou, tříletá praxe a profesní kvalifikace pro činnost strážného dle zvláštního právního předpisu [19].

Konkrétní projevy nabízených kategorií činností dle tohoto nařízení vlády jsou pak fyzického, technického či poradenského charakteru. Užívané metody primárně fyzických činností jsou následující:

1. **Metoda fyzického pozorování;**
2. **metoda kontroly osob;**
3. **metoda osobní prohlídky a kontroly batohy;**
4. **metoda kontroly vozidel a nákladu;**
5. **metoda kontroly stavu;**
6. **metoda fyzických zábran a bariér;**
7. **metoda nasazení cvičeného psa;**
8. **metoda evakuačních a ochranných opatření;**
9. **metoda zajištění místa činu [19, 20].**

➤ Občanský zákoník – doplňuje Listinu základních lidských práv a svobod v kontextu soukromých bezpečnostních služeb o skutečnost, že jsou subjekty oprávněny zajistit ochranu života a majetku svépomocí. Zde je tedy svépomoc vnímána soukromými agenturami jako mezera, kterou mohou zaplnit [21].

➤ Trestní zákoník – zde dochází k přímému křížení se státním bezpečnostním sektorem, jelikož dle trestního zákoníku nemají zaměstnanci soukromých bezpečnostních služeb žádná oprávnění na vymáhání práva. Tím jsou postaveni na úroveň „běžných“ občanů ČR a mohou se řídit pouze paragrafy týkajícími se krajní nouze a nutné obrany. V případě ochrany majetku nebo osoby musí zaměstnanci bezpečnostních agentur postupovat kooperativně s PČR [22].

➤ Občanský soudní řád – tento právní dokument je bezpečnostními agenturami využíván zejména k volnému překladi činností služeb soukromého

detektiva. V případě vyžádání je osoba povinna zajišťovat a zachovávat důkazy spojené s dokazováním svého tvrzení v případě spáchání trestného činu, případně jsou detektivové předvoláváni jako svědci v soudním procesu [23].

➤ Zákoník práce – zde je v podstatě vymezen primární rozdíl mezi pracovníky SBS a příslušníky bezpečnostních sborů. Zaměstnanci bezpečnostních agentur jsou v pracovně-právním vztahu ke svému zaměstnavateli, a tudíž s ohledem na kladenou bezpečnost práce mohou odmítat některé úkoly spojené s jejich vlastním ohrožením, na rozdíl od příslušníků státních bezpečnostních sborů [24].

➤ Zákon o zbraních a střelivu – tento zákon upravuje obecně držení a používání zbraně. Jelikož se v případě bezpečnostních agentur nejedná o držení zbraně služební, musí se řídit tímto zákonem jako každý jiný občan. Pro pracovně-ochranné účely vymezuje zákon speciální kategorii D. Ovšem stále může být použita jen při ohrožení vlastního bezpečí [25].

Vlastní shrnutí

Výše uvedená legislativa je souhrnem právního rámce SBS v ČR. Nutno podotknout, že je ČR téměř posledním evropským státem, která nemá otázku zákona o komerční bezpečnosti vyřešenou, jak bude analyzováno v dalších kapitolách. Praktický rozdíl se pak odráží v profesionalitě bezpečnostních agentur. Zásadní dokument současné doby, tedy živnostenský zákon byl sice několikrát pozměněn během let, ovšem bez výrazných změn na funkci a strukturu SBS. To samé platí pro zákon o obsahových náplních jednotlivých živností, kde proběhla snaha o aktualizaci ve jménu stanovení minimálních standardů pro fungování bezpečnostních agentur. Opět bez výraznějšího úspěchu. Rešerše aktuálního právního rámce ve vztahu k funkci SBS dokazuje nedostatečnost a legislativní roztržičnost komerčního bezpečnostního prostoru.

2.1.2 Profesní sdružení soukromé bezpečnosti v České republice

V ČR v současnosti neexistuje zákonem zřízená profesní komora pro oblast soukromé bezpečnosti. Přesto však působí několik profesních sdružení a asociací, jak bylo výše již zmíněno, které se věnují zastupování zájmů bezpečnostních agentur a pracovníků, ovlivňují do jisté míry návrhy legislativy, podílí se na vzdělávání a rozvoji oboru a podporují etické a odborné standardy.

Unie soukromých bezpečnostních služeb České republiky (USB ČR) patří k nejvýznamnějším oborovým sdružením. Reprezentuje SBS vůči veřejné správě, podílí

se na připomínkování legislativních návrhů a podporuje profesní standardy. Zajišťuje odborná setkání a spolupracuje s Ministerstvem vnitra [26].

Asociace technických bezpečnostních služeb Grémium Alarm (AGA) sdružuje především firmy zaměřené na elektronické zabezpečovací systémy (EVS – elektronické zabezpečovací systémy, CCTV – closed circuit television (kamery), PZTS – požární a tísňové systémy). Spolupracuje s PČR, MV a dalšími subjekty na zvyšování kvality v oblasti technické bezpečnosti [27].

Česká komora detektivních služeb (ČKDS) se specializuje na oblast detektivních služeb a poradenské bezpečnostní činnosti. Sdružuje detektivní kanceláře i jednotlivce a podporuje etiku a kvalitu v tomto specifickém segmentu bezpečnosti [28].

Komora podniků komerční bezpečnosti ČR (KPKB ČR) je profesní sdružení, které usiluje o zvyšování odborné úrovně a etiky v oboru. Zapojena je do legislativních konzultací i vzdělávacích aktivit [29].

2.1.3 Historický exkurz a geneze návrhů zákona o soukromých bezpečnostních službách

Od roku 1993 bylo v ČR předloženo několik návrhů zákona o SBS. Každý návrh se snažil zavést právní rámec pro činnost SBS, specifikovat podmínky odborné způsobilosti a bezúhonnosti pracovníků a definovat systém licencování a dozoru. Přestože některé návrhy prošly vládou, žádný z nich nebyl dosud přijat jako zákon. Hlavními důvody byly politické neshody či obavy z privatizace bezpečnosti [30].

Již v začátcích komerční bezpečnosti v ČR byl vydán návrh zákona „Zákon o provozování SBS a obdobných činností“, který proběhl v roce 1993. Tento zákon by případně shrnoval činnosti bezpečnostních agentur a rozděloval je do několika kategorií, mezi které patřily hlídací služby zaměřené na ochranu majetku na veřejně přístupných i jiných místech, při přepravě, ochraně osob, zajišťování pořádku na akcích a provoz ústředí zabezpečovacích systémů, tedy pulty centrální ochrany. Detektivní služby by se pak věnovaly vyhledávání osob a majetku, získávání důkazů, informací o osobním stavu a odhalování jednání ohrožujících obchodní tajemství. Technické služby zahrnovaly vývoj, instalaci, údržbu a opravy technických zabezpečovacích systémů. Součástí bezpečnostních prostředků byly také věcné prostředky, včetně zviřat, které mohou sloužit k ochraně, a další technická zařízení využívaná při fyzické ostraze nebo pátrání. Fyzická ostraha pak představuje přímý výkon ochrany na určeném místě, zatímco pátrací činnost se zaměřuje výhradně na vyhledávání osob.

Dlouhodobé nepřijetí konečné právní úpravy pro soukromý bezpečnostní sektor se obecně dává za vinu parlamentu, který vnímá tento sektor jako běžnou podnikatelskou činnost, a proto ho nechává pod živnostenským zákonem [5].

2.1.3.1 Návrh zákona o soukromých bezpečnostních službách z roku 2012/2013

Další pokus o legislativní zakotvení činnosti soukromých bezpečnostních služeb proběhl v letech 2012 až 2013. Ministerstvo vnitra připravilo návrh, jehož hlavním cílem bylo definovat podmínky pro výkon činnosti, zejména požadavky na odbornou způsobilost, bezúhonnost a fyzickou způsobilost zaměstnanců. Součástí návrhu byly i ustanovení o povinné registraci a základním dozoru nad těmito službami. Po připomínkovém řízení byl však návrh stažen a přepracován, především kvůli rozporům ohledně rozsahu pravomocí a regulace trhu [30,31].

2.1.3.2 Návrh zákona o soukromých bezpečnostních službách z roku 2015

Tento návrh zákona řeší tři základní oblasti:

1. Podmínky podnikání v oboru bezpečnostní činnosti.
2. Podmínky výkonu některých bezpečnostních činností pro vlastní potřebu.
3. Působnost Ministerstva vnitra a dalších orgánů vykonávajících státní správu na úseku bezpečnostní činnosti.

V první zmíněné oblasti dochází k optimalizaci nabízených služeb jak z pohledu kategorizačního, tak obsahového. Nově dělí nabízené služby do pěti kategorií:

1. Ostraha osob a majetku
2. Činnost soukromých detektivů
3. Převoz hotovosti a cenin
4. Technická služba k ochraně osob a majetku
5. Bezpečnostní poradenství [32].

Druhá oblast, tedy podmínky výkonu některých bezpečnostních činností pro vlastní potřebu, řešila zejména problematiku současného stavu založeného na živnostenském zákoně. Tedy podmínkou pro soukromě bezpečnostní činnost je zisk koncese. Dle tohoto návrhu zákona by změna spočívala v nutnosti zisku autorizované licence od Ministerstva vnitra. Tento model byl inspirován zahraniční praxí a rozhodně by vedl k navýšení profesionality bezpečnostních agentur, jelikož návrh zákona by stanovoval i přesná kritéria pro splnění k zisku zmíněné licence. Dále z výše uvedeného plyne, že ačkoliv působí SBS v segmentu vnitřní bezpečnosti

státu a veřejného pořádku, mají značně omezené možnosti v případě zásahu navzdory svému speciálnímu vybavení a „lidským možnostem“. Tento návrh zákona tuto okolnost nijak zásadně nemění. Jediný celkem zásadní poznatek plynoucí z návrhu je skutečnost, že by koordinačně-kontrolní roli plnilo ministerstvo vnitra skrze PČR. Nová možnost nutící bezpečnostní agentury fungovat v řekněme profesionálnější módou jsou sankce udílené ministerstvem vnitra na popud PČR v případě zjištěných nesrovnalostí či nedodržování závazků soukromými subjekty daných případným zákonem. Nedílnou součástí vykonávání soukromé bezpečnostní praxe jsou fyzické a psychologické podmínky k přijetí potenciálních pracovníků [33,34].

2.1.3.3 Návrh zákona o soukromých bezpečnostních službách z roku 2020

Další návrh zákona o SBS byl předložen v roce 2020. Tento návrh rozšířil dosavadní úpravy a definoval šest hlavních licencovaných činností: ochranu osob, ochranu majetku, přepravu hotovosti a cenností, provozování bezpečnostních technologií, detektivní služby a bezpečnostní poradenství. Návrh obsahoval také přísnější požadavky na kvalifikaci a bezúhonnost pracovníků a počítal s vytvořením samostatného registru těchto komerčně-bezpečnostních subjektů. Přestože návrh získal podporu vlády, nebyl projednán v Poslanecké sněmovně a legislativní proces opět skončil bez výsledku [31].

2.1.3.4 Návrh zákona o soukromých bezpečnostních službách z roku 2024

Poslední návrh zákona o soukromých bezpečnostních službách v České republice pochází z roku 2024. Tento návrh připravilo Ministerstvo vnitra ČR a měl by být předložen vládě v září 2024. Nový zákon měl vstoupit v platnost v lednu 2025, v případě schválení. Tento zákon má za cíl regulovat činnost soukromých bezpečnostních služeb, stanovit minimální standardy pro bezpečnostní pracovníky i firmy a zlepšit spolupráci mezi státními složkami a komerčními bezpečnostními službami [35].

Hlavní body posledního návrhu zákona o SBS, který byl připraven Ministerstvem vnitra a předložen vládě, jsou následující:

Kategorizace licencí: Nový zákon stanovuje šest typů licencí pro různé druhy bezpečnostní činnosti:

Licence skupiny A: Ochrana osob a majetku.

Licence skupiny B: Ochrana majetku ve zvláštních případech.

Licence skupiny C: Služba soukromého detektiva.

Licence skupiny D: Převoz hotovosti, cenin a cenných předmětů nad 5 milionů Kč.

Licence skupiny E: Technická služba k ochraně osob a majetku.

Licence skupiny F: Bezpečnostní poradenství.

Kvalifikační předpoklady: Pro výkon bezpečnostní činnosti budou stanoveny požadavky na věk, odbornou způsobilost, bezúhonnost, bezdlužnost a zdravotní způsobilost, pokud to konkrétní činnost vyžaduje. Zvláštní pozornost bude věnována fyzické zdatnosti zaměstnanců u určitých činnostech.

Právní rámec pro soukromé detektivní služby: Zákon vymezuje, jaké osobní údaje mohou soukromí detektivové zpracovávat, aby byla zajištěna ochrana soukromí a osobnosti sledovaných osob.

Regulace technických a praktických postupů: Stanovení jasných pravidel pro výkon jednotlivých druhů bezpečnostních služeb ve vztahu k osobám a místům, včetně tzv. „měkkých cílů“ a kritické infrastruktury. Zákon také zahrnuje postupy pro zvládání mimořádných událostí

Ochrana zákazníků: Provozovatelé budou mít omezenou volnost v uzavírání smluv, což má zajistit ochranu zákazníků a zabránit tomu, aby soukromé bezpečnostní služby mohly pracovat „proti“ svým klientům.

Prověрка a evidence subjektů: Nová právní úprava zajistí centrální evidenci subjektů působících v oblasti komerční bezpečnosti, což umožní lepší přehled a kontrolu nad jejich činnostech [36, MVČR].

Vlastní shrnutí

Kapitola geneze zákona o SBS ukazuje vývoj návrhů samostatného právního dokumentu k bezpečnostním agenturám v ČR. Je patrné, že jednotlivé návrhy a pokusy o jejich zavedení v dobách vydání odrážely mezinárodní, zejména evropskou situaci a chtěly se přiblížit k těmto modelům. Naneštěstí, politická neochota, nedostatek financí či lobby nikdy nedovolily vzniknout samostatnému zákonu, včetně poslední verze z roku 2024, která měla vejít v platnost po odložení na začátku roku 2025. Tento krok byl opět odložen z důvodu nedostatku financí. Nadále tak zůstává prostor tento poslední návrh diskutovat a navrhnout efektivnější skladbu problematiky i ve vztahu k ochraně měkkých cílů. Co lze však z tohoto návrhu zákona považovat za inspirativní, je kategorizace licencí k nabízeným službám SBS, které se stanou součástí navrhované metodiky hodnocení měkkých cílů za následného využití SBS k jejich ochraně.

2.2 Charakteristika měkkých cílů

Kapitola v odborné příručce, kterou napsal přední odborník na terorismus A. Schmid, poskytuje konceptuální rámec ochrany MC na globální úrovni. Klíčová je analýza, proč jsou MC stále častěji terčem útoků (trend nárůstu útoků tzv. osamělých aktérů na snadno zranitelná místa apod.). MC hrají významnou roli v bezpečnostním prostředí, protože představují místa s vysokou koncentrací lidí, která jsou relativně snadným cílem pro různé druhy útoků či narušení. Tato místa nejsou obvykle vybavena stejnou úrovní bezpečnostních opatření jako klíčové infrastruktury nebo vládní budovy, což je činí zranitelnějšími [37,38].

Celá problematika MC je již delší dobu diskutovaným tématem v oblasti bezpečnosti. Základním problémem je široké spektrum samotného významu pojmu. Jednotná definice není dána, důležité jsou podmínky k naplnění významu měkkého cíle. Jedná se tedy o objekt nebo prostor s významným počtem osob a vůči tomu neúměrně nízkou mírou zabezpečení [39].

Z tohoto základního vymezení významu lze logicky odvodit vhodnost MC k potenciálním útokům. Důvody takového útoku mohou být již různorodé (teroristický, organizovaný zločin, útok osamělého vlka, útok ve jménu radikalizace či extremismu atd.), přičemž společným jmenovatelem bude demonstrativnost takového útoku. Na MC dokáže útočník největší slabost svého protivníka, je schopen za nízké nákladnosti a vcelku jednoduché proveditelnosti způsobit významné škody, a hlavně upoutat na sebe pozornost ve jménu sdělení svého poselství. Opakem MC jsou pak tvrdé cíle, tedy „hard targets“, které naopak oplývají vysokou mírou zabezpečení, kterými jsou dobře chráněné a střežené objekty (například některé státní objekty, vojenské objekty, objekty bezpečnostních složek, ale i některé dobře chráněné či střežené nestátní či komerční objekty) [40,41].

Jak již bylo uvedeno, MC neboli „soft targets“, obecně označujeme otevřené prostranství nebo uzavřené prostory či jiná prostředí, na která má veřejnost volný přístup, a která mohou být vzhledem k vysoké koncentraci osob zde se pohybujících označena za potenciálně vhodný cíl útočníků či teroristů. Je nutné zdůraznit, že ochrana MC spočívá v ochraně osob, kteří jsou právě cílem páchaného násilného útoku. Útokem na ně lze snadno způsobit vysoký počet obětí na zdraví a životech a tím také přitáhnout mimořádnou pozornost veřejnosti a médií, a tak velmi efektivně způsobit negativně na psychiku obyvatel [42].

Mezi měkké cíle lze všeobecně zařadit:

- Bary, kluby, diskotéky, restaurace a hotely;

- kina, divadla, koncertní sály, zábavní centra;
- komunitní centra;
- kulturní, sportovní, náboženské a další akce;
- náboženské památky a místa určená k uctívání;
- nákupní centra, tržiště a obchodní komplexy;
- nemocnice;
- parky a náměstí;
- politická shromáždění, průvody, demonstrace;
- sportovní haly a stadióny;
- školská zařízení, koleje, menzy, knihovny;
- turistické památky a zajímavosti, muzea, galerie;
- veřejné instituce;
- významné dopravní uzly, vlaková a autobusová nádraží, letištní terminály;
- jiná symbolicky významná místa či akce atd. [43,44].

Dle výčtu některých MC vyplývá další z problémů této kategorie, a to sice že je jejich provozovatelem velmi často soukromý subjekt. Zde vzniká otázka, zda vůbec a do jaké míry může stát ovlivnit bezpečnost těchto objektů. Dále je z výčtu evidentní ojedinělost každého měkkého cíle. To znamená, že každý prvek musí být zvlášť analyzován a zabezpečen vzhledem k jeho funkci a systému jako takového, který má oproti ostatním MC odlišná a svá specifická slabá místa [45].

Atraktivitu měkkého cíle pro útočníky mohou zvyšovat tato kritéria:

- Otevřenost pro veřejnost;
- přítomnost a kvalita bezpečnostního personálu;
- množství a koncentrace osob;
- přítomnost PČR nebo obecní (městské) policie;
- přítomnost médií;
- symboličnost cíle.

Dle druhu útočníka se liší i konkrétní MC. Pro útoky teroristické budou vhodnější cíle s vysokou symbolikou, pro osamělého vlka zase ty, kde bude vysoký počet lidí a přítomnost médií apod. Společnou vhodnou vlastností je však zpravidla volný přístup. Podle formy zvoleného útoku mohou útočníci snadno vstoupit do prostor, kde splynou s davem a je značně složitá předběžná identifikace hrozícího chování nebo útoku. V současné době je tak na jednotlivých provozovatelích těchto prostor a objektů, aby měli zájem na co možná nejvyšším zabezpečení. Celý systém ochrany MC v ČR je založen hlavně na zájmu, spolupráci a výměny informací mezi sférou státní a nestátní. Snaha ČR je nějaký fungující model vytvořit převážně na principu prevence, a tak jednotlivé MC „zodolňovat“. Bohužel však na své snahy nenavázala novou aktualizací Koncepce ochrany měkkých cílů pro roky 2017-2020 [39].

2.2.1 Kategorizace typů útoků na měkké cíle

Pro potřeby výstupů disertační práce v podobě vlastní metody hodnocení rizikovosti MC je potřeba vydefinovat typy útoků na tyto objekty a prostředí. Ideální se jeví rozdělení z metodiky Vyhodnocení ohroženosti měkkého cíle, která definuje typologii hrozeb takto:

Hrozby pro měkké cíle:

1. Násilníci zapojení do klasické kriminální činnosti;
2. psychicky nemocné osoby;
3. mstící se zaměstnanci nebo klienti;
4. skupiny organizovaného zločinu;
5. extremisté a osoby útočící z nenávisti (útočníci páchající tzv. hate crime);
6. teroristé [44].

Způsoby útoku na měkké cíle:

1. Napadení chladnou zbraní (bodné, sečné, tupé apod.);
2. napadení střelnou zbraní (krátkou, dlouhou);
3. žhářský útok;
4. braní rukojmí a barikádová situace;
5. napadení měkkého cíle davem (násilná shromáždění);
6. útok nájezdem vozidla do lidí;

7. jedovatá látka v poštovní zásilce;
8. nastražení imitace výbušniny;
9. falešné oznámení umístění výbušniny (popř. jiných nebezpečných látek);
10. výbušnina v zaparkovaném vozidle;
11. umístění výbušniny do určitého prostoru (bez přítomnosti útočníka, např. odložené zavazadlo);
12. únos osoby;
13. fyzické napadení v blízkém okolí objektu (zejména napadení osob atraktivních pro útočníky svou symbolikou);
14. verbální agrese (jednotlivce či skupiny) s hanlivými prvky a potenciálem přerůst do fyzického násilí v blízkém okolí objektu;
15. sebevražedný útok s použitím výbušniny;
16. nájezd vozidla s výbušninou se sebevražedným útočníkem [44].

Tato kategorizace typů útoků i jejich potenciálních původců poukazuje na možné slabiny v ochraně MC. Dalším podnětem může být pouhá poplašná zpráva. Aby mohl být útok realizován, útočník musí nejprve překonat fyzické nebo technické bariéry, ať už formou průchodu přes pasivní překážku, nebo prostřednictvím dopravního prostředku umožňujícího rychlý průnik do cílové oblasti. Zároveň je možné identifikovat samotné nositele hrozeb, mezi které patří jak psychicky narušené osoby, tak organizované skupiny s teroristickým či kriminálním pozadím. Tento přehled podtrhuje nutnost víceúrovňového přístupu k zabezpečení a prevence, který dokáže reflektovat co nejvyšší rozsah hrozeb.

2.2.2 Strategické a metodické rámce ochrany měkkých cílů v České republice

Základním dokumentem pro kategorii měkkých cílů v ČR je výše zmíněná Koncepce ochrany měkkých cílů 2017-2020. Ta uvádí, že ačkoli není ČR primárním terčem útoků teroristických či jinak významných ve světovém měřítku, musí se aktivně připravovat a navyšovat svou ochranu s proměňujícím se bezpečnostním prostředím jako takovým. Vyšší pozornost je pak právě věnována objektům s nízkou mírou zabezpečení vůči významné koncentraci osob. Zásadní důvod vzniku dokumentu bylo přijetí usnesení vlády č. 711 k Protiteroristickému balíčku. Cílem dokumentu je pak vytvořit ucelený systém ochrany a reakce aparátu soukromého i státního na případná ohrožení.

V současnosti neexistuje v ČR jednotný právní předpis, který by komplexně a závazně upravoval ochranu MC a stanovil jasné povinnosti jejich provozovatelům nebo státním orgánům. Ochrana je řešena spíše prostřednictvím strategických, metodických a technických dokumentů, které mají převážně doporučující charakter. Jedním ze základních rámcových dokumentů je Bezpečnostní strategie České republiky (2023), která definuje základní bezpečnostní zájmy státu a reaguje na aktuální světové a domácí bezpečnostní hrozby. Ačkoliv zde nejsou MC explicitně zmíněny jako samostatná kategorie, jejich ochrana je obsahově zahrnuta v rámci ochrany obyvatelstva, boje proti terorismu a zajištění vnitřní bezpečnosti [46,47].

Na tuto strategii navazuje Audit národní bezpečnosti (2016), který zpracovala vláda ČR jako odpověď na měnící se bezpečnostní prostředí. Audit identifikuje klíčová slabá místa v systému bezpečnosti, včetně nedostatečné připravenosti na asymetrické hrozby a potřeby zlepšení ochrany veřejných prostor, tedy typických MC [6].

Ministerstvo vnitra dále vytvořilo několik standardizačních a metodických dokumentů, které poskytují návod, jak k ochraně MC přistupovat. Patří mezi ně zejména dokumenty jako například metodika Základy ochrany měkkých cílů nebo sektorové metodiky pro specifické typy objektů, např. školy, nemocnice nebo obchodní centra. Tyto materiály jsou však nezávazné a mají pouze doporučující charakter, což je významná mezera v této problematice [44].

I státní normy mohou naplňovat funkci opory pro ochranu MC, i když jen okrajově. Příkladem je technická norma ČSN 73 4400:2016, která se zaměřuje na řízení bezpečnosti při plánování, realizaci a užívání školských zařízení. Tato norma poskytuje konkrétní technická a organizační doporučení pro zvýšení bezpečnosti škol, které jsou typickým příkladem MC [48].

V širším kontextu má vliv také evropský právní rámec, zejména v oblasti veřejného varování a krizové komunikace. Směrnice jako European Electronic Communications Code (EECC) požadují zavedení systémů veřejného varování obyvatelstva (např. Reverse 112), které mohou sehrát významnou roli při ochraně měkkých cílů před hrozbami. Tento model však není v ČR systémově zaveden a toto téma bude diskutováno v návrhové části práce [49].

Vlastní shrnutí

Tato kapitola shrnuje základní principy problematiky MC. Zásadní je opět skutečnost, že stejně jako SBS je legislativní opora nedostatečná, respektive v oblasti MC naprosto absentuje. Jak je v kapitole analyzováno, existuje několik doporučujících dokumentů či doktrinálních zdrojů v ČR, které se problematiky MC a jejich ochrany přímo či nepřímo dotýkají. Konkrétní zákony však zcela chybí. Dle významu, povahy MC je zřejmé, jak důležité je zajistit jejich ochranu komplexně, což je pro státní aparát velice široký a drahý úkol. Je třeba podotknout, že ČR je jedna z posledních států EU, který nemá problematiku MC zakotvenou legislativně. Proto není ani nijak vynutitelné, aby byly tyto objekty metodicky chráněny anebo musely splňovat specifické povinnosti.

2.2.3 Modely ochrany měkkých cílů ve světě ve veřejně-soukromé spolupráci

Existují různé druhy spolupráce mezi veřejným a soukromým sektorem v ochraně MC. Jedná se zejména o modely komunikace mezi objekty spadajícími do této kategorie a státními bezpečnostními orgány, případně mezi jednotlivými provozovateli MC vzájemně k výměně zkušeností a navýšení bezpečnosti. Pro možný další rozvoj v ČR, nutno říci, že mimo „dobrovolnickou“ komunikaci mezi vrcholnými a bezpečnostními managementy jednotlivých provozovatelů, například zdravotnické provozy či obchodní řetězce v různých regionech (na bázi níže popsané horizontální spolupráce) jiné další formy absentují. Tyto příklady navýšení ochrany MC na bázi komunikace, sdílení zdrojů a vzájemnou přípravu na možná ohrožení mohou být inspirací pro český segment MC do budoucna [49,50].

2.2.3.1 Veřejno–soukromé partnerství

Public–private partnership (dále PPP) představuje model spolupráce mezi veřejným a soukromým sektorem v oblasti ochrany MC, který kombinuje jejich zdroje, odborné znalosti a provozní kapacity. Zahrnuje sdílení informací o hrozbách, společná školení a cvičení, koordinovanou prevenci a reakci na incidenty, jakož i sdílení technických prostředků. PPP dále napomáhá vytváření právního rámce a posiluje bezpečnostní povědomí veřejnosti. Významnou roli v systému hrají právě provozovatelé MC, kteří nesou odpovědnost za zavádění opatření napřímo [50].

Propojení různých zdrojů, odborných kapacit a provozních možností přispívá k vytváření základního bezpečnostního systému. Evropská unie tento přístup dlouhodobě podporuje jako funkční doplněk k bezpečnosti státní zajišťující veřejnou bezpečnost. Hlavní úlohu

v tomto procesu zastávají právě samotní provozovatelé a vlastníci MC, kteří nejlépe znají specifika svých objektů a zároveň nesou odpovědnost za realizaci vhodných preventivních opatření [43,51,39].

Například studie Evropské komise k ochraně veřejných prostor klade důraz na nutnost koordinovaného sdílení informací mezi soukromými aktéry a orgány veřejné správy. Zajištění kyber-fyzické integrace, tedy propojení fyzických bezpečnostních opatření s digitálními systémy je dle této studie označováno jako hlavní výzva pro budoucí PPP modely v MC [52].

PPP v oblasti ochrany měkkých cílů se v různých státech uplatňuje v odlišných podobách. Francie nabízí model kombinující státní dohled s výkonnou rolí soukromých subjektů. Tamní orgán CNAPS (Conseil National des Activités Privées de Sécurité – Národní rada pro soukromé bezpečnostní činnosti) uděluje licence a dohlíží na činnost bezpečnostních agentur, přičemž samotná odpovědnost za zajištění bezpečnosti při hromadných akcích spočívá na organizátorech, kteří využívají služeb SBS. Tento model bude v práci dále rozebírán. Ve Velké Británii zase vznikají metodiky pro ochranu veřejných prostranství a připravuje se legislativa známá jako „Martyn’s Law“, která zavede povinnost vypracovat bezpečnostní plán pro určité objekty a akce. Policie aktivně spolupracuje se soukromým sektorem na školeních, simulacích a krizovém plánování [43,53].

V Německu je zase běžná operativní spolupráce měst a bezpečnostních služeb, například prostřednictvím delegování pravomocí na SBS v ochraně veřejných prostor, zejména večer nebo při kulturních akcích, a to na základě zákonného rámce (§34a Gewerbeordnung), který bude v práci dále detailněji rozebírán u komparace s německým modelem.

Ve Spojených státech je spolupráce postavena především na výměně informací, bezpečnostním povědomí veřejnosti a podpoře prostřednictvím SAFETY Act, který chrání soukromé provozovatele aplikující schválené bezpečnostní technologie. V Nizozemsku je ochrana MC součástí konceptu „community policing“, kdy policie, místní podnikatelé, občané a SBS tvoří lokální bezpečnostní síť s důrazem na prevenci. Finsko zase nabízí hybridní model, ve kterém mají SBS přímý statut podpůrných složek při mimořádných událostech. Bezpečnostní opatření jsou zde jasně definována zákonem a spolupráce s policií se týká nejen reakcí, ale i plánování a školení. Vybrané fungující evropské modely budou předmětem komparace v analytické části práce, nicméně model PPP s globálně jeví jako fungující preventivní opatření v ochraně MC [51].

Článek napsaný experty z ASIS a policejních asociací shrnuje přínosy PPP v oblasti bezpečnosti z globální perspektivy. Policie často trpí rozpočtovým a personálním omezením, zatímco trh soukromé bezpečnosti globálně roste. PPP umožňují spojit kapacity obou sektorů, např. soukromá bezpečnost může poskytnout další vycvičené osoby, technologie, a finance. Studie citovaná v tomto článku ukázala, že PPP v bezpečnosti vedou ke zvýšení efektivity a inovacím, primárně díky sdílení zpravodajských informací a osvědčených postupů. Policie se tak dostane k detailním znalostem bezpečnostních rizik ve firmách a komerční sféře obecně,

a naopak firmy získají lepší přehled o hrozbách. Společné projekty pak (např. společné hlídky, bezpečnostní akce apod.) zvyšují důvěru veřejnosti. PPP se osvědčily při teroristických útocích např. při níže v práci zmíněném bombovém útoku na maraton v Bostonu (2013), kde spolupráce policie a privátních bezpečnostních týmů v okolí pomohla rychle zareagovat a dopadnout pachatele [54].

2.2.3.2 Horizontální spolupráce mezi subjekty měkkých cílů

Jednou z alternativních forem k PPP je horizontální spolupráce, která se odehrává přímo mezi jednotlivými subjekty MC, jako jsou obchodní centra, kulturní instituce nebo zdravotnická zařízení. Tato spolupráce spočívá ve výměně informací, sdílení scénářů hrozeb a osvědčených postupů proti nim. Horizontální spolupráce je efektivní zejména v rámci lokálních bezpečnostních seskupení, kde jednotlivé subjekty nacházející se v blízkosti spolupracují bez nutnosti zásahu státu [55,56].

2.2.3.3 Asociativní a sektorové platformy

Další formou je spolupráce v rámci profesních asociací nebo sektorových platform. V tomto případě se subjekty MC sdružují podle odvětví, například v dopravě, zdravotnictví nebo kultuře. Tyto platformy často vytvářejí vlastní bezpečnostní standardy, certifikační procesy nebo doporučené postupy. Zahraničním příkladem je třeba americký sektor zdravotnictví, kde funguje platforma HC3 zaměřená na sdílení kybernetických hrozeb. Tato spolupráce je žádoucí zejména při zaměření na specifická odvětvová rizika a zajištění konzistentní úrovně ochrany [57,58].

2.2.3.4 Multilaterální partnerství

Multilaterální partnerství, označovaná jako PPP+ (rozšíření Public private partnership), představují širší zapojení aktérů, které zahrnuje nejen stát a soukromý sektor, ale také neziskové

organizace, univerzity a další komunitní struktury. Cílem je vytvoření komplexního rámce bezpečnosti, který reflektuje lokální potřeby a zapojuje veřejnost. V USA například fungují tzv. „fusion centers“, které propojují federální a místní složky s komunitami a firmami. V evropském prostoru se tento model uplatňuje zejména v konceptech chytrých měst, kde se při návrhu bezpečnostních opatření zohledňují i sociální a urbanistické stránky [59].

2.2.3.5 Peer-to-peer spolupráce a benchmarking

Zajímavou možností je také peer-to-peer spolupráce, kdy si jednotlivé subjekty vzájemně sdělují zkušenosti, hodnotí své systémy a provádějí benchmarking (porovnávání). Tato forma posiluje kulturu kvality a umožňuje sdílet osvědčené praxe napříč různými segmenty. Existují mezinárodní platformy, jako je například IAVM (International Association of Venue Managers), které sjednocují bezpečnostní standardy pro kulturní a sportovní zařízení zejména v USA. V prostředí MC (zejména kulturních a sportovních událostí) je Peer-to-peer spolupráce často efektivnější než oficiální regulace bezpečnosti. Sdílení zkušeností mezi provozovateli může výrazně urychlit aplikaci osvědčených opatření i bez zásahu státu [60, 61].

2.2.3.6 Komunitně řízená bezpečnost

Komunitně řízená bezpečnost (Community-Based Security) je model, který staví na aktivní roli občanů, zaměstnanců a dobrovolníků. Obce nebo městské části a celá města spolupracují se svými obyvateli, například prostřednictvím školení, dobrovolných hlídek nebo krizových plánů. Tento přístup je založen na důvěře a lokální znalosti prostředí. Jeho hlavním přínosem je prevence a rychlé rozpoznání potenciálních hrozeb [62].

Vlastní shrnutí

Kapitola shrnuje různé druhy spolupráce mezi veřejným a soukromým sektorem v oblasti bezpečnosti. Tyto modely ukazují různorodé přístupy k ochraně veřejných prostor a MC, a mohou sloužit jako inspirace pro budování účinného systému PPP v ČR. Z vlastních zkušeností se v ČR objevuje primárně model komunikace mezi provozovateli MC stejného zaměření, kteří si v rámci svých provozů předávají informace “best practice” k navýšení bezpečnosti viz horizontální spolupráce. Komerčně–státní vztah podtrhuje důraz na vazby obou sektorů a dle předložených modelů také efektivitu a v podstatě nezbytnost k zachování bezpečnosti jako celku. V současné době tyto formy spolupráce v ČR ovlivňuje skutečnost, zda je daný bezpečnostní či vrcholný management provozu (MC) ochoten bezpečnostní problematiku řešit a uvolňovat finance. Dokud bude i tato problematika otázkou financí

a nebude legislativně vyhraněna, jsou tyto typy spolupráce alespoň na komunikační bázi možným řešením ke zvýšení bezpečnosti MC v ČR. Jakou roli v těchto komunikačních uzlech může hrát SBS bude rozebráno v návrhové části práce.

2.2.4 Trendy v ochraně měkkých cílů a inovace pomocí nestandardních prostředků

Nejnovější trendy v ochraně MC se soustředí na různé strategie a technologie k minimalizaci rizik a zvýšení bezpečnosti na veřejně přístupných místech. Navyšování bezpečnosti a odolnosti MC, zejména tedy těch, které jsou tvořené objekty, spočívá primárně ve stavebním z odolňování a instalaci pasivních prvků ochrany. Tento druh ochrany nevyžaduje následnou aktivní obsluhu ze strany zaměstnanců provozů či jiných osob. Na druhou stranu taková instalace pomáhá následně i aktivnímu řešení vzniklých bezpečnostních incidentů, například v případě pasivních blokových překážek před objekty, kdy tyto získávají čas včasné detekci před případným útokem s použitím automobilu. Níže jsou definovány některé moderní přístupy k ochraně MC obecně v širším využití.

2.2.4.1 Zpevňování lokalit (Site Hardening)

Dle J. Hastermannové se jedná o zlepšování fyzické bezpečnosti prostřednictvím instalace bariér, kontrolních bodů a bezpečnostních plotů, aby se omezil přístup potenciálním útočníkům a snížilo riziko útoků na MC. Jedná se o důležitou součást vícevrstvého bezpečnostního systému, kdy se pomocí preventivních kroků upravuje prostor tak, aby byl méně atraktivní a méně přístupný pro potenciální útočníky, a zároveň stále přístupný a komfortní pro běžné uživatele (tzv. balance mezi bezpečností a otevřeností).

Mezi klíčové prvky patří instalace fyzických bariér, které brání volnému vjezdu vozidel (např. sloupky, betonové kvádry, hydraulické zábrany) často nasazované u vládních budov, památek nebo na veřejných náměstích. Významnou úlohu sehrává i kontrola vstupů pomocí bezpečnostních rámu, turniketů a systému identifikačních průkazů. Další vrstvu tvoří oplocení, uzamykatelné vstupy a bezpečnostní zámky.

Příkladem může být Londýn po útocích v roce 2017, kde město posílilo fyzickou ochranu pěších zón pomocí ocelových sloupků a mobilních zábran. Podobná opatření byla aplikována i ve Francii na adventních trzích a během Tour de France. Spojené státy zase zavádějí zpevnění pomocí balistických zastávek u školních areálů.

Součástí site hardeningu je i koncept „Crime Prevention Through Environmental Design“ (CPTED), který využívá architektonické a urbanistické nástroje pro snížení kriminality.

Například otevřený výhled z recepcie na vstupní prostor, instalace kamer s dobře viditelnými tabulkami, nasměrování toků lidí do kontrolovatelných zón. Zahrnuje i eliminaci tzv. mrtvých zón (kouty, slepé uličky), lepší osvětlení a zapojení přirozeného dohledu veřejnosti. Příkladem využití CPTED může být letiště Schiphol v Amsterdamu, které po roce 2016 reorganizovalo čekací zóny a odstranilo části, kde mohli lidé stát bez kontroly. Přemístění sedacích souprav a kamerové pokrytí přineslo vyšší bezpečnost bez zásahu do komfortu cestujících.

Přestože každá lokalita vyžaduje individuální přístup, principy site hardeningu mohou tvořit univerzální kostru bezpečnostního plánu. Implementace do prostředí České republiky by měla zahrnovat i participaci soukromých bezpečnostních služeb jako koordinátorů preventivních opatření [43].

2.2.4.2 Technologie pro detekci a reakci

Rozvoj a implementace pokročilých technologií, jako jsou systémy pro rozpoznávání obličejů, kamery s umělou inteligencí a senzory, které mohou detekovat podezřelé chování a hrozby v reálném čase. Možné další využití těchto technologií a vybavení pro zaměstnance SBS bude předmětem návrhové části práce.

2.2.4.3 Ochrana proti výbuchům a útokům s vysokým dopadem

V rámci fyzické ochrany MC představuje prevence a zmírňování důsledků výbuchů zásadní složku tzv. pasivní bezpečnostní infrastruktury. Cílem není jen zabránit samotnému útoku, ale minimalizovat jeho účinky na osoby, infrastrukturu a kontinuitu provozu.

K ochraně objektů před explozemi se využívá kombinace specializovaných stavebních řešení, odolných materiálů a konstrukčních opatření, jejichž cílem je zmírnit účinky následných tlakových vln a poškození. Jedním z nejčastěji používaných prvků je speciální vrstvené zasklení (tzv. blast resistant glazing), například vrstvená skla se speciální fólií, která se při explozi neroztříští na ostré střepy, ale zůstávají celistvá. Takové zasklení je běžně využíváno u budov se zvýšenými bezpečnostními nároky, jako jsou ambasády, vládní instituce nebo letiště. Dalším příkladem jsou energii absorbující fasády, tvořené například vrstvenou ocelí nebo kompozitními panely, které při výbuchu pohlcují část energie a tím napomáhají zabránit zborcení konstrukce. K mechanické ochraně slouží tzv. blast walls, nejčastěji železobetonové bariéry, jež zadržují tlakovou vlnu i rozlétávající se úlomky po výbuchu. Významnou roli sehrávají také tzv. standoff zóny, tedy bezpečnostní odstupy mezi chráněným objektem a veřejným prostorem, které bývají vytvořeny prostřednictvím urbanistických prvků, jako jsou

lavičky, květináče nebo betonové bloky, jejichž smyslem je zamezit přiblížení výbušného zařízení přímo ke konstrukci budovy. V neposlední řadě se u vybraných prostor (například technického zázemí) aplikují i odlehčené střešní systémy, které se při vnitřním výbuchu uvolní směrem ven, čímž dochází ke snížení tlaku redukcí škod uvnitř objektu [63,64,65].

2.2.4.4 Zaměření na otevřené prostory

Zvýšená pozornost na bezpečnost v otevřených prostorech, jako jsou parky a venkovní festivaly, kde je obtížné kontrolovat přístup a pohyb lidí. To zahrnuje lepší monitorování a nasazení mobilních bezpečnostních týmů. Provádí se různé druhy režimových opatření a synchronizovaného postupu bezpečnostních složek [66].

Vlastní shrnutí

Tyto trendy odrážejí rostoucí potřebu adaptace bezpečnostních opatření na dynamické a stále se zesilující hrozby, kterým čelí veřejně přístupná místa. V návaznosti na předchozí kapitoly a celkový záměr práce poukazují tyto trendy (mimo ty, které jsou technického charakteru) na možnost aktivního propojení státního a soukromého sektoru. Nejen vzhledem k využití personálních zdrojů, ale i zajištění efektivnější bezpečnosti komplexně. Tyto organizační přístupy k ochraně MC slouží jako přehled současného stavu a také jako podklad k návrhové části práce, kde budou doplněny o další možnosti přístupů či nová technologická řešení s důrazem na implementaci v podmínkách ČR. Taktéž je tato kapitola důležitá k rozpracování vlastního modelu hodnocení TRS, a to zejména ke stanovení jednotlivých kritérií a jejich hodnotám.

3 CÍLE PRÁCE

Ochrana MC v ČR naráží na absenci systémového ukotvení komerční bezpečnosti do rámce národní bezpečnosti. Současně chybí jednotná metodika pro hodnocení rizik MC s konkrétním doporučením na bezpečnostní opatření ze strany SBS. Vzhledem k těmto zjištěním si disertační práce klade za cíl analyzovat možnosti systémového začlenění SBS do ochrany MC a vytvořit praktický nástroj pro posouzení jejich rizikovosti.

Hlavní cíl práce

- **HC1: Navrhnout rámec řízení rizik měkkých cílů s využitím soukromých bezpečnostních služeb v podmínkách České republiky**

K naplnění hlavních cílů práce je potřeba vytyčit a splnit dílčí cíle práce, které stanoví celkový podklad tématu a zhodnocení aktuálního stavu problematiky. Jedná se zejména o analytickou a návrhovou část práce, které podtrhnou potřeby finalizace hlavního cíle a navrhnou další možné směry komerční bezpečnosti v ČR nejen při ochraně MC.

Dílčí cíle práce

- **DCI: Provést audit současného stavu komerční bezpečnosti a ochrany měkkých cílů v České republice**
- **DCII: Vytvořit genezi návrhů zákona o soukromých bezpečnostních službách v České republice**
- **DCIII: Zpracovat kvantitativní analýzu míry využití bezpečnostních agentur v České republice**
- **DCIV: Komparovat systémy komerční bezpečnosti v České republice a vybraných evropských státech**
- **DCV: Zpracovat SWOT analýzu současného stavu soukromých bezpečnostních služeb při ochraně měkkých cílů v ČR**
- **DCVI: Vytvořit a aplikovat vlastní metodu vyhodnocení rizikovosti měkkých cílů – TRS (total risk score)**
- **DCVII: Navrhnout inovativní prostředky a metody pro vývoj zapojení soukromých bezpečnostních služeb v České republice k ochraně měkkých cílů**

Stanovení výzkumných hypotéz

Na základě vymezených cílů disertační práce a identifikace klíčových tematických problémů byly formulovány výzkumné hypotézy. Tyto reflektují předpokládané vztahy mezi zkoumanými jevy v oblasti komerční bezpečnosti a ochrany MC, přičemž slouží jako výchozí rámec pro empirickou část práce. Stanovené hypotézy umožňují strukturované testování věcných závěrů a napomáhají naplnění a ověření cílů práce.

- **H1: Je současná legislativní opora soukromých bezpečnostních služeb v České republice dostatečná vůči evropskému standardu?**
- **H2: Zapojení soukromých bezpečnostních služeb do systému ochrany měkkých cílů v České republice není efektivní především kvůli absenci jasného legislativního rámce.**
- **H3: Lze vytvořit efektivní metodiku pro hodnocení rizikovosti měkkých cílů, která bude zahrnovat i doporučení pro využití soukromých bezpečnostních služeb ochraně těchto cílů?**

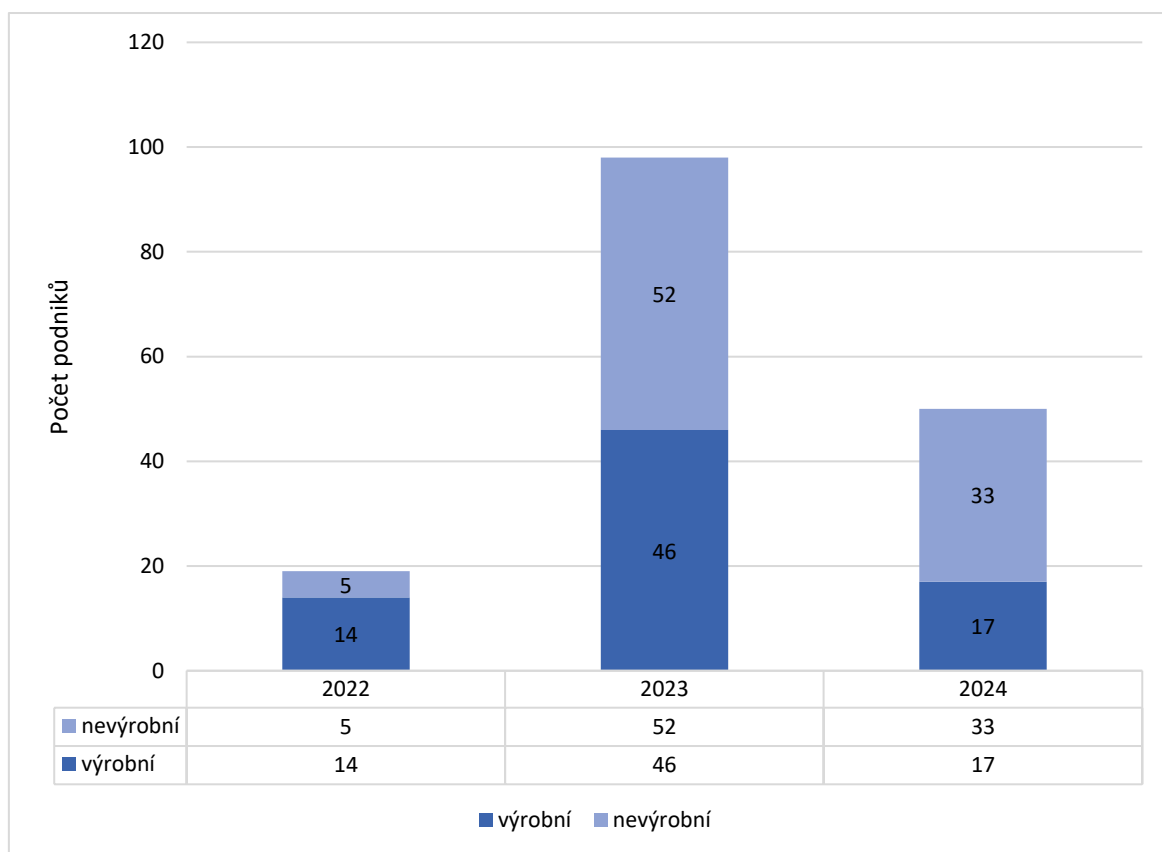
4 ANALYTICKÁ ČÁST

Analytická část práce poskytne některé výstupy poukazující na logický sled kroků v tomto dokumentu k následnému využití v dalších kapitol či do zasazení kontextu a potřeb zvoleného tématu. Cílem této kapitoly je potvrdit nutnost zájmu o komerční bezpečnostní sektor a potřeby je profesionalizace. Tato potvrzení a výstupy pomocí vlastní analýzy dat míry využití bezpečnostních agentur v ČR, statistickými údaji o útocích na MC, a také komparací komerčního bezpečnostního modelu v ČR s vybranými evropskými státy. Výstupy analytické části práce budou taktéž směřovat k modelaci vlastního návrhu metody vyhodnocení rizikovosti MC s následnými doporučenými bezpečnostními opatřeními včetně možností zapojení bezpečnostních agentur a SBS jako celku.

4.1 Analýza využití bezpečnostních agentur v České republice

Jedním z cílů této práce je analyzovat využívání bezpečnostních agentur v ČR, a to na základě vlastní analýzy dat, která zahrnuje 167 subjektů a zaměřuje se na formy jejich spolupráce s nasmlouvanými bezpečnostními agenturami. Sběr dat probíhal v letech 2022-2024. Druhým aspektem zpracování analýzy je získání podkladových dat využitelných v návrhu metody hodnocení rizikovosti MC, kde tyto výstupy mohou na základě reálných dat z terénu poukázat na potřeby soukromého sektoru v zabezpečení. Vlastní výzkum probíhal za laskavé pomoci společnosti RENOMIA, a.s., kde bylo možné v rámci pracovní náplně rizikového inženýra vlastní statistiku provádět. Šetření analyzuje vzorek subjektů, zda a jakou formou využívají služeb komerčních bezpečnostních agentur. Výstupem analýzy je mimo výše uvedené poukázat na nutnost vzniku legislativní opory pro komerční bezpečnost v ČR vzhledem k současnému a v dalších letech pravděpodobnému rozmachu využití SBS.

Mimo výše definované výstupy budou vzorky rozděleny na společnosti a objekty výrobního a nevýrobního charakteru tak, aby se interpretoval důraz na potřeby fyzické ochrany a výši bezpečnosti v těchto dvou analyzovaných sférách. Analyzované subjekty vzhledem k formě výzkumu zůstávají v anonymitě, co je však možné zveřejnit, jsou konkrétní bezpečnostní agentury, které jsou společnostmi využívány.

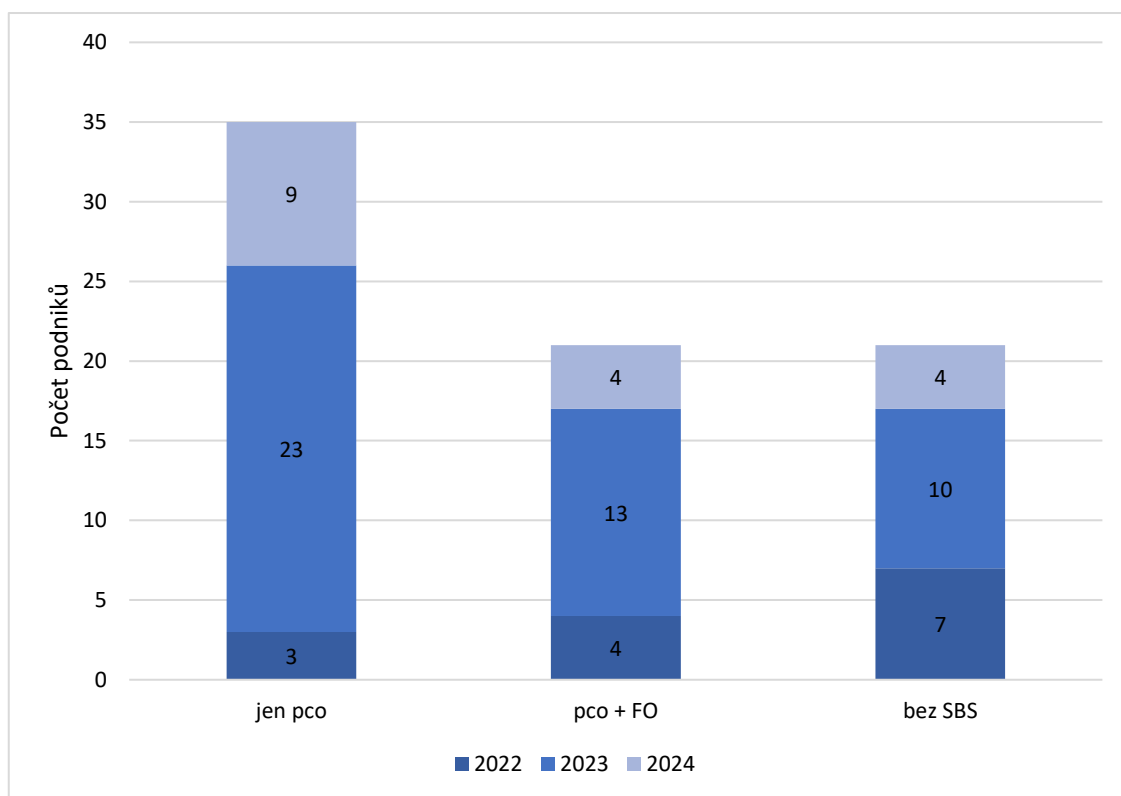


Obrázek 1 - Analyzované podniky za jednotlivé roky (zdroj: vlastní).

Celkem bylo v letech 2022-2024 analyzováno 167 subjektů. Z toho 90 byly podniky výrobního a 77 nevýrobního charakteru v gesci státu či subjekty soukromé. Cílem vlastního výzkumu bylo zjistit míru využívání soukromých bezpečnostních agentur získat tak procentuální obraz o charakteru tohoto propojení s komerční bezpečností.

Zájmovými oblastmi šetření bylo zjištění, zda vůbec subjekt nějakým způsobem využívá služeb SBS. Pokud ano, jakou formou, či je bezpečnost zajišťována pouhým dálkovým napojením na konkrétní bezpečnostní agentury, nebo jsou přítomny fyzické síly v místě poskytování ochrany.

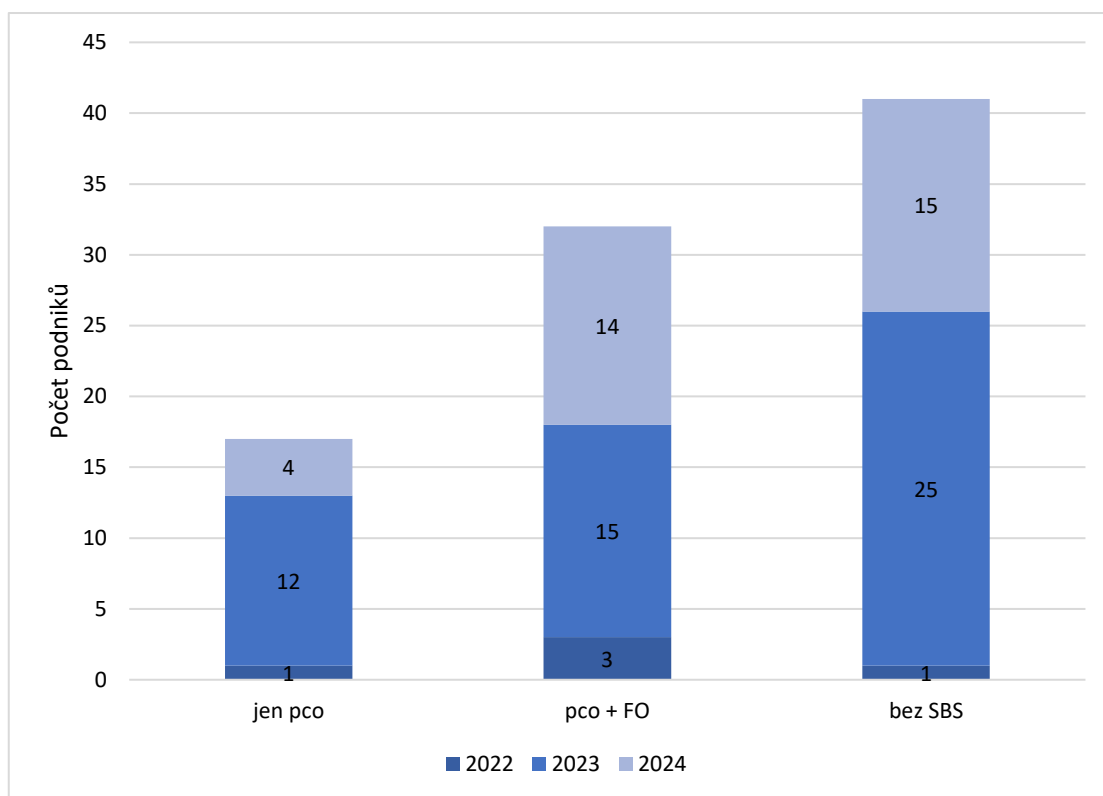
Co se týká struktury analyzovaných subjektů, jedná se o oblasti zemědělství, strojírenství, automotive, dřezpracující průmysl, keramický průmysl. U nevýrobních subjektů se jedná o logistické parky, civilní objekty, zdravotnictví, obchod, školství apod. Na konci této kapitoly budou definovány analyzované objekty, které by naplnily definici měkkých cílů a budou tak definována specifika a formy využití SBS.



Obrázek 2 - Formy využití SBS výrobními podniky v jednotlivých sledovaných obdobích (zdroj: vlastní).

- PCO – Pult centralizované ochrany,
- FO – fyzická ochrana.

Propojení s SBS analyzovaných subjektů výrobního charakteru poukazuje na vyšší míru využití pouhého připojení kamerových a elektronických zabezpečovacích systémů k pultu centralizované ochrany (dále PCO) konkrétních bezpečnostních agentur. Méně výrobních společností pak využívá služeb přítomné fyzické ochrany. Z praktického pohledu je nutné říct, že míra využití s převažujícím formátem samotného napojení na PCO vybraných SBS je dáno nároky pojišťoven jako nutné minimum v oblasti fyzické bezpečnosti k následnému pojistnému krytí. Toto je primární důvod využití SBS v oblasti výrobní soukromé sféry.

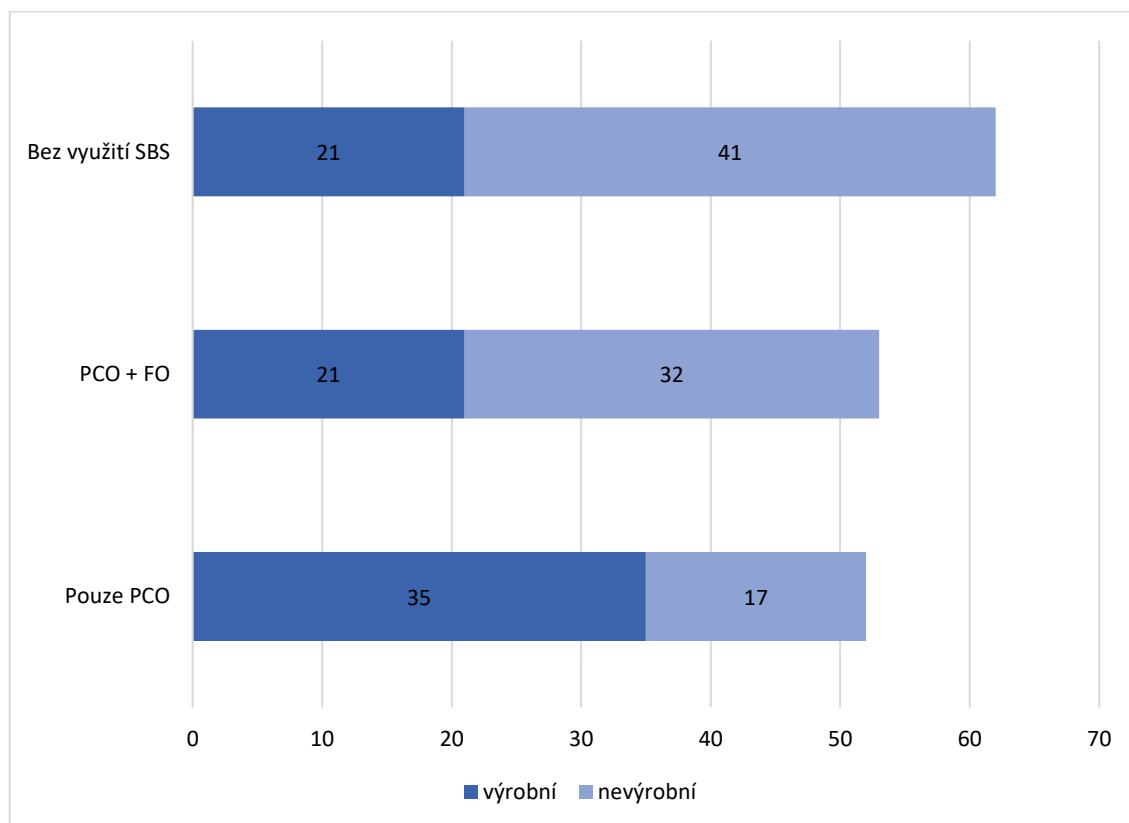


Obrázek 3 - Formy využití SBS nevýrobními podniky v jednotlivých sledovaných obdobích (zdroj: vlastní).

Naopak v oblasti analyzovaných podniků nevýrobních lze spatřit rozdíl v druhu napojení, a to s převažující přítomností fyzických osob z řad zaměstnanců SBS v těchto objektech. Značné množství těchto objektů komerční bezpečnost nevyužívá vůbec. Zde je nutné doplnit, že se jedná jak o objekty a podniky soukromé, tak ty, které jsou v majetku státu.

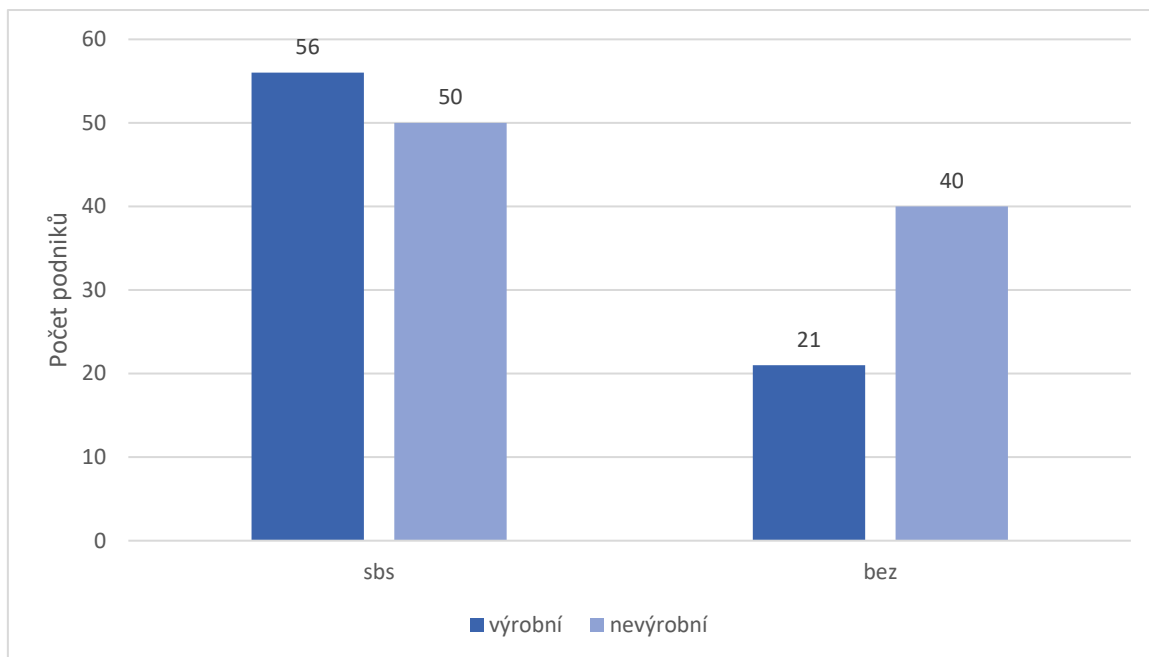
Z těchto nevýrobních objektů je celkem 27 subjektů které spadají do kategorie MC za celé 3 roky provádění statistického šetření. Jedná se o zdravotnická zařízení, školská zařízení, obchodní domy či jiné veřejné objekty. Pro další naplnění cílů práce je nutné konstatovat, že většina těchto objektů služeb komerční bezpečnosti využívá, a to primárně formou fyzické přítomnosti zaměstnanců SBS v místě určení. Výstupy vedou opět k nutnosti profesionalizace, jelikož v současné době plní SBS v těchto místech převážně roli situační prevence.

Následující graf porovnává souhrnné využití SBS mezi výrobními a nevýrobními podniky.



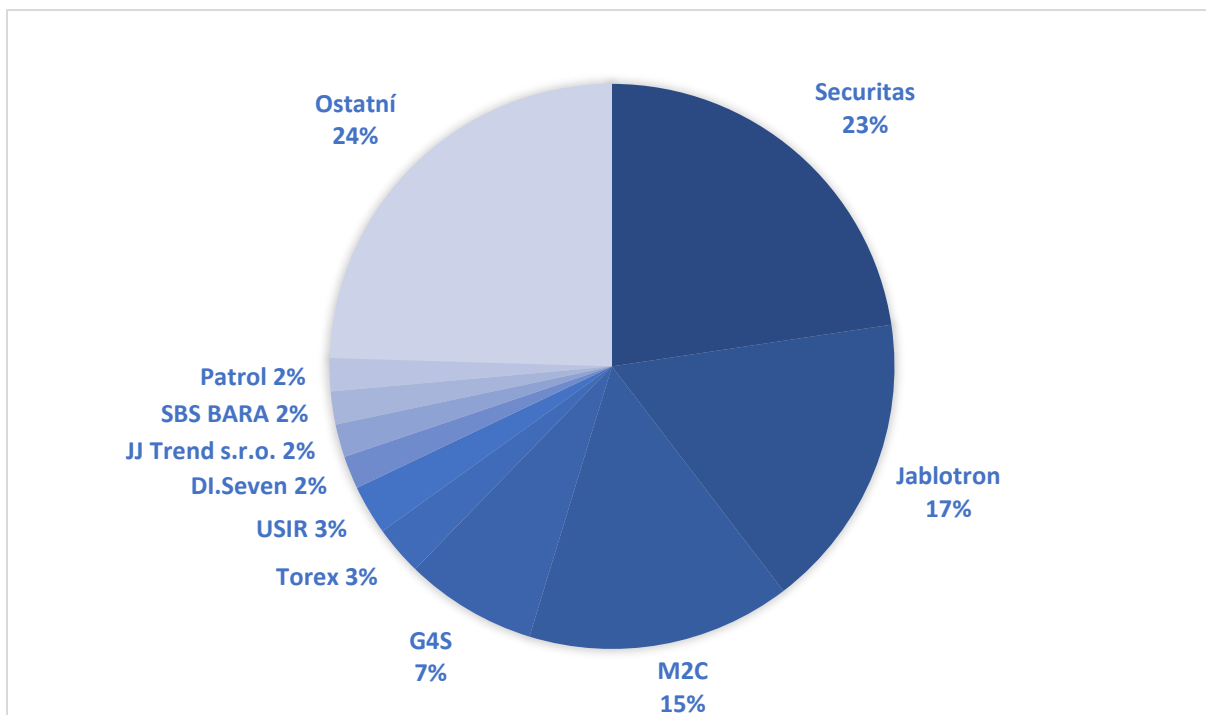
Obrázek 4 - Celkový poměr druhu využití SBS analyzovanými subjekty (zdroj: vlastní).

Dle níže uvedeného rozdílového grafického vyjádření lze konstatovat, že 61 z celkových 167 subjektů nevyužívalo služeb komerční bezpečnosti vůbec. Zástupci subjektů uvádějí jako důvod nevyužití primárně cenu, a pak také prostý nezájem o navýšení bezpečnosti ze strany vrcholného managementu.



Obrázek 5 - Celkový rozdíl ve využití SBS analyzovaných podniků (zdroj: vlastní).

Poslední graf ukazuje procentuální vyjádření v zastoupení nasmlouvaných bezpečnostních agentur u analyzovaných vzorků. Toto zastoupení je také ovlivněno dislokací subjektů, a tedy lokálním působením daných bezpečnostních agentur. Jedná se o lokální služby v daném regionu. Větší bezpečnostní agentury typu Securitas, M2C či Jablotron (zde z pohledu bezpečnostních agentur nutno podotknout, že tato společnost vyvíjí prostředky technické bezpečnosti a z pohledu SBS poskytuje pouze trvalý monitoring) poskytují celoplošnou na území ČR působnost a případně i služby do zahraničí.



Obrázek 6 - Procentuální využití jednotlivých bezpečnostních agentur (zdroj: vlastní).

I přes to, z vlastní analýzy vyplývá, že přes 60 % vzorků z celkového počtu sledovaných subjektů využívá služeb komerční bezpečnosti, což je i za současné absence legislativy a garance kvality poměrně vysoká míra využití. Tato skutečnost opět odvolává na vysoký potenciál bezpečnostních agentur k možnému efektivnějšímu využití případně dokonce dublování činnosti legitimních bezpečnostních orgánů a složek tak, aby byla zajištěna vyšší bezpečnost státu jako celku. V oblasti propojení s ochranou MC se využití soukromých bezpečnostních agentur nabízí jako konkrétní řešení problematiky a toto vlastní statistické šetření na tuto možnost přímo poukazuje a potvrzuje její potřebu.

4.2 Případové analýzy komerční bezpečnosti vybraných evropských států

Státy, které byly do komparace zahrnuty, byly vybrány na základě několika parametrů. Jedná se o Německo, Itálii, Finsko, Slovensko, Nizozemsko a Francii. Všechno jsou to státy v Evropě, které jsou součástí Evropské unie, tedy zavázány shodným vrcholným legislativním rámcům stejně jako ČR. Výčet komparovaných států poukazuje na diverzifikaci v rámci evropského sektoru tak, aby byly porovnány státy přímo sousedící s ČR, zástupce států severských, západních a jižních. Získané parametry budou podkladem pro návrh bodového modelu komerční bezpečnosti v ČR v návrhové části práce.

4.2.1 Soukromá bezpečnostní činnost v Německu

V Německu jsou SBS regulovány především § 34a Zákona o obchodu a průmyslu (Gewerbeordnung), který stanovuje podmínky pro jejich provozování i pro zaměstnance. Pro jejich SBS je nezbytná licence vydávaná místním úřadem, jejíž získání je vázáno na prokázání bezúhonnosti, spolehlivosti a odborné způsobilosti. Ta se ověřuje složením zkoušky před průmyslovou a obchodní komorou, zaměstnanci pak absolvují školení zahrnující právní rámec, bezpečnostní techniky či komunikaci. Provozovatelé i pracovníci musí dále splňovat požadavky na spolehlivost, doložit odpovídající pojištění a dodržovat související právní předpisy, například v oblasti ochrany osobních údajů nebo pracovního práva. Zvláštní úprava se týká i nošení zbraní, které je povoleno jen na základě specifické licence a po přísném výcviku včetně střeleckých zkoušek. Zbraně lze použít pouze k odvrácení bezprostředního útoku a mimo výkon služby musejí být bezpečně uskladněny v souladu se zákonem o zbraních. Dodržování těchto pravidel pravidelně kontrolují místní úřady a jejich porušení může vést ke ztrátě licence či k trestnímu postihu. Tento komplexní rámec má zajistit, že činnost SBS probíhá bezpečně, legálně a s důrazem na vysokou úroveň integrity a spolehlivosti [8,67,68,69,70,71].

Určující legislativa SBS v Německu

- **§ 34a Gewerbeordnung (Zákon o obchodu a průmyslu)** – úprava podmínek licencování a odborné způsobilosti pracovníků [67].
- **Waffengesetz (Zákon o zbraních)** – stanovení pravidel pro držení, nošení a bezpečné nakládání se zbraněmi [71].

4.2.2 Soukromá bezpečnostní činnost ve Francii

Ve Francii je oblast SBS regulována zejména zákonem č. 83-629 o bezpečnostních agenturách (Loi sur les agences de sécurité), který vymezuje podmínky jejich činnosti a licencování. Provozovatelé agentur musejí získat povolení od Ministerstva vnitra, přičemž licenční proces zajišťuje CNAPS (Národní rada pro soukromé bezpečnostní činnosti), což je veřejný administrativní orgán odpovědný také za kontrolu, vzdělávání a standardizaci sektoru. Zákon stanovuje povinnost odborného školení a licenci i pro samotné pracovníky SBS, jejichž činnost je právně omezena zejména při použití síly. Specifická pravidla pro nošení a využití zbraní nejsou v zákoně č. 83-629 detailně upravena, ale v této otázce na něj navazuje Code de la sécurité, který tuto oblast specifikuje. Obecně platí, že ozbrojení mohou být pouze pracovníci, jejichž činnost to vyžaduje (např. převoz hotovosti či ochrana vysoce rizikových

objektů), a to na základě zvláštního povolení prefekta. Povolené jsou zpravidla neletální prostředky nebo vybrané střelné zbraně kategorie B, přičemž vždy je vyžadován speciální státem akreditovaný výcvik zaměřený jak na praktické dovednosti, tak na právní rámec jejich použití [72,73].

Určující legislativa SBS ve Francii

- **Loi n° 83-629 du 12 juillet 1983 (Zákon o bezpečnostních agenturách)** – základní zákon o bezpečnostních agenturách vymezující činnost SBS a podmínky jejich provozování [72].
- **Code de la sécurité intérieure – Livre VI : Activités privées de sécurité (Kodex vnitřní bezpečnosti – Kniha VI: Soukromé bezpečnostní činnosti)** – součást bezpečnostního kodexu, která detailně upravuje pravidla pro licencování, činnost pracovníků SBS a dohled nad sektorem [73].

4.2.3 Soukromá bezpečnostní činnost v Itálii

V Itálii je činnost SBS neboli „vigilanza privata“ regulována zákonem č. 269/2010, který stanovuje organizační a kvalitativní požadavky na fungování těchto služeb a tvoří základní rámec pro jejich činnost. SBS zde vykonávají široké spektrum úkolů, od ochrany osob a majetku, přes zajištění veřejného pořádku a fyzické zabezpečení objektů až po monitorovací a technické služby. Legislativa zároveň ukládá povinnost licencování, pravidelného školení personálu a dodržování právních předpisů v oblasti ochrany soukromí a opět osobních údajů jako u států předešlých. Významným prvkem je úzká spolupráce se státními bezpečnostními složkami, zejména policií a Carabinieri, která se uplatňuje při krizových situacích, ochraně objektů a hromadných akcí, výměně informací i v oblastech, jako je kybernetická bezpečnost či ochrana kritické infrastruktury. Stát zároveň vykonává dohled nad činností SBS a jejich dodržováním stanovených norem.

Zákon č. 269/2010 dále upravuje podmínky používání zbraní. Zaměstnanci SBS mohou nosit zbraň pouze s licenci vydanou příslušným orgánem a po splnění přísných kritérií, mezi něž patří fyzická způsobilost, absolvování specializovaného školení a respektování přísných pravidel používání. Zbraně smějí být využity jen v přesně vymezených případech, jako je oprávněná obrana či ochrana života a majetku klienta. Školení zajišťují pouze akreditovaná pracoviště a zahrnuje právní aspekty, techniku použití zbraní i etiku výkonu služby. Dodržování předpisů

je pravidelně kontrolováno prostřednictvím dohledu, revizí a auditů ze strany státních orgánů, jehož cílem je zajistit vysoký standard bezpečnosti a profesionality tohoto sektoru [74,75].

Určující legislativa SBS v Itálii

- **Decreto del Ministero dell'Interno 1 dicembre 2010, n. 269 – Regolamento recante disciplina delle caratteristiche minime del progetto organizzativo e dei requisiti minimi di qualità degli istituti e dei servizi di vigilanza privata (Nařízení stanovující minimální požadavky na organizační uspořádání a minimální standardy kvality institucí a služeb soukromé ostrahy)** – stanovuje základní požadavky na organizaci, kvalitu a fungování soukromých bezpečnostních služeb [74].

4.2.4 Soukromá bezpečnostní činnost v Nizozemsku

V Nizozemsku je taktéž konkrétní zákon k organizaci SBS, a to zákon o soukromých bezpečnostních organizacích a vyšetřovacích agenturách z roku 1997 (Wet particuliere beveiligingsorganisaties en recherchebureaus), který vymezuje jejich roli, povinnosti a legislativní rámec. Provozování SBS je podmíněno licenci vydávanou Ministerstvem spravedlnosti (Ministerie van Justitie en Veiligheid) a veřejné bezpečnosti, přičemž klíčové požadavky zahrnují finanční stabilitu a odbornou kvalifikaci zaměstnanců. Tyto organizace jsou povinny dodržovat přísné standardy, respektovat práva jednotlivců a chránit osobní údaje opět v souladu s právními předpisy. Zaměstnanci musí absolvovat povinné školení, které zahrnuje právní rámec, etické zásady i technické dovednosti, a jsou oprávněni použít přiměřenou sílu pouze v zákonem vymezených situacích. Zákon rovněž umožňuje úzkou spolupráci SBS s policií, zejména při řešení mimořádných událostí a ochraně veřejného pořádku. Používání zbraní je povoleno jen vybraným pracovníkům na základě zvláštní licence udělované ministerstvem, a to pouze při specifických úkolech, kde je nezbytná ochrana osob či majetku. Podmínkou je absolvování certifikovaného školení a průběžný dohled nad dodržováním stanovených pravidel použití zbraní [76].

Určující legislativa SBS v Nizozemsku

- **Wet particuliere beveiligingsorganisaties en recherchebureaus (Zákon o soukromých bezpečnostních organizacích a vyšetřovacích agenturách)** – základní zákon upravující fungování soukromých bezpečnostních organizací a vyšetřovacích agentur v Nizozemsku [76].

- **Wet wapens en munitie (Zákon o zbraních a municích)** – tento zákon stanovuje podmínky pro držení a používání zbraní, což se přímo týká i zaměstnanců SBS, kteří mohou získat speciální oprávnění k jejich nošení [77].

4.2.5 Soukromá bezpečnostní činnost na Slovensku

Na Slovensku je oblast SBS komplexně upravena zákonem č. 473/2005 Z.z., o poskytování služeb v oblasti súkromnej bezpečnosti. Tento předpis vymezuje formy činnosti soukromého bezpečnostního sektoru, stanovuje podmínky licencování, povinnosti provozovatelů, systém kontrol a rámec kvalifikačních zkoušek. Služby jsou rozděleny na technické (montáž, správa a revize bezpečnostních technologií) a bezpečnostní (převoz hotovosti, strážní a detektivní činnost, školení či poradenství).

Licence k provozování SBS vydávají okresní ředitelství Policie SR a jejich udělení je podmíněno odbornými zkouškami způsobilosti, čímž je zajištěna profesionalita poskytovatelů. Agentury mají povinnost vést podrobnou evidenci zásahů a každoročně podávat zprávu

o činnosti Ministerstvu vnitra SR. Dohled nad kvalifikací a činností zajišťuje vedle Ministerstva vnitra a Policie SR také Úřad súkromých bezpečnostných služieb. Výběr a odborná příprava zaměstnanců podléhá přísným pravidlům; pracovníci, kteří nesplní podmínky, mohou vykonávat jen omezené činnosti. Zvláštní regulace se vztahuje i na detektivní služby, jejichž výkon nesmí porušovat osobní práva sledovaných osob, přičemž zjištěné skutečnosti relevantní pro trestní řízení musí být předány státním orgánům.

Zákon rovněž stanovuje podmínky používání zbraní zaměstnanci SBS. Ti musí mít speciální licenci vydanou Policejním sborem SR, která je časově omezená a vyžaduje složení odborných zkoušek včetně prověření psychické a fyzické způsobilosti. Zbraň lze použít pouze v nezbytných situacích při ochraně života, zdraví či majetku, a to vždy v souladu s právními předpisy. Používání zbraní podléhá pravidelnému dohledu a kontrolám, které mají zabránit jejich zneužívání [78,79].

Určující legislativa SBS na Slovensku

- **Zákon č. 473/2005 Z.z., o poskytování služeb v oblasti súkromnej bezpečnosti a o zmene a doplnení niektorých zákonov** – primární zákon upravující systém fungování SBS na Slovensku [79].

4.2.6 Soukromá bezpečnostní činnost ve Finsku

Další zemí z EU přiložené do komparace je Finsko. Ve Finsku je oblast soukromé bezpečnosti regulována konkrétním zákonem o komerční bezpečnosti (Yksityisistä turvallisuukspalveluista annetun lain). Můžeme ho označit za jeden z nejpreciznějších systémů v oblasti komerční bezpečnosti. Svědčí o tom i skutečnost, že Finsko eviduje každou soukromou bezpečnostní organizaci v centrálním statistickém systému země. Stejně jako Slovenská republika, má i Finsko samostatný zákon o soukromých bezpečnostních službách, který je v současné podobě platný od roku 2002. Systém se skrze zákon orientuje primárně na ochranu spotřebitele (zákazníka) a spolupráci mezi státním a komerčním aparátem. Onu spolupráci koordinuje přítomný poradní orgán.

Na rozdíl od rozdělení činností v ČR a například SR zde figurují dvě hlavní kategorie. Jsou to služby strážní a bezpečnostní. První jmenované jsou služby konané za úplatu a navržené klientem, tedy ochrana věcí, ostraha osob, doprovody, převozy či služby detektiva. Druhé zmíněné obsahují navíc použití technických prostředků. Důležitá je zde skutečnost, že dle finské legislativy mají bezpečnostní agentury chráněný prostor ve své správě a ze zákona mají v případě provádění ochranné činnosti právo vykázat nepovolanou osobu z pozemku. Mají taktéž pravomoc zadržet pachatele v případě protiprávního jednání na zájem chráněný jejich činností nebo přímo na zaměstnance samotné, a to do příjezdu povolaných bezpečnostních orgánů. Souběžně s tím mohou podezřelé či zadržené osoby prohlédat za podmínky, že nalezené předměty související s pácháním trestné činnosti odevzdají taktéž policejním orgánům. Dalším značným rozdílem je, že za určitých podmínek daných zákonem může bezpečnostní služba použít násilná opatření proti osobě páchající trestné jednání. Samozřejmě jen pokud se jedná o naléhavé případy, kdy nelze ukončit trestné jednání jiným mírnějším způsobem. Problematika používání zbraní je upravena tak, že soukromé bezpečnostní subjekty mohou tyto používat při vykonávání pracovní činnosti, striktně ne však mimo ni. To vše za podmínek splnění speciálního výcviku a vědomí policejních orgánů. Podmínky definovaných kritérií jsou vztaženy i na hlídací psy, kteří musí taktéž projít speciálními zkouškami tak, aby mohli být použiti k výkonu fyzické ostrahy.

Poskytovatelé bezpečnostních služeb soukromého charakteru musí být opět držiteli náležité certifikace, kterou definuje zákon. Vydávání certifikací a licencí je opět ve správě Ministerstva vnitra Finské republiky, a to na dobu neurčitou. Jasně vymezení pak mezi státním a soukromým sektorem je, že provozování soukromých bezpečnostních služeb nesmí bránit výkonu služby vnitřní bezpečnosti státu, veřejného pořádku či vyšetřování trestného činu policejními orgány.

Stejně jako u slovenského modelu, i ve Finsku předkládají soukromé subjekty každoročně Ministerstvu vnitra souhrnnou zprávu o výkonu bezpečnostní činnosti [80,81].

Provedená analýza od Ditrycha a Bahenského na zapojení soukromého a nevládního sektoru do systému bezpečnosti státu na příkladu Finska a možnosti aplikace v ČR. Ta popisuje finský koncept “komplexní bezpečnosti”, založený na totální obraně. Celá společnost (státní instituce, firmy, akademie, občané) se podílí na zajištění základních funkcí státu viz výše. Analýza doporučuje pro ČR např. ustavit platformu pro spolupráci mezi státem a soukromým sektorem v oblasti hybridních hrozeb, posílit sdílení informací s akademickou sférou a zahrnout soukromé firmy do plánování ochrany kritické infrastruktury. Dále navrhuji vzdělávací kurzy bezpečnostní politiky pro soukromý a neziskový sektor, aby se zvýšila společná odolnost společnosti [82].

Určující legislativa SBS ve Finsku

- **Yksityisistä turvallisuuksalveluista annetun lain (Zákon o komerční bezpečnosti)** – zákon vymezuje právní rámec fungování soukromých bezpečnostních služeb ve Finsku, včetně podmínek licencování, kvalifikace pracovníků a pravidel pro výkon činnosti [81].

4.2.7 Vlastní závěry případových analýz

Analýza vybraných evropských států ukazuje, že SBS představují pevně ukotvenou součást systému vnitřní bezpečnosti. Přestože se jednotlivé státy liší v míře detailu legislativní úpravy či rozsahu pravomocí, společným jmenovatelem je důraz na striktní regulaci, státní dohled a vysokou míru profesionalizace.

V Německu, Itálii, Francii, Nizozemsku, Slovensku i Finsku je provozování SBS podmíněno licencí, kterou udělují buď příslušná ministerstva, nebo policejní orgány. Licence je vždy spojena s požadavky na odbornou způsobilost, absolvování školení a průběžné vzdělávání. Školení zpravidla zahrnuje nejen technické a taktické dovednosti, ale také znalost právního rámce a etických zásad. Tím je posilována profesionalita sektoru a současně i jeho společenská legitimita.

Významným prvkem, který se prolíná napříč všemi státy, je regulace použití zbraní. Přístup k nim je možný pouze na základě speciální licence a po absolvování přísného výcviku. Ve všech analyzovaných státech je zbraň chápána jako krajní prostředek, jehož využití je jasně definováno, typicky při ochraně života, zdraví či majetku. Přesto lze vysledovat určité rozdíly

ve využití zbraní. Zatímco ve Francii a Finsku je povolení velmi omezené a fakticky se vztahuje jen na vybrané činnosti primárně s ohrožením života, Německo či Slovensko jsou v užití zbraní SBS benevolentnější, ovšem za podmínky intenzivního dohledu.

Důležitým aspektem je také spolupráce mezi SBS a veřejnými bezpečnostními složkami. V Itálii a Francii je spolupráce legislativně ukotvena a SBS jsou chápány jako doplňkový prvek policejních sil, zejména v rámci ochrany veřejného pořádku nebo při zvládání krizových situací. V Nizozemsku a Německu má spolupráce spíše praktickou podobu a probíhá především na základě výměny informací a koordinace zásahů. Slovensko a Finsko pak kladou důraz na transparentnost činností SBS prostřednictvím pravidelného vykazování a kontroly ze strany státních orgánů.

Z těchto poznatků lze pro ČR vyvodit několik závěrů. Především je patrné, že v evropském kontextu je trendem stále těsnější propojování soukromého a veřejného sektoru v oblasti bezpečnosti, avšak při zachování jasného státního dohledu. Inspirací pro ČR může být zejména důraz na pravidelný reporting, jako na Slovensku, formalizovaná spolupráce při krizových událostech př. Itálie a Francie či propracovaný systém školení a licencí jako v Německu a Finsku. Tyto prvky mohou přispět ke zvýšení důvěry veřejnosti v soukromý bezpečnostní sektor a zároveň k jeho efektivnějšímu začlenění do širšího bezpečnostního rámce státu. Nejen tyto koncepční body budou předmětem rozpracování v návrhové části práce.

Z analýz státních systémů lze konstatovat, že SBS jsou v Evropě chápány jako doplňující, nikoliv konkurenční složka vůči státním bezpečnostním orgánům. Jejich role spočívá především v zajišťování fyzické ochrany osob a majetku, technickém zabezpečení a podpoře při zvládání mimořádných situací. Klíčem k jejich legitimnímu fungování je vždy vyvážení dvou principů, a to profesionality a státní kontroly. Tento univerzální výstup poslouží jako východisko pro úvahy o dalším rozvoji systému SBS v ČR.

4.3 Komparace vybraných evropských modelů komerční bezpečnosti

Tabulka 1 - Komparace současného stavu komerční bezpečnosti v ČR se zahraničními modely (zdroj: vlastní).

<u>Kritéria</u>	Francie	Itálie	Nizozemsko	Německo	Finsko	Slovensko	Česká republika
Zákon o SBS	✓	✓	✓	✓	✓	✓	✗
Použití zbraně zaměstnancem	Stanoveno zákonem o SBS	Stanoveno zákonem o SBS	Stanoveno zákonem o SBS	Stanoveno zákonem o SBS	Stanoveno zákonem o SBS	Stanoveno zákonem o SBS	Stanoveno zákonem o zbraních a střelivu
Spolupráce komerční a státní bezpečnosti	✓	✓	✓	✓	✓	částečně	částečně
Nutnost držení licence k podnikání	✓	✓	✓	✓	✓	✓	✗
Nutnost archivace záznamů o činnosti	✓	✓	✓	✓	✓	✓	✗
Periodické přezkušování a výcvik zaměstnanců	✓	✓	✓	✓	✓	✓	✗

Tabulka 1 shrnuje a komparuje zásadní rozdíly mezi analyzovanými komerčně bezpečnostními systémy v jednotlivých evropských zemích. Komparace poskytuje podněty k zamyšlení, které budou předmětem dalšího metodického zkoumání vedoucího ke vzniku návrhů na zlepšení současné situace v ČR.

Komparace je omezena na vybrané evropské státy, ačkoli v teoretické části práce jsou rozebírány i další světové modely SBS. Toto zúžení bylo záměrné, jelikož hlavní myšlenkou komparace je poukázat na realitu, že by komerční bezpečnostní sektor v ČR měl být minimálně na shodné úrovni, jako ostatní státy EU.

Porovnání bezpečnostních modelů ve Francii, Itálii, Nizozemsku, Slovensku, Německu, Finsku a Slovensku vůči ČR ukazuje rozmanitost přístupů k regulaci soukromých bezpečnostních služeb. Každý stát má své specifické legislativní, organizační a provozní modely, které odrážejí jejich historický vývoj, právní kulturu a bezpečnostní požadavky. Záměrem je porovnání těchto modelů z hlediska legislativních omezení, školení a kvalifikací, spolupráce s veřejnými bezpečnostními orgány a přístupu k používání zbraní.

Výsledky komparace potvrzují tristní nedostatky v legislativním rámci působení bezpečnostních agentur v ČR. Od toho se odvíjí i vybavenost a rozsah činností jejich zaměstnanců. Bohužel toto zjištění odráží i skutečnost, že ČR zaostává za ostatními evropskými státy v této problematice. Návrhová část práce poskytne nejen návrh hlavních systémových bodů jakožto evropský „best practice“, které by v novém právním uspořádání SBS neměly být opomenuty, ale takéž nové organizační i technologické návrhy k transformaci a zefektivnění činnosti komerčního bezpečnostního sektoru v ČR mimo jiné ve jménu ochrany MC

Výsledky vlastní komparace potvrzují výstupy studie komparativní analýzy regulace SBS ve 26 státech EU od Buttona a Stiernstedta. Zde byl vytvořen hodnotící model o 22 kritériích (legislativa + společenské faktory) k „bodování“ kvality zahrnující povinné licence pro agentury i pracovníky, důkladné prověrky, povinný výcvik a státní dozor, jak je zavedeno v některých státech. Naproti tomu jiné země dosud nemají jednotný zákon (výslovně zmiňovány problémy roztržitosti, což je přesně případ ČR). Výrazné rozdíly v přístupech komplikují vytvoření jednotného trhu bezpečnostních služeb v EU. Výstupem analýzy je zvažít minimální standardy na úrovni EU (např. vzájemné uznávání licencí, společné kvalifikační požadavky apod.) [83].

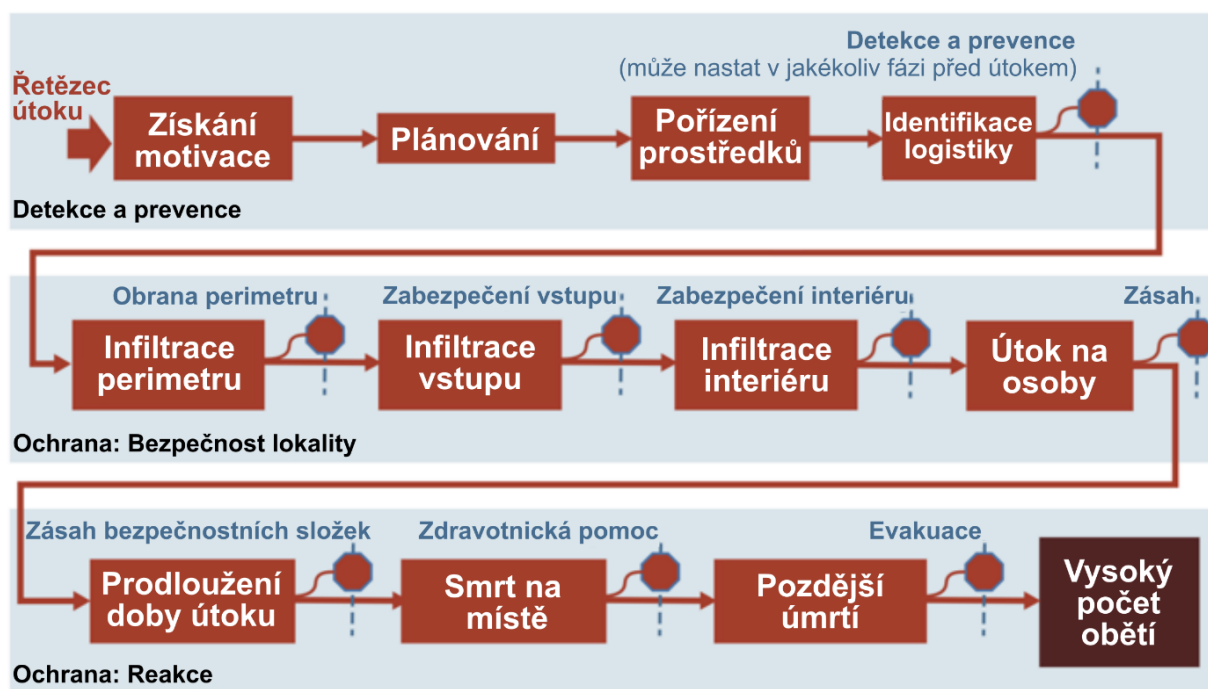
Tato případná evropská regulace může vést k „partnerství“ mezi státem a SBS, pokud jsou nastavena jasná pravidla, soukromá bezpečnost se stává uznávaným doplňkem policie. Zároveň však příliš benevolentní regulace (či samoregulace) nese riziko, že slouží hlavně k legitimizaci sektoru bez reálného zvýšení kvality. Balance mezi ochranou veřejného zájmu a podporou odvětví je tedy klíčová [84].

Zajímavým doplňkem k otázce role státu a soukromého sektoru v oblasti bezpečnosti je také koncept policejního dobrovolnictví, na který upozorňují Krulík a Klíma ve svém článku. V některých zemích střední a východní Evropy fungují dobrovolníci jako pomocná složka policie, podílejí se na dohledu nad veřejným pořádkem nebo na preventivních aktivitách v komunitách. Tento model však není vždy legislativně ukotven a někdy může sklouzávat k neformálním iniciativám bez dostatečné kontroly, což s sebou nese i bezpečnostní rizika. Potvrzuje se tak, že ať už jde o komerční bezpečnost nebo policejní dobrovolnictví, klíčovým faktorem zůstává jasně nastavený právní rámec [85].

4.4 Statistická analýza útoků na měkké cíle ve světě a v České republice

Statistickou analýzou útoků na měkké cíle ve světě, Evropské unii a České republice je třeba poukázat na aktuálnost tématu vzhledem k četnosti a velikosti útoků na MC. Cílem je identifikovat hlavní hrozby pro MC z historických zkušeností, popsat trendy a posoudit roli či absenci SBS při těchto incidentech. Analýza vychází z aktuálních statistik, případových studií a odborných zpráv z let 2010–2024. Cílem kapitoly je taktéž poukázat na aktuálnost tématu vzhledem k evropské i světové vývojové stránce v oblasti bezpečnosti. Dalším záměrem je poukázat na současnou roli SBS během těchto událostí pro další možné návrhy využití ochrany.

Následující obrázek z literatury Mass Attacks Defense Toolkit znázorňuje řetězec útoku, tedy postupné kroky, kterými útočník prochází od prvotní motivace až po realizaci útoku a jeho důsledky. Současně ukazuje, na jakých úrovních je možné uplatnit obranné vrstvy tzv. „defensive layers“, které mohou útok zastavit, zpomalit nebo alespoň zmírnit jeho dopady. Tento model je důležitý při analýze a ochraně MC, jelikož zde útočníci hledají nejzranitelnější místa, kde lze potenciální bránu vstupu obejít nebo překonat.



Obrázek 7 - Řetězec útoku a odpovídající obranné vrstvy pro měkké cíle a frekventovaná místa [86].

Model řetězce útoku na MC dělí ochranu do tří hlavních fází:

Detekce a prevence (Detection and Prevention): snaha odhalit a přerušit přípravu útoku již ve fázi motivace, plánování, obstarávání materiálu nebo logistiky k útoku.

Ochrana místa (Protection - Site security): obranné vrstvy na úrovni perimetru, vstupu, interiéru a přímé intervence proti útočníkovi na místě.

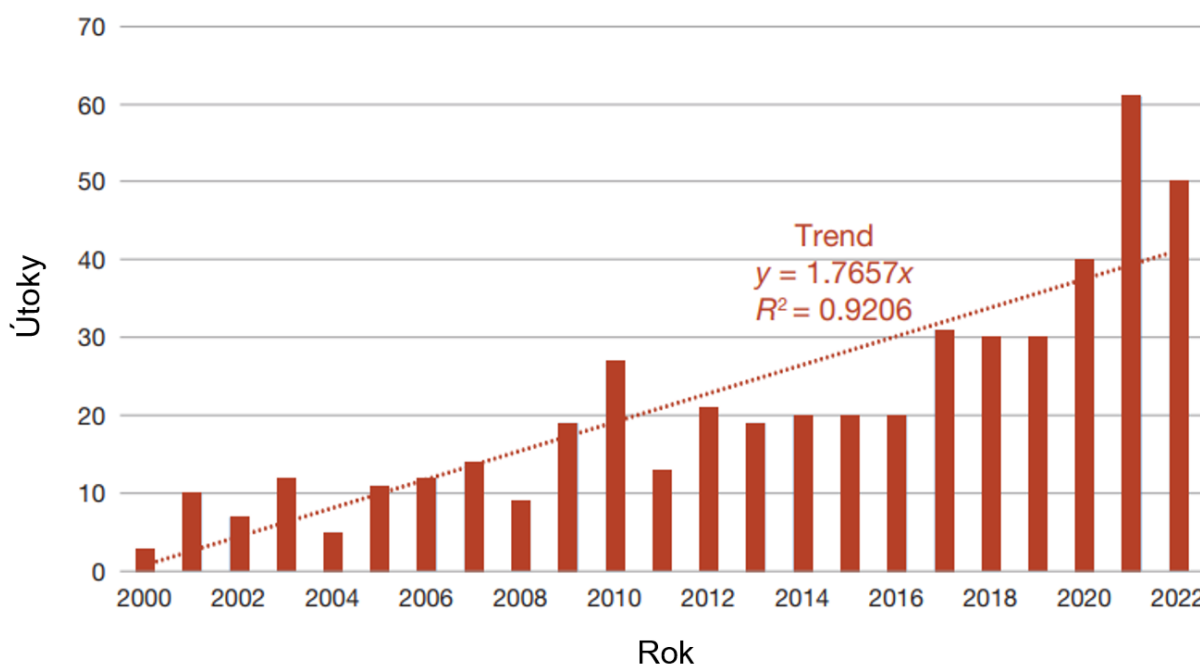
Reakce (Protection – Response): reakce složek (státní složky či právě SBS), které mohou prodloužit dobu útoku, zmírnit následky a minimalizovat počty obětí.

V kontextu útoků na MC tento model ukazuje, že k efektivní ochraně je potřeba vícevrstvá obrana „layered security“. Nelze spoléhat jen na fyzickou ostrahu u vstupu, ale na kombinaci opatření napříč celým řetězcem, od včasné identifikace hrozeb po rychlou reakci po útoku. Z analýzy útoků ve světě (viz níže) vyplývá, že selhání často nastává právě v přechodu mezi jednotlivými vrstvami – proto je důraz kladen na propojení bezpečnostních složek, soukromých bezpečnostních služeb a krizového managementu [86].

4.4.1 Útoky na měkké cíle ve světě

Dle statistik v USA opět ze zdroje Mass Attacks Defense Toolkit mezi lety 2000 až 2022 je znatelná vzestupná tendence útoků aktivních střelců. Tyto incidenty probíhají zejména v budovách univerzit či zdravotnických zařízení. Útoky aktivních střelců či amoky a osamělí vlci jsou primárně v těchto objektech, vzhledem k maximální efektivnosti na dopadech

na lidské životy. Nejen v USA jsou tyto incidenty na stálém vzestupu, níže bude rozveden útok na pražské Karlově univerzitě, či příkladem může být nedávný útok na základní škole v rakouském Štýrském Hradci 21 letým, legálně ozbrojeným, bývalým studentem ústavu [86,87].



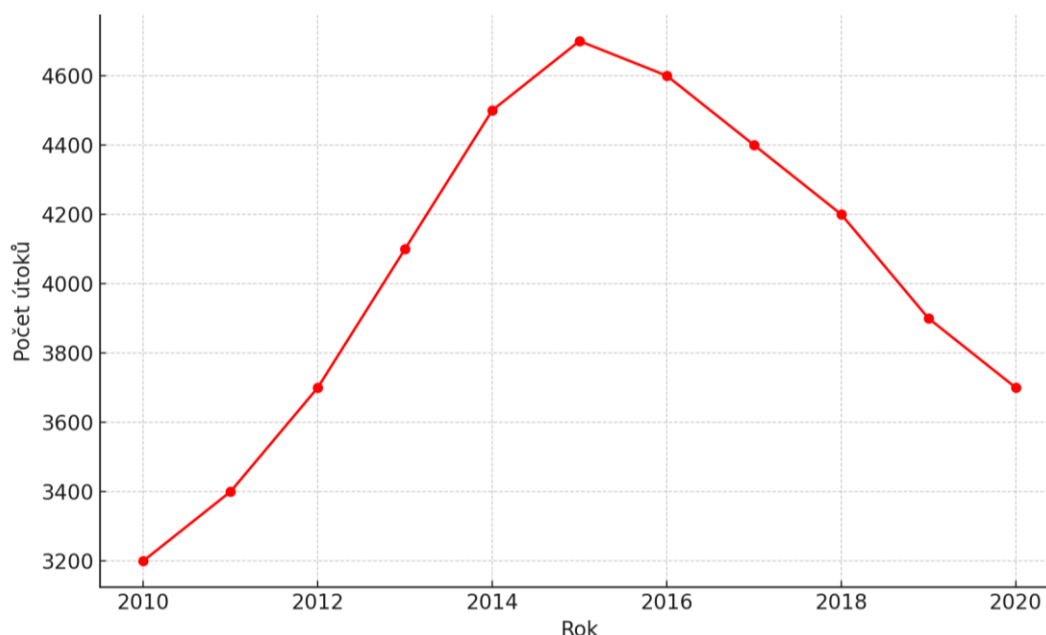
Obrázek 8 - Útoky aktivního střelce v USA od roku 2000 [86].

V posledních letech lze pozorovat změnu profilů hrozeb pro MC. Vedle islamistického terorismu narůstají útoky pravicově extremisticky motivované dle zpráv Global Terrorism Index stoupl počet útoků ve vyspělých zemích výrazně, zejména kvůli nárůstu aktivity krajní pravice. Např. v Severní Americe, Západní Evropě a Oceánii vzrostl počet útoků krajní pravice v letech 2013–2018 o 320 % [88].

Tyto útoky (např. střelby v mešitách, synagogách – Christchurch 2019, nebo Halle 2019) cílí často právě na MC s cílem způsobit masové oběti a šok. Ochranná opatření se proto musejí zaměřit nejen na džihádistické hrozby, ale i na lokální extremisty a tzv. osamělé vlky inspirované různými ideologiemi. To zahrnuje rozšíření spolupráce zpravodajských složek, monitoringu internetové radikalizace a posílení prevence (programy proti radikalizaci, ostražitost komunity). ČR čelí zatím těmto hrozbám v menší míře, ale trendy ze zahraničí jsou varovné. PČR i civilní zpravodajská služba BIS (Bezpečnostní informační služba) v posledních zprávách zmiňují riziko osamělých aktérů inspirovaných např. manifesty zahraničních útočníků [89].

Podle poslední zprávy Global Terrorism Index (2025) byly v období 2010–2024 nejvíce zasaženými zeměmi Afghánistán, Irák, Somálsko, Sýrie a Pákistán. Objekty škol, nákupních center, místa bohoslužeb a sportovní události, zůstávají preferovanými cíli teroristických útoků. Vzhledem k velice komplikované bezpečnostní i politické situaci jsou útoky tohoto typu v těchto lokalitách bohužel velice časté. Obrázek č. 8 poukazuje právě na vývoj výskytu aktivního střelce v USA od roku 2000 a jeho související tendenci. Výskyt aktivních střelců zpravidla bývá v objektech a prostorách škol, univerzit či nemocnic [90].

Následující graf znázorňuje počet útoků na MC ve světě v období 2010 až 2020. Je patrný nárůst útoků do roku 2015, po němž následuje postupný pokles v důsledku mezinárodních bezpečnostních opatření a postupu covidové vlny, a tedy i omezení pohybu osob.



Obrázek 9 - Celkový počet útoků na měkké cíle ve světě (2010-2020) [91,92].

K významným útokům patří například Bostonský maraton (2013), kde dva útočníci odpálili bomby poblíž cíle závodu, což vedlo ke třem úmrtím a více než 260 zraněným. Dalším klíčovým incidentem byl útok na koncert v Manchesteru (2017), kde sebevražedný útočník zabil 22 lidí a více než 500 zranil [93].

Jako reakce na uvedené trendy ohrožení MC vydala Austrálie v roce 2017 národní Strategii pro ochranu míst velké koncentrace osob (crowded places) před terorismem. Důraz se posouvá k proaktivním opatřením, zákony a předpisy mají stanovit povinnosti pro provozovatele míst s velkými shromážděními civilního obyvatelstva (risk assessment, krizové plány atd.).

Australský incident obléhání kavárny Lindt v Sydney (2014) je varováním, že ani tento kontinent není imuní vůči ohrožení MC [94].

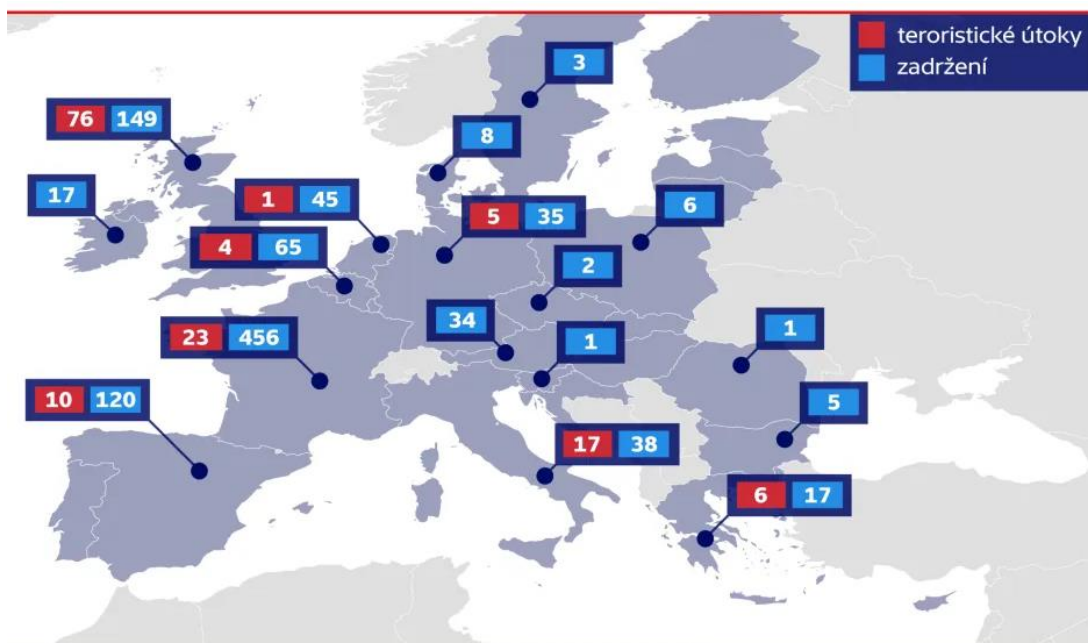
Role SBS ve světě se liší. V USA jsou SBS aktivně zapojeny do zabezpečení velkých veřejných akcí, poskytují fyzickou ostrahu, kontrolu přístupu a monitoring pomocí CCTV. Po útoku na zmíněný Bostonský maraton byla bezpečnostní opatření posílena, což vedlo k většímu zapojení SBS při plánování a realizaci bezpečnostních opatření na sportovních a kulturních akcích [95].

4.4.2 Útoky na měkké cíle v Evropské unii a Velké Británii

V Evropské unii bylo v letech 2010–2024 evidováno přes 250 teroristických útoků na MC. Nejvíce incidentů bylo zaznamenáno ve Francii, Velké Británii, Německu a Španělsku. K nejtragičtějším patří útok v Nice (2016), kde útočník najel nákladním vozem do davu při oslavách Dne Bastily, zabil 86 lidí a více než 400 zranil. Dalším byl útok na koncertní sál Bataclan v Paříži (2015), při němž ozbrojenci zabili 90 osob [96].

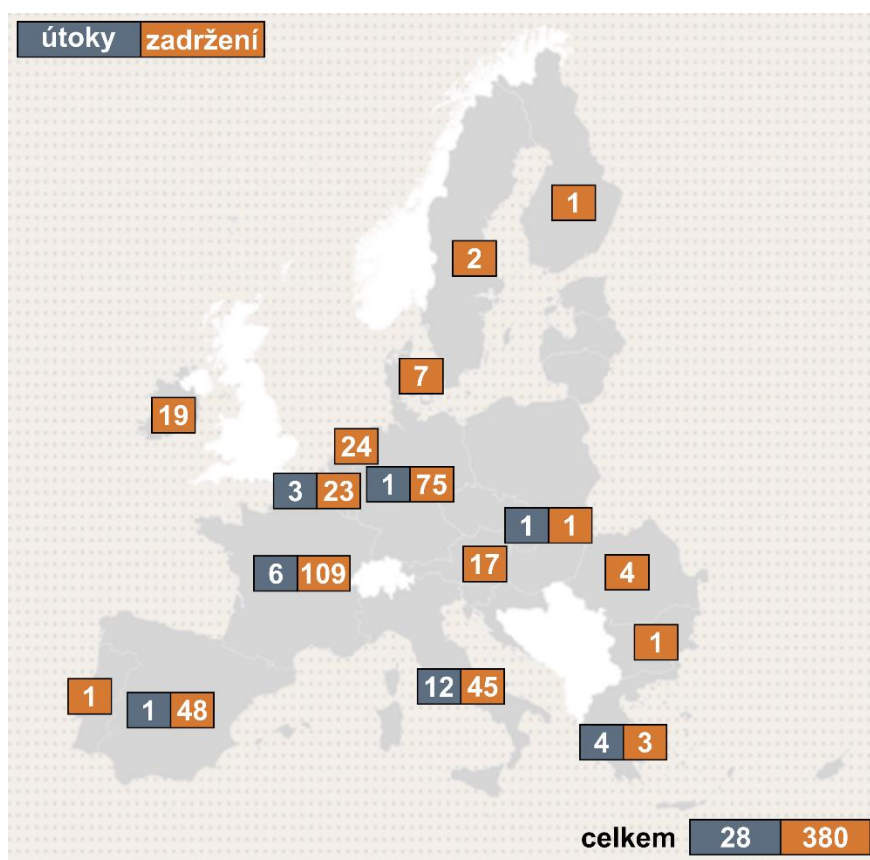
Role SBS v EU je významná, přesto se jejich zapojení liší mezi jednotlivými státy, jak bylo výše komparací prokázáno. Například ale ve Francii a Velké Británii jsou SBS běžnou součástí bezpečnostních opatření na veřejných akcích a v komerčních objektech. Po útocích v Paříži a Nice byly posíleny bezpečnostní protokoly, včetně zvýšené přítomnosti SBS, lepší koordinace s policejními složkami a zavedení kontrolních zón na velkých akcích [96,97].

Navzdory těmto opatřením došlo k selhání například při útoku v Berlíně (2016), kdy nebyla dostatečně chráněna vánoční tržnice. Tento případ ukázal potřebu posílit plánování a koordinaci mezi SBS a veřejnými složkami [96].



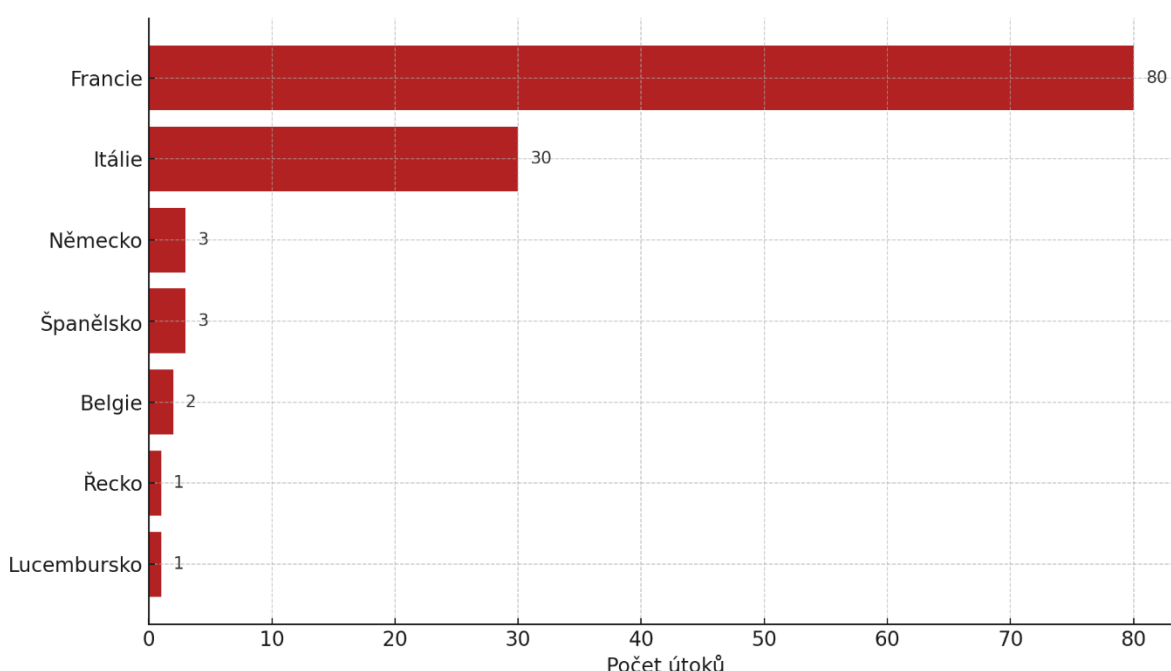
Obrázek 10 - Teroristické útoky na MC a zadržení ve státech EU a Velké Británii v roce 2016 [98].

Ilustrativní obrázek počtu teroristických útoků na MC v Evropě v roce 2016 a počet zadržení s nimi spojených versus stejná statistika z roku 2022.



Obrázek 11 - Teroristické útoky na MC v EU a Velké Británii v roce 2022 [99].

Podle zprávy EU Terrorism Situation and Trend Report 2024, kterou zveřejnil Europol, bylo v roce 2023 v EU zaznamenáno 120 teroristických útoků, z nichž 98 bylo dokončeno, 9 selhalo a 13 bylo zmařeno. Toto představuje výrazný nárůst oproti 28 útokům v roce 2022. Většina dokončených útoků byla provedena separatistickými skupinami. Džihádistické skupiny dokončily pět útoků, které způsobily největší počet obětí – 12 zraněných a 6 mrtvých. Opět se jedná o útoky na MC jak bylo zmíněno v kapitole výše. Nárůst útoků oproti roku 2022 lze shledat v rozvolnění cestování po ukončení covidových opatření. Velký význam na snížení celkových počtů útoků v EU má také výstup Velké Británie, která je velkým terčem teroristických útoků včetně těch na MC. Každopádně tyto statistiky dokazují, že bezpečnostní situace v EU nebude mít s nejvyšší pravděpodobností tendence ke zlepšování. Efektivnější využití SBS a podpoře státních orgánů je přímo vybízející [100].



Obrázek 12 - Teroristické útoky na MC v EU ve vybraných státech v roce 2023 [100].

4.4.3 Útoky na měkké cíle v České republice

ČR zaznamenala méně teroristických či jiných útoků na MC než jiné evropské země, avšak incidenty jako útok ve Žďáru nad Sázavou (2014), kde útočnice vnikla do školy a zabila studenta, či střelba v nemocnici v Ostravě (2019), kde střelec zabil šest lidí v čekárně ukazují na rizika i v českém prostředí. Jednou z nejdiskutovanějších událostí z poslední doby je útok na Karlově univerzitě na Filosofické fakultě (2023), kde útoku a jeho následkům podlehl 14 osob. Tento incident bude níže rozebrán jako případová studie [101,102].

Nejvíce jsou SBS v ČR využívány k ochraně nákupních center, kulturních akcí či sportovních stadionů. Ve školách, nemocnicích a menších institucích často zcela chybí. Po útoku ve Žďáru nad Sázavou byla doporučena rozsáhlejší spolupráce škol s bezpečnostními složkami včetně SBS, ovšem stále bez legislativní opory. Vzhledem k bezpečnostnímu vývoji a atraktivitě MC obecně ve světě, a taktéž narůstajícímu náporu na přijímání uprchlíků ať už válečných, či ekonomických, je potenciál k využití SBS pro zapojení do bezpečnostního aparátu aktuální. Dle vzoru okolních analyzovaných států by mohli zaměstnanci SBS být adekvátně připraveni na rizika a hrozby pro MC vyhodnocené níže [103].

4.4.4 Případová studie útoku aktivního střelce na Karlově univerzitě s vlastními náměty na možnosti zlepšení řešení situace

Pro potřeby poukázání významu vztahu SBS a ochrany MC bude v následující kapitole analyzována událost střelby na Filosofické fakultě Karlovy univerzity v Praze.

Dne 21. prosince 2023 došlo k tragické střelbě na Filozofické fakultě Univerzity Karlovy v Praze. Útočník, student této fakulty, vstoupil do budovy a ozbrojen legálně drženými zbraněmi zastřelil 14 lidí a desítky dalších zranil. Jednalo se o nejtragičtější útok tohoto druhu v novodobé historii České republiky. Policie dorazila na místo během několika minut, zajištěním perimetru a evakuací studentů minimalizovala další možné škody. Útočník spáchal sebevraždu ještě před přímou konfrontací s policejními složkami.

Popis útoku

Pachatel vstoupil do hlavní budovy Filozofické fakulty Univerzity Karlovy na náměstí Jana Palacha krátce po třinácté hodině. Nesl s sebou velký kufr obsahující střelné zbraně a munici. Krátce poté do budovy dorazili policisté, kteří vrátným ukázali fotografie hledaných osob, mezi nimiž byl i pachatel. Vrátní uvedli, že nikoho z nich neviděli, a policie vedení fakulty o důvodu svého pátrání neinformovala.

Samotný útok začal před patnáctou hodinou, kdy útočník zahájil střelbu ve čtvrtém patře fakulty, konkrétně v učebně č. 423. Během několika minut zde zabil devět osob a dalších dvanáct zranil. Zároveň policie přijala první tísňová volání o střelbě.

První hlídky dorazily na místo krátce po zahájení útoku. Policisté začali okamžitě s evakuací osob z budovy a současně pátrali po střelci. Po dosažení čtvrtého patra se rozdělili, část zasahujících pokračovala v hledání pachatele, zatímco druhá skupina poskytovala první pomoc zraněným. Útočník ještě několik minut střílel, než sám obrátil zbraň proti sobě a spáchal

sebevraždu. Policisté cca v 15:20 vstoupili do učeben, kde útok probíhal, a poskytli pomoc přeživším.

Kroky přijaté po útoku

Bezprostředně po oznámení střelby byla aktivována jednotka URNA (Útvar rychlého nasazení), která provedla zásah a prohledání objektu. Proběhla koordinace složek IZS (integrovaný záchranný systém), rychlá lékařská pomoc, uzavření budovy a informování veřejnosti. Univerzita a město Praha zřídily krizové linky, byla nabídnuta psychologická pomoc. Policie zahájila vyšetřování a dočasně zvýšila bezpečnostní opatření ve školských zařízeních v celé zemi [104,105].

Tragédie na Filozofické fakultě UK odhalila zranitelnost MC v ČR. Dále také skutečnost, že tyto útoky nemusí přicházet pouze ze stran různých teroristických uskupení, ale jedná se o komplexní bezpečnostní problematiku, která je i v ČR velice aktuální viz Vyhodnocení ohroženosti MC výše. Posílení prevence, zavedení technických opatření a promyšlené zapojení SBS do bezpečnostního rámce by mohly výrazně přispět ke snížení rizika podobných událostí v budoucnosti. Klíčová je především prevence, včasná detekce a případná rychlá reakce.

4.4.5 Možnosti zlepšení bezpečnostního rámce a možná role komerční bezpečnosti v řešení modelové situace útoku na Filozofické fakultě Univerzity Karlovy

Z pohledu preventivní bezpečnosti by bylo možné zavést komplexní systém elektronického zabezpečení s monitoringem vstupů, detektory kovů na vybraných místech nebo chytré kamerové systémy s funkcí automatického rozpoznání podezřelého chování. Dále lze zvážit zavedení bezodkladného varovného systému pro studenty a zaměstnance pomocí mobilních aplikací nebo rozhlasových hlášení.

Za současného legislativního rámce by bylo možné zapojení SBS pouze na základě smluvního vztahu s univerzitou. Bezpečnostní agentura by mohla zajišťovat kontrolu vstupů, kamerový dohled, monitoring podezřelého chování a asistenci při krizových situacích. Objekt by byl napojen na PCO vybrané agentury a fyzicky přítomní zaměstnanci by tak byly komunikačním prvkem v místě určení. Zřízen by byl velín pro bezpečnostní agenturu, na vrátnici univerzity by pak mohla být zdvojena stráž. Například 1 zaměstnanec univerzity, 1 zaměstnanec bezpečnostní agentury. Ve zmíněném velíně ostrahy už pak jen zaměstnanec či zaměstnanci bezpečnostní agentury. Tento model by zefektivnil režimová opatření jako celek, tedy včasnou detekci útočníka a zvýšení pravděpodobnosti zmaření pokusu

a násilnou akci. V případě vzniku takovéto události mohou pak zaměstnanci SBS spouštět prvotní kroky k řešení krizové situace, tedy detekce a lokalizace narušitele, komunikace jak s vlastní PCO, tak státními složkami včetně IZS. Dále pomoc ohroženým osobám skrze řízenou evakuaci z objektu. Tento model je za současné funkce SBS a legislativních nastavení možný, ovšem jeho limity jsou především v ochotě a finančních možnostech dané univerzity takovýto druh ochrany financovat.

V případě rozšíření pravomocí a posílení legislativy by mohli být pracovníci SBS vyškoleni jako první reakční složka v modelu například tzv. obrácené 112 (bude detailně rozebráno v návrhové části práce), kde by poskytovali pomoc ještě před příjezdem IZS. Největší síla by ovšem byla v možnosti legitimního ozbrojení zaměstnanců dané bezpečnostní agentury po vzoru jiných evropských států a možnosti samostatného zásahu přímo v místě lokalizovanými zaměstnanci SBS. Dle struktury nového zákona a jejich možností, vybavenosti, vycvičenosti a profesionalitě dané SBS by v ideálním případě došlo ke zneškodnění a vyřešení celé krizové situaci již v počátcích útoku. Přínosy takového modelu jsou ve značném snížení dopadů jak primárně na lidských životech, tak na majetku univerzity a také nelze opomenout reputaci instituce, což je zmiňovaný prvek v práci výše.

4.5 SWOT analýza možností využití soukromých bezpečnostních služeb k ochraně měkkých cílů v současných legislativních podmínkách České republiky

Záměr zapojit bezpečnostní agentury (dále BA) do ochrany MC v podmínkách ČR naráží na několik významných limitů, které je třeba reflektovat při strategickém hodnocení jejich role. Prvním a nejzásadnějším faktorem je několikrát zmíněná absence komplexního legislativního rámce, což komplikuje jasné vymezení odpovědnosti a pravomocí k výkonu této činnosti, což jasně vyplývá z výše provedené komparativní části. Z toho dále vyplývají omezené pravomoci pracovníků SBS, kteří nemají zákonné oprávnění k preventivním zásahům, kontrolám osob či výkonu pomoci donucovacích prostředků mimo rámec smluvního vztahu s chráněným subjektem. Další slabinou je neharmonizovaná úroveň kvalifikace a výcviku mezi jednotlivými agenturami napříč nabídkou v ČR, přičemž neexistuje žádný centrálně uznávaný standard odbornosti. Problematická může být i veřejný pohled na soukromou bezpečnost, která je v některých případech vnímána spíše jako „nižší“ bezpečnostní složka, čímž dochází k oslabování její legitimacy v očích veřejnosti.

V neposlední řadě je zapojení SBS limitováno i institucionálně. Stát v současnosti nedisponuje nástrojem, jak tyto složky systémově a finančně začlenit do zabezpečení veřejných prostor či událostí, jak je opět výše v práci definováno. Přesto však daná oblast představuje významný potenciál, který by při vhodném legislativním a organizačním zakotvení mohl významně posílit schopnost státu čelit hrozbám směřujícím nejen vůči MC. Tento pohled hodnocení současného stavu SBS v ČR analyzovaném v předchozích kapitolách je předmětem vlastní SWOT analýzy:

Tabulka 2 - SWOT analýza možností využití SBS k ochraně MC v ČR (zdroj: vlastní).

Kategorie	Položka	Důležitost	Váha	Skóre
Silné stránky	Flexibilita SBS v nasazení a rozsahu služeb	5	0.3	1.5
Silné stránky	Znalost lokálního prostředí místními BA	3	0.2	0.6
Silné stránky	Možnost nepřetržité přítomnosti na místě	4	0.2	0.8
Silné stránky	Využití technických prostředků SBS (CCTV, monitoring apod.)	4	0.3	1.2
Slabé stránky	Absence legislativního rámce pro SBS	5	-0.3	-1.5
Slabé stránky	Omezené pravomoci SBS (zásah, zadržení apod.)	4	-0.3	-1.2
Slabé stránky	Nerovnoměrná kvalita a výcvik napříč BA	4	-0.2	-0.8
Slabé stránky	Negativní vnímání veřejnosti o schopnostech SBS	3	-0.2	-0.6
Příležitosti	Přijetí zákona o SBS	5	0.3	1.5
Příležitosti	Zavedení standardů kvality a výcviku + rozvoj technologií	4	0.2	0.8
Příležitosti	Zvýšení spolupráce s IZS	4	0.3	1.2
Příležitosti	Změna vnímání SBS jako bezpečnostní struktury	3	0.2	0.6
Hrozby	Náhlý teroristický či jiný útok na měkký cíl	5	-0.2	-1.0
Hrozby	Zneužití pravomocí SBS bez právního rámce	4	-0.2	-0.8
Hrozby	Veřejná nedůvěra a mediální skandály	3	-0.2	-0.6
Hrozby	Nedostatek kvalifikovaných pracovníků	4	-0.2	-0.8

Celkové skóre

Součet: $4,10 - 4,10 + 4,10 - 3,20 = 0,90$

Silné stránky vyplývají zejména z flexibilního charakteru soukromého sektoru, schopnosti SBS adaptovat se na konkrétní podmínky objektů a situací, jejich technického vybavení a možnosti permanentního působení v terénu. Tyto kapacity z nich činí důležité doplňkové aktéry k veřejným bezpečnostním složkám, především v oblasti prevence, monitoringu a rychlé reakce. Touto flexibilitou je míněna i decentralizace některých větších BA, které jsou schopny poskytovat své služby plošně včetně zahraniční.

Na druhé straně slabé stránky vycházejí především z legislativní absence, kde se SBS v ČR nacházejí. Neexistence zákona, chybějící standardizace výcviku, kvalifikací i dohledových mechanismů vytváří prostředí právní nejistoty a omezuje možnosti systémového nasazení těchto složek. Významným problémem je také obecně omezený rozsah jejich zákonných pravomocí a nejednotné vnímání jejich společenské role.

Příležitosti se tak logicky otevírají v oblasti právní a institucionální. Přijetí zákona o SBS, zavedení profesních standardů, rozvoj kooperace s IZS a systematická profesionalizace komerční bezpečnosti by mohly významně rozšířit možnosti jejich reálného zapojení. Změna vnímání SBS jako důvěryhodného bezpečnostního partnera by navíc mohla podpořit jejich širší využití i ze strany veřejnosti a samospráv a dala by tak prostor novým inovativním využití těchto osob a jejich služeb, což je předmětem návrhové části práce. Jednou z těchto služeb ve jménu navýšení efektivity a profesionality SBS je zavedení a používání stávajících, či inovativních technologií.

Hrozby představuje především možnost zneužití pravomocí v prostředí bez legislativních ohraničení agentur, narušení veřejné důvěry např. v důsledku značného pochybení, nebo obecný nedostatek kvalifikovaných pracovníků. Bez systémového řešení se také SBS nemohou adekvátně zapojit do reakce na mimořádné události u MC, čímž zůstává část potenciálu nevyužita.

Komplexní SWOT analýza ukazuje, že ačkoliv současné postavení SBS v oblasti ochrany MC v ČR naráží na řadu omezení, zejména v legislativní a strukturální rovině, tak zároveň odhaluje výrazný potenciál pro jejich budoucí rozvoj. Současné legislativní podmínky zatím neumožňují plné využití těchto služeb, a jejich role v ochraně MC zůstává poddimenzovaná a systémově nezakotvená. Přesto však SWOT analýza potvrzuje, že při vhodném legislativním zakotvení, například podle modelu navrženého v návrhové části práce inspirovaného

zahraničními systémy, mohou být SBS profesionalizovány a efektivně začleněny do bezpečnostního rámce státu. Tím by se mohly stát nejen podpůrným, ale potenciálně i klíčovým nástrojem prevence a ochrany v oblasti MC a v celém tomto sektoru tak ulevit státním bezpečnostním složkám. Příležitosti, které v tomto směru existují, jsou v českém prostředí vlivem dosavadní absence konkrétní úpravy v podstatě otevřené.

5 POUŽITÁ METODIKA

Za ústřední metodiku disertační práce jsem zvolil metodu analýzy a syntézy k potvrzení nebo vyvrácení stanovených hypotéz. Tato kombinace metod umožňuje v práci detailní rozbor současného stavu a definování problémů v zájmových sektorech, které jsou následnou formou syntézy navrhovány v konkrétní řešení a příležitosti či tvorby návrhu nové metody.

Analýza v kontextu DP

- Rozbor právního rámce jednotlivých států;
- rozklad funkčních modelů ochrany MC (včetně využití případových studií);
- identifikace klíčových prvků veřejně-soukromé spolupráce;
- definice následně zkoumaných problémů tématu.

Syntéza v kontextu DP

- Vytvoření uceleného přehledu dosavadních přístupů k regulaci SBS a ochraně MC;
- návrh vlastního modelu kategorizace rizikovosti MC a zapojení SBS do systému ochrany;
- formulace doporučení a návrhů pro podmínky v ČR na základě porovnání a propojení poznatků z komparovaných států;
- návrh nových přístupů k zapojení SBS do ochrany MC nejen v ČR.

6 SYNTETICKÁ – NÁVRHOVÁ ČÁST

Návrhová část práce je syntetickou částí dokumentu, která navazuje na předešlé teoretické a analytické podklady. Navrhuje možné nové přístupy ke komerční bezpečnosti v ČR. Některé další dílčí návrhy, včetně technologických jsou spíše futuristickou vizí, ale s reálnými podmínkami by přinesly vysokou přidanou hodnotu k využití SBS a jejich zaměstnanců při ochraně MC a podpoře komplexní bezpečnosti státu. V digitalizované společnosti v budoucnu jsou tyto technologie očekávané, v některých západních státech již realizované a z praxe plyne, že jejich správná implementace má pozitivní efekt při ochraně MC.

Vzhledem k tomu, že legislativní ukotvení SBS není v podmínkách ČR dotaženo do právních aktů, některé návrhy a závěry disertace budou mít i nesmělé ambice k právnímu ukotvení.

6.1 Návrh a uplatnění semikvantitativní metody Total Risk Score

Hlavním cílem práce a jedním z cílů dílčích je na základě rešerše literatury a získaných poznatků z teoretické a analytické části práce vytvořit nástroj k obecně realizovatelnému hodnocení rizikovosti MC. Toho jsem dosáhl formou návrhu semikvantitativní metody hodnocení rizikovosti MC, vycházející z konceptu Total Risk Score (dále jen metoda TRS). Návrh metody kombinuje kvantitativní přístup na základě výpočtu níže definovanou rovnicí a kvalitativního přístupu pomocí checklistů. Jedná se tak o návrh semikvantitativní metody.

Jednou z inspirací je technicky zaměřený článek ze Safety Science představující metodiku hodnocení rizikovosti MC. Autoři navrhuje model, který pro konkrétní prostor (např. nákupní centrum či koncertní sál) vyčíslí úroveň ohrožení na základě různých faktorů jako pravděpodobnost útoku, zranitelnost místa a dopady útoku. Výsledkem je tzv. „hazard level“ pro daný MC, který umožňuje porovnání objektů podle rizika a prioritizaci ochranných opatření. Jedná se o kvantitativní metodiku [106].

Další významný přístup k návrhu metody je ovlivněn monografií J. Hasterman poskytující detailní typologii MC a pro každý uvádí případovou studii útoků včetně úspěšně odvrácených incidentů. Zdroj zdůrazňuje strategii “target hardening”, který jako jeden z přístupů byl analyzován v práci výše [43].

V DP jsem navrhl metodu TRS, jelikož je založena na důkazech, je exaktnější a tím i důvěryhodnější jak pro hodnocení hypotéz disertace, tak pro využití v praxi. Navazuje na zmíněnou Koncepci ochrany měkkých cílů 2017–2020 a implementuje Metodiku

vyhodnocení ohroženosti měkkého cíle. Zmíněný přístup rozšiřuje dosavadní zásady o kvantitativní metody inspirované mezinárodními standardy ISO 31000:2018 pro management rizik, doporučeními evropských směrnic CFPA Europe Guidelines a CPNI Guidelines. Návrh zahrnuje tři klíčové faktory, **zranitelnost (vulnerability, dále V)**, **dopad/kritičnost (criticality, dále C)** a **hrozbu (threat, dále T)**. Celkové rizikové skóre, tedy TRS (dále takto označována samotná metoda) je pak určeno kombinací těchto faktorů, přičemž metodika zohledňuje i přítomnost bezpečnostních opatření již zavedených, která mohou výsledné riziko snižovat.

Navrženou metodu jsem pak dále doplnil o poslední návrh zákona o SBS z roku 2024 z pohledu kategorizace poskytovaných služeb (viz kapitola 2.1.3.4), který definuje šest kategorií těchto bezpečnostních služeb (A–F), a implementuje tak konkrétní doporučení pro formu využití bezpečnostních agentur směrem k ochraně MC. Typologie MC uvedená v teoretické části práce byla zohledněna při konstrukci parametrů rizikové matice v rámci navrhované TRS. Jednotlivé prvky a váhy navrhované v této metodě byly stanoveny na základě expertního odhadu v kombinaci s inspirací s výše uvedenými zdroji.

6.1.1 Struktura a princip metody Total Risk Score

Metodika TRS hodnotí celkové riziko jako vztah třech zmíněných faktorů V, C, T následovně:

$$\text{TRS}_{\text{final}} = \max(0, \min(300, \text{TRS}_{\text{base}} \times (1 - \frac{R_{\text{sbs}}}{100}))),$$

přičemž,

$$\text{TRS}_{\text{base}} = \min(300, V + C + T).$$

$\text{TRS}_{\text{final}}$ je procentuálně redukována verze TRS_{base} podle R_{sbs} . Jedná se tedy o číselnou finální hodnotu míry rizika, která charakterizuje analyzovaný MC na stupnici od 0 do 300 (0 = žádné riziko, 300 = maximální riziko). Jasně rozmezí hodnoty finálního rizika eliminuje nesmyslnost výsledků při aplikaci metody v praxi.

Prvek kompletní rovnice TRS_{base} je redukčním činitelem, který, jak je vidět v rovnici ovlivňuje hodnotu skóre dle určení definovaných hodnot V, C a T, jejichž samostatné výpočty budou definovány níže. Prvky V, C a T jsou specifikovány konkretizovanými checklisty, které jsou uvedeny v přílohách práce.

Posledním redukčním prvkem hlavní rovnice je R_{sbs} , který ovlivňuje procentuální efektivitu výsledného navrhovaného využití SBS v analyzovaném provozu, a taktéž do výpočtu zohledňuje v analyzovaném MC případnou již využívanou formu SBS. Bude dále specifikováno.

Hodnocení zranitelnosti (V)

Zranitelnost hodnoceného objektu je dimenzována jako kombinace tří oblastí: fyzické zabezpečení, technická ochrana a personální opatření. Každá ze složek je hodnocena zvlášť, a to pomocí checklistu, který přiděluje bodové hodnoty podle toho, kolik typických opatření bylo na objektu implementováno již před samotným hodnocením.

- **Ochrana proti vnějšímu vniknutí** – zahrnuje např. oplocení, bezpečnostní brány, kontrolované vstupy či osvětlení.
- **Technické zabezpečení** - pokrývá systémy typu CCTV, elektronický přístup, detekční techniku nebo napojení na PCO.
- **Fyzická ostraha** - zahrnuje přítomnost ostrahy, bezpečnostní recepce, režimová opatření se zápisy do knihy návštěv, proškolení zaměstnanců a nouzové plány apod.

Pro každou oblast je stanoven maximální bodový strop (33–34 bodů), celková zranitelnost pak dosahuje maximálně 100 bodů. Čím vyšší hodnota, tím hůře je objekt chráněn.

Hodnocení kritičnosti (C)

Kritičnost MC byla zvolena na základě hodnocení společenské a ekonomické důležitosti objektu.

- **Společenská kritičnost** zohledňuje např. symbolický význam, medializaci, poskytování klíčových veřejných služeb (zdravotnictví, školství) nebo vládní status.
- **Ekonomická kritičnost** bere v úvahu hodnotu majetku, kontinuitu provozu a dopady v případě výpadku činnosti.

Obě složky přispívají rovnoměrně, každá až 50 body, což opět dává maximálně 100 bodů. Tato část hodnotí, jak vážné by byly dopady útoku či jiného incidentu.

Hodnocení hrozby (T)

Třetí složkou je hrozba, ta odráží pravděpodobnost útoku a reflektuje riziko útoku z hlediska svého okolí a historických událostí neboli minulých bezpečnostních incidentů či specifických faktorů atraktivity pro útok samotný.

- **Bezpečnostní rizika** zahrnují např. výskyt kriminality, protestů, organizovaného zločinu či zmíněných minulých incidentů.
- **Dostupnost pomoci** pak hodnotí vzdálenost a reakční časy IZS, zdravotních služeb nebo samotných bezpečnostních agentur.

Každá z oblastí může přinést až 50 bodů, výsledkem je tedy opět rozsah 0–100 bodů. Vysoké hodnoty znamenají, že objekt se nachází v prostředí, kde útoky jsou pravděpodobnější nebo pomoc hůře dostupná.

Skóre ze všech tří dimenzí se sečtou a tvoří právě zmíněné TRS_{base} , které poskytuje počáteční odhad celkové rizikovosti MC. Metoda je navržena v jazyce R, programována a vizualizována na platformě R Shiny. Jedná se o open-source platformu pro jazyk R, která umožňuje tvorbu interaktivních webových aplikací.

Obrázek 13 - Vstupní údaje hodnoceného MC (zdroj: vlastní - RShiny).

6.1.2 Kategorizace a využití soukromých bezpečnostních služeb v metodice Total Risk Score

Další proměnná, hodnota R_{sbs} se stanovuje podle zavedených kategorií bezpečnostních opatření, které odpovídají navrhovaným kategoriím A–F v rámci koncepce regulace soukromého bezpečnostního sektoru z posledního návrhu zákona o SBS z roku 2024. Tento faktor se odečítá od TRS_{base} a vzniká tak finální výše v rovnici uvedené hodnocení TRS_{final} . Jedná se o unikátní a inovativní prvek v této metodice, která dokáže do stanovení rizikovosti MC odrazit již zavedený způsob ochrany ze strany komerční bezpečnosti a naopak pro posílení ochrany konkrétní nové možnosti navrhnout.

Tabulka 3 - Specifikace kategorií SBS s orientačními náklady (zdroj: vlastní).

Kategorie	Název	Základní popis	Aplikační oblast
A	Ochrana osob a majetku	Fyzická ostraha	Všechny MC
B	Specializovaná ochrana	Ochrana speciálních prostor	Kritické zóny MC
C	Detektivní služby	Vyšetřování	Ad-hoc případy
D	Převoz cenin	Transport >5 mil. Kč	Banky, klenotnictví
E	Technické služby	Monitoring, údržba	Všechny MC
F	Bezpečnostní poradenství	Analýzy, audity	Strategické plánování

- **Kategorie A:** Fyzická ostraha (např. stálá strážní služba), významně snižuje riziko přímým zásahem a odpuzujícím efektem. Fyzická ostraha (redukce až 25 %), ovlivněná rozsahem služby (8/12/24h) a výzbrojí.
- **Kategorie B:** Vyškolený personál a krizové řízení, přispívá ke schopnosti reagovat na incidenty a minimalizovat škody. Specializovaná ochrana, například ozbrojený doprovod, psovodi, případně osobní ochrana VIP osob. (až 30 % redukce), závislá na výcviku personálu.
- **Kategorie C a D:** Zlepšují koordinaci a rychlost reakce v krizových situacích. Detektivní služby a převoz cenin (8 % a 12 %), neovlivňují ovšem přímou ochranu MC.
- **Kategorie E:** Technická opatření (CCTV, alarmy, řídicí systémy), která zajišťují detekci a monitorování. Zahrnuje využití bezpečnostních technologií, typicky PCO, dálkový monitoring, poplachové systémy a napojení na zásahové jednotky. Technické zabezpečení (až 18 %), modifikováno přítomností monitoringu a rychlostí zásahu.
- **Kategorie F:** Zahrnuje pravidelné bezpečnostní audity, kontroly, konzultace a celkový proces neustálého zlepšování ochrany. Tyto na první pohled administrativní nástroje mají ovšem velký význam v prevenci (15% redukce rizika).

Každá z definovaných šesti kategorií bezpečnostních služeb má v metodice přidělenou základní míru snížení rizika. Součet jejich přínosů může být navýšen bonusem za kombinaci (tzv. synergický efekt), který reflektuje přínos komplexní ochrany. Pokud jsou zavedeny alespoň dvě různé kategorie, metoda TRS přičítá kombinační bonus a u většího počtu opatření roste i jejich vzájemná účinnost.

Tabulka 4 - Redukční faktory kategorií SBS (zdroj: vlastní).

SBS Kategorie	Základní redukce	Modifikátory
Kategorie A	25 %	Pokrytí × Ozbrojení
Kategorie B	30 %	Speciální výcvik
Kategorie C	8 %	Žádné
Kategorie D	12 %	Žádné
Kategorie E	18 %	Monitoring × Odezva
Kategorie F	15 %	Žádné
Kombinační bonus	+10-15 %	Počet kategorií
Celková SBS redukce	Max 80 %	Součet všech

6.1.3 Výsledné Total Risk Score a interpretace rizikové úrovně

Po výpočtu finální hodnoty TRS_{final} , které se pohybuje v rozsahu 0-300 spadá analyzovaný objekt do jedné z pěti kategorií. Metodika, jak bylo výše zmíněno, na základě úrovně rizika nabízí zvolení adekvátní kategorie SBS a konkrétní bezpečnostní opatření vedoucí k navýšení ochrany tohoto MC.

Tabulka 5 - Kvantitativní klasifikace rizikových úrovní s doporučenou kategorií SBS (zdroj: vlastní).

Rizikové skóre	Úroveň rizika	Priorita	Doporučené SBS kategorie	Časový rámec implementace
0-75 bodů	Nízké	Rutinní opatření	F (poradenství)	3-6 měsíců
76-150 bodů	Střední	Zvýšená pozornost	A (8-12h) + E nebo E + F	1-3 měsíce
151-225 bodů	Vysoké	Okamžitá opatření	A (12-24h) + E + F	2-4 týdny
226-300 bodů	Kritické	Urgentní akce	A (24h) + B + E + F	1-7 dní

Rizikové úrovně definované v rámci metody TRS slouží jako praktický nástroj pro rozhodování o tom, jaká bezpečnostní opatření zvolit a jak případně efektivně rozdělit investice. Ke každému pásmu rizika jsou přiřazena konkrétní doporučení. Včetně návrhu časového rámce k implementaci těchto doporučení v závislosti na úrovni rizika.

Nízké riziko (TRS = 0 až 75). V tomto případě je stav zabezpečení považován za optimální, kde objekt vykazuje nízkou zranitelnost, není pro útočníky příliš atraktivní nebo se nachází v bezpečném prostředí.

Doporučení: Udržovat současný stav, pokračovat v monitoringu a pravidelných auditech (SBS kategorie F). Případná zlepšení jsou spíše drobná a preventivní.

Střední riziko (TRS = 76 až 150). Mohou se vyskytovat menší slabiny nebo mírně vyšší míra hrozby, celkově ale není situace nijak alarmující. Doporučuje se pokračovat v dohledových činnostech a zvážit například častější preventivní kontroly.

Doporučení: Provést základní preventivní opatření a udržovat dohled. Například rozšířit kategorii F o preventivní kontroly kategorií A, zajistit, aby současná opatření neklesala v účinnosti. Stále platí, že stávající úroveň zabezpečení je většinou dostatečná a riziko akceptovatelné.

Vysoké riziko (TRS = 151 až 225). Situace je vážná, objekt má vysoké zranitelnosti nebo působí v rizikovém prostředí. Bezpečnostní opatření jsou zjevně nedostatečná

Doporučení: Intervenovat cíleně tam, kde jsou slabiny. Např. posílit fyzickou ochranu, zvážit zavedení ostrahy (SBS kategorie A) alespoň po kritické hodiny dne, případně kombinovat elektronická opatření (SBS kategorie E, např. lepší přístupové systémy) s auditem (SBS kategorie F). Cílem je aktivně snížit riziko na přijatelnější úroveň, což může zahrnovat ad-hoc investice do bezpečnosti a organizační změny.

Kritické riziko (TRS = 226 až 300). Objekt je vysoce ohrožen, a jeho současné zabezpečení je zcela nevyhovující.

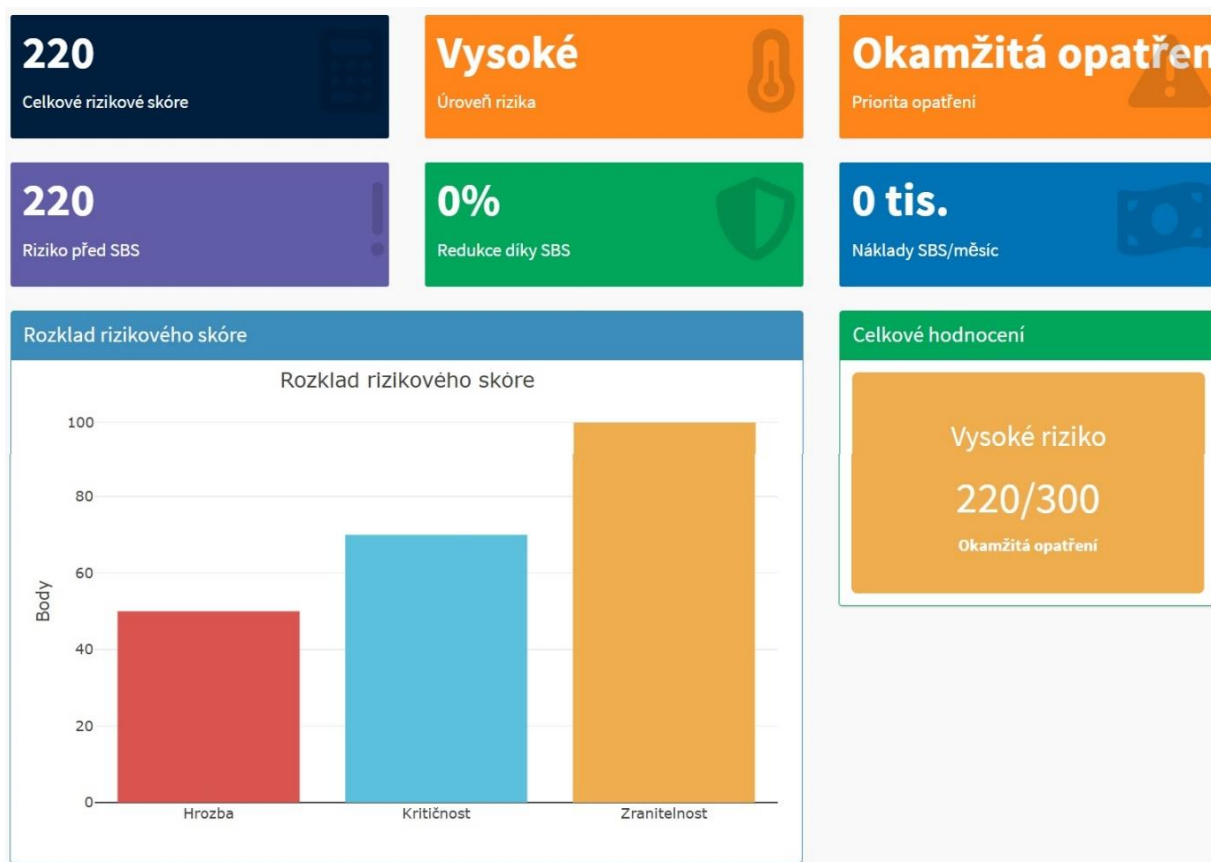
Doporučení: Okamžitě zavést komplexní soubor opatření a plně implementovat všechny kategorie bezpečnostních služeb (A + B + E + F). To znamená nasadit 24/7 ozbrojenou ostrahu, vyškolit personál, zprovoznit špičkové technické systémy s centralizovaným dohledem a zavést intenzivní režim auditů a kontrol. Nezbytná je také úzká spolupráce s PČR, případně dalšími státními bezpečnostními složkami. V této fázi se zpravidla realizují krizová opatření a může být

zvažováno i omezení provozu či dočasné uzavření objektu, dokud není zajištěna vyšší míra bezpečnosti.

6.1.4 Aplikace metodiky TRS a závěry

Navržená metodika TRS je konstruována tak, aby byla prakticky použitelná pro široké spektrum MC. Metoda TRS je univerzální a lze ji přizpůsobit různým typům MC. Základní rámec VxCxT zůstává stejný, ale důraz na jednotlivé složky se liší podle typu analyzovaného objektu.

TRS tyto rozdíly zohledňuje pomocí konkretizovaných check-listů (kapitola 15) a umožňuje objektivní porovnání podobných lokalit. Například lze identifikovat, proč je jedno nákupní centrum rizikovější než jiné. Metodika je navržena tak, aby byla srozumitelná i pro osoby mimo oblast bezpečnosti. Barevně rozlišené stupně rizika (např. zelená = nízké, červená = kritické) a přiřazené konkrétní doporučení k navýšení bezpečnosti tak vizuálně zjednodušují výstupy vyhodnocení a jejich výklad. Pro ilustraci je předložen výstup hodnoceného fiktivního MC se slabým zabezpečením, bez nasmlouvaných služeb SBS a tím vysokou V (zranitelností) a C (kritičností). Výsledkem je zařazení objektu do kategorie vysokého rizika (TRS = 220).



Obrázek 14 - Vizualizovaný výstup metodiky TRS (zdroj: vlastní - RShiny).

Dle kategorie TRS jsou automaticky navržena konkrétní opatření k redukci rizika, včetně definované formy nasmlouvání SBS. Návrh metody je připraven i na případné vyčíslení nákladů na SBS pro daný MC například i pro potřeby pojištění, ovšem tato funkcionality je v přípravné fázi a je zatím v metodě nastavena pouze orientačně. Doporučení a opatření nastavené k adekvátní kategorii TRS jsou ve výstupech prezentována formou jednotlivých bodů s doporučeným časovým rozpětím jejich implementace.

Prioritní doporučení

⚠ VYSOKÉ RIZIKO - Rychlá opatření

Doporučené SBS kategorie:

- **Kategorie A** - 12h fyzická ostraha v provozní době
- **Kategorie E** - technické služby a monitoring
- **Kategorie F** - bezpečnostní poradenství

Další opatření:

- Upgrade současných bezpečnostních systémů
- Školení zaměstnanců v bezpečnostních postupech
- Registrace návštěvníků

Očekávaná redukce rizika: 45-60% | Náklady: 150-300 tis. Kč/měsíc

Implementační kroky

Okamžité kroky (1-7 dní):

1. Kontakt na bezpečnostní firmu
2. Základní bezpečnostní opatření
3. Informování zaměstnanců

Krátkodobé kroky (1-4 týdny):

1. Implementace doporučených systémů
2. Školení personálu
3. Testování postupů

Obrázek 15 - Návrh opatření k navýšení bezpečnosti MC a jednotlivé implementační kroky (zdroj: vlastní - RShiny).

V tabulce 5 je uveden přehled typologických MC a stanovení jejich TRS na základě teoretických předpokladů provedených testovacích vyhodnocení MC. Výstupem je souhrnný benchmarking pro tyto typové MC.

Tabulka 6 - Benchmarking dle typologie objektů MC (zdroj: vlastní).

Typ objektu	Průměrné TRS	Nejlepší praxe	Kritické hodnoty	Doporučené SBS
Nemocnice	145 ± 25	<100	>200	A + E + F
Základní školy	120 ± 30	<80	>180	A + F
Obchodní centra	160 ± 35	<120	>220	A + B + E
Nádraží	180 ± 40	<140	>240	A + B + E + F
Stadiony	200 ± 45	<150	>260	A + B + E + F
Univerzity	135 ± 25	<100	>190	A + E + F
Úřady	125 ± 20	<90	>170	A + F

Důležitým přínosem navržené metodiky je, že poskytuje podložená doporučení pro rozhodování. Dokáže identifikovat konkrétní slabiny (např. nedostatečné kamerové pokrytí nebo absence fyzické ostrahy apod.) a přiřadit jim priority. Je tedy nejen akademickým

nástrojem v rámci výstupů disertační práce, ale i praktickou pomůckou pro orgány státní správy, bezpečnostní agentury ale i přímo pro samotné provozovatele MC a jejich bezpečnostní management, který zodpovídá za přijetí adekvátních bezpečnostních opatření.

Mezi klíčové inovační prvky vlastní navržené metody TRS patří zejména:

- **Objektivní metriky:** Všechny vstupní parametry hodnocení jsou založeny na měřitelných veličinách v souladu se standardy ISO 31000:2018. Hodnocení je opakovatelné a lze ho provést jak online, tak fyzicky v místě hodnoceného MC.

Konkrétní návrh využití SBS: Inovativní výstupy z navrhované metody přímo doporučují na základě velikosti TRS formu využití bezpečnostních agentur a jejich služeb. Jedná se tak o první metodu, která nabízí jako konkrétní formu ochrany MC využití SBS.

- **Prediktivní schopnosti:** Díky kvantitativní povaze lze model využít k modelování budoucích scénářů a predikci dopadů změn (např. simulace zvýšení hrozby či účinku nových opatření). Jinými slovy je metoda velice flexibilní a dokáže porovnávat různé bezpečnostní verze téhož MC. Tato funkcionalita je velice cenná pro bezpečnostní management jednotlivých MC, jelikož takto navržená metoda dokáže pomoci v prioritizaci zavádění bezpečnostních a ochranných opatření.

Metodika umožňuje měřit efektivnost navržených opatření, srovnávat různé objekty, a tím vědecky přispět k diskusi o optimálních strategiích ochrany MC v ČR, i globálně ve světě. Přínos této metody je zejména v navržení konkrétních opatření pro výslednou hodnotu TRS s aktivním a konkrétním zapojením SBS. Navržená metodika byla validována především na základě teoretických předpokladů a ilustračních případů, reálné ověření vyžaduje pilotní testování v praxi.

6.2 Návrh optimálního modelu komerční bezpečnosti v České republice

Na základě komparace jednotlivých evropských modelů komerční bezpečnosti a zkušeností se zapojením SBS lze navrhnout optimální model pro ČR, což je jedním z cílů mé disertace. Navržený model kombinuje osvědčené principy z analyzovaných států (kapitola 4.2) a přizpůsobuje je legislativnímu, kulturnímu i bezpečnostnímu prostředí ČR. Cílem je vytvořit systém, který bude efektivní, transparentní, právně ukotvený a funkčně provázaný s veřejným bezpečnostním sektorem. Komerční bezpečnost přitom nelze chápat jako náhradu státních bezpečnostních složek, ale jako jejich důležitého partnera, který má potenciál posílit prevenci kriminality, vnitřní bezpečnost státu a ochranu MC, pokud mu k tomu stát vytvoří vhodné

podmínky. Můj návrh bodů potenciálního vzniku nového systému, tedy nehledě na poslední návrh zákona o SBS, zahrnuje následující dílčí okruhy.

Legislativní rámec

- Zavedení samostatného zákona o SBS, který by jednoznačně vymezil rámec činnosti včetně práv a povinností subjektů, způsobů licencování a kontroly, sankčního systému a podmínek zajištění odpovědnosti za způsobenou škodu. Tedy legislativní rámec příbuzný analyzovaným zahraničním modelům, mnohem užší než současný poslední návrh zákona o SBS.

6.2.1 Tří úroňová kvalifikace pracovníků

V rámci návrhu nového konceptu ochrany MC navrhuji systematickou kategorizaci zaměstnanců SBS. Tato reflektuje nejen specifika jednotlivých úkolů v MC či jiného navrhovaného zapojení do státních struktur bezpečnosti, ale i rostoucí požadavky na odborné a osobnostní předpoklady jednotlivých pracovníků. Na rozdíl od návrhu kategorizace z posledního návrhu zákona o SBS z roku 2024 by bylo efektivnější rozdělit samotné zaměstnance do kategorií, kteří by následně mohli vykonávat služby dle licencování A-F (viz kapitola 2.1.3). V případě podobného rozdělení na státní úrovni by toto mohlo být rozšířením pro navrženou metodu TRS.

I. Kategorie - základní bezpečnostní pracovník

Základní bezpečnostní pracovník je určen pro činnosti s nízkým až středním rizikem. Typicky se jedná o výkon recepčních služeb, kontrolu vstupů, monitoring kamerových systémů nebo obchůzkovou činnost. Tito pracovníci by měli projít základním kurzem odborné způsobilosti, který by zahrnoval právní minimum, základy komunikace, základy první pomoci a technické aspekty ochrany objektů.

Typické nasazení:

- Administrativní budovy, školy, veřejné instituce.
- Události s nízkou mírou rizika (např. kulturní akce lokálního charakteru).

II. Kategorie - pokročilý bezpečnostní pracovník

Tito pracovníci by byli vyšší úrovní v rámci SBS. Byli by nasazováni do lokalit a situací se zvýšeným rizikem, kde je vyžadována vyšší úroveň odborné přípravy, schopnost zvládat krizové situace a v některých případech i ozbrojená služba. Výcvik by měl zahrnovat taktické

prvky, pokročilou zdravotnickou přípravu, práci s davu a schopnost koordinace s IZS, jak budu dále navrhopvat v dalších kapitolách.

Typické nasazení:

- Velká veřejná shromáždění (koncerty, sportovní utkání apod.).
- Ochrana prvků infrastruktury, logistických center.
- Přeprava hotovostí, cenin a citlivých materiálů vysoké hodnoty.

III. Kategorie - specialista bezpečnostní analýzy a koordinace

Tato kategorie by zahrnovala vysoce kvalifikované zaměstnance SBS, kteří plní funkci analytiků, plánovačů bezpečnostních opatření a koordinátorů se státní správou a složkami IZS. Tito specialisté by byli schopni provádět bezpečnostní audity, plánovat opatření na základě rizikové analýzy, zajišťovat krizovou komunikaci a metodicky vést základní a pokročilé pracovníky. Jejich školení by mělo odpovídat úrovni vysokoškolského studia nebo specializovaných odborných kurzů v oblasti bezpečnosti a krizového řízení.

Typické nasazení:

- Koordinace bezpečnosti na velkých událostech.
- Vytváření plánů ochrany pro MC nebo kritickou infrastrukturu (dále jen KI).
- Spolupráce s veřejnou správou, krizovým řízením a státními bezpečnostními orgány.

Státní dohled

Zřízení centrálního orgánu státního dohledu, který by vedl registr SBS, vydával licence, prováděl kontroly a měl pravomoc pozastavit činnost agentury v případě jednání v nesouladu s legislativními nároky. Inspirací může být např. francouzský systém státního orgánu CNAPS, který kromě dohledu zajišťuje i vzdělávací standardy (viz kap. Analýza francouzského modelu bezpečnosti). V podmínkách ČR by se nabízelo, aby tento dohledový orgán byl pod Ministerstvem vnitra ČR. To by za příznivých podmínek dostatečné profesionalizace SBS mohlo vést až k možnosti, že by se bezpečnostní agentury pod centralizovaným dohledem státu mohly stát jeho organizační složkou po vzoru PČR či HZS ČR.

6.2.2 Efektivní spolupráce s veřejnými orgány

Spolupráce mezi soukromými a veřejnými bezpečnostními složkami by zahrnovala sdílení informací a společné řešení krizových situací. Státní orgány by pak tvořili zároveň výkonný dozor a funkci kontroly nad činností SBS.

Standardizace a audit

Zavedení minimálních standardů kvality služeb, včetně mezinárodních certifikací (např. ISO normy), povinných auditů a profesní odpovědnosti. Každá SBS by měla vést podrobnou evidenci výkonu činností a být připravena na pravidelné kontroly.

Možnost ozbrojení

Zbraně by měly být vyhrazeny pouze pracovníkům, kteří prokazatelně absolvovali výcvik a disponují odpovídající licencí. Použití zbraní by mělo být omezeno na přísně vymezené situace, jako je převoz cenností, osobní ochrana VIP osob či zásah při přímém ohrožení života. V souladu s výše navrhovanou kategorizací pracovníků SBS by se ozbrojení týkalo II. a III. kategorie.

Profesní komora

Zřízení profesní komory SBS, která by zastupovala zájmy subjektů, vydávala stanoviska k legislativním změnám a spolupodílela se na tvorbě odborných standardů. Komora by mohla být také platformou pro vzdělávání a profesní růst pracovníků. Silným doporučením by však bylo, aby tato komora byla centralizovaná, jednotná a podléhala příslušnému ministerstvu na rozdíl od současného decentralizovaného stavu v ČR a existenci několika na sobě nezávislých subjektů.

Zapojení do veřejné bezpečnosti

SBS by mohly na základě smluv s veřejnou správou chránit vybrané kompletní městské části. Spolupráce by měla být formálně zakotvena a vymezena. V tomto konceptu by bylo možné posadit SBS na úroveň městské či obecní policie. I za současného stavu plní zaměstnanci SBS formu primárně situační prevence, ovšem za jasných legislativních podmínek a vztahů, by toto mohly oficiálně dělat pro vybraná území a do jisté míry i práci městských či obecních policistů nahrazovat. Tím by se uvolnily kapacity a tito nestátní policisté by mohli být využíváni efektivněji. Zaměstnanci by měli samozřejmě povinně absolvovat odborné školení,

kteře by zahrnovalo právní předpisy, etiku a techniky používání zbraní. Tato školení by měla být jak vstupní, tak periodická.

Navržené hlavní systémové body, reflektují potřebu profesionalizace a efektivního začlenění soukromého bezpečnostního sektoru do širšího bezpečnostního rámce státu. Významné je zejména nastavení spolupráce mezi SBS a veřejnými složkami, včetně vzájemného respektu, standardizace a kontroly. Takový přístup by mohl zvýšit důvěryhodnost sektoru, posílit ochranu MC a přispět k celkové bezpečnostní stabilitě ČR.

6.3 Inovace v ochraně měkkých cílů a možná nová technologická řešení

Následující část představuje můj analyticko-vizionářský pohled na možné směry technologického rozvoje a vývoje technologií zbraní pro využití SBS, které by mohly být implementovány při dodržení zásad proporcionality, odpovědnosti a právní kontroly, která by musela jít ruku v ruce s těmito návrhy. V textu jsou představeny konkrétní příklady využitelných prostředků, jejich přínosy, nároky na personál a možné scénáře nasazení. Jedná se zejména o nové technické návrhy vybavení zaměstnanců SBS, za splnění předpokladů nárůstu profesionality zejména v oblasti personálních zdrojů a při případné aplikaci výše navrhovaného systému komerční bezpečnosti v ČR.

6.3.1 Technologická výbava pracovníků soukromých bezpečnostních služeb

Moderní technologie jsou skutečnou příležitostí pro pracovníky SBS od pasivního dozorování ke skutečně inteligentnímu výkonu bezpečnostní praxe. Příkladem mohou být systémy na bázi „SmartVest“, tedy vestu vybavenou GPS lokalizací, biometrickými senzory (srdeční tep, tělesná teplota, hladina stresu apod.), nouzovým tlačítkem, integrovanou HD kamerou a připojením na centrální dispečink (velín v místě MC nebo dálkové PCO). Takový systém umožní dispečerům okamžité sledování lokace a stavu všech pracovníků SBS v reálném čase. Navíc, v případě náhlého poklesu vitálních funkcí může systém automaticky spustit alarm a vyslat pomoc během řešení krizové situace. Tento přístup, označovaný jako povědomí či znalost situace (situation awareness), významně ovlivňuje plánování i rychlost zásahu. Na centrálním pultu je možné v reálném čase sledovat pohyb hlídek SBS, jejich počet, výzbroj i technické vybavení, což umožňuje řídicímu důstojníkovi efektivně rozhodnout, která z dostupných hlídek v okolí incidentu bude pověřena jeho řešením. Tento můj návrh efektivnějšího zapojení SBS je určitou analogií armádního systému známého jako „blue force tracking“, samozřejmě s jiným rozsahem a určením.

Další inovací ve výstroji SBS by mohlo být využití chytrých brýlí s rozšířenou realitou. Tyto by mohly SBS pracovníkům zobrazovat informace například o nejbližších evakuačních cestách, profilu podezřelé osoby podle databáze nebo stav bezpečnostních systémů v budově. Zaměstnance SBS lze dle mého návrhu vybavit moderní IT technikou zahrnující mapové podklady, informace o objektech, návrhy zásahových scénářů či dokonce umělou inteligenci schopnou optimalizovat postupy zasahujících týmů. Ačkoli se tento navrhovaný koncept může zdát futuristický a těžko realizovatelný, dynamický rozvoj AI a její rychlá implementace v prakticky všech oborech naznačují, že podobné aplikace mohou být v blízké budoucnosti překvapivě dobře dosažitelné.

Podmínkou pro využití a implementaci mých návrhů by ovšem byla dobrá prostorová orientace pracovníka, znalost krizových scénářů a schopnost práce pod tlakem. Vzdělávání by muselo zahrnovat nejen technický výcvik, ale i psychologickou přípravu na přetížení informacemi. Součástí přijímacího řízení by tak například pro uchazeče byly povinné psychologické testy, což je dle mého zajímavý podnět k diskuzi pro právní ukotvení v rámci připravovaného zákona [107].

Zajímavou možností je také využití nositelných mikroprocesorů například v podobě náramků (Armband computing units), které jsou napojené na kamerový systém a AI analytiku. Tyto jednotky by umožnily detekci podezřelého chování (např. shlukování osob, zrychlený pohyb proti směru proudění davu) a zasílaly by notifikace přímo pracovníkovi například do sluchátek. V praxi by to znamenalo snížení reakčního času při identifikaci hrozby z minut na sekundy. Samozřejmě veškeré tyto návrhy s vyhodnocením by musely vycházet ze strukturované databáze tak, aby byla varování AI a technologií validní, přece jen následující reakcí ze strany SBS by bylo zadržení či jiné omezení podezřelé osoby, pro takovou akci by musela být vyhodnocení co nejpřesnější.

6.3.2 Technologická řešení po vzoru společnosti Genasys

Směrnice Evropského parlamentu a Rady (EU) 2018/1972 v čl. 110 ukládá členským státům povinnost vybudovat systém veřejného varování, který dokáže prostřednictvím mobilních sítí (cell broadcast či SMS) automaticky oslovit všechny osoby nacházející se v ohrožené oblasti, bez nutnosti registrace a včetně doručení varovné zprávy cizincům. Zprávy mají být cílené, srozumitelné a doručené v co možná nejkratší době. Společnost Genasys je příkladem řešení, které tyto požadavky technicky naplňuje prostřednictvím svého vícekanálového systému hromadného varování (Mass Notification System - MNS). Jádrem systému je integrace

s mobilními sítěmi a možnost geo-cíleného rozesílání zpráv včetně podpory více světových jazyků. Systém navíc kombinuje mobilní komunikaci s dalšími kanály, jako jsou akustické sirény, sociální média, veřejné databáze či specializované aplikace, a díky modularitě a škálovatelnosti jej lze přizpůsobit podmínkám jednotlivých států. Genasys tak nejen splňuje legislativní rámec EU, ale umožňuje efektivně reagovat na různé typy krizí, od přírodních katastrof po bezpečnostní hrozby včetně útoků na MC [108].

Systém Genasys NEWS (Notification, Emergency, Warning System) zase zahrnuje prvky jako jsou Long Range Acoustic Device (dále LRAD - akustická varovná zařízení), zmíněné geo-lokalizované cell broadcast SMS zprávy a další. Cloudová infrastruktura systému zároveň zaručuje spolehlivý provoz.

SBS jsou často fyzicky přítomny v místech, které ochraňují. Pokud by byli jejich zaměstnanci vybaveni přístupem k systému podobného typu jako je společnost Genasys, mohli by přímo ze svého zařízení předávat relevantní informace do systému a zároveň přijímat aktuální pokyny nebo výstrahy. Technologie jako LRAD mohou být instalovány v perimetru chráněných lokalit a ovládány pracovníky SBS v případě vyhlášení krizové situace (např. evakuace, útok, požár, únik nebezpečných látek apod.).

Pracovníci SBS by mohli figurovat jako operátoři s definovanými rolmi v rámci krizového hlášení včetně možnosti předávat hlasové zprávy, aktivovat digitální výstrahy a koordinovat své kroky s dispečinkem složek IZS. V prostředí obchodních center nebo uzavřených kampusů by systém mohl fungovat jako vnitřní bezpečnostní síť, s rozdělením odpovědností a centrální kontrolou.

6.3.3 Funkce reverzní 112

Je to forma krizové komunikace, která využívá mobilní síť k cílenému varování obyvatelstva v určité lokalitě, kde hrozí nebezpečí nebo již došlo k mimořádné události. Tato technologie má potenciál hrát klíčovou roli nejen v IZS, ale také při zajišťování ochrany MC za účasti SBS. V hypotetickém rozšířeném modelu spolupráce by mohli zaměstnanci SBS fungovat jako operátoři nebo aktivní distributoři informací v rámci systému reverzní 112. V případě výskytu hrozby (např. připravovaný útok, nález podezřelého balíčku, výskyt ozbrojené osoby apod.) by zaměstnanci SBS mohli okamžitě skrze digitální platformy nebo operační střediska IZS aktivovat zprávu, která by se na základě geolokace dostala k osobám nacházejícím se v rizikové oblasti.

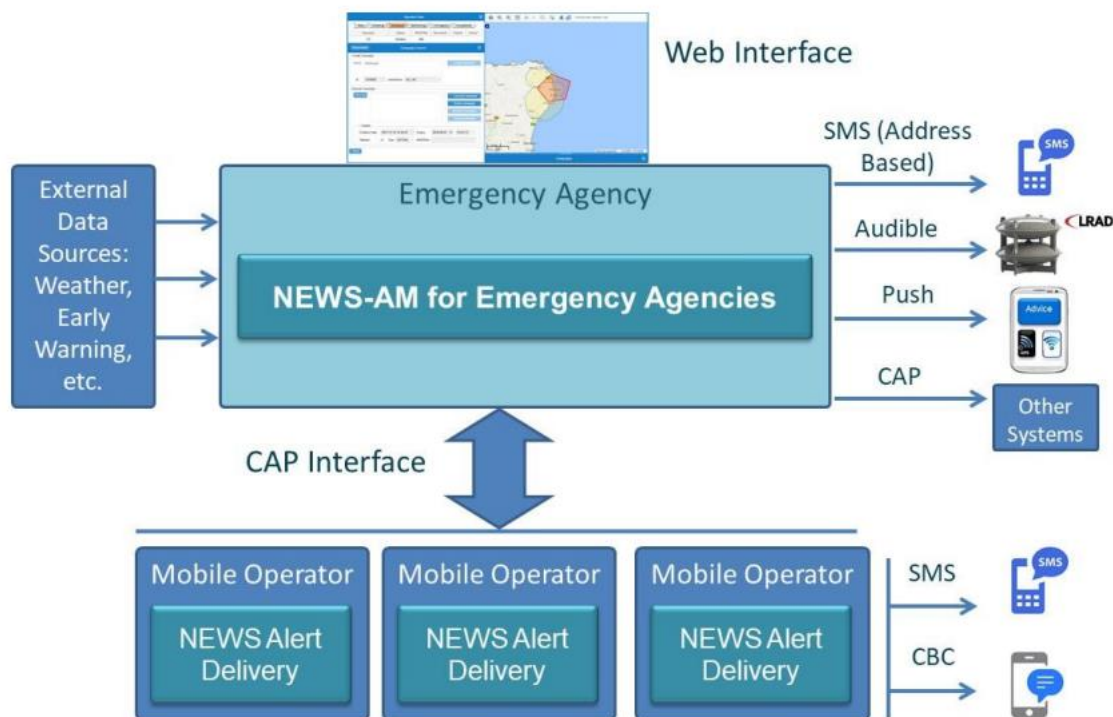
Tato funkce by byla mimořádně efektivní zejména v prostorách MC. V případě útoku by zaměstnanci SBS mohli neprodleně informovat příslušný orgán IZS o situaci, ten by v kooperaci s technologickým operátorem spustil textovou nebo hlasovou zprávu určenou obyvatelům v oblasti, obsahující pokyny pro uchování (např. "Zůstaňte na místě a uzamkněte dveře," "Odejděte směrem k východu A" apod.). Zaměstnanci SBS by také mohli sloužit jako zprostředkovatelé zpětné vazby. Pokud jsou přímo fyzicky v místě mimořádné události, mohou poskytovat doplňující informace k aktualizaci obsahu zpráv. V kombinaci se systémy typu zmíněného Genasys NEWS, by mohli disponovat mobilní aplikací s oprávněním pro vstup do platformy a spuštění hlášení, který by byl koordinován po linii IZS.

Důležitá je také preventivní role. Zaměstnanci BA by v základním modelu mohli být začleněni do krizových plánů obcí a organizací jako podpůrná jednotka pro šíření informací při mimořádných událostech a pro poskytování asistované evakuace (bude rozebráno níže v rámci IZS).

Ačkoliv by praktické nasazení reverzní 112 skrze SBS vyžadovalo legislativní a technické podmínky, akademická úvaha o této formě spolupráce ukazuje na možnost využití stávajících personálních kapacit pro zlepšení reaktivity a efektivity ochrany MC v ČR již teď. Implementace tohoto typu systému u SBS by zvýšila míru samostatnosti a akceschopnosti těchto jednotek. Pracovníci by se mohli stát efektivním prvkem krizového řízení s možností podávat výstrahy, vést osoby k evakuaci, a zajišťovat přenos klíčových informací mezi místem incidentu a OPISy složek IZS [109,110,111,112,113,114].

V současných podmínkách ČR by implementace systému jako je Genasys mohla probíhat ve spolupráci s mobilními operátory, krajskými krizovými štáby a velkými správci veřejných prostor a MC. SBS by mohly zaujmout místo operativních partnerů v terénu, čímž by se zvýšila rychlost reakce a pokrytí při mimořádných událostech a útocích.

Pro představu je přiloženo schéma využití mobilních operátorů (obr. 16) v systému varování právě společností Genasys, jedná se o zpracování dat a informací, které jsou následně distribuovány koncovým uživatelům (obyvatelstvu) či do dalších systémů. Vzhledem k ukázce funkce systému a jeho autentičnosti nebyl obrázek překládán do českého jazyka.



Obrázek 16 - Využití mobilních operátorů v systému varování společnosti Genasys[109].

6.3.4 Neletální zbraňové systémy a jejich možnosti využití v komerční bezpečnosti

Neletální prostředky mohou sehrát významnou roli v ochraně MC, především v těch s vysokou koncentrací civilního obyvatelstva. Akustické zařízení typu LRAD, které je výše zmíněné, je schopno vydávat hlasité výstražné zprávy až bolestivě intenzivní zvuky vedoucí k odvrácení osob bez nutnosti fyzického kontaktu. Nasazení tohoto zařízení SBS pracovníkem by vyžadovalo nejen školení v oblasti fyziky zvuku, ale také znalost právních limitů, např. v ochraně zdraví neslyšících osob nebo dětí. Jinými slovy by bylo využití tohoto typu technologického prostředku velice náročné, jelikož nelze očekávat stejnou reakci ode všech osob, některým by mohla způsobit fatální následky, a nejen krátkodobou paralyzaci [115].

Další alternativou v oblasti neletálních technologií jsou neletální projektily jako jsou paintballové nebo pepřové kapsle vystřelované například z FN303 nebo systému PepperBall. Zbraně umožňují označit útočníka, dočasně ho dezorientovat a zároveň minimalizovat riziko trvalého zranění. Systém může být efektivní zejména při ochraně vstupních bran na stadionech či při odklonu davu. Pracovníci SBS by v takovém případě museli projít balistickým výcvikem, znalostí efektivní vzdálenosti střelby a rozpoznáním zdravotních kontraindikací u zasažených osob [116].

Speciální síťové vystřelovače lze použít k rychlému znehybnění útočníka z bezpečné vzdálenosti. Výhodou je schopnost zasáhnout osobu v úzkém prostoru nebo ve chvíli, kdy se útočník pokouší uprchnout. Tento prostředek je však nutno použít s maximální přesností, trénink by musel zahrnovat simulace v reálném prostředí. Tato varianta by pro vybavení zaměstnanců SBS byla vhodnější k ochraně symbolických MC s nižší koncentrací civilního obyvatelstva, ovšem s vyšší nutností citlivého zneškodnění ve jménu ochrany majetku a reputace místa [107].

6.3.5 Letální prostředky ochrany

Použití střelné zbraně pracovníkem SBS je nejzazším řešením, které by mělo být dovoleno pouze ve výjimečných a legislativně přesně vymezených situacích tak, jak je tomu nastaveno ve výše analyzovaných modelech jiných evropských států. Opět několikrát zmiňovaný francouzský model CNAPS ukazuje, že omezené ozbrojení SBS může být možné při přísném licencování, pravidelném výcviku a státním dozoru. Návrh na ozbrojení kategorií zaměstnanců SBS byl výše v práci zmíněn.

Letální výbava by dále mohla zahrnovat pistole se smart-lock mechanismem, který znemožňuje použití zbraně neoprávněnou osobou tak, aby se předešlo odcizení a zneužití. Součástí výbavy by bylo záznamové zařízení s GPS a akcelerometrem. Systém by uchovával digitální záznam každého výstřelu pro případné přezkoumání důvodů a okolností střelby. Uplatnění je představitelné v prostředích s reálným rizikem útoku střelnou zbraní např. VIP akce nebo rizikové převozy finančních hotovostí. Tento příklad spíše prezentuje doplnění existujících zbraňových prostředků a je závislé na možnosti užit zbraní ze strany SBS jako takové.

6.4 Pohled do blízké budoucnosti a vize soukromých bezpečnostních služeb

6.4.1 Využití personálu a civilního obyvatelstva ke zvýšení bezpečnosti

Budoucnost může přinést další revoluci v ochraně MC, pokud budou SBS vybaveny technologiemi, které dnes známe spíše z vědecko-fantastických filmů.

Například exoskeletony by umožnily pracovníkům SBS nosit těžké vybavení, zasahovat déle bez vyčerpání a přemísťovat zraněné osoby, jelikož by samotná konstrukce dopřávala uživateli značnou sílu. K tomu by však bylo třeba zdravotních předpokladů, speciální

biomechanické diagnostiky a značné energetické zabezpečení (např. přenosné baterie s výdrží alespoň více než 8 hodin vhodných pro zásah ve složitých podmínkách, například po útoku).

Užití mikrodronů pro průzkum interiérů by mohlo pracovníkům SBS umožnit získat přehled o situaci v uzavřených prostorech během několika sekund. Mohly by být naprogramovány na letové vzorce např. po budově školy při podezření na aktivního střelce. Ovládání by vyžadovalo trénink na simulátorech a schopnost vyhodnocení dat z termokamery nebo jiných detekčních čidel.

Dalším z možných prvků budoucnosti je využití nositelných zařízení s rozšířenou realitou, která byla výše již zmíněna.

Zavádění tzv. „biometrických zón“ využívajících stochastické profilování je možnou další cestou navýšení efektivity ze strany SBS. Tyto zóny, např. v okolí letišť, by sledovaly chování osob bez nutnosti přímé identifikace, analyzovaly by držení těla, styl chůze, mimiku a další biometrické ukazatele. Pomocí umělé inteligence by se vyhodnocovalo možné rizikové chování a pracovníci SBS by byli včas upozorněni na potřebu prověřit určitou osobu. Takový systém musí být navržen v souladu s právními předpisy a s ohledem na ochranu osobních údajů (viz kap. 4.3).

Zpevňování lokalit není jen otázkou betonu a techniky. Klíčová je i příprava zaměstnanců a návštěvníků. Personál by měl být školen v rozpoznávání neobvyklého chování, ve vyhlašování evakuace, i v zachování klidu. V USA a Izraeli se používá tzv. „behavioral detection“, kdy vycvičení pracovníci sledují mimiku, pohyb a známky nervozity. V těchto případech je velice důležité zachovat klid a klidné prostředí během detekce potenciálního útočníka tak, aby nedošlo k davovému šílenství během masových akcí nebo jiné aktivity spojené s MC. Zde je opět velice důležitá případná souhra mezi zaměstnanci daného objektu, tedy MC a zaměstnanci SBS [117].

Na myšlence využití samotného civilního obyvatelstva staví mezinárodně rozšířená kampaň 'If You See Something, Say Something', která byla poprvé spuštěna v New Yorku po 11. září 2001 a později převzata Ministerstvem vnitřní bezpečnosti USA. Cílem této iniciativy je aktivní zapojení veřejnosti do procesu včasné identifikace podezřelého chování, předmětů nebo osob, a následné upozornění příslušných autorit. Pro SBS je důležité zpracovat manuály, vizuální přehledy nebezpečných situací a standardizované reakční postupy, čímž lze zvýšit efektivitu ochrany měkkých cílů bez nárůstu stresu nebo paniky mezi lidmi [118].

Veřejnost totiž představuje největší a zároveň nejrozptýlenější „senzorový“ systém, lidé jsou přítomní v každodenním provozu a mají nejlepší představu o tom, co je v daném prostoru obvyklé a co ne. Typické příklady zahrnují ponechané zavazadlo v dopravním uzlu, podezřelé chování u vstupu do školy či nákupního centra, manipulaci s technickými zařízeními nebo výstupními cestami, projev nervozity, mapování prostoru nebo záznam vybavení na kameru. Pro úspěšné využití tohoto principu v ČR by bylo důležité kultivovat bezpečnostní gramotnost veřejnosti. Veřejné informační kampaně mohou přispět ke zvýšení vnímavosti k bezpečnostním signálům bez vzniku zbytečné paniky.

SBS by pak byly v novém formátu prvním fyzicky přítomným bezpečnostním prvkem v místě MC. Vhodně školení pracovníci SBS by měli být vybaveni nejen dovednostmi, jak na taková hlášení reagovat, ale také jak komunikovat s veřejností důvěryhodně, klidně a efektivně. Měli by být viditelně identifikováni, procházet školením v oblasti komunikačních dovedností a krizové komunikace, a mít přístup k jednoduchým operačním protokolům pro evidenci a eskalaci incidentů.

Moderní přístup ke konceptu 'See Something, Say Something' využívá i mobilní aplikace pro anonymní hlášení podezřelé aktivity, jako je například AlertCops ve Španělsku, či technologie které dokázaly několika útokům předejít díky včasným hlášením v USA. Tyto technologie (kamerové systémy s AI, detekce zbraní apod.) jsou slibné, ale je nutné vyhodnocovat jejich efektivitu. Tyto konkrétní zahraniční technologie a jejich využití jsou opět inspirací pro využití v ČR a například propojení obdobných aplikací s SBS, které by mohly plnit funkci ověřovacího prvku s následným rozhodnutím o zásahu [119,120].

6.4.2 Návrh možných forem zapojení soukromých bezpečnostních služeb v integrovaném záchranném systému České republiky

IZS ČR je primární platforma pro řešení mimořádných událostí a krizových situací. Je tvořen základními složkami a ostatními složkami, které se podílejí na plnění specifických úkolů a mezi sebou spolupracují. Přestože SBS v současné době nejsou oficiální součástí IZS, představují významný potenciál pro rozšíření jeho kapacit a zefektivnění reakce na krizové situace, zejména pak v prostředí MC.

Opět za předpokladu legislativního ukotvení, ať tedy vzniku nového zákona o SBS či úpravou krizových zákonů by mohly být SBS zapojeny jako ostatní složka IZS se specifickou působností v oblasti fyzické bezpečnosti, krizové komunikace, základní první pomoci (například v podobě tzv. „first responders“) nebo řízení evakuace. Tito pracovníci

by byli vyškoleni v základních procedurách ochrany obyvatelstva a koordinace se složkami IZS. Mohli by například působit jako styčný bod mezi místem události a krizovým štábem, poskytovat informace o počtech osob, charakteru hrozby či průběhu evakuace.

Ve vztahu k PČR by SBS mohly spolupracovat na zajištění perimetru, usměrnění davu, předání podezřelých osob nebo monitoringu pomocí kamerových systémů, celkově jako podpora udržení veřejného pořádku. V rámci Zdravotnické záchranné služby (dále jen ZZS) by SBS pracovníci vyškolení jako „first responders“ a mohli by asistovat při třídění zraněných, provádět základní resuscitaci či navigaci pacientů k ošetření. V oblasti požární ochrany a funkce HZS ČR by mohli SBS pomoci při evakuaci objektů, zajištění bezpečnostních koridorů nebo komunikaci s přítomnými civilisty.

Na MC představují SBS často jedinou fyzicky přítomnou bezpečnostní sílu v prvních minutách incidentu. Jejich zařazení do systému IZS by umožnilo okamžitou aktivaci koordinace, např. digitálním hlášením operačnímu středisku (například pomocí systému Genasys, jak bylo výše diskutováno), organizací únikových cest či psychologickou intervencí u evakuovaných osob. SBS by mohly rovněž fungovat jako lokální informační uzel pro příjezdové jednotky IZS.

V modelovém scénáři aktivního střelce v obchodním centru by SBS zaměstnanec provedl okamžité spuštění poplachu, aktivaci evakuačních tras, přivolání PČR a zahájení zajištění prostoru. Při hromadné dopravní nehodě na železničním nádraží by mohli SBS řídit dav, poskytovat psychologickou podporu a pomáhat s prvotním roztríděním raněných. Nebo například při chemickém úniku v průmyslové zóně by SBS zajistili prostor, upozornili přítomné a spolupracovali s HZS na bezpečné evakuaci. Tyto možnosti by nebyly ani legislativně náročné, vztah by se dal smluvně vyjednat. Ale v současné době pro tento model v ČR chybí profesionalita zaměstnanců SBS.

Naopak začlenění SBS do základních složek IZS by vyžadovalo jasné právní ukotvení, definici kompetencí, systém certifikace, pravidelný výcvik apod. Výměnou za to však může stát získat flexibilní a rychle nasaditelnou kapacitu, která je přítomna v místech mimořádných událostí dříve než profesionální složky a za okolností profesionalizace i velice široce využitelná. Toto tvrzení vychází ze současné dislokaci bezpečnostních agentur po území ČR, která je velice komplexní. Pro tento model spolupráce se ale nabízí, aby SBS spadaly přímo pod příslušné ministerstvo, jak bylo výše skrze kontrolní orgán diskutováno, a po vzoru PČR či HZS ČR byly organizačním nástrojem státu a jeho bezpečnostní platformou s jasnou

hierarchickou organizací. Tento návrh však naráží na problematiku vysokého nárůstu státních zaměstnanců, což by bylo neprůchodné politické rozhodnutí v ČR.

6.4.3 Role First Responders v rámci soukromých bezpečnostních služeb při ochraně měkkých cílů

Role SBS jako „first responders“ byla v minulé kapitole zmíněna. V ČR je inspirativním příkladem implementace tohoto konceptu projekt Zdravotnické záchranné služby Královéhradeckého kraje (dále ZZS KHK). Zde byli vybrané civilní osoby školeni ve spolupráci se ZZS KHK k poskytování první pomoci a rychlé reakci na krizové situace spojené se zdravotními příčinami. Díky speciálnímu výcviku mohou být přivoláni dispečerem ZZS KHK jako nejbližší dostupná jednotka, která do příjezdu profesionální pomoci zahájí základní záchranné kroky. Tito dobrovolníci bývají vybaveni AED (automatickým externím defibrilátorem), krvácivými sadami a základními ochrannými pomůckami.

Princip by bylo možno efektivně využít právě při ochraně MC, přednostně u hromadných akcí. Fyzicky přítomní zaměstnanci SBS, kteří mají k dispozici prostředky a školení, mohou být v krizových chvílích zásadním spojem mezi ohroženými civilisty a profesionálními zdravotníky. Při útoku, zdravotní příhodě nebo panice mohou jako první zahájit krizovou komunikaci, stabilizovat situaci a řídit prvotní evakuaci. Jejich činnost by tím zvyšovala šanci na přežití obětí a snižovala rozsah paniky.

Aby bylo možné efektivně implementovat systém „first responders“ skrze SBS, je nutné zajistit vhodný výběr zaměstnanců z řad BA, absolvování odborného kurzu první pomoci (ve spolupráci se ZZS), pravidelná cvičení, koordinace s krajskými operačním střediskem IZS, jasně stanovené pravomoci a odpovědnosti, a právní ošetření odpovědnosti za zásah. Tyto kroky vyžadují nejen ochotu na straně SBS, ale také a opět metodickou a legislativní podporu ze strany státu.

Začlenění principu „first responders“ do činnosti SBS může zefektivnit ochranu MC. Příklad systému z Královéhradeckého kraje ukazuje, že i bez rozsáhlých legislativních změn lze vybudovat funkční spolupráci, která pomáhá zachraňovat životy a posílit kapacity ZZS. Tento model je dobře využitelný právě v kontextu ochrany MC, a to právě při útocích s vyšším počtem raněných, jak bude dále diskutováno [121].

6.4.4 Možné zapojení zaměstnanců soukromých bezpečnostních služeb do třídění raněných při mimořádných událostech měkkých cílů

V případě hromadných neštěstí medicíny katastrof je triage (třídění zraněných) klíčovým prvkem zajištění účinné efektivní záchrany osob, jelikož se jedná zpravidla o nepoměr mezi zasaženými a poskytujícími první pomoc. Vzhledem k tomu, že zaměstnanci SBS bývají na místě incidentu dříve než jednotky IZS, pokud v dané lokalitě mají smluvní vztah, otevírá se otázka jejich možného zapojení do základní formy třídění postižených v případě útoku na MC.

Přestože zaměstnanci SBS nejsou zdravotnickými profesionály, mohou opět při adekvátním výcviku a vybavení sehrát důležitou roli v tomto prvotním třídění a poskytnutí první pomoci, jehož účelem je rychlé rozpoznání život ohrožujících stavů a jejich označení pro příjezd ZZS. Tento model by mohl vycházet z jednoduchých triage systémů jako START (Simple Triage and Rapid Treatment), kde se zranění rozdělují do čtyř kategorií dle naléhavosti pomoci barevných označení.

Můj návrh tedy spočívá ve vybavení zaměstnanců SBS jednoduchými triage kartami, reflexními páskami pro označení pacientů a základním vybavením k zajištění životních funkcí (např. resuscitační masky, škrtidla, AED). Po přijetí incidentu by pracovníci prováděli prvotní průchod zasaženou oblastí a poskytli informace o rozsahu zranění příslušným složkám IZS. Aby byla tato role reálná, je nezbytný pravidelný standardizovaný výcvik ve spolupráci s ZZS krajů, jak bylo rozebíráno výše u modelu „first responders“. SBS pracovníci by měli být schopni spolupracovat se zasahujícími složkami v rámci předem definovaných scénářů. Výcvik by zahrnoval rozpoznání typových poranění, krizovou komunikaci či například řízení paniky a prováděl by se společně s pravidelnými cvičeními složek IZS. Tento model dalšího zapojení SBS by potenciálně vedl ke snižování počtu obětí během útoků na MC.

6.4.5 Možnosti zapojení soukromých bezpečnostních služeb k ochraně kritické infrastruktury

Kritická infrastruktura (dále KI) představuje soubor prvků, systémů a služeb, jejichž narušení by mělo vážné dopady na bezpečnost a chod státu, bezpečnost jeho obyvatel nebo ekonomickou stabilitu. Tradičně je ochrana těchto prvků v gesci státu, především ozbrojených bezpečnostních složek, jako jsou PČR nebo Armáda ČR. Vzhledem k rozšiřujícím se hrozbám a nárokům na zabezpečení je můj další návrh zapojení SBS jako podpůrného prvku ochrany KI. Nabízí se jejich využití jako prvního stupně fyzické ochrany KI, zejména fyzická

ostraha perimetru a daného objektu, kontrola přístupu a monitorování pomocí kamerových a senzorických systémů. Zde by SBS mohly snížit zátěž státních složek a zároveň zvýšit flexibilitu systému ochrany. Další významnou oblastí je krizové řízení. V rámci modelu rozšířeného IZS diskutovaného v práci výše, do kterého by SBS byly zahrnuty například jako ostatní složka IZS, by bylo možné tyto subjekty využívat při evakuaci, zajištění vnějších perimetrů či ochraně například skladů humanitární pomoci a nemocničních zařízení během krizových stavů. Toto by bylo předmětem optimalizace zákona o IZS v případě přijetí SBS do tohoto systému, případně části nově vzniklého zákona o SBS, která by tento vztah vymezovala. Současně lze uvažovat o možnosti zapojení SBS do oblasti technologické podpory ochrany KI, například v rámci provozu dronů pro dohled, nasazení autonomních bezpečnostních robotů či využití pokročilých systémů detekce (např. termovize, rozpoznávání SPZ či obličejů). Využívání těchto technologií by bylo výhodné především v rozsáhlých nebo odlehlých oblastech, kde není efektivní trvalá přítomnost státní složky jak z pohledu personálního, tak i finančního.

Vhodná by byla samostatná certifikace či odborná způsobilost agentur určených pro spolupráci při ochraně KI, garantovala by schopnosti jejích zaměstnanců k těmto úkolům a spolupracovala se státními složkami při tvorbě bezpečnostních protokolů k ochraně KI.

Například ve Velké Británii, je taková spolupráce již běžná, SBS zde plní podřízenou, ale důležitou roli v rámci bezpečnostního rámce státu z pohledu KI. Například společnosti jako Mitie spolupracují s policií na ochraně maloobchodních prostor a dalších veřejných míst, čímž doplňují omezené kapacity policejních složek jak v ohledu MC tak i KI. SBS jsou také zapojeny do ochrany podmořských kabelů a plynovodů, které jsou zásadní pro energetickou a internetovou konektivitu Velké Británie. Vzhledem k rostoucím hrozbám ze strany států jako Rusko a Čína je ochrana těchto zařízení prioritou, přičemž soukromé firmy hrají důležitou roli v monitorování a rychlé reakci na incidenty právě těchto prvků [122].

Další možností rozšíření působnosti SBS v ochraně KI je jejich zapojení do kybernetické bezpečnosti jednotlivých objektů do KI spadajících. Mnoho těchto zařízení či potenciálně do nich zařaditelných jako jsou elektrárny, rozvodné stanice, nemocnice nebo letiště, využívá komplexní digitální infrastrukturu, která je náchylná nejen k externím hackerským útokům, ale i ke kombinovaným hybridním hrozbám. SBS by v této oblasti mohly plnit roli jakési technicko-dozorčí pro detekci fyzického narušení, které by mohlo být součástí kyberútoku. Například neautorizovaný vstup do serveroven, úmyslné poškození komunikačních uzlů apod. Tato synergie mezi kybernetickou a fyzickou bezpečností

je zmiňována i v rámci doporučení Evropské agentury pro kybernetickou bezpečnost ENISA jako klíčová pro ochranu „kritických entit“ [123].

Dalším potenciálním směrem využití SBS by bylo jejich začlenění do programu „red teaming“, tedy simulovaného testování bezpečnostních opatření na objektech KI. Zde by mohly bezpečnostní agentury fungovat jako smluvní externí oponenti systému, pod dohledem státních složek by prováděly simulované průniky či vyhodnocovaly schopnost bezpečnostního systému daného provozu reagovat na nečekanou událost. Tento přístup je běžný například v Izraeli a částečně i v Německu a umožňuje rychlou identifikaci slabých míst v systému ochrany [43].

Z hlediska strategického plánování může SBS sehrát roli v lokálním mapování hrozeb v reálném čase. V některých regionech USA, například ve státě Texas, se SBS podílejí na provozu tzv. „fusion center“, zpravodajsko-bezpečnostních center, kde dochází ke sdílení informací mezi federálními, státními a soukromými složkami. Můj návrh je aplikovat tento model v ČR, zejména ve spolupráci SBS s PČR nebo HZS ČR. Součástí spolupráce by mohla být nejen výměna informací, ale i školení a vývoj společných bezpečnostních protokolů. Tato forma spolupráce by po dokončení právní úpravy byla v praxi efektivní a nevyžadovala mnoho organizačních úprav [124].

V neposlední řadě by měly být SBS zvažovány také jako součást rezervních složek pro nouzový nebo válečný stav, obdobně jako je tomu v některých východoevropských zemích, kde mají bezpečnostní agentury povinnost poskytnout kapacity a techniku pro podporu ochrany infrastruktury státu. Podobný systém existuje například v Estonsku v rámci systému Kaitseliit, kde soukromý sektor spolupracuje s civilní obranou při ochraně energetických, dopravních i telekomunikačních uzlů. Ovšem toto téma by zasluhovalo vlastní komplexní zpracování [125].

7 DISKUSE

Právní ukotvení komerční bezpečnosti – inspirace zahraničím

Jedním z ústředních témat práce je potřeba legislativního a systémového ukotvení soukromého bezpečnostního sektoru v ČR. Analýza odhalila, že dosavadní absence zvláštního zákona o SBS představuje zásadní překážku efektivního zapojení tohoto sektoru do ochrany MC. V minulosti vzniklo několik návrhů zákona, avšak žádný doposud nevešel v platnost. Poslední návrh připravený Ministerstvem vnitra měl být předložen vládě v září 2024 a počítal se vstupem zákona v účinnost od ledna 2025. Tento trend potvrzuje, že si odborná veřejnost uvědomuje nutnost právně vymezit postavení a činnost soukromých bezpečnostních služeb. Na druhou stranu je finální dokončení a přijetí zákona historicky bojkotováno nebo v rámci úspor nerealizováno.

Na základě komparace zahraničních přístupů práce navrhuje přijetí samostatného zákona o SBS, jenž by jasně definoval práva a povinnosti soukromých bezpečnostních služeb, stanovil systém licencování, dohledu a kontroly jejich činnosti a upravil odpovědnost i sankce. Inspiraci lze čerpat ze zemí, kde obdobná legislativa úspěšně funguje. České prostředí by si zasloužilo ekvivalentní nástroj, který zajistí právní jistotu všem zúčastněným stranám. Komparativní analýza v práci taktéž ukázala, že úroveň komerční bezpečnosti v ČR by se měla minimálně vyrovnat standardům běžným v jiných evropských státech, alespoň těch nejbližších. Zavedení legislativního rámce by umožnilo jasně vymezit kompetence zaměstnanců bezpečnostních agentur a vytvořit podmínky pro jejich systémové začlenění do celkové bezpečnostní architektury státu.

Propojení veřejného a soukromého sektoru v ochraně veřejných prostor a KI

Významným závěrem disertace je také zjištění, že existuje široký prostor pro intenzivnější propojení veřejného a soukromého sektoru při ochraně veřejných prostranství ale i kritické infrastruktury. Státní bezpečnostní složky disponují omezenými kapacitami a nemohou být trvale přítomny u všech potenciálních cílů. SBS proto mohou sehrát roli v zastoupení sil a zaplnit mezery v systému. Mnohé prvky KI jsou navíc ve vlastnictví či správě privátních subjektů, což například v zahraničí je až 80 % z celkového počtu. První linii obrany tedy často zajišťuje právě soukromý sektor a efektivní ochrana vyžaduje sdílenou odpovědnost veřejných i soukromých zástupců [126].

Práce dokládá, že spolupráce mezi státem a SBS má velký potenciál. Jednou z možností je zapojit SBS formálně do systému IZS. To by ovšem vyžadovalo jasná pravidla, výcvik a legislativní úpravy. Návrhová část dále rozvíjí myšlenky využití SBS i technologicky, například k provozu dronů, robotických hlídek nebo pokročilých detekčních systémů na místech, kde nelze nasadit státní složky nepřetržitě. Důležitá by také byla certifikace agentur, které by měly chránit kritickou infrastrukturu, aby byla zajištěna odbornost a důvěryhodnost.

Inspirací mohou být například USA, kde fungují centra pro sdílení informací mezi státními a soukromými bezpečnostními odborníky, nebo Estonsko, kde existují dobrovolné rezervní složky. Významným trendem je i propojování fyzické a kybernetické bezpečnosti – moderní hrozby často kombinují útoky na systémy i budovy. Podle evropské agentury ENISA by tedy měla být ochrana koordinovaná a zahrnovat i specialisty z komerční sféry. Správně nastavená spolupráce může výrazně zlepšit ochranu MC a KI, aniž by stát ztratil kontrolu nad bezpečnostní politikou.

Reflexe návrhu metody TRS

Disertační práce představila originální metodiku TRS pro hodnocení rizikovosti MC. Tato metodika je založena na mezinárodních standardech řízení rizik (např. ISO 31000:2018), koncepčních dokumentech a osvědčených postupech hodnocení MC, což zajišťuje transparentnost a opakovatelnost hodnocení. TRS zároveň integruje kategorizaci bezpečnostních opatření A–F (převzatou z návrhu zákona o SBS z roku 2024) přímo do výpočtu rizika, čímž propojuje teoretickou analýzu rizik s praktickými návrhy, výsledné skóre okamžitě odráží, jak dobře je daný MC chráněn zavedenými opatřeními v podobě SBS. Tato konstrukce je v kontextu České republiky novátorská a univerzální, neboť umožňuje aplikaci na různé typy MC (od škol a nemocnic po obchodní centra či kulturní objekty) při zachování jednotného způsobu vyhodnocení.

Metodika TRS prokazuje významné přínosy pro hodnocení rizik. Na základě kvantifikace dílčích faktorů dokáže identifikovat slabá místa ochrany (například nedostatečné kamerové pokrytí nebo absenci fyzické ostrahy) a stanovit jejich priority pro zlepšení. Každému hodnocenému objektu je tak přiřazeno celkové rizikové skóre a zároveň konkrétní doporučení ke zvýšení bezpečnosti s využitím SBS. Tyto výstupy potvrzují, že navržená metodika není jen akademickým konceptem, ale může sloužit jako praktický nástroj pro orgány státní správy, bezpečnostní složky i samotné provozovatele MC. TRS metoda představuje moderní přístup

k řízení rizik, jenž kombinuje mezinárodně ověřené modely s domácími bezpečnostními koncepcemi, a přináší tak originální řešení do kontextu ochrany MC v ČR.

Návrhy, analýzy a závěry disertační práce tak reflektují cíle, které si stanovila a tímto je naplňuje. Naplněním cílů taktéž práce poskytuje komplexní souhrn témat, kterým se věnuje, a upozorňuje na systémové nedostatky, které podtrhuje. Záměrem disertace bylo nabídnout i možná řešení a ukázat nové směry vývoje tématu komerční bezpečnosti ve vztahu k ochraně MC v ČR.

Relevance výzkumu v současném kontextu

Výzkum je vysoce relevantní v kontextu současných bezpečnostních hrozeb, kterým čelí Evropa i ČR. V posledním desetiletí došlo v Evropě k sérii tragických teroristických útoků zaměřených na MC. Z provedených analýz vyplývá, že právě Francie, Velká Británie, Německo či Španělsko zaznamenaly nejvíce těchto incidentů, a v reakci na ně posílily spolupráci s privátním sektorem při zajištění bezpečnosti veřejných míst. Například ve Francii a Británii se po útocích výrazně zvýšila přítomnost soukromých hlídek na veřejných akcích a zlepšila koordinace mezi policií a BA. ČR se těmito extrémním případy zatím vyhýbá, navzdory tomu práce detailně dává příkladem útok ve Fakultní nemocnici Ostrava v roce 2019, kdy útočník zabil 6 lidí v čekárně nebo útok na Filozofické fakultě Univerzity Karlovy v roce 2023, která je zde v disertaci případovou studií. Útoky ukazují, že riziko obdobných činů existuje i v českém prostředí a se světovým vývojem bezpečnosti lze očekávat další negativní vývoj. Tyto události odhalily zranitelnost MC a vyvolaly společenskou diskusi o zlepšení preventivních opatření. Práce na tyto potřeby reaguje, navržená metodika TRS a celkový koncept zapojení SBS cílí právě na prevenci, včasnou detekci hrozby a rychlou reakci, což jsou faktory rozhodující pro minimalizaci dopadů útoků na MC.

Kromě terorismu se bezpečnostní situace v současnosti komplikuje působením hybridních hrozeb. Ty představují kombinaci různých forem útoku často vedených státními či nestátními aktéry s cílem destabilizovat společnost. V hybridním konfliktu mohou být MC zneužity k vyvolání paniky nebo narušení kritických funkcí státu a jsou tedy v práci taktéž reflektovány. Jak upozorňují odborné analýzy, podstatná část KI je v rukou privátních subjektů a první obranná linie proti hybridním útokům tedy leží mimo státní aparát. To klade důraz na sdílenou odpovědnost, ochrana MC a KI musí být výsledkem spolupráce veřejného a soukromého sektoru, jinak nelze dosáhnout dostatečné odolnosti vůči novým typům hrozeb.

Relevance výzkumu se projevuje i v kontextu limitovaných kapacit PČR a dalších ozbrojených složek státu. Stát nemá neomezené lidské ani finanční zdroje k pokrytí všech rizikových lokalit, zejména v době zvýšených nároků (např. při teroristické hrozbě nebo v situaci, kdy část sil odčerpává krize typu pandemie či pomoc spojencům v rámci NATO apod.). Zapojením SBS jako podpůrného pilíře lze aktivně zvýšit celkovou úroveň ochrany. Disertační práce nabízí konkrétní návrhy, které počítají s využitím existujícího potenciálu cca 40 tisíc pracovníků soukromé bezpečnosti v ČR (tj. počtu řádově srovnatelného s početním stavem Policie ČR, přičemž je toto číslo hrubě zaokrouhleno, pracovníků SBS ČR je více ale návrhy počítají s kvalitnějšími personálními zdroji) pro potřeby národní bezpečnosti.

V současném nejistém prostředí poznamenaném probíhajícím konfliktem na Ukrajině, hrozbami ze strany mezinárodního terorismu i možnými útoky na civilní cíle představují závěry a doporučení práce aktuální a prakticky využitelný příspěvek k posílení bezpečnostního systému.

Limity práce a náměty pro další výzkum

Přestože práce přináší nové poznatky, je nezbytné kriticky hodnotit limity výzkumu a vymezit oblasti pro další zkoumání. Jednou z hlavních limitací je samotný kontext ČR, absence komplexního legislativního rámce pro soukromý bezpečnostní sektor nadále trvá a komplikuje jednoznačné určení odpovědností, pravomocí i standardů výkonu této činnosti. Z toho plynou i omezené pravomoci pracovníků SBS, kteří v současnosti nemají žádné zvláštní zákonné oprávnění k preventivním bezpečnostním zásahům či použití donucovacích prostředků (mimo krajní nouzi a nutnou obranu shodnou s fyzickými osobami), a fakticky jsou na úrovni běžných občanů. Tento právní deficit snižuje efektivitu navržených opatření, neboť bez legislativních změn by rozsah působnosti SBS zůstal omezen převážně na smluvní vztahy s chráněnými subjekty a na pasivní dohled. Dále byla identifikována institucionální mezera, na rozdíl od zahraničí stát doposud nemá vytvořený nástroj ani mechanismus, jak soukromé složky systematicky začlenit do zabezpečení veřejných prostor či akcí a případně je spolufinancovat. Tento nedostatek brání plnému využití potenciálu komerční bezpečnosti.

Za zmínku stojí i další omezení, a to nejednotná kvalita v rámci odvětví a přetrvávající nedůvěra části veřejnosti. Úroveň odborné přípravy a výcviku se mezi jednotlivými bezpečnostními agenturami liší a dosud neexistuje centrálně uznávaný standard kvalifikace. To vede k rozdílům v profesionální úrovni poskytovaných služeb. Současně část veřejnosti vnímá soukromé bezpečnostní pracovníky jako „nižší“ složku bezpečnosti, což oslabuje jejich

legitimitu a akceptaci při nasazení ve veřejném prostoru. Laicky řečeno, pro většinu společnosti je zaměstnanec bezpečnostní agentury „strážný“ v supermarketu, a tedy vnímají SBS spíše jako situační prevenci. Tyto etické a společenské aspekty naznačují, že samotné technické a organizační inovace musí být doprovázeny budováním důvěry, zvyšováním profesionality a komunikací s veřejností.

Vzhledem k výše uvedenému se otevírá několik směrů pro další výzkum. Prvním z nich je praktické otestování a rozvoj metodiky TRS, například prostřednictvím případových studií na různých typech MC a vyhodnocení účinnosti navržených bezpečnostních opatření v reálném provozu. Další výzkum by mohl model dále zdokonalit, například přidáním dynamických parametrů reagujících na měnící se hrozby (aktuální stupně ohrožení, krátkodobé varovné signály apod.) nebo rozšířením o kybernetickou dimenzi rizika či jiných v čase se vyvíjejících hrozeb. Druhým směrem je studie optimálních forem spolupráce mezi SBS a státními složkami, nabízí se empiricky zkoumat pilotní projekty společných hlídek, sdílení informačních systémů či zapojení soukromých pracovníků do cvičení IZS, a hodnotit přínosy i úskalí takového propojení v reálném provozu. Třetím okruhem výzkumu je analýza legislativních a organizačních opatření, detailně rozpracovat varianty zákonného ukotvení komerční bezpečnosti (včetně ekonomických modelů financování posílené ochrany MC) a zkoumat zkušenosti ze zahraničí při zavádění podobných právních úprav. Toto by byla ovšem již otázka samotného zákonodárství.

V neposlední řadě může další výzkum směřovat k technologickým inovacím, například posoudit efektivitu nasazení inteligentních kamer, dronů, automatizovaných detekčních systémů či systémů včasného varování v prostředí MC a roli, kterou při jejich obsluze či monitoringu může hrát privátní sektor. Tyto náměty přesahují rámec disertace, ale přímo navazují na její zjištění a mohou napomoci dalšímu rozvoji bezpečnostního managementu MC. Je to otázka technologické části disertační práce, která zde byla ovšem sekundární.

Přínos práce pro praxi

Výsledky disertační práce mají výrazný praktický přínos pro všechny zainteresované subjekty v oblasti ochrany MC. Navržená metodika TRS poskytuje systematický nástroj pro hodnocení rizik, který mohou využít jak státní orgány (např. útvary Policie ČR odpovědné za prevenci kriminality či odbory krizového řízení na municipalitách a další), tak soukromé bezpečnostní agentury a samotní provozovatelé potenciálních MC v celém spektru odvětví

(zdravotnictví, školství, služby apod.). Pro státní sektor může TRS sloužit jako podklad pro rozhodování o prioritách k zabezpečení, umožní identifikovat, které objekty v daném regionu vykazují nejvyšší míru rizika a kde je žádoucí posílit ochranná opatření či provést bezpečnostní audit. Pro SBS nabízí metodika jednotný rámec, podle nějž mohou auditovat bezpečnost svých klientů a navrhnout adekvátní opatření. Lze očekávat, že větší poskytovatelé bezpečnostních služeb metodiku využijí pro zkvalitnění své nabídky, například při návrhu zabezpečení nového obchodního centra mohou postupovat podle TRS k identifikaci všech relevantních rizik a optimálního konceptu bezpečnostních opatření. Municipality a obce mohou díky TRS získat lepší přehled o zranitelnosti veřejných prostranství (např. náměstí, kulturní zařízení, sportoviště) a cíleně investovat do zvýšení jejich zabezpečení, případně spolupracovat s místními BA na zajištění akcí s větší koncentrací osob. V praxi krizového řízení lze výstupy TRS využít při tvorbě případných plánů ochrany měkkých cílů, identifikované slabiny a návrhy opatření se mohou promítnout do konkrétních krizových plánů, havarijního plánování či metodik a společných cvičení.

Dalším praktickým přínosem je, že práce otevírá cestu ke standardizaci, pokud by navržený model byl přijat na národní úrovni, mohl by se stát základem pro jednotné metodické postupy při ochraně MC v ČR. To by usnadnilo spolupráci mezi subjekty státní i nestátní úrovně, jelikož by sdílely společný jazyk a kritéria hodnocení rizikovosti. Legislativní doporučení formulovaná v návrhové části práce mohou posloužit jako podklad pro tvorbu či úpravu právních předpisů. Pro tvůrce bezpečnostních politik nabízí disertace ucelený přehled možností, jak efektivně zapojit privátní sektor do ochrany veřejného prostoru, a to od krátkodobých opatření realizovatelných v rámci stávajících zákonů (např. uzavírání partnerství mezi policií a bezpečnostními firmami pro dohled nad vytipovanými MC) až po systémové změny vyžadující nové zákonné úpravy.

Z praktického hlediska je významné i to, že práce se nezaměřuje pouze na teoretické koncepty, ale poskytuje konkrétní návody a doporučení. Například součástí metodiky jsou mnou vytvořené kontrolní seznamy a tabulky hodnotící jednotlivé aspekty zranitelnosti, kritičnosti a hrozeb. Tyto checklisty mohou bezpečnostní manažeři přímo využít při posuzování objektů. Navržené škály rizika s vymezením úrovně (nízké, střední, vysoké riziko) zase usnadňují srozumitelnou komunikaci výsledků směrem k vedení organizací či veřejnosti. V neposlední řadě přináší práce praktický přínos i tím, že zdůrazňuje nutnost profesionálního přístupu v komerční bezpečnosti a volá po vyšší odborné přípravě, standardech a certifikacích, což může motivovat samotné bezpečnostní agentury k zdokonalování svých služeb.

Motivace této skutečnosti je podložena děním ve světě a samotnou analytickou částí práce, která tyto potřeby potvrzuje. Celkově tak lze konstatovat, že realizace navržených opatření by vedla k posílení bezpečnosti v praxi a lepší ochraně obyvatelstva před útoky na MC.

Přínos práce pro vědecké poznání

Disertační práce má rovněž přínos pro rozvoj vědeckého poznání v oblasti bezpečnostních studií a souvisejících oborů. Především představuje nový metodologický přístup k hodnocení rizik MC. Kvantitativní model TRS, který kombinuje více kritérií do jednoho celkového skóre, doplněný o faktor snižující riziko na základě aplikovaných opatření, je inovací přispívající k modernizaci dosavadních přístupů k analýze rizik. Vědecky zajímavé je, že tento model umožňuje měřit efektivnost bezpečnostních opatření a srovnávat různorodé objekty z hlediska rizika na jednotné škále. To vytváří předpoklady pro další akademické bádání, například pro komparativní studie mezi různými regiony či sektory (lze porovnat rizikovost škol vs. nemocnic, veřejných vs. privátních objektů apod.) a pro objektivní vyhodnocování dopadů nových bezpečnostních politik. Pro další vědecké uplatnění lze navrženou metodu dále rozvíjet vložením multikriteriálních pohledů a rozšiřováním možností automatizovaného zpracování s využitím vyhodnocovacích algoritmů umělé inteligence, či ji využít jako podklad ke konkretizaci pro konkrétní oblast, kde by byla nosným nástrojem pro hodnocení.

Práce má také výrazný interdisciplinární charakter, který je dán již samotným tématem. Propojuje poznatky z bezpečnostního managementu, krizového řízení, práva, technologie a socio-ekonomických analýz. V teoretické části integruje terminologii a koncepty z různých disciplín od samotné souvztažné teorie SBS a MC, definice terorismu a další typologie útoků přes legislativní rámce až po technické aspekty fyzické ochrany. Tato syntéza různých úhlů pohledu umožnila vytvořit komplexní model zapojení soukromého sektoru do ochrany MC. Vědecký přínos spočívá i v tom, že práce vyplňuje mezeru v české odborné literatuře, dosud chyběla ucelená studie pojednávající o komerční bezpečnosti v kontextu ochrany MC s srovnáním zahraničních přístupů a návrhem konkrétní metodiky. Disertace tak rozšiřuje teoretickou základnu pro tuto problematiku a může sloužit jako východisko pro další výzkum či pedagogické účely (např. v kurzech bezpečnostních studií či u vzdělávání samotných zaměstnanců SBS).

Návrhy na zapojení SBS do státního bezpečnostního systému (včetně krizového řízení ochrany KI) mohou inspirovat obdobné debaty i v dalších zemích, kde se stále hledá rovnováha mezi veřejnou a privátní rolí v zajištění bezpečnosti. Vědecký přínos práce tedy nespočívá

pouze v obohacení domácí debaty, ale i v potenciálním přesahu do zahraničního kontextu. Závěrem lze konstatovat, že disertace svými výsledky podporuje odbornou diskusi o optimálních strategiích ochrany MC, přináší nový pohled na využití kvantitativních metod v bezpečnostním výzkumu a vytváří most mezi teorií a praxí, který je nezbytný pro další rozvoj efektivních bezpečnostních opatření.

Vyhodnocení cílů práce

Disertační práce stanovila hlavní cíl práce a několik cílů dílčích. Hlavní cíl práce **HC1: Navrhnout rámec řízení rizik měkkých cílů s využitím soukromých bezpečnostních služeb v podmínkách České republiky** – se **podařilo naplnit**, a to formou navržené metody vyhodnocení rizikovosti MC, která má potenciál stát se nosným prvkem v řízení rizik MC za konkrétního využití SBS k jejich ochraně. Současně disertace navrhuje další rozvoj SBS v ČR, což je za současné právní situace v tomto oboru předmětná diskuse.

DCI: Provést audit současného stavu komerční bezpečnosti a ochrany měkkých cílů v České republice – první z dílčích cílů práce lze považovat za **splněný**, teoretická část disertace, tedy kapitola 2 Přehled současného poznání analyzuje aktuální stav a právní zakotvení obou problematik v ČR.

DCII: Vytvořit genezi návrhů zákona o soukromých bezpečnostních službách v České republice – tento cíl práce **byl splněn** v kapitole 2.1.3, která analyzuje jednotlivé návrhy zákona v oblasti SBS v ČR, až po ten poslední z roku 2024, který se současně stal podkladem k navržené metodě vyhodnocení rizikovosti MC.

DCIII: Zpracovat kvantitativní analýzu míry využití bezpečnostních agentur v České republice – cíl práce vlastní analýzy využití bezpečnostních agentur v ČR **byl splněn** v kapitole 4.1, kde jsou výsledky prezentovány formou grafů.

DCIV: Komparovat systémy komerční bezpečnosti v České republice a vybraných evropských státech – komparace **byla provedena** v kapitolách 4.2 a 4.3, přičemž výsledky byly použity v navazující návrhové části práce k charakteristice koncepce efektivního modelu komerční bezpečnosti v ČR.

DCV: Zpracovat SWOT analýzu současného stavu soukromých bezpečnostních služeb při ochraně měkkých cílů v ČR – cíl zpracování komplexní SWOT analýzy **byl splněn** v kapitole 4.5, kde jsou výstupy analýzy vizualizované v přehledové tabulce.

DCVI: Vytvořit a aplikovat vlastní metodu vyhodnocení rizikivosti měkkých cílů – Total Risk Score (TRS) – metoda byla navržena a vytvořena s potenciálem dalšího rozvoje, doplnění dat a testování jejího využití v praxi. Pilotní model je funkční a vizualizovaný. Tento cíl práce **splňuje** kapitola 6.1.

DCVII: Navrhnout inovativní prostředky a metody pro vývoj zapojení soukromých bezpečnostních služeb v České republice k ochraně měkkých cílů – tento cíl **splňuje** celá kapitola 6 Návrhová část práce, která definuje novátorská řešení zapojení SBS do konceptu bezpečnosti v ČR a některé vizionářské možnosti vývoje samotných SBS a jejich schopností.

8 ZÁVĚR

Disertační práce se zaměřila na problematiku komerční bezpečnosti v ČR s důrazem na ochranu MC. Obě oblasti, které jsou v bezpečnostním prostředí úzce propojené, reflektují aktuální výzvy spojené s rostoucí diverzitou bezpečnostních hrozeb ve světě i ČR, omezenými kapacitami státních bezpečnostních složek a potřebou efektivnější ochrany veřejného prostoru ve jménu komplexní vnitřní bezpečnosti státu. Vzhledem k absenci systematické legislativní úpravy soukromého bezpečnostního sektoru v ČR se práce věnovala také návrhu jeho možného systémového ukotvení, a to na základě komparace se zahraničními modely a poznatky z praxe.

V první části práce byly analyzovány legislativní a koncepční rámce fungování SBS v ČR a identifikovány klíčové nedostatky. Komparativní analýza vybraných zahraničních modelů nabídla inspiraci pro možné systémové body využitelné v modifikaci české komerčně bezpečnostní struktury. Tato zjištění tvořila teoretický základ zejména pro návrhovou část práce, která je tak výstupem současného stavu s možnými vývoji SBS do budoucna jak v prostředí ČR, tak globálně.

Jádrem praktické části výzkumu je návrh nové metodiky hodnocení rizikovosti MC, která byla vytvořena s důrazem jak na aplikaci v prostředí ČR, tak komplexní využití. Metodika vychází z principů rizikové analýzy a využívá kontrolní checklisty a skórovací tabulky s cílem identifikovat úroveň celkové rizikovosti na daném objektu. Součástí výstupu metodiky je i návrh konkrétních opatření ke zvýšení bezpečnosti, a to primárně formy využití SBS jako součásti ochranného systému. Metodika je univerzální a přenositelná na různé typy MC, což představuje významný přínos jak pro bezpečnostní praxi, tak pro další vědecké zkoumání a vývoj.

Z výše uvedeného v disertační práci vyplynulo několik hypotéz, jejichž vyhodnocení je důsledkem zpracování jednotlivých navazujících kapitol disertace:

H1: Současná legislativní opora soukromých bezpečnostních služeb v České republice je dostatečná vůči evropskému standardu.

- Detailním rozbořem současného právního rámce SBS v ČR bylo detekováno několik nedostatků. Zásadní je úplná absence zvláštního zákona upravující fungování SBS. Na základě výsledků provedené analýzy několika vybraných evropských států ohledně systému komerční bezpečnosti a následné komparace s ČR, lze **H 1 falzifikovat**. ČR nesplňuje standardy evropské

legislativy v oblasti komerční bezpečnosti vzhledem k nejednotnosti a roztržitosti právního ukotvení.

H2: Zapojení soukromých bezpečnostních služeb do systému ochrany měkkých cílů v České republice není efektivní především kvůli absenci jasného legislativního rámce.

- Na základě analytického rozboru současného stavu ochrany MC a fungování komerční bezpečnosti v ČR lze konstatovat, že ani jedna z těchto oblastí není legislativně plně ošetřena. Pokud by stát jasně definoval, které MC spadají do jeho prioritní ochrany, a současně vymezil roli SBS jako primárního nástroje této ochrany, vznikl by legislativně ukotvený a státem vymahatelný vztah mezi ochranou MC a činností SBS. Z tohoto pohledu lze **H 2 verifikovat**, díky absenci legislativního rámce chybí jasné vymezení možností zapojení komerční bezpečnosti k ochraně MC, vynutitelnost a systém financování.

H3: Lze vytvořit efektivní metodiku pro hodnocení rizikovosti měkkých cílů, která bude zahrnovat i doporučení pro využití soukromých bezpečnostních služeb v ochraně těchto cílů?

- Hlavním cílem disertační práce bylo vytvořit návrh komplexní metody vyhodnocení rizikovosti či kritičnosti MC s přímým návrhem využití SBS dle výsledné rizikovosti. Tuto metodu se podařilo navrhnout, je popsána, funkční a inovativní vzhledem ke skutečnosti, že po vyhodnocení daného MC a jeho rizikovosti nabízí konkrétní formu využití komerčních bezpečnostních služeb, čímž lze **H 3 verifikovat**.

Závěrem lze konstatovat, že disertační práce nabízí konkrétní nástroje i systémová doporučení, která mohou přispět k odborné diskuzi o budoucnosti komerční bezpečnosti v ČR. Současně přináší nový pohled na možnosti zapojení soukromého sektoru do ochrany MC a veřejného prostoru jako celku. Při adekvátní legislativní a koncepční podpoře by SBS mohly hrát důležitou roli při odlehčení státním složkám a současně zvýšit úroveň bezpečnosti v ČR.

9 SEZNAM PUBLIKACÍ DISERTANTA VZTAHUJÍCÍCH SE K DISERTAČNÍ PRÁCI

- MIROVSKÝ, P. a H. FOJTÁŠKOVÁ PETŘEKOVÁ. Údržba a řízení bezpečnosti kritické infrastruktury v ČR. *Forenzní vědy, právo, kriminalistika*. 2023, roč. 8., s. 6. ISSN 2533-4395.
- MIROVSKÝ, P. a H. PETŘEKOVÁ. Analýza bezpečnosti zdravotnického zařízení. *Bezpečnost s profesionály: Časopis komory podniků komerční bezpečnosti ČR*. KPKB ČR Praha 5, 2020, **2020**, 2. ISSN 2336-4793.
- MIROVSKÝ, P. Evakuační plán a aspekty zajištění evakuace v soukromé sféře. *Forenzní vědy, právo, kriminalistika*. Vysoká škola finanční a správní, a.s. Praha, 2022, **7**(1), 10. ISSN 2533-4387. Dostupné z: doi:<http://dx.doi.org/10.37355/fvpk>
- FOJTÁŠKOVÁ PETŘEKOVÁ, H. a P. MIROVSKÝ. Využití vícekritériálního rozhodování při zabezpečení objektu. In: RALBOVSKÁ, D., J. HALAŠKA a D. ČERMÁKOVÁ, eds. *Aspekty práce pomáhajících profesí 2023. Aspekty práce pomáhajících profesí*, Kladno, 2023-10-27. Praha: ČVUT. Fakulta biomedicínského inženýrství, 2023. s. 293-310. ISBN 978-80-01-07165-6.
- FOJTÁŠKOVÁ PETŘEKOVÁ, H. a P. MIROVSKÝ. Komparace systémů vybraných zahraničních soukromých bezpečnostních služeb a návrh ideálního modelu komerční bezpečnosti. *Forenzní vědy, právo, kriminalistika*. 2024 – článek přijat k recenzovanému posouzení.
- FOJTÁŠKOVÁ PETŘEKOVÁ, H. a P. MIROVSKÝ. Soukromé bezpečnostní služby a kritická infrastruktura. *Bezpečnost s profesionály*. 2022, 17-18. ISSN 2336-4793.

Ostatní publikace disertanta

- MIROVSKÝ, P. a M. STANĚK. Využití programu XVR a virtuální reality při přípravě a cvičení složek IZS. In: RALBOVSKÁ, Dana Rebeka a Jiří HALAŠKA. *Aspekty práce pomáhajících profesí 2021: Sborník příspěvků ze studentské vědecké konference AWHP 2021*. Praha: ČVUT v Praze, 2021, s. 17. ISBN 978-80-01-06852-6. Dostupné z: doi:<https://doi.org/10.14311/BK.9788001068526>.
- MIROVSKÝ, P. a M. STANĚK. Návrh optimalizace požární ochrany v soukromém sektoru nezařazených podniků. In: RALBOVSKÁ, Dana Rebeka a Jiří HALAŠKA. *Aspekty práce pomáhajících profesí 2020: Sborník příspěvků ze studentské vědecké konference AWHP 2020*. Praha: ČVUT v Praze, 2020, s. 11. ISBN 978-80-01-06783-3. Dostupné z: doi:<https://doi.org/10.14311/BK.9788001068526>.

10 SEZNAM POUŽITÝCH ZKRATEK

- SBS – soukromé bezpečnostní služby
- ČR – Česká republika
- EU – Evropská unie
- MC – měkké cíle
- EZS – elektronické zabezpečovací systémy
- CCTV – Closed Circuit Television (kamerové systémy)
- PZTS – požární a tísňové systémy
- STO – systémy technické ochrany
- PPP – Public Private Partnership
- BA – bezpečnostní agentura
- CNAPS - Conseil National des Activités Privées de Sécurité
- PCO – pult centralizované ochrany
- FO – fyzická ochrana
- BIS – Bezpečnostní informační služba
- URNA – Útvar rychlého nasazení
- IZS – integrovaný záchranný systém
- KI – kritická infrastruktura
- VIP – Very Important Person
- HD – High Definition
- MNS - Mass Notification Systém
- NEWS - Notification, Emergency, Warning System
- OPIS – Operační a informační středisko
- LRAD - Long Range Acoustic Device
- ZZS – Zdravotnická záchranná služba
- HZS – Hasičský záchranný sbor
- PČR – Policie ČR
- ZZS KHK – Zdravotnická záchranná služby Královéhradeckého kraje
- AED – automatický defibrilátor
- START - Simple Triage and Rapid Treatment
- KI – kritická infrastruktura
- ENISA - Evropská agentura pro kybernetickou bezpečnost

11 SEZNAM POUŽITÉ LITERATURY

- [1] van STEDEN, R. a SARRE, R. The Growth of Private Security: Trends in the European Union. *Security Journal*, 2007, vol. 20, no. 4, s. 222–235. ISSN 0955-1662.
- [2] LIMNÉLL, J. Countering Hybrid Threats: Role of Private Sector Increasingly Important. Helsinki: Hybrid CoE, 2018. ISBN 978-952-7282-55-7.
- [3] EVROPSKÁ KOMISE. ProtectEU: Strategie vnitřní bezpečnosti EU. Brusel, 1. 4. 2025. Tiskové prohlášení.
- [4] KAMENÍK, J., F. BRABEC a kol., 2007. Komerční bezpečnost: Soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur. Vyd. 1. Praha: ASPI. ISBN 978-80-7357-309-6.
- [5] BUREŠ, O. a kol., 2013. Privatizace bezpečnosti: české a zahraniční zkušenosti. Vyd. 1. Praha: Grada Publishing. ISBN 978-80-247-4601-2.
- [6] AUDIT NÁRODNÍ BEZPEČNOSTI ČESKÉ REPUBLIKY [online]. Praha: Úřad vlády České republiky, 2016 [cit. 2025-05-12]. Dostupné z: <https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-2016.pdf>.
- [7] BUREŠ, O. Private Security Assemblage(s) and Powers of Private Security Companies. In: STRÍTECKÝ, V. et al. (eds.). *Central and Eastern European Perspectives on International Relations*. Cham: Springer International Publishing, 2021, s. 35–79. ISBN 978-3-030-88906-7. doi:10.1007/978-3-030-88907-4_3.
- [8] MACEK, P. a kol., 1997. Soukromé bezpečnostní služby. Vyd. 1. Praha: Policejní akademie České republiky. ISBN 80-85981-62-9.
- [9] LILLY, D., 2000. The privatization of security and peacebuilding: a framework for action [online]. Vyd. 1. London: International Alert [cit. 2022-10-08]. ISBN 1-898702-06-6. Dostupné z: http://psm.du.edu/media/documents/reports_and_stats/ngo_reports/intlalert_lilly_private_security_peacebuilding_2000.pdf
- [10] MACEK, P. a F. NOVÁK. Privátní bezpečnostní služby. Praha, Police History 2005, ISBN:80-86477-23-1.
- [11] ČESKÝ KLUB BEZPEČNOSTNÍCH SLUŽEB. Historie klubu [online]. Praha: ČKBS, ©2024 [cit. 2025-08-10]. Dostupné z: <https://ckbs.cz/historie-klubu/>.

- [12] MACEK, P. Bezpečnostní služby. 1. Praha: Police history, 2008. ISBN 9788086477480.
- [13] HULVA, T. Ochrana majetku. Praha: Linde, 2008. ISBN 9788072017126.
- [14] BORN, H., CAPARINI, M., & COLE, E. (2007). Regulating Private Security in Europe: Status and Prospects. Ženeva: DCAF (Policy Paper č. 20). Volně dostupné na webu DCAF (PDF).
- [15] ČESKÁ REPUBLIKA. Ústavní zákon č. 1/1993 Sb., Ústava České republiky [online]. Praha: Parlament České republiky, 1993 [cit. 2024-05-09]. Dostupné z: <https://www.zakonyprolidi.cz/cs/1993-1>.
- [16] ČESKÁ REPUBLIKA. Usnesení předsednictva ČNR č. 2/1993 Sb., Listina základních práv a svobod [online]. Praha: Česká národní rada, 1993 [cit. 2024-05-09]. Dostupné z: <https://www.zakonyprolidi.cz/cs/1993-2>.
- [17] ČESKÁ REPUBLIKA. Zákon č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon) [online]. Praha: Ministerstvo průmyslu a obchodu, 1991 [cit. 2024-05-09]. Dostupné z: <https://www.zakonyprolidi.cz/cs/1991-455>.
- [18] ČESKÁ REPUBLIKA. Zákon č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon) [online]. Praha: Ministerstvo průmyslu a obchodu, 1991 [cit. 2024-05-09]. Dostupné z: <https://www.zakonyprolidi.cz/cs/1991-455>
- [19] ČESKÁ REPUBLIKA. NV č. 278/2008 Sb., o obsahových náplních jednotlivých živností [online]. Praha: Ministerstvo vnitra, 2008 [cit. 2024-05-09]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2008-278>
- [20] BRABEC, F. a kol. Bezpečnost pro firmu, úřad, občana, Public History, 2001, ISBN: 80-86445-04-06.
- [21] ČESKÁ REPUBLIKA. Zákon č. 89/2012 Sb., občanský zákoník [online]. Praha: Parlament České republiky, 2012 [cit. 2024-05-09]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2012-89>.
- [22] ČESKÁ REPUBLIKA. Zákon č. 40/2009 Sb., trestní zákoník [online]. Praha: Parlament České republiky, 2009 [cit. 2024-05-09]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2009-40>.

- [23] ČESKÁ REPUBLIKA. Zákon č. 99/1963 Sb., občanský soudní řád [online]. Praha: Parlament České republiky, 1963 [cit. 2024-05-09]. Dostupné z: <https://www.zakonyprolidi.cz/cs/1963-99>.
- [24] ČESKÁ REPUBLIKA. Zákon č. 262/2006 Sb., zákoník práce [online]. Praha: Parlament České republiky, 2006 [cit. 2024-05-09]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2006-262>.
- [25] ČESKÁ REPUBLIKA. Zákon č. 119/2002 Sb., o střelných zbraních a střelivu (zákon o zbraních) [online]. Praha: Parlament České republiky, 2002 [cit. 2024-05-09]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2002-119>.
- [26] UNIE SOUKROMÝCH BEZPEČNOSTNÍCH SLUŽEB ČESKÉ REPUBLIKY. Online. Dostupné z: <https://www.usbscr.cz/>. [cit. 2025-05-19].
- [27] ASOCIACE TECHNICKÝCH BEZPEČNOSTNÍCH SLUŽEB Grémium Alarm. Online. Dostupné z: <https://www.gremiumalarm.cz/>. [cit. 2025-05-19].
- [28] ČESKÁ KOMORA DETEKTIVNÍCH SLUŽEB. Online. Dostupné z: <https://ckds.cz/>. [cit. 2025-05-19].
- [29] KOMORA PODNIKŮ KOMERČNÍ BEZPEČNOSTI ČR. Online. Dostupné z: <https://www.kpkbcr.cz/>. [cit. 2025-05-19].
- [30] E-NEWS.CZ. Zákon o bezpečnostních službách se psal už za Rumla. Pořád není [online]. Dostupné z: <https://e-news.cz/legislativa/zakon-o-bezpecnostnich-sluzbach-se-psal-uz-za-rumla-porad-neni/>.
- [31] SECURITAS ČR. Zákon o soukromých bezpečnostních službách se schvaluje už 30 let [online]. Dostupné z: <https://www.securitas.cz/novinky--blog/novinky/zakon-o-soukromych-bezpecnostnich-sluzbach-se-schvaluje-uz-30-let/>.
- [32] ČESKÁ TELEVIZE. Na bezpečnostní agentury dohlédne stát. Budou muset mít licenci [online]. Dostupné z: <https://ct24.ceskatelevize.cz/clanek/domaci/na-bezpecnostni-agentury-dohledne-stat-budou-muset-mit-licenci-132481>.
- [33] VLÁDA SCHVÁLILA NÁVRH ZÁKONA O SOUKROMÝCH BEZPEČNOSTNÍCH SLUŽBÁCH. Online. Ministerstvo vnitra České republiky. 2020. Dostupné z: <https://www.mvcr.cz/clanek/vlada-schvalila-navrh-zakona-o-soukromych-bezpecnostnich-sluzbach.aspx>. [cit. 2024-08-25].

- [34] ZÁKONY PRO LIDI. Návrh zákona o soukromé bezpečnostní činnosti a o změně souvisejících zákonů [online]. Dostupné z: <https://www.zakonyprolidi.cz/monitor/5649429.htm>.
- [35] HRBÁČEK, J. Vnitro chystá léta chybějící zákon o soukromých bezpečnostních agenturách. Online. Česká justice.cz. 2022, s. 1. Dostupné z: <https://www.ceska-justice.cz/2022/01/vnitro-chysta-leta-chybejici-zakon-o-soukromych-bezpecnostnich-agenturach/>. [cit. 2024-07-03].
- [36] NOVOTNÁ, A. Zákon o bezpečnostních službách – konečně se dočkáme. Online. SecurityGuide. 2022, s. 1. Dostupné z: <https://securityguide.cz/zakon-o-bezpecnostnich-sluzbach-konecne-se-dockame/>. [cit. 2024-07-03].
- [37] RANDA, M. Měkké cíle a jejich ochrana – perspektiva spolupráce veřejného a soukromého sektoru. Tzbinfo [online]. 2018 [cit. 2024-04-24]. Dostupné z: <https://www.tzbinfo.cz/bezpecnost/18312-mekke-cile-a-jejich-ochrana-perspektiva-spoluprace-verejneho-a-soukromeho-sektoru>,
- [38] SCHMID, A. P. (2021). Layers of Preventive Measures for Soft Target Protection against Terrorist Attacks. In A. P. Schmid (Ed.), Handbook of Terrorism Prevention and Preparedness (Chapter 27). Haag: ICCT Press. Dostupné z: <https://icct.nl/handbook-terrorism-prevention-and-preparedness>.
- [39] KONCEPCE OCHRANY MĚKKÝCH CÍLŮ PRO ROKY 2017–2020 [online]. Praha: Ministerstvo vnitra České republiky, 2017 [cit. 2025-05-12]. Dostupné z: <https://www.mvcr.cz/soubor/koncepce-ochrany-mekkych-cilu-pro-2017-2020-pdf.aspx>.
- [40] HOBSBAWM, E. J. Globalizace, demokracie a terorismus. Praha: Academia, 2009. XXI. století. ISBN 978-80-200-1725-3.
- [41] FAGEL, M. J. a HESTERMAN, J. 2017. Soft Targets and Crisis Management: What Emergency Planners and Security Professionals Need to Know. Boca Raton: CRC Press, Taylor & Francis Group. ISBN 9780367596095.
- [42] CORTE IBÁÑEZ, L. Logika terorismu. Praha: Academia, 2009. Historie (Academia). ISBN 9788020017246.
- [43] HESTERMAN, J. (2019). Soft Target Hardening: Protecting People from Attack. 2nd ed. Boca Raton: CRC Press. ISBN 978-1138391086.

- [44] ZÁKLADY OCHRANY MĚKKÝCH CÍLŮ – METODIKA [online]. Praha: Ministerstvo vnitra České republiky, 2016 [cit. 2025-05-12]. Dostupné z: <https://www.mvcr.cz/soubor/metodika-zaklady-ochrany-mekkych-cilu-pdf.aspx>.
- [45] HOFREITER, L., BEREZUTSKYI, V., FIGULI, L., & ZVAKOVÁ, Z. (2020). Soft Target Protection: Theoretical Basis and Practical Measures. 1st ed. Dordrecht: Springer. ISBN 978-9402417548.
- [46] ČESKÁ REPUBLIKA. Bezpečnostní strategie České republiky. Praha: Úřad vlády ČR, 2015.
- [47] USNESENÍ VLÁDY ČESKÉ REPUBLIKY č. 711 ze dne 19. září 2016 k tzv. Protiteroristickému balíčku. In: Vládní dokumenty ČR. [online]. Dostupné z: <https://apps.odok.cz/veklep-detail?pid=KORNAQ3KFSRH>.
- [48] ČESKÝ NORMALIZAČNÍ INSTITUT. ČSN 73 4400:2016 Prevence kriminality – řízení bezpečnosti při plánování, realizaci a užívání škol a školských zařízení. Praha: ÚNMZ, 2016.
- [49] EVROPSKÝ PARLAMENT A RADA EU. Directive (EU) 2018/1972 establishing the European Electronic Communications Code (EECC). Official Journal of the European Union, 17.12.2018.
- [50] CLEARY, C. (2017). Public-Private Partnerships: Security Organizations. SpringerLink. Retrieved from <https://link.springer.com/article/10.1007/s12027-017-0479-3>.
- [51] HOFREITER, L. Bezpečnostní prostředí současného světa. VerBuM, Zlín, 2016. 160 s. ISBN 978-80-87500-79-8.
- [52] EUROPEAN COMMISSION. Good practices to support the protection of public spaces, 2020.
- [53] RASHEED, N., SHAHZAD, W., KHALFAN, M., & ROTIMI, J. O. B. (2022). Risk Identification, Assessment, and Allocation in PPP Projects: A Systematic Review. Buildings, 12(8), 1109. doi:10.3390/buildings12081109.
- [54] CONLEY, T., WASYLYSHYN, M., & TOBIN, T. (2024). Public-Private Partnerships: A Keystone for Safer Communities Worldwide. ASIS International Blog, 22. 3. 2024. Dostupné z: <https://www.asisonline.org/publications--resources/news/blog/2024/public-private-partnerships-a-keystone-for-safer-communities-worldwide/#:~:text=security%20services%20projected%20to%20reach,the%20capacity%20to%20secure%20communities>

- [55] EUROPEAN COUNCIL OF SHOPPING PLACES. (2022). Guidance for Safer Retail Spaces. Brussels: ECSP.
- [56] FEMA. (2020). Protecting Houses of Worship: Collaborating with Partners. U.S. Department of Homeland Security.
- [57] EUROPEAN UNION AGENCY FOR CYBERSECURITY. (2021). Cybersecurity in Hospitals – Threat Landscape. ENISA.
- [58] U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES. (2022). HC3 Sector Alert: Cyber Threats in Healthcare. Washington, DC: HHS.
- [59] U.S. DEPARTMENT OF HOMELAND SECURITY. (2020). Fusion Centers and Intelligence Sharing. Washington, DC: DHS.
- [60] INTERNATIONAL ASSOCIATION OF VENUE MANAGERS. (2021). Best Practices in Venue Security. Dallas: IAVM.
- [61] OSCE. (2022). Good Practices in the Protection of Public Spaces. Vienna: Organization for Security and Co-operation in Europe
- [62] OECD. (2020). Engaging Communities for Safer Cities: Lessons from Global Initiatives. Paris: OECD Publishing.
- [63] BRITISH STANDARDS INSTITUTION. BS EN 13123-2: Windows, doors and shutters – Resistance to explosion. London: BSI, 2001.
- [64] U.S. DEPARTMENT OF HOMELAND SECURITY. Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks. FEMA 427. 2003.
- [65] NaCTSO. Crowded Places: Guidance and Design Principles. London: Home Office, 2017.
- [66] MOSQUEDA, S. Active Assailants Increasingly Seek Open Spaces, FBI Data Finds. Online. Security Management. 2024, s. 1. Dostupné z: <https://www.asisonline.org/security-management-magazine/articles/2024/03/site-hardening/active-assailants-open-spaces/>. [cit. 2025-07-05].
- [67] NĚMECKO. § 34a Gewerbeordnung. In: Gewerbeordnung für die Bundesrepublik Deutschland [online]. Berlin: Bundesministerium der Justiz, 2024 [cit. 2024-05-11]. Dostupné z: https://www.gesetze-im-internet.de/gewo/__34a.html.

[68] PIEPER, O. German immigration policy: What's changing in 2024? [online]. 2024 [cit. 2024-04-24]. Dostupné z: <https://www.dw.com/en/german-immigration-policy-whats-changing-in-2024/a-67753472>.

[69] OLTMER, J. a V. HANEWINKEL. Germany's Migration Policies. Bundeszentrale für politische Bildung [online]. 2018 [cit. 2024-04-24]. Dostupné z: <https://www.bpb.de/themen/migration-integration/laenderprofile/english-version-country-profiles/262811/germany-s-migration-policies/>.

[70] PINNA, M. Germany's U-turn on migration: Is it necessary or just politics? Euronews. [online]. 2024 [cit. 2024-04-24]. Dostupné z: <https://www.euronews.com/2024/02/02/germanys-u-turn-on-migration-is-it-necessary-or-just-politics>.

[71] NĚMECKO. Waffengesetz (WaffG) – Gesetz über das Waffenrecht und die Kontrolle von Kriegswaffen [online]. Berlin: Bundesministerium der Justiz, 2024 [cit. 2025-05-11]. Dostupné z: <https://www.gesetze-im-internet.de/waffg/>

[72] FRANCIE. Loi n° 83-629 du 12 juillet 1983 réglementant les activités privées de sécurité [online]. Paris: Journal officiel de la République française, 1983 [cit. 2024-05-09]. Dostupné z: <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000511726/>

[73] FRANCIE. Code de la sécurité intérieure – Livre VI : Activités privées de sécurité [online]. Paris: Légifrance, 2012 [cit. 2025-05-12]. Dostupné z: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000025503132/LEGISCTA000025506179/.

[74] ITÁLIE. Decreto del Ministero dell'Interno 1 dicembre 2010, n. 269 – Regolamento recante disciplina delle caratteristiche minime del progetto organizzativo e dei requisiti minimi di qualità degli istituti e dei servizi di vigilanza privata [online]. Roma: Gazzetta Ufficiale della Repubblica Italiana, 2010 [cit. 2025-05-09]. Dostupné z: <https://www.normattiva.it/uri-res/N2Ls?urn:nir:ministero.interno:decreto:2010-12-01;269>.

[75] LA NUOVA NORMATIVA SUGLI ISTITUTI DI VIGILANZA E DI INVESTIGAZIONE PRIVATA E SULLE GUARDIE GIURATE. Bari: Cacucci Editore, 2009. ISBN 8884228492.

- [76] NIZOZEMSKO. Wet particuliere beveiligingsorganisaties en recherchebureaus [online]. Den Haag: Ministerie van Justitie en Veiligheid, 1997 [cit. 2025-05-09]. Dostupné z: <https://wetten.overheid.nl/BWBR0008973>.
- [77] NIZOZEMSKO. Wet wapens en munitie – Weapons and Ammunition Act [online]. Den Haag: Ministerie van Justitie en Veiligheid, 1997 [cit. 2025-05-09]. Dostupné z: <https://wetten.overheid.nl/BWBR0008804>.
- [78] KAMENÍK, J. a F. BRABEC. Komerční bezpečnost. 2. vydání. Praha: Wolters Kluwer, 2019. ISBN 978-80-7598-303-9., KRIŽOVSKÝ, S. Služby súkromnej bezpečnosti. Košice: Vysoká škola bezpečnostného manažérstva v Košiciach, 2007. ISBN 978-80-89282-10-4.
- [79] SLOVENSKÁ REPUBLIKA. Zákon č. 473/2005 Z.z., o poskytovaní služieb v oblasti súkromnej bezpečnosti a o zmene a doplnení niektorých zákonov [online]. Bratislava: Národná rada Slovenskej republiky, 2005 [cit. 2024-05-11]. Dostupné z: <https://www.zakonypreludi.sk/zz/2005-473>).
- [80] KAMENÍK, J. a F. BRABEC. Komerční bezpečnost. 2. vydání. Praha: Wolters Kluwer, 2019. ISBN 978-80-7598-303-9.
- [81] FINSKO. Yksityisistä turvallisuuksipalveluista annetun lain (Private Security Services Act) [online]. Helsinki: Ministerstvo vnitra Finska, 2002 [cit. 2024-05-12]. Dostupné z: <https://www.finlex.fi/fi/laki/ajantasa/2002/20020882>.
- [82] DITRYCH, O., & BAHENSKÝ, V. (2021). Finský model členení hybridním hrozbám: inspirace pro ČR. Praha: Ústav mezinárodních vztahů (Policy paper). Dostupné z: <https://www.iir.cz/finsky-model-celeni-hybridnim-hrozbam-inspirace-pro-ceskou-republiku#>.
- [83] BUTTON, M., & STIERNSTEDT, P. (2018). Comparing Private Security Regulation in the European Union. *Policing and Society*, 28(4), 398–414. Dostupné z: <https://repository.uwl.ac.uk/id/eprint/6179/1/Button%20and%20Stiernstedt%20%282018%29%20Comparing%20private%20security%20regulation%20in%20the%20European%20Union.pdf#:~:text=Button%2C%20Mark%20and%20Stiernstedt%2C%20Peter,document%20in%20an%20alternative%20format>.
- [84] SMITH, M., & WHITE, A. (2014). The Paradox of Security Regulation: Public Protection versus Normative Legitimation. *Policy and Politics*, 42(3), 421–437. DOI:10.1332/030557312X655495.

[85] KRULÍK, O. a P. KLÍMA. 'Police volunteering' in Central and Eastern Europe. *Cogent Social Sciences*, 2024, roč. 10, č. 1, článek č. 2371660. DOI: 10.1080/23311886.2024.2371660.

[86] HOLLYWOOD, J. S., et al. *Mass Attacks Defense Toolkit*. Santa Monica: RAND Corporation, 2020. SBN-13 9781977412614.

[87] The Times. Austria school shooting: 10 dead, including suspect, and 12 hurt in Graz [online]. London: The Times, 10. 6. 2025 [cit. 10. 6. 2025]. Dostupné z: <https://www.thetimes.co.uk/article/austria-school-shooting-graz-news-d9qzx9jjd>.

[88] QUAGLIARINI, E.; FATIGUSO, F.; LUCESOLI, M.; BERNARDINI, G. a CANTATORE, E. Risk Reduction Strategies against Terrorist Acts in Urban Built Environments: Towards Sustainable and Human-Centred Challenges. DICEA Department, Università Politecnica delle Marche, 60131 Ancona, Italy. Online. 2021, s. 29. Dostupné z: <https://doi.org/10.3390/su13020901>. [cit. 2025-06-15].

[89] REID, S. The Halle, Germany, Synagogue Attack and the Evolution of the Far-Right Terror Threat. CTC Sentinel [online]. West Point: Combating Terrorism Center at West Point, 2019, roč. 12, č. 11, s. 14–20. [cit. 2025-08-16]. Dostupné z: <https://ctc.westpoint.edu/halle-germany-synagogue-attack-evolution-far-right-terror-threat/>.

[90] VISION OF HUMANITY. Global Terrorism Index 2025 [online]. Sydney: Institute for Economics and Peace, 2025 [cit. 2025-05-08]. Dostupné z: <https://www.visionofhumanity.org>.

[91] GLOBAL TERRORISM DATABASE. Global Terrorism Database (GTD) [online]. College Park: National Consortium for the Study of Terrorism and Responses to Terrorism (START), 2024 [cit. 2025-05-08]. Dostupné z: <https://www.start.umd.edu/gtd/>.

[92] OUR WORLD IN DATA. Terrorism [online]. Oxford: Our World in Data, 2024 [cit. 2025-05-08]. Dostupné z: <https://ourworldindata.org/terrorism>.

[93] UN SECURITY COUNCIL. Analytical Brief: Soft Targets [online]. New York: United Nations Security Council Counter-Terrorism Committee, 2021 [cit. 2025-05-08]. Dostupné z: <https://www.un.org/securitycouncil/ctc>.

[94] HAGHANI, M. (2024). Safeguarding Crowded Spaces against Terrorism. *Australian Journal of Emergency Management*, 39(1), 60–62. Dostupné z: <https://knowledge.aidr.org.au/media/10508/ajem-2024>

01_14.pdf#:~:text=Legislation%20plays%20a%20pivotal%20role,Named%20after%20Marty
n.

- [95] FEDERAL EMERGENCY MANAGEMENT AGENCY. Security of Soft Targets and Crowded Places – Resource Guide [online]. Washington, D.C.: FEMA, 2019 [cit. 2025-05-08]. Dostupné z: <https://www.fema.gov>).
- [96] ELIAMEP. Policy Paper on Counter-Terrorism in Europe [online]. Athens: Hellenic Foundation for European and Foreign Policy, 2023 [cit. 2025-05-08]. Dostupné z: <https://www.eliamep.gr>.
- [97] HOME OFFICE. Crowded Places: The Planning System and Counter-Terrorism [online]. London: Home Office, 2012 [cit. 2025-05-08]. Dostupné z: <https://www.gov.uk/government/publications/crowded-places-guidance>.
- [98] EUROPOL. European Union Terrorism Situation and Trend Report [online]. The Hague: Europol, 2017 [cit. 2024-05-08]. Dostupné z: <https://www.europol.europa.eu>.
- [99] EUROPOL. European Union Terrorism Situation and Trend Report [online]. The Hague: Europol, 2023 [cit. 2024-05-08]. Dostupné z: <https://www.europol.europa.eu>.
- [100] EUROPOL. EU Terrorism Situation and Trend Report (TE-SAT) 2024 [online]. Den Haag: European Union Agency for Law Enforcement Cooperation, 2024 [cit. 2025-05-12]. Dostupné z: <https://www.europol.europa.eu/publications-events/main-reports/eu-terrorism-situation-and-trend-report-te-sat-2024>.
- [101] MDPI. 2021. Review of Security in Czech Soft Targets. Basel: Multidisciplinary Digital Publishing Institute. ISSN 2313-576X.
- [102] CFPA EUROPE. Security Guidelines for Businesses [online]. Brussels: Confederation of Fire Protection Associations Europe, 2023 [cit. 2024-05-08]. Dostupné z: <https://cfpa-e.eu>.
- [103] KALVACH, Z., et al. Basics of Soft Targets Protection Guidelines [online]. Praha: Soft Targets Protection Institute, z. ú., 2016 [cit. 2025-08-23]. Dostupné z: <https://www.mvcr.cz/chh/soubor/basics-of-soft-target-protection-guidelines.aspx>.
- [104] ČESKÁ TELEVIZE. (2024). Policie představila závěry vyšetřování střelby na FF UK, zásah byl podle ní bez pochybení. [online]. Praha: ČT24. Dostupné z: <https://ct24.ceskatelevize.cz/domaci/3662912-policie-predstavila-zavery-vysetrovani-strelby-na-ff-uk-zasah-byl-podle-ni-bez>.
- [105] iROZHLAS. (2024). Policie hájí postup při zásahu na FF UK. Nešlo o systémové selhání, říká ministerstvo vnitra. [online]. Praha: Český rozhlas. Dostupné z:

https://www.irozhlas.cz/zpravy-domov/tiskova-konference-policie-ministerstvo-vnitra-zasah-strelba-filozoficka-fakulta_2401091400_pik.

[106] CUESTA, A., ABREU, O., BALBOA, A., & ALVEAR, D. (2019). A New Approach to Protect Soft-Targets from Terrorist Attacks. *Safety Science*, 120, 877–885. Dostupné z: <https://www.sciencedirect.com/science/article/abs/pii/S0925753518310993>.

[107] A CONNECTED ECOSYSTEM FOR PUBLIC SAFETY SOLUTIONS. Online. Dostupné z: <https://wrap.com/>. [cit. 2025-05-26].

[108] EVROPSKÁ UNIE. Směrnice Evropského parlamentu a Rady (EU) 2018/1972 ze dne 11. prosince 2018, kterou se stanoví evropský kodex pro elektronické komunikace. In: Úřední věstník Evropské unie [online]. 17.12.2018, L 321, s. 36–214 [cit. 2025-08-17]. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32018L1972>.

[109] GENASYS INC. (2019). NEWS Extended Presentation [pdf]. San Diego: Genasys Inc. Dostupné z: interní dokumentace.

[110] GENASYS INC. (2019). MNS – EECC Public Warning [pdf]. San Diego: Genasys Inc. Dostupné z: interní dokumentace.

[111] GENASYS INC. (2019). Genasys MNS 3.0 Presentation [pdf]. San Diego: Genasys Inc. Dostupné z: interní dokumentace.

[112] GENASYS INC. (2019). MNS User Manual v1.1 [pdf]. San Diego: Genasys Inc. Dostupné z: interní dokumentace.

[113] GENASYS INC. (2019). Genasys Public Safety Overview v2.0 [pdf]. San Diego: Genasys Inc. Dostupné z: interní dokumentace.

[114] EUROPEAN EMERGENCY NUMBER ASSOCIATION. (2019). EENA EECC Presentation [pdf]. Brussels: EENA. Dostupné z: interní dokumentace.

[115] NATIONAL RESEARCH COUNCIL. Assessment of Technologies Deployed to Improve Aviation Security. Washington, D.C.: National Academies Press, 2004. ISBN 978-0-309-08924-9.

[116] UNITED STATES DEPARTMENT OF DEFENSE. Non-Lethal Weapons Reference Book. Quantico, VA: Joint Non-Lethal Weapons Directorate, 2004. [cit. dne 9.7.2025] Dostupné z: <https://jnlwp.defense.gov>.

- [117] GREENBERG, M. S. a DANIELS, W.. Behavioral Detection of Threats: Study of Behavioral Indicators of Malicious Intent. Washington, D.C.: U.S. Department of Homeland Security, Transportation Security Administration, 2009. Dostupné z: <https://www.dhs.gov/publication/behavioral-detection>.
- [118] U.S. DEPARTMENT OF HOMELAND SECURITY. If You See Something, Say Something® – Campaign Overview. Washington, D.C.: DHS, 2020. Dostupné z: <https://www.dhs.gov/see-something-say-something>.
- [119] MINISTERIO DEL INTERIOR (Spain). AlertCops: Security in Your Hand. Madrid: Spanish Ministry of Interior, 2022. Dostupné z: <https://alertcops.ses.mir.es>.
- [120] HOLLYWOOD, J. S., GIERLACK, K., MOORE, P., GOODE, T., WILLIS, H. H., ... (2024). Keeping Soft Targets and Crowded Places Safe from Mass-Casualty Attacks: Insights from a Landscape Assessment. Santa Monica: RAND Corporation.
- [121] ZDRAVOTNICKÁ ZÁCHRANNÁ SLUŽBA KRÁLOVÉHRADECKÉHO KRAJE, interní dokumentace a veřejné prezentace projektu First Responder (2022). Dostupné také z: <https://www.zzskhk.cz/kurzy-pro-first-responder/>.
- [122] OUR UNDERSEA CABLES AND PIPELINES NEED URGENT PROTECTION. Online. The Times. Dostupné z: <https://www.thetimes.com/>. [cit. 2025-05-29].
- [123] ENISA. (2022). Threat Landscape for Critical Entities. Luxembourg: Publications Office of the European Union. ISBN 978-92-9204-577-5.
- [124] CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY. (2021). Protective Security Coordination Division Annual Report. Washington D.C.: U.S. Department of Homeland Security.
- [125] ESTONIAN MINISTRY OF THE INTERIOR. (2020). Estonia's National Defence Strategy. Tallinn.
- [126] LIMNÉLL, J. Countering Hybrid Threats: Role of Private Sector Increasingly Important – Shared Responsibility Needed. Hybrid CoE Strategic Analysis 6. Helsinki: European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), březen 2018. ISBN 978-952-7282-55-7.

12 SEZNAM POUŽITÝCH OBRÁZKŮ

Obrázek 1 - Analyzované podniky za jednotlivé roky (zdroj: vlastní).....	37
Obrázek 2 - Formy využití SBS výrobními podniky v jednotlivých sledovaných obdobích (zdroj: vlastní).	38
Obrázek 3 - Formy využití SBS nevýrobními podniky v jednotlivých sledovaných obdobích (zdroj: vlastní).	39
Obrázek 4 - Celkový poměr druhu využití SBS analyzovanými subjekty (zdroj: vlastní).	40
Obrázek 5 - Celkový rozdíl ve využití SBS analyzovaných podniků (zdroj: vlastní).....	41
Obrázek 6 - Procentuální využití jednotlivých bezpečnostních agentur (zdroj: vlastní)....	42
Obrázek 7 - Řetězec útoku a odpovídající obranné vrstvy pro měkké cíle a frekventovaná místa [86].....	53
Obrázek 8 - Útoky aktivního střelce v USA od roku 2000 [86].....	54
Obrázek 9 - Celkový počet útoků na měkké cíle ve světě (2010-2020) [91,92].	55
Obrázek 10 - Teroristické útoky na MC a zadržení ve státech EU a Velké Británii v roce 2016 [98].	57
Obrázek 11 - Teroristické útoky na MC v EU a Velké Británii v roce 2022 [99].	57
Obrázek 12 - Teroristické útoky na MC v EU ve vybraných státech v roce 2023 [100]. ...	58
Obrázek 13 - Vstupní údaje hodnoceného MC (zdroj: vlastní - RShiny).	70
Obrázek 14 - Vizualizovaný výstup metodiky TRS (zdroj: vlastní - RShiny).....	74
Obrázek 15 - Návrh opatření k navýšení bezpečnosti MC a jednotlivé implementační kroky (zdroj: vlastní - RShiny).....	75
Obrázek 16 - Využití mobilních operátorů v systému varování společností Genasys[109].	84

13 SEZNAM POUŽITÝCH TABULEK

Tabulka 1 - Komparace současného stavu komerční bezpečnosti v ČR se zahraničními modely (zdroj: vlastní).	50
Tabulka 2 - SWOT analýza možností využití SBS k ochraně MC v ČR (zdroj: vlastní). ..	63
Tabulka 3 - Specifikace kategorií SBS s orientačními náklady (zdroj: vlastní).	71
Tabulka 4 - Redukční faktory kategorií SBS (zdroj: vlastní).	72
Tabulka 5 - Kvantitativní klasifikace rizikových úrovní s doporučenou kategorií SBS (zdroj: vlastní).	72
Tabulka 6 - Benchmarking dle typologie objektů MC (zdroj: vlastní).	75

14 SEZNAM POUŽITÝCH PŘÍLOH

Příloha 1 - Checklist parametru bezpečnostní situace (zdroj: vlastní - RShiny).....	122
Příloha 2 – Checklist parametru dostupnosti pomoci (zdroj: vlastní - RShiny).....	122
Příloha 3 - Checklist parametru ekonomického dopadu (zdroj: vlastní - RShiny).....	123
Příloha 4 - Checklist parametru personální bezpečnosti (zdroj: vlastní - RShiny).	123
Příloha 5 – Checklist parametru společenského významu (zdroj: vlastní - RShiny).	124
Příloha 6 – Checklist parametru technických zabezpečení (zdroj: vlastní - RShiny).	124
Příloha 7 – Checklist parametru fyzické ochrany (Zdroj: vlastní - RShiny).....	125
Příloha 8 – Základní komponenty TRS (zdroj: vlastní).	125
Příloha 9 – Checklist fyzických bezpečnostních opatření (zdroj: vlastní).	126
Příloha 10 – Checklist faktorů kritičnosti (zdroj: vlastní).	127
Příloha 11 – Checklist hrozeb a rizikových faktorů (zdroj: vlastní).....	127

15 PŘÍLOHY

Příloha 1 - Checklist parametru bezpečnostní situace (zdroj: vlastní - RShiny).

Checklist bezpečnostní situace

- ☐ Vysoká kriminalita v oblasti
- ☐ Bezpečnostní incidenty v minulosti
- ☐ Možný teroristický cíl
- ☐ Časté protesty v okolí
- ☐ Činnost skupin/gangů v oblasti

Skóre bezpečnostní situace:

0 bodů (max 50)

Příloha 2 – Checklist parametru dostupnosti pomoci (zdroj: vlastní - RShiny).

Checklist dostupnosti pomoci

- ☐ Policie vzdálena více než 10 min
- ☐ Nemocnice vzdálena více než 15 min
- ☐ Žádná bezpečnostní služba v okolí
- ☐ Obtížný přístup pro záchranné služby
- ☐ Odlehlá lokalita

Skóre dostupnosti pomoci:

0 bodů (max 50)

Checklist ekonomického dopadu

- ☐ Vysoká hodnota majetku (>100 mil. Kč)
- ☐ Kritické pro chod firmy
- ☐ Více než 100 zaměstnanců
- ☐ Velký ekonomický dopad při útoku
- ☐ Problémy s pojištěním při útoku

Skóre ekonomického dopadu:

0 bodů (max 50)

Checklist personální bezpečnosti

- ☐ Bezpečnostní služba na místě
- ☐ Bezpečnostní recepce
- ☐ Proškolený personál
- ☐ Registrace návštěvníků
- ☐ Nouzové postupy

Skóre personální bezpečnosti:

33 bodů (max 33)

Checklist společenského významu

- ☐ Objekt je často v médiích
- ☐ Má symbolický význam
- ☐ Vládní/státní zařízení
- ☐ Více než 5000 návštěvníků denně
- ☐ Poskytuje nezbytné služby

Skóre společenského významu:

0 bodů (max 50)

Checklist technických systémů

- ☐ CCTV pokrytí hlavních oblastí
- ☐ 24h monitoring CCTV
- ☐ Elektronické přístupové karty
- ☐ Poplachový systém
- ☐ Detektory kovů na vstupech
- ☐ Komunikační systém pro bezpečnost

Skóre technických systémů:

34 bodů (max 34)

Checklist fyzické ochrany

☐ Oplocení celého pozemku
☐ Kontrolované vstupy
☐ Bezpečnostní brány/turnikety
☐ Protivozidlové bariéry
☐ Dostatečné osvětlení

Skóre fyzické ochrany:

33 bodů (max 33)

Příloha 8 – Základní komponenty TRS (zdroj: vlastní).

Komponenta	Rozsah	Interpretace
Fyzická zranitelnost	0-33 bodů	n_fyz = počet fyzických opatření
Technická zranitelnost	0-34 bodů	n_tech = počet technických systémů
Personální zranitelnost	0-33 bodů	n_pers = počet personálních opatření
Celková zranitelnost	0-100 bodů	Součet všech zranitelností
Společenská kritičnost	0-50 bodů	n_spol = počet společenských faktorů
Ekonomická kritičnost	0-50 bodů	n_ekon = počet ekonomických faktorů
Celková kritičnost	0-100 bodů	Součet kritičností
Bezpečnostní hrozba	0-50 bodů	n_bezp = počet bezpečnostních rizik
Hrozba dostupnosti pomoci	0-50 bodů	n_pomoc = počet omezení pomoci
Celková hrozba	0-100 bodů	Součet hrozeb

Příloha 9 – Checklist fyzických bezpečnostních opatření (zdroj: vlastní).

Oblast	Opatření	Bodová hodnota	Kritéria hodnocení
Perimetr	Oplocení celého pozemku	6,6 bodů	Výška min. 2m, nepřerušovaný
	Kontrolované vstupy	6,6 bodů	Max. 2 hlavní vstupy s kontrolou
	Bezpečnostní brány/turnikety	6,6 bodů	Elektronické, s kamerou
	Protivozidlové bariéry	6,6 bodů	U všech vstupů pro vozidla
	Bezpečnostní osvětlení	6,6 bodů	Min. 20 lux, bez slepých míst
Technické systémy	CCTV pokrytí hlavních oblastí	5,67 bodů	Min. 70% pokrytí
	24h monitoring CCTV	5,67 bodů	Nepřetržité sledování
	Elektronické přístupové karty	5,67 bodů	Pro všechny zaměstnance
	Poplachový systém	5,67 bodů	Napojený na PCO
	Detektory kovů na vstupech	5,67 bodů	Na hlavních vstupech
	Komunikační systém	5,67 bodů	Pro nouzové situace
Personál	Bezpečnostní služba na místě	6,6 bodů	Min. 8h denně
	Bezpečnostní recepce	6,6 bodů	Školený personál
	Proškolený personál	6,6 bodů	Pravidelná školení
	Registrace návštěvníků	6,6 bodů	Povinná registrace
	Nouzové postupy	6,6 bodů	Písemné postupy, cvičení

Příloha 10 – Checklist faktorů kritičnosti (zdroj: vlastní).

Dimenze	Faktor	Bodová hodnota	Kritéria hodnocení
Společenský význam	Mediální pozornost	10 bodů	Často v médiích (>5× ročně)
	Symbolická hodnota	10 bodů	Národní/regionální symbol
	Vládní/státní zařízení	10 bodů	Státní správa, justice
	Vysoká návštěvnost	10 bodů	>5000 návštěvníků denně
	Nezbytné služby	10 bodů	Zdravotnictví, vzdělání
Ekonomický dopad	Vysoká hodnota majetku	10 bodů	>100 mil. Kč celková hodnota
	Kontinuita podnikání	10 bodů	Kritické pro chod organizace
	Počet zaměstnanců	10 bodů	>100 zaměstnanců
	Ekonomický dopad útoku	10 bodů	Velké finanční ztráty
	Pojistné problémy	10 bodů	Problémy s pojištěním

Příloha 11 – Checklist hrozeb a rizikových faktorů (zdroj: vlastní).

Dimenze	Rizikový faktor	Bodová hodnota	Kritéria hodnocení
Bezpečnostní situace	Vysoká kriminalita v oblasti	10 bodů	>40 trestných činů/1000 obyvatel
	Bezpečnostní incidenty	10 bodů	Incident v posledních 2 letech
	Možný teroristický cíl	10 bodů	Symbolická hodnota/médií
	Časté protesty v okolí	10 bodů	>3 protesty ročně
	Činnost gangů v oblasti	10 bodů	Známá přítomnost org. zločinu
Dostupnost pomoci	Vzdálená policie	10 bodů	>10 min doba příjezdu
	Vzdálená nemocnice	10 bodů	>15 min doba příjezdu
	Žádná bezpečnost v okolí	10 bodů	Žádné SBS firmy v regionu
	Obtížný přístup	10 bodů	Komplikovaný přístup pro IZS
	Odlehlá lokalita	10 bodů	Mimo městské centrum