



Zdravotně
sociální fakulta
Faculty of Health
and Social Sciences

Jihočeská univerzita
v Českých Budějovicích
University of South Bohemia
in České Budějovice

Ochrana zdravotnických zařízení před terorismem

DIPLOMOVÁ PRÁCE

Studijní program:

OCHRANA OBYVATELSTVA

Autor: Bc. Anna Klečková

Vedoucí práce: Mgr. Zuzana Freitinger-Skalická, Ph.D.

České Budějovice 2022

Prohlášení

Prohlašuji, že svoji diplomovou práci s názvem *Ochrana vybraných zdravotnických zařízení před terorismem* jsem vypracovala samostatně pouze s použitím pramenů v seznamu citované literatury.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské/diplomové práce, a to v nezkrácené podobě elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby diplomové práce. Rovněž souhlasím s porovnáním textu mé diplomové práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

V Českých Budějovicích dne 9. 5. 2022

.....

Bc. Anna Klečková

Poděkování

Na tomto místě bych ráda poděkovala Mgr. Zuzaně Freitinger–Skalické, Ph.D. za odborné vedení mé diplomové práce, metodickou pomoc a cenné rady. Dále bych ráda poděkovala Bc. Jaroslavu Kubínovi za jazykovou korekturu.

Ochrana vybraných zdravotnických zařízení před terorismem

Abstrakt

Diplomová práce se zabývá analýzou zabezpečení vybraných zdravotnických zařízení, jejich zkušeností s teroristickými i kyberteroristickými útoky a analýzou rozdílů v ohrožení a zabezpečení zdravotnických zařízení v České republice a vybraných státech. K naplnění prvního cíle práce a zodpovězení výzkumných otázek byl proveden kvantitativní výzkum pomocí dotazníkového šetření a k naplnění druhého cíle byl proveden kvalitativní výzkum formou polostrukturovaných rozhovorů se zaměstnanci zdravotnických zařízení, kteří mají zkušenost ze zahraničních stáží/misí ve zdravotnictví ve vybraných státech. Data získaná výzkumem a provedeným šetřením byla vyhodnocena pomocí přehledných grafů a grafických znázornění. Na základě vyhodnocení získaných dat lze konstatovat, že ve většině zdravotnických zařízeních (ZZ) není zabezpečen vstup, nenacházejí se v něm bezpečnostní rámy a vstup pro zaměstnance není oddělen ani zabezpečen. Ve většině ZZ se nekoná školení na reakci na terorismus, zaměstnanci nejsou obeznámeni s opatřeními proti terorismu, většina respondentů by však takové školení uvítala. Z polostrukturovaných rozhovorů bylo zjištěno, že zabezpečení ZZ je pro každý stát individuální, odvíjející se od konkrétní situace. Zaměstnanci se ve většině zemí neškolí. Ohrožení zdravotnického zařízení bylo ve většině případů větší než v ČR. Většina respondentů vnímá rozdíl v zabezpečení ZZ a myslí si, že prvky zabezpečení jsou aplikovatelné v ČR. Tyto aspekty jsou dále diskutovány a porovnány se zahraničními výzkumy. Dále jsou nastíněny další možnosti výzkumu, slabiny v ochraně ZZ a doporučení pro praxi. Závěry plynoucí z diplomové práce mohou být využity ke zlepšení prostředků ochrany ZZ před terorismem.

Klíčová slova

nemocnice; ochrana zdravotnických zařízení; terorismus; školení; zahraniční mise

Protecting hospitals from terrorism

Abstract

The diploma thesis deals with the analysis of the security of selected medical facilities (hospitals), their experience with terrorist and cyber-terrorist attacks and the analysis of differences in the threat and security of medical facilities in the Czech Republic and selected countries. To fulfil the first goal of the work and to answer research questions, a quantitative research was conducted using a questionnaire survey, and to fulfil the second goal, a qualitative research in the form of semi-structured interviews with employees of medical facilities who have experience from foreign internships/missions in health care in selected countries was conducted. The data obtained from the research and the survey were evaluated using graphs and graphical representations. Based on the evaluation of the obtained data, it can be stated that in most medical facilities (hospitals) the entrance is not secured, there are no security check door frames and the entrance for employees is not separated or secured. Most hospitals do not provide training, employees are not familiar with counter-terrorism measures, but most respondents would welcome terrorism response training. From the semi-structured interviews, it was found that the level of security is individual for each state, depending on the current situation. In most countries, employees are not trained to respond to terrorism. The threat to the medical facility in other countries was in most cases more severe than in the Czech Republic. Most respondents perceive differences in hospital security and think that some security features used elsewhere are applicable in the Czech Republic. These aspects are further discussed and compared with foreign research. Furthermore, other research possibilities, weaknesses in hospital protection and recommendations for practise are also outlined. The conclusions resulting from the diploma thesis can be used to improve the means of protecting hospitals from terrorism.

Key Words

Foreign missions; Hospitals; Protection of medical facilities; Terrorism; Training

Obsah

Úvod.....	8
1 Současný stav	10
1.1 Terorismus	10
1.1.1 Typologie terorismu	12
1.1.2 Historie a vývoj terorismu	15
1.1.3 Terorismus v České republice	22
1.2 CBRN Terorismus	24
1.3 Kyberterorismus.....	24
1.4 Útoky na zdravotnická zařízení v ČR v souvislosti s terorismem	27
1.5 Boj proti terorismu	28
1.6 Boj proti terorismu na nadnárodní úrovni.....	30
1.7 Ochrana kritické infrastruktury zdravotnictví.....	33
1.8 Legislativa související s terorismem.....	34
2 Cíle práce a výzkumná otázka.....	39
2.1 Formulace problému	39
2.2 Cíle práce	39
2.3 Výzkumné otázky	39
3 Operacionalizace pojmů použitých v cíli práce	40
4 Metodika	41
5 Výsledky	44
5.1 Současné zabezpečení a struktura nemocnic	44
5.2 Výsledky dotazníků	46
5.3 Výsledky polostrukturovaných rozhovorů.....	77
6 Diskuse.....	93
6.1 Diskuse vztahující se k cíli práce č. 1	94
6.1.1 Zabezpečení vstupu do ZZ	94

6.1.2	Zkušenosti ZZ s teroristickým nebo kyberteroristickými útokem	95
6.1.3	Školení zaměstnanců na nácvik reakce na teroristický útok	98
6.2	Diskuse vztahující se k cíli práce č. 2.....	100
	Závěr.....	105
	Seznam použitých zdrojů	108
	Seznam obrázků	120
	Seznam tabulek	122
	Seznam příloh.....	123
	Příloha 1 - Vzor dotazníku	124
	Příloha 2 - Vzor polostrukturovaného rozhovoru	132
	Seznam zkratk	133

Úvod

V současné době je terorismus největší bezpečnostní výzvou pro demokratické země na celém světě. Ačkoliv v posledních letech nabývá na síle, a i díky digitalizaci a globalizaci světa zaujímá podstatné postavení v mediálním prostoru, jeho definice je dosud polemizovaná a nejednotná. Obrana a prevence před ním jsou nedostatečné a ohrožení především měkkých cílů, tedy míst s vysokou koncentrací osob a nízkou úrovní zabezpečení, vzrůstá. Nejen v Evropě se diskutuje o problematice zabezpečení měkkých cílů proti terorismu. Za posledních dvacet let se odehrávaly teroristické útoky v metropolích některých vyspělých zemí, např.: New York, Berlín, Paříž atd. Ani v Čechách není toto téma nepodstatné. Během posledních pěti let jsme zaznamenali několik útoků na zdravotnická zařízení, a to jak zbraněmi, tak v podobě kyberterorismu. V dnešní době představuje hrozbu právě proto, že dochází k naprosto nezastavitelné inovaci informačních technologií, vývoji zbraní, masovému vlivu médií, internetu a sociálních sítí, otevírání hranic států za účelem volného pohybu osob apod. Tato práce se zaměřuje na terorismus z pohledu měkkých cílů, tedy právě zdravotnických zařízení, jejich možnosti ochrany a na zjištění stávajících prostředků jejich ochrany.

Cílem diplomové práce je analyzovat zabezpečení vybraných zdravotnických zařízení a jejich zkušeností s teroristickými a kyberteroristickými útoky a analyzovat rozdíly v ohrožení a zabezpečení zdravotnických zařízení v České republice a vybraných zahraničních státech.

Teoretická část je rozdělena do osmi tematických celků, které jsou tvořeny informacemi z rešerší odborné literatury týkající se problematiky diplomové práce. V první kapitole s názvem *Terorismus* je definován a popsán pojem terorismus, rozdělení terorismu, jeho historický vývoj ve světě a v České republice (ČR). Druhá kapitola s názvem *CBRN (chemický, biologický, radiologický a nukleární) terorismus* stručně definuje možnosti použití zbraní hromadného ničení. Ve třetí kapitole s názvem *Kyberterorismus* je definován tento pojem a jsou zde popsány způsoby jeho použití. Čtvrtá kapitola s názvem *Útoky na zdravotnická zařízení v ČR v souvislosti s terorismem* se zabývá teroristickými a kyberteroristickými útoky na nemocnice v ČR. Pátá kapitola s názvem *Boj proti terorismu* se věnuje způsobům zamezení této činnosti v ČR. Šestá kapitola s názvem *Boj proti terorismu na nadnárodní úrovni* se zabývá spoluprací ČR s organizacemi, které zabraňují šíření terorismu. V předposlední kapitole s názvem *Ochrana kritické infrastruktury zdravotnictví*

je definován tento pojem a ochrana nemocnic z pohledu ochrany kritické infrastruktury. V poslední kapitole s názvem *Legislativa související s terorismem* jsou popsány nejdůležitější právní předpisy týkající se terorismu.

Hlavní metodou pro zpracování výzkumné části a zodpovězení výzkumných otázek je šetření formou dotazníků a polostrukturovaných rozhovorů. Výzkumná část diplomové práce se zabývá zkoumáním responzí na zpracované dotazníky a odpovědí ze strany stážístů nebo účastníků misí. Data získaná šetřením jsou zpracována do přehledných grafů.

1 Současný stav

V roce 2013 bylo spácháno přibližně 100 teroristických útoků v nemocnicích po celém světě, ve 43 zemích na všech kontinentech. Útoky zabily přibližně 775 lidí a zranily 1 217 dalších. V roce 2018 bylo spácháno 973 útoků na zdravotnická zařízení ve světě, bylo zabito 167 zdravotníků a více než 700 jich bylo zraněno. Lze tedy usoudit, že teroristické útoky na zdravotnická zařízení mají stoupající tendenci (Rubenstein, 2018). Nemocnice jsou atraktivním cílem pro teroristické organizace z důvodu umístění materiálů a znalosti, které by mohly být snadno zneužitelné: léky, jedy, radioaktivní materiály, biologické kultury (Ganor a Wernli, 2013).

V této kapitole bude definován a popsán pojem terorismus, jeho typologie a historický vývoj. Dále bude popsán pojem kyberterorismus a v další podkapitole budou uvedeny případy útoku na nemocnice v České republice. Další podkapitoly se budou věnovat boji proti terorismu v České republice a na mezinárodní úrovni. Bude zde popsána také ochrana kritické infrastruktury zdravotnictví a na závěr budou uvedeny nejdůležitější právní předpisy týkající se terorismu.

1.1 Terorismus

Od druhé poloviny dvacátého století nabývá terorismus na síle a významu oproti předchozímu období. Svůj původ má v latinském slově „*terror*“ (strach, hrůza, zděšení, věc působící strach), či ve slově „*terrero*“ (třást se, nahánět strach). Tento je definován jako nahánění nebo šíření strachu. I přes jasný původ slova mnozí autoři uvádějí, že terorismus nelze jednoduše definovat, a přestože definic existuje nespočet, žádná není obecně uznávaná (Mareš, 2005; Řehák *et al.*, 2008; Ibáñez, 2009; Miller a Mitchel, 2009; Kraus, 2014; Procházková, 2014; Filipec, 2017; Šín *et al.*, 2017; Nekola, 2017; Dolliver a Kearns, 2019; Court *et al.*, 2020). Dále je tento pojem velmi široce pojat z důvodů odlišných pohledů vědců, vládních autorit, veřejnosti a samotných teroristů a jejich sympatizantů (Řehák *et al.*, 2008; Mareš, 2005).

Jedním z důvodů složitosti uchopení pojmu je jeho častá záměna za jiné formy politického násilí (guerilla, konvenční válka, občanská válka, povstání). V současné době se vzhledem k charakteru válečných konfliktů rozdíl mezi terorismem, guerillovou válkou a konvenční válkou stírají (Mareš, 2005; Šín *et al.*, 2017). Válka je konflikt minimálně dvou stran, jednu stranu musí tvořit vojsko, válku řídí centrální organizace

a vykazuje strategii. V těchto konfliktech hraje dominantní roli stát. Civilní obyvatelstvo by se nemělo války účastnit. Účastníci konvenční války zpravidla respektují určitá pravidla (rozlišení, nepoužití některých zbraňových systémů, ochrana civilního obyvatelstva, základní práva pro zajatce...). Na rozdíl od války, v terorismu nejsou respektovány žádné konvence a je zde mnohdy využíváno momentu překvapení. Při terorismu není rozlišováno mezi civilními a vojenskými cíli a krom vedení ilegálního boje, není problémem využití zbraní hromadného ničení. Dle definice, vojáci uskutečňují legálně organizované státní násilí, oproti tomu teroristé cílí násilnými činy proti státu a proti společnosti (Mareš, 2005; Řehák *et al.*, 2008).

Občanskou válkou rozumíme organizovaný ozbrojený boj o státní moc mezi odlišnými sociálními, politickými nebo národnostními skupinami, který se děje uvnitř státu. Klasická forma guerilly (partyzánského způsobu boje) probíhá pomocí partyzánských operací, které podporují válečnou snahu svého státu na území, které je obsazeno, nebo je protivníka. Také se objevuje jako povstání, snaha o svržení politického systému násilím. Používají se při ní spíše lehké typy zbraní (pušky, část dělostřelectva), praktikuje se boj taktikou vojenského povelu nebo rozkazu, účinkem není zničení nepřítele jako při konvenční válce, ale jeho vojenské oslabení; od konvenční války se také liší domácí ilegalitou (Mareš, 2005; Řehák *et al.*, 2008).

První pokus o definici pojmu terorismus se uskutečnil v roce 1937 při jednání Společnosti národů ohledně uzavření „*Úmluvy o prevenci a potlačování mezinárodního terorismu*“, která nakonec nebyla většinou států ratifikována (Řehák, *et al.*, 2008). Terorismus byl vymezen široce, a to jako činy, které byly cílené proti státu a s cílem vyvolat teror u veřejnosti (Strmiska, 1996). Terorismus se může projevovat mnoha různými formami a uplatňuje širokou škálu metod i taktických a strategických přístupů (Mareš, 2005). Pro účely této práce bylo vybráno několik nejdůležitějších definic a pokusů o vymezení tohoto pojmu. Jedna ze starších definic národního terorismu zní: „*Je to akt nebo hrozba násilí proti nebojujícím, s cílem vymáhat pomstu, zastrašování nebo jiné ovlivňování dotčených osob.*“ Splňuje 2 charakteristiky – (1) je zaměřen na nebojující; (2) je užít k dramatickým účelům a vyvolání strachu v cílové populaci (Ron a Shama, 2014, str. 354).

Mareš (2005) vybírá do své knihy definici poukazující na použití agresivního a excesivního naplánovaného násilí s účelem vyslat zastrašující poselství většímu publiku, než jsou lidé, kteří jsou těmito akty bezprostředně poškozeni. Španělský sociolog

Luis de la Corte Ibáñez (2009, str. 19) určuje terorismus složitým předmětem studia a nabízí nám na základě historické analýzy a zhodnocení rozličných úhlů pohledu tuto definici: „*Jde o promyšlenou sérii násilných a zastrašujících činů, které míří proti nebojujícím obyvatelům a jsou naplánovány tak, aby psychologicky zapůsobily na mnohem větší počet osob, než jsou přímé oběti, a slouží tak k dosažení konkrétního, téměř vždy politického cíle*“.

Court *et al.* (2020) nabízejí ve své studii naopak spíše lékařskou definici terorismu. Ta se, na rozdíl od tradičních definic, na terorismus zaměřuje z hlediska zdravotní péče: úmyslné násilí, skutečné nebo hrozící, proti jednomu nebo více nebojujícím osobám a/nebo službám nezbytných pro ochranu jejich zdraví, což má za následek nepříznivé účinky na zdraví osob, které jsou bezprostředně postiženy, a jejich komunity, od ztráty pohody nebo bezpečí po zranění, nemoc a smrt.

Globální databáze terorismu uvádí definici terorismu jako „*Hrozící nebo skutečné použití nelegálních sil a násilí ze strany nestátního subjektu k dosažení politického, ekonomického, náboženského, nebo sociálního cíle prostřednictvím strachu, nátlaku nebo zastrašování*“ (GTD,2022).

V roce 2016 byl pod záštitou Ministerstva vnitra ČR proveden audit národní bezpečnosti za účelem vyhodnocení aktuálních problémů a hrozeb mezinárodního terorismu, radikálního extremismu, organizovaného zločinu a kyberterorismu. V rámci tohoto auditu byl také objasněn postoj ČR k neurčitým pojmům souvisejících s terorismem. ČR tedy terorismus definuje jako „*... takové jednání, které je politicky, nábožensky či jinak ideologicky motivováno a užívá násilí či jeho hrozby zejména s cílem vyvolat strach*“ (Ministerstvo vnitra ČR, 2016).

1.1.1 Typologie terorismu

Stejně jako existuje mnoho definic, setkáváme se i s mnoha různorodými typy terorismu dle rozličných kritérií. Aktéři nutně nemusí splňovat jedno kritérium pro zařazení do jedné skupiny, naopak často existuje více důvodů a motivací pro jejich jednání (Procházková, 2014). Původ či aktéři terorismu jsou kritéria, podle kterých se rozlišuje státní, nestátní a individuální terorismus. Rozsah teroristické činnosti jej člení na mezinárodní a lokální terorismus. Dle použitých prostředků se rozlišuje na konvenční (klasický) a nekonvenční (superterorismus), spojený se zbraněmi hromadného ničení (ZHN),

a dle příčin vzniku a šíření se rozlišuje terorismus politický, ideologický, kriminální, nacionalistický a psychologický. Další dělení terorismu jsou poměrně vágní, jejich úplná typologie by byla neúměrně rozsáhlá a výčet by působil pouze demonstrativně, z tohoto důvodu byla vybrána klasifikace podle zdroje motivace (Šín *et al.*, 2017):

Nábožensky inspirovaný

Do této kategorie patří terorismus židovský, křesťanský, islámský a další, který se odvíjí z náboženských sekt (Filipec, 2017). Z důvodu lepšího pochopení nábožensky motivovaného terorismu je nutné vymezit pojem fanaticismus. Fanaticismus je osobní přesvědčení, které je vztažené na omezené obsahy a hodnoty. Projevuje se také neschopností kompromisu a dialogu s jiným systémem a jinými lidmi. Fanatik bojuje s ostatními lidmi nebo se systémem jako s nepřítelem a snaží se nasadit všechny dostupné prostředky (Hole, 1998).

Jeden z příkladů křesťanské teroristické organizace je v USA Ku Klux klan, jenž prosazuje nadvládu bílé rasy a rasismus. Je také protikatolický a jeho základy vzešly z protestantské víry. V Africe vznikly křesťanské milice Antibalaka, které se dopouštějí vražd muslimského obyvatelstva. Tyto organizace spojuje radikální interpretace křesťanství spojená s radikálními politickými cíli. Židovské organizace jsou činné i mimo Svatou zemi, v USA od roku 1968 působí Židovská obranná liga, zřízení na obranu židů proti projevům antisemitismu. Islámský terorismus je složitý a uvést příklady vyžaduje určitý prostor, který přesahuje rozsah této práce, budu se tedy věnovat tomu nejdůležitějšímu. Radikální teroristické organizace vycházejí z principů saláfismu a wahhábismu, které usilují o návrat k islámu podle proroka Mohameda. Jejich cílem je také obnovení chalífátu, tudíž principu vládnutí muslimského vládce podle islámských norem a principů, které ovšem nejsou slučitelné s demokratickým zřízením (Filipec, 2017).

Islámský svět se dělí na zemi míru a zemi války, kde žijí nevěřící. U jednotlivých organizací se politické cíle liší. Např. Hamás bojuje proti Izraeli, Al-káida usiluje o sjednocení islámského světa. Křesťanský a židovský terorismus považujeme za lokalizovaný, ale z islámského terorismu se stala výzva pro světovou bezpečnost (Filipec, 2017). I buddhismus má své teroristické organizace, bojující např. za „vyčištění“ země od cizích kultur. Apokalyptická sekta, která se inspirovala buddhismem, Óm šinrikjó působící v Tokiu, způsobilá sarinový útok v roce 1995 (Filipec, 2017; Šín *et al.*, 2017).

Etno-nacionalistický a separatistický

Tento druh terorismu je motivovaný nacionalismem, etnickou příslušností či náboženstvím. Jeho podstatou je snaha získat vlastní stát nebo autonomii. Separatistické teroristické skupiny mají v zemích EU největší podíl na uskutečněných útocích, nicméně četnost útoků v posledním období klesá. Používána jsou improvizovaná výbušná zařízení a střelné zbraně. Své útoky zaměřují na materiální a policejní cíle za účelem svržení nadvlády (Šín *et al.*, 2017). Příkladem je Euskadi Ta Askatasuna (ETA, v překladu „Baskický stát a svoboda“), baskická organizace, založena 31. 8. 1959, s ideologií marxismu-leninismu a požadavky na vytvoření nezávislého Baskického státu. Marxismus-leninismus je souhrn poznatků, teorií, interpretačních principů a přesvědčení vybraný z díla Karla Marxe, Friedricha Engelse a Vladimira Iljiče Lenina, kodifikovaný na počátku 30. let 20. století J. V. Stalinem jakožto oficiální světónázorová a politická doktrína komunistických stran (Havelka, 2017). Tato organizace působila na severu Španělska a v jihozápadní Francii a má na svědomí atentát na španělského admirála a předsedu vlády Luise Carrera Blancu v roce 1973 (Buchtele, 2001; Filipec, 2017 David a Malacka, 2005). ETA působila do roku 2018 (Křovák, 2018).

Levicový a anarchistický

Levicové teroristické skupiny se snaží změnit celý politický, sociální a ekonomický systém státu podle levicového modelu. Ten je typický prudkými metodami prosazujícími komunistické nebo anarchistické ideologie, které jsou často marxisticko-leninské. K útokům využívají především improvizovaná výbušná zařízení, zápalné lahve a střelné zbraně. Jelikož jde o politický terorismus, cílem útoků jsou vládní budovy za účelem změny nebo svržení vlády. Tyto skupiny jsou neaktivnější v Řecku, Itálii a Španělsku (Řehák *et al.*, 2008; Šín *et al.*, 2017). Jako dobrý příklad slouží skupina Frakce Rudé Armády, která upoutala pozornost ve druhé polovině 20. století. Členové této skupiny spáchali bombové útoky na obchodní domy ve Frankfurtu nad Mohanem v roce 1968 (Filipec, 2017).

Pravicový terorismus

Podobně jako levicový je hodnotově pestrým proudem, sahá od fašismu a nacismu až po antikomunismus. Jedná se o skupiny vymezující se proti národnostním nebo rasovým menšinám, zřídka kdy se však jedná o organizované teroristické útoky (Filipec, 2017).

Pokud se tak stane, hovoříme o „homegrown terrorism“ neboli o domácím terorismu, který se vyskytuje v rozdělených společnostech s velkými komunitami přistěhovalců (Department of Homeland Security, 2019). Jako příklad lze uvést případ Anderse Breivika, který vystupoval ostře proti islámu a volal po deportaci muslimů z Evropy. V červenci 2011 při bombovém útoku a následné střelbě zabil 77 lidí na ostrově Utøya. V roce 2016 jím inspirovaný Němec íránského původu zastřelil 9 přistěhovalců (Filipec, 2017).

Monotematický terorismus

Monotematický, nebo také single-issue terorismus je zaměřený na jeden cíl s přáním změny politiky nebo praxe v rámci některé cílové skupiny ve společnosti (Šín *et al.*, 2017). Vymezení monotematického terorismu není zcela jednoznačné a lze jej definovat pomocí dvou prvků. Tím prvním je ohraničení výšeče politické ideologie nebo náboženství, přičemž nejde přímo o naplňování ideologie či hodnot, ale spíše o reálné účelové následky. Druhým prvkem je přesvědčení o morálním úpadku společnosti či její nedokonalosti, přičemž akt je zasazen do tohoto kontextu a na jeho základě zdůvodněn (Filipec, 2017). Hlavními oblastmi projevození monotematického terorismu jsou environmentální témata, např. negativní dopad lidské činnosti na životní prostředí či boj za práva zvířat (Šín *et al.*, 2017). Jako příklad je možné uvést teroristu Erica Roberta Rudolpha, jenž zničil bombovým útokem potratovou kliniku v alabamském Birminghamu a Atlantě. Dále také odpálil bombu v lesbickém baru v Atlantě z motivu přesvědčení o jeho sexuální nemorálnosti. Z ekologických teroristů lze uvést například organizace Fronta za osvobození zvířat, Fronta za osvobození země a PETA (People for The Ethical Treatment of Animals) (Filipec, 2017).

1.1.2 Historie a vývoj terorismu

Za posledních padesát let proběhly tři velké vlny politického násilí. V 60. až 70. letech to byly pokusy malých elitních skupin především v západní Evropě o svržení režimu nebo dosažení cílů separatistického nacionalismu. Koncem 80. a během 90. let proběhla na pozadí zhroucení režimů vlna občanských nepokojů ve státech Afriky, Středního východu a jižní a jihovýchodní Asie. Od počátku 21. století má pak politické násilí globální povahu, což lze vysvětlit ustavením teroristického hnutí operujícího na nadnárodním principu. V minulosti byly cíle teroristických útoků lokalizovány do několika málo oblastí světa, dnes je tomu právě naopak. Dříve, během 70. let, bylo přibližně 70 % útoků

zaměřeno proti budovám a majetku obecně a lidé byli jejich terčem pouze ve 30 % případů, nyní je tento poměr opačný (Mareš, 2005).

Publikace, které se zabývají dějinami terorismu, jej člení dle chronologie. Pro tuto práci bylo vybráno členění reflektující technologický rozvoj (Filipec, 2017).

Éra primitivního terorismu

První důkazy o organizovaných skupinách páchajících terorismus pocházejí z prvního století n. l., a to o organizaci Zélótů v Římány okupovaném Jeruzalémě, kteří bojovali proti okupantům. Bylo to extremistické židovské hnutí. Zélóti často prováděli vraždy nejvlivnějších představitelů římské komunity s demonstrativním významem. Ranný terorismus představovala islámská sekta Haš-Išim, která působila v 11. století v oblasti Perského zálivu. Od ní se poté oddělila jedna ze známějších sekt, známá jako kult asasínů, který mezi 11. a 13. stoletím terorizoval Blízký a Střední východ, rozšířil se na území Sýrie a Persie a tam zabíjel místní vládcy. V tomto období se jednalo spíše o geograficky izolované útoky s jednoduchými zbraněmi. Milníkem primitivní a začátkem nové éry je stanovena Francouzská revoluce (Řehák *et al.*, 2008; Filipec, 2017; Procházková, 2014).

Éra pokročilého terorismu

V průběhu této éry dochází ke zřetelnějšímu členění, a to na terorismus státní a protistátní. Po vynálezu střelného prachu a jeho rozšíření do Evropy se rozšířily možnosti teroristů. Mnohem důležitějším a pro teroristy významnějším vynálezem byl dynamit, jenž byl velice populární a dostupný díky využívání v těžebním průmyslu a měl jednoduché využití, k jeho zapálení stačila jediná osoba. Mezi Irskem a Velkou Británií se v letech 1881–1885 vedla tzv. „dynamitová válka“, v níž šlo Irům o vzepření se britské nadvládě. Výbuch dynamitu několikrát ochromil Londýn, což britskou vládu upozornilo na irskou otázku a ta se na čas stala hlavním bodem britské politiky. V roce 1886 začala „éra dynamitového terorismu“ ve Spojených státech, a to výbuchem v Chicagu, který způsobil smrt sedmi lidí. Třetí země, které se dotkl vynález dynamitu, je Rusko, zde pracovala především organizace Narodnaja volja, která ve stejné době, tj. 80. léta 19. století, bojovala např. za zrušení samoděržaví, svobodu tisku a projevu. Organizace má na svědomí zavraždění cara Alexandra II. Útočník sám útok nepřežil, čímž se stal prvním doloženým mezinárodním sebevražedným teroristou (Procházková, 2014; Filipec, 2017).

V zemích Evropy na počátku 20. století můžeme jako příklady uvést Španělsko, kde Mateo Morral hodil bombu zamaskovanou v pugétu na kočár krále Alfonse XIII. a jeho snoubenku. Tento útok z roku 1906 připravil o život 22 lidí. V Srbském království byla v roce 1911 založena organizace Černá ruka, která proslula úspěšným atentátem na Františka Ferdinanda d'Este roku 1914, čímž odstartovala řetězec událostí vedoucí k první světové válce. I v České republice jsme se v meziválečném období setkali s atentátem, a to na prvního ministra financí Aloise Rašina 5. 1. 1923 (Filipec, 2017).

Činy spojené s druhou světovou válkou můžeme považovat za jednání proti vybraným skupinám obyvatel s cílem naplnění politické ideologie (Filipec, 2017). Útoky na civilní obyvatelstvo, svržení atomových bomb na Japonsko, vyhlazování vesnic, ponorková válka proti obchodním lodím dokazují, že i stát je protagonistou válečných podob terorismu (Bonanate, 1997). Podrobně naplánované vyhlazování celých národů chápeme jako nejvyšší dosaženou míru státního terorismu a podobně tak nahlížíme na sovětské gulagy (Filipec, 2017).

Éra moderního terorismu

Tato éra začíná s koncem druhé světové války a dochází v ní k rozvoji zejména mezinárodního terorismu, a to v souvislosti se studenou válkou (1946–1989). Mezinárodní terorismus se rozvinul i v souvislosti s lepšími možnostmi cestování (Řehák *et al.*, 2008; Filipec, 2017). V Japonsku můžeme hovořit o rozvoji tzv. „kamikaze“, sebevražedných útocích pilotů, se kterými Japonci začali právě tehdy. V období studené války se také rozmohly sebevražedné útoky žen, které do té doby nebyly doloženy. Jedním z milníků rozvoje mezinárodního terorismu je útok skupiny Černé září, jejíž členové zajali během mnichovské olympiády v roce 1972 jedenáct izraelských sportovců. Poté se domáhali propuštění 234 aktivistů palestinského odboje a bezpečné dopravy do Káhiry. Nikdo ze zajatců tuto událost nepřežil a po neúspěšném zásahu policie bylo několik členů organizace zabito (Crawford, 2002). Díky této události začaly vznikat nové instituce zaměřené na boj proti terorismu, agentury a výbory pro boj s terorismem. Také se o toto téma začalo zajímat více odborníků (Filipec, 2017; Řehák *et al.*, 2008).

Na začátku 80. let se terorismus obecně rozšířil, a to zejména sebevražedný. Tento typ terorismu má vysoké cíle a specifickou organizaci. První sebevražedné teroristické útoky se objevily v roce 1982, po vpádu Izraele do Libanonu. Byly to např. nárazy nákladních aut s výbušninami do vojenských subjektů nepřítele. Únosy letadel také nebyly ojedinělé,

dokonce se objevil i záměr použít unesené letadlo jako vražednou zbraň (v roce 1994). Kromě letadel se hojně útočilo i na vlaky (např. únos vlaku v Nizozemí v roce 1975). Od roku 2003 narůstala nová vlna terorismu týkající se zejména Blízkého východu (Filipec, 2017; Řehák *et al.*, 2008).

Éra postmoderního terorismu

Jako začátek tohoto období může být určen sarinový útok v tokijském metru 20. 3. 1995, kdy poprvé došlo k užití chemické látky (sarinu) vyrobené teroristy (Řehák *et al.*, 2008). O něco lépe se jako začátek této éry určují teroristické útoky z 11. září 2001, a to z následujících důvodů: teroristé provedli vysoce koordinovaný útok; jejich akce vedla k vysokému počtu mrtvých, strach jako hlavní cíl teroru zasáhl mnohem větší počet obyvatel než jen zasažené oběti; byly použity občanské prostředky s větší účinností, než mají vojenské předměty; dopad byl umocněn médii, která vysílala útok v živém přenosu. Charakteristickým pro postmoderní terorismus je právě sebevražedný terorismus, který od 11. září 2001 rapidně narostl. Éra postmoderního terorismu souvisí zejména s Al-Káídou a s globální válkou vedenou proti terorismu na její popud. Ta byla zahájena v roce 2001 a zahrnuje přítomnost USA v Afghánistánu (2001-2014), Iráku (2003-2011), Pákistánu, Jemenu a její zapojení do mezinárodní kampaně proti organizaci Islámský stát (Filipec, 2017). Organizace Islámský stát má velmi dobré zdroje financí zejména z expanze na nové území, velmi dobře propracovává výstupy v několika jazycích, které jsou šířeny tak, aby přilákaly pozornost médií, využívají sociální sítě pro přilákání nových rekrutů nebo i pro komunikaci a šíření propagandy (Basit *et al.*, 2019).

Éra současnosti

Terorismus se v současné době stupňuje a riziko napadení se zvětšuje. Útočníci nemají žádné zábrany. Je to forma psychologické války, která má dát najevo nesouhlas např. Islámského státu se způsobem života v západním světě (Procházková, 2014). Kyberterorismus je v tomto období novým způsobem útoků. Primárně cílí na informace a data v kyberprostoru, proto může být chápán jako neletální způsob terorismu. V některých případech však může způsobit i ztráty na životech (více viz kapitola 1.3 Kyberterorismus) (Filipec, 2017). Poslední vlna terorismu na celém světě zaznamenala výrazné využití světových zbraní „nízké technologie“, jako jsou užitkové nože a civilní vozidla (Rozenfield *et al.*, 2019).

Pro přiblížení dění v Afghánistánu a nastínění současné situace je vysvětlen pojem Tálíbán (radikální nábožensko-politické hnutí v Afghánistánu). V letech 1996-2001 reálně vládlo na většině území Afghánistánu, byť se mu diplomatického uznání dostalo pouze od tří zemí: Saúdské Arábie, Spojených arabských emirátů a Pákistánu. Vláda Tálíbánu byla svržena díky americké intervenci, hnutí si však i přesto zachovalo kontrolu nad některými odlehlejšími oblastmi a od roku 2000 ve spojitosti s klesající americkou vojenskou přítomností jeho síla rostla. Tálíbán tak postupně rozšiřoval území pod svou kontrolou (Raschid, 2000).

Strategií Tálíbánu je postavit vládu mimo moc. Rok 2019 byl pro Afghánistán důležitým rokem, především kvůli volbám afghánského prezidenta (Basit *et al.*, 2019). Ghanímu se podařilo mandát obhájit. Ghaního konkurent, Abdulláh, výsledek voleb neuznal a oznámil, že vytvoří vlastní vládu. V březnu oba, Abdulláh i Ghaní, paralelně provedli inauguraci. Dvojvládí skončilo až v květnu 2020, kdy rivalové podepsali dohodu o dělbě moci (Qazi, 2020).

Dále měli o přítomnosti vojáků v Afghánistánu rozhodnout americké volby. USA rozhodla o stažení vojsk k 11. 9. 2021 a také o přesunutí protiteroristických bojovníků. Ti si zachovávají významná aktiva v regionu, aby čelili možnému znovuoobjevení se teroristické hrozby pro USA z Afghánistánu a drželi Tálíbán v jeho závazku, kterým je zajistit, aby Al-Káida znovu neohrožovala USA ani její zájmy nebo spojence. Podle USA Afghánci rozhodli o své budoucnosti sami. Po dosažení významných územních zisků v létě 2021 zemi ovládl Tálíbán, který 19. srpna 2021 vyhlásil vznik nového státního útvaru – Islámského emirátu Afghánistán), a to bez mezinárodního akceptování ostatními státy (Basit *et al.*, 2019; Macias, 2021; Doucet, 2021; Novotná, 2021b; Fiala a Luptáková, 2021; Jemelka, 2021).

V Afghánistánu byly velmi často cílem útoků nemocnice. Např. v roce 2011 nemocnice v Kábulu v okrese Azra v Kábulu. Při tomto útoku zahynulo 60 lidí (ČTK, 2011). V září 2019 zaútočil Tálíbán na nemocnici na jihu Afghánistánu, který měl za následek 39 mrtvých a 140 zraněných. V květnu 2020 organizace Islámský stát zaútočila na porodnici, což mělo za následek 24 obětí. Při útoku v Kábulu v listopadu 2021 zahynulo minimálně 25 obětí a 50 lidí bylo zraněno. K akci se přihlásila organizace Islámský stát. K 17. 3. 2022 WHO ověřila 89 útoků na ZZ (ČTK, 2011, 2019a; Šmigol, 2020; ČTK, 2021, 2022).

Terorismus v době pandemie COVID - 19

Dopad, který má pandemie COVID-19 na riziko terorismu, není markantní. Pandemie představuje pro teroristy výzvy i příležitosti. Kvůli nebezpečí nakažení a opatřením, která se dotkla společnosti, mohou být jejich operace zastaveny. Teroristé však mají tendenci přizpůsobit se změnám a využít i nestabilitu a nejistotu ke svému prospěchu. Některé následky pandemie, např. blokování pohybu přes hranice do jisté míry brání teroristickým útokům. Rada Evropské unie z důvodu potencionálních hrozeb, které by mohly být následkem pandemie COVID-19, přijala závěry a vyzvala členské země, aby jednaly za účelem odvrácení hrozeb (Ackerman a Peterson, 2020; Kubátová, 2020; Rada EU, 2021a).

Nespokojenost s vládními reakcemi na COVID-19, umocněná konspiračními teoriemi šířenými řadou stran, pravděpodobně zvýrazní stávající úroveň frustrace a podnítl zejména protivládní extremismus. První část tohoto argumentu je založena na obecně reaktivní a nekompetentní reakci vlád po celém světě na pandemii. To nepochybně podlomilo důvěru veřejnosti ve vládnoucí režimy a sloužilo jen k dalšímu narušení legitimacy vlády. Druhá část spočívá v tom, jak se extrémisté, jejichž ideologie je obzvláště nepřátelská, vrhli na vládní přešlapy (Ackerman a Peterson, 2020).

Někteří teroristé se uchýlili k práci z domova, to zahrnuje širokou škálu elektronických činností ISR (zpravodajské, sledovací a průzkumné), od hodnocení potenciálních cílů pomocí aplikace Google Earth až po zřízení a častější využívání kanálů Dark Web, pomocí nichž lze získávat nelegální materiály, které lze použít pro výrobu zbraní. Kyberteroristé jsou aktivnější. Hackeři například maskují viry odkazy na aktuální zprávy. U sebevražděných teroristů není vyloučeno použití COVID-19 jako zbraně, zejména proto, že je vysoce nakažlivý a vzorky jsou snadno dostupné (Ackerman a Peterson, 2020; Kubátová, 2020; Rada EU, 2021a).

Konvenční útoky během pandemie nejsou moc populární, protože obchodní centra atd. jsou opuštěná. Existuje však jedna výjimka, a to zdravotnická zařízení. Ta jsou pro teroristy během pandemie atraktivnějšími cíli kvůli větší koncentraci potencionálních obětí, a to nevyjímaje kyberterorismus (Ackerman a Peterson, 2020).

Válečný konflikt na Ukrajině

Rusko zahájilo 24. února útok na Ukrajinu, který následuje po dlouhodobě zhoršujícím se vztahu mezi Ruskem, Ukrajinou a Západem. Riziko terorismu narůstá s intenzitou konfliktu. Mezi terorismem a konfliktem existuje silný vztah, přičemž 97 procent všech úmrtí teroristů je zaznamenáno v zóně konfliktu. Také kybernetické útoky na Ukrajinu za poslední desetiletí výrazně vzrostly, a to zejména v měsících a týdnech před válkou. Vzhledem k obtížnosti přiřazování takových útoků není hranice mezi tím, co představuje kybernetický útok, kybernetickou válku nebo kybernetický terorismus, jasná. Ukrajinská vláda vycvičila dobrovolné hackery, aby zaútočili na Rusko (Institute for Economics & Peace, 2022).

Od začátku války na Ukrajině Světová zdravotnická organizace ověřila nejméně 43 útoků na zdravotní péči, včetně útoků na pacienty, zdravotnické pracovníky, zařízení nebo infrastrukturu. Více než 300 zdravotnických zařízení se nachází v bojových zónách nebo oblastech, které nyní Rusko kontroluje. Útok na porodnici v přístavním městě Mariupol 9. března si vyžádal 3 mrtvé a 17 zraněných. Na základě událostí z března 2022 jsou nemocnice, školy a další civilní místa možná nebezpečnější než vojenská místa. Kromě toho, že válka vážně poškodila infrastrukturu zdravotní péče, ztížila dostupnost život zachraňujících léků. Doručování léků do obležených měst je podle humanitárních pracovníků na místě stále obtížnější. Zjevné rozsáhlé ničení civilních objektů, jako jsou nemocnice a kliniky, vedlo k obviněním, že Rusko spáchalo řadu válečných zločinů (Simon, *et al.*, 2022).

Když země zaútočí na zdravotnická zařízení, vysílají tím zprávu, že nemají žádné hranice toho, co mohou dělat. Zaměřují se na pacienty, kteří reálně nepředstavují hrozbu a ani se nemohou bránit. Jít do nemocnice se stává nebezpečným, jít tam pro pomoc znamená riskovat svůj život. Nemocnice nemusí mít zkušenosti s řešením složitých zranění způsobených výbušninami. Může být také přítomno méně zaměstnanců, kvůli emigraci. Úřad OSN pro lidská práva uvedl svou ověřenou bilanci od začátku konfliktu na 636 zabitých civilistů a 1125 zraněných k 13. 3. 2022, ale uznává, že je pravděpodobně mnohem vyšší. Mezitím byly v zemi vysídleny téměř 2 miliony lidí a 2,8 milionu uprchlo do sousedních zemí (Besheer, 2022; Cole, 2022).

1.1.3 Terorismus v České republice

Česká republika patří k bezpečným zemím (Procházková, 2014), což mimo jiné můžeme vydedukovat z homogenní společnosti, která není výrazně nábožensky nebo etnicky rozdělena (Filipec, 2017).

Terorismus v ČR před rokem 1989

Již v období první republiky se setkáváme s terorismem na našem území, a to ve formě atentátů na představitele státu (Karel Kramář 1919, Alois Rašín 1923). Významné byly i česko-německé vztahy, které velmi poznamenal nacionalismus a nacismus. Např. vznikala řada skupin, které se podílely na teroristické činnosti a kvůli sabotáži překračovaly hranice s falešnými pasy, např. VDA (Volksbund für Deutschtum im Ausland). V září 1938 byla založena teroristická organizace Sudetoněmecký dobrovolnický sbor, který provedl přes 300 akcí, zabil 110 lidí a více než 2 000 občanů odvedl do Německa. Tento příklad byl jedním z úvodní etapy teroru, který následoval v období protektorátu Čechy a Morava (Procházková, 2014; Filipec, 2017).

Po konci druhé světové války se objevuje terorismus státní, směřovaný proti určitým skupinám obyvatelstva a doprovázený podporou zahraničních organizací šířících komunismus, popřípadě akce prováděné StB (státní bezpečností). StB hrála významnou roli v podpoře terorismu v 70. a 80. letech např. výcvikem teroristů v Praze. Československo podporovalo levicový terorismus, a to především materiálním a logistickým zázemím pro teroristy (Procházková, 2014; Filipec, 2017).

I protistátní terorismus byl v tomto období přítomný. Uvedme několik příkladů:

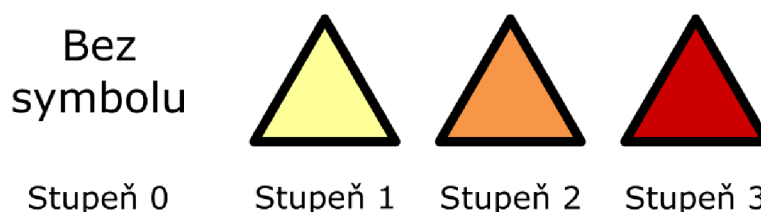
V srpnu 1978 byla odhalena skupina 35 mladých lidí ve věku okolo 15 let, kteří se domlouvali na likvidaci příslušníků SNB (Sboru národní bezpečnosti). Závažnými případy jsou také únosy autobusů a letadel s cestujícími. Největší počet případů této trestné činnosti byl bezpochyby v roce 1978, kdy bylo zabráněno 21 pokusům o únos letadel. Během let 1980-83 došlo v Jihomoravském kraji, včetně města Brna, k minimálně čtyřem případům použití zbraní pachatelů proti příslušníkům SNB. V jednom případě, který není dosud objasněn, pachatel při vloupání do lékárny jednoho příslušníka SNB zranil a druhého usmrtil (Zouhar, 1985).

Terorismus v ČR po roce 1989

Prvních deset let po roce 1989 nebyla naše země zasažena silnou vlnou klasického terorismu a jednalo se spíše o trestné činy, které vykazovaly známky terorismu. Politický i náboženský terorismus se ČR vyhýbá, pokud jde o jeho přímé důsledky. Proběhlo zde celkem 21 teroristických útoků, např. v roce 1990 v Praze na podstavci Jana Husa vybuchla bomba ve sportovní tašce, pachatel i motiv však zůstávají dodnes neobjasněny. V létě 2017 byl v České republice proveden teroristický útok, který měl za následek nehodu vlaků v důsledku pokácení dvou stromů na železniční trať. Pachatel se stal první osobou odsouzenou za trestný čin teroristický útok v České republice po novele legislativy (viz kapitola 1.8. *Legislativa související s terorismem*) (Procházková, 2014; Filipec, 2017; Svoboda, 2019).

V souvislosti se současnou bezpečnostní situací v Evropě přistoupila ČR k vytvoření systému vyhlášení stupňů ohrožení terorismem. Systém definuje 4 stupně ohrožení 0 až 3 (stupeň 0 – ideální stav, stupeň 1 – upozorňuje na existenci obecného ohrožení terorismem, stupeň 2 – upozorňuje na existenci zvýšené pravděpodobnosti ohrožení terorismem, stupeň 3 – teroristický útok očekáván nebo již proběhl). Stupně jsou také barevně znázorněny žlutou, oranžovou a červenou barvou uvnitř černě lemovaného trojúhelníku (viz obr. 1). Vývoj situace v posledních letech si vyžádal komplexní řešení tématu ochrany měkkých cílů. Skutečnost, že těchto cílů je velké množství, limituje jejich zabezpečení ze strany státu. Byla tedy zpracována metodika ochrany měkkých cílů s názvem *Základy ochrany měkkých cílů* (Soft Targets Protection Institute, 2016), která uvádí doporučení pro zabezpečení měkkých cílů ze strany správců těchto cílů. K 1. 7. 2021 je v ČR vyhlášen stupeň 1 (Šín *et al.*, 2017; Ministerstvo vnitra ČR, 2021a).

Stupně ohrožení terorismem



Obrázek 1. Stupně ohrožení terorismem (podle EXANPRO 2005, upraveno).

Řešením následků případných teroristických útoků se zabývají složky integrovaného záchranného systému (dále IZS). Nezastupitelnou úlohu má zdravotnictví a jednotlivé

články zdravotnického záchranného řetězce. Nemocnice musí být připraveny zvládnout následky těchto útoků, při kterých se počet raněných pohybuje až po několik stovek osob. Pro účely spolupráce všech složek byly zpracovány typové činnosti složek IZS při společném zásahu, např. „Reakce na chemický útok v metru“. Zdravotnická zařízení používají tzv. traumatologické plány pro rychlou, plynulou a dobře organizovanou neodkladnou nemocniční péči při všech hromadných neštěstích. Při prověřování připravenosti IZS na zvládnání následků teroristických útoků jsou cvičení, jejichž scénáře jsou motivované uskutečněnými teroristickými útoky ve světě. Smyslem těchto cvičení je zlepšit efektivitu řešení následků teroristických útoků (Mareš, 2005; Šín *et al.*, 2017).

1.2 CBRN Terorismus

Pod pojmem CBRN terorismus se rozumí použití toxických chemických látek, toxinů, infekčních materiálů, radionuklidů, případně útoky proti chemickým, petrochemickým, biologickým a jaderným zařízením jednotlivci, nestátními skupinami nebo státem podporovanými aktéry proti konkrétní sociální skupině k vyvolání strachu nebo teroru. Nejvyšší forma CBRN terorismu je založena na použití zbraní hromadného ničení. Vědeckotechnický pokrok a zpřístupnění informací o technologiích přípravy chemických, biologických, radiologických a jaderných látek a materiálů vede k úvahám o zvyšování pravděpodobnosti jejich nevojenského použití a nárůstu jejich psychologického účinku. Problém je však komplikovanější, na základě kvalifikovaného odhadu lze soudit, že nebezpečí představuje i teroristické použití vysoce nebezpečných chemických látek, příp. bojových chemických látek. Na rozdíl od použití jaderných výbušných náloží, jejichž použití je spíše hypotetické. V minulosti bylo již několik chemických útoků ve světě zaznamenáno. Největší dopad měly aktivity japonské náboženské sekty Óm šinrikjó s použitím sarinu, látky VX a kyanovodíku (Šín *et al.*, 2017).

1.3 Kyberterorismus

Kyberprostor je nyní považován za samostatnou doménu konfliktů spolu se zemí, mořem, vzduchem a vesmírem, což je jasně naznačeno ve vojenských doktrínách nejsilnějších národů na světě, tj. v Rusku, Číně a USA (Goel, 2020). Bezpečnostní systémy vlády, armády, korporací, finančních institucí, nemocnic a dalších podniků procvičují bezpečnostní postupy, nástroje k řešení rostoucí úrovně a složitosti kybernetických útoků a ochraně citlivých informací uložených v databázích, sítích a serverech (Awan *et al.*, 2017).

Národní centrum kybernetické bezpečnosti vymezilo pro účely auditu v roce 2016 novou definici kyberterorismu, která zní: „*Kyberterorismus zahrnuje agresivní a excesivní jednání, které je prováděno se záměrem vyvolat strach ve společnosti, a jehož prostřednictvím je dosahováno politických, náboženských nebo ideologických cílů. Za využití kyberprostoru a informačních a komunikačních technologií ohrožuje chod státu, jeho ústavní zřízení nebo obranyschopnost mimo jiné cílením na kritickou informační infrastrukturu a významné informační systémy*“ (Ministerstvo vnitra ČR, 2016b). V české legislativě existuje zákon č. 181/2014 Sb., o kybernetické bezpečnosti, jehož podstatou je bezpečnost kybernetického prostoru a ochrana části kritické infrastruktury, jež je pro správné fungování státu nezbytná a jejíž oslabení by vedlo k ohrožení či porušení zájmu České republiky. Mezi kritickou infrastrukturu zařídíme i zdravotnictví (viz kapitola 1.7 *Ochrana kritické infrastruktury*) (zákon č. 181/2014 Sb.)

Díky hluboké integraci internetu do společenského rámce se stal kyberterorismus účinným nástrojem pro ovlivňování geopolitických konfliktů, včetně zasahování do vnitřních záležitostí jiných národů, podkopávání národní bezpečnosti, destabilizace a útoků na kritickou infrastrukturu. V reakci na tyto hrozby země podporují svoji obranu a zároveň pracují na vývoji kybernetických zbraní a zkoumání kybernetické obrany jiných zemí. Kybernetické útoky již byly použity k doplnění vojenských nebo odvetných zásahů a k zásahům do voleb jiných zemí (Goel, 2020).

Jako příklad útoku můžeme uvést operaci Cleaver, uskutečněnou v Íránu v roce 2012. Vedla významnou globální kampaň pro sledování a infiltraci amerického námořnictva. Úspěšně se vyhnula detekci a využila běžné nástroje k útoku a ohrožení cílů po celém světě. Cíle zahrnovaly armádu, průmysl těžby a zpracování ropy a plynu, energetický průmysl a veřejné služby, dopravu, letecké společnosti, letiště, nemocnice, telekomunikace, technologie, vzdělávání, letecký průmysl, chemické společnosti a vlády. Útok vyústil v krádež citlivých informací nebo převzal kontrolu nad sítěmi kritické infrastruktury v mnoha zemích (Kanada, Čína, Anglie, Francie, Německo, Indie, Izrael, Kuvajt, Mexiko, Pákistán, Katar, Saúdská Arábie, Jižní Korea, Turecko, Spojené arabské emiráty a Spojené státy americké). Dalším důležitým útokem bylo porušení Demokratického národního výboru (DNC) během amerických voleb v roce 2016. Tehdy byl zorganizován útok z Ruska na e-mailové servery DNC a gmailový účet předsedy prezidentské kampaně Hillary Clintonové, Johna Podesta. Nejméně 60 000 e-mailových zpráv bylo odcizeno

a následně zveřejněno ve Wikileaks, což vedlo k rezignacím nejvyšších činitelů a velkým rozpakům pro DNC a kampaň Clintonové (Goel, 2020).

Každý z těchto útoků představuje jasný politický cíl, tj. zasahování do voleb, způsobení ekonomické ztráty během konfliktu, odvetu proti útoku a shromažďování vojenských zpravodajských informací. Z logiky věci vyplývá, že s rozvojem technologií se jimi zprostředkované útoky budou stupňovat. Bylo provedeno několik pokusů o vytvoření smlouvy, která by omezila nárůst kybernetických zbraní, nicméně zvyšování zranitelnosti a eskalace ekonomické rivality mezi národy ztěžuje budování konsensu kolem těchto smluv (Goel, 2020). V tomto kybernetickém věku globální kybernetické zákony neposkytují přijatelné oficiální mechanismy, které by kybernetické boje řídily. K překonání těchto typů trestné činnosti a kybernetických útoků nebo hrozeb je navržen bezpečnostní technický rámec, který je užitečný pro národní databáze, které nabízejí služby přes internet. Bezpečnostní rámec, který byl v souvislosti s kyberterrorismem navržen, skenuje zranitelná místa v průběhu 3 hodin. Navrhovaný bezpečnostní rámec je kompatibilní pouze s operačním systémem Windows a funguje v prohlížeči Mozilla Firefox (Awan *et al.*, 2017).

V Číně je největší online populace na světě. Až 2 miliony zaměstnanců propagandy mají na starosti prestiž a integritu čínské komunistické strany. Podobně jsou na tom Saudská Arábie a Írán, kde vlády cíleně cenzurují informace. Existují důkazy o tom, že některé země, jako například Uganda, používají software vyrobený v Číně ke sledování internetu, zdánlivě k boji proti zločinu. Je to nejen problém východu (Rusko, Čína), ale i Západu (USA), který po zásahu do amerických voleb přistoupil k cenzuře některých dat (Goel, 2020).

Nedávne četné kybernetické útoky na nemocnice, jejichž výsledkem bylo hlavně to, že pachatelé získali neoprávněný přístup k osobním údajům pacientů a zaměstnanců nemocnice nebo lékařů, varovaly zdravotnictví. Kromě krádeže osobních údajů mohou kybernetické útoky ovlivnit také řádné fungování nemocnic. V lednu 2005 útok botnetů zničil počítače v nemocnici Northwest Hospital and Medical Facility v Seattlu ve Washingtonu v USA a mnoha způsoby ovlivnil nemocniční systémy. Dveře na operační sály se neotevřely, pagery lékařů nefungovaly a počítače v jednotce intenzivní péče se vypnuly. Botnet je pojmenování pro softwarové agenty nebo pro internetové roboty, kteří mají automatickou funkci. V současné době je termín nejvíce spojován s malwarem, kdy botnet označuje

sít počítačů infikovaných speciálním softwarem, který je řízen z jednoho centra. Botnet poté vykonává určité činnosti, ke kterým byl naprogramován, např.: rozesílání spamu, blokace přenosu informací atd. (de Cauwer *et al.*, 2017).

1.4 Útoky na zdravotnická zařízení v ČR v souvislosti s terorismem

V ČR se setkáváme jen ojediněle s útoky agresivními pacientem nebo agresivním střelcem. Pokud se tomu tak stane, následky jsou velmi vážné. Nelze podceňovat prevenci, a to včetně potenciálně hrozícího teroristického útoku. V této kapitole budou popsány případy násilných napadení a útoků v nemocnicích v ČR, včetně kyberútoků (ČTK, 2019b).

V září 2005 zaútočil agresivní muž v Nemocnici Tábor a.s. na policisty. Jednomu vzal z opasku služební zbraň a vystřelil. Incident se obešel bez zranění. V lednu 2010 šestatřicetiletý muž, který byl hospitalizovaný na Psychiatrické klinice v Praze na Karlově, usmrtil jiného pacienta. Měl poté nařízenou ochrannou ústavní léčbu. V červnu 2014 střílel pacient ostravské Fakultní nemocnice, který zbraň sebral pracovníkovi ochranky. V září téhož roku vyhrožoval opilý muž se zbraní v ruce v pražské Střešovické nemocnici. V listopadu 2015 psychicky nemocný muž surově napadl sanitáře ve Fakultní nemocnici Olomouc. Útočník poté zemřel na následky použití paralyzéro. V březnu 2019 ve Fakultní nemocnici Královské Vinohrady na hematologické klinice postřelil čtyřiasedmdesátiletý pacient dva další pacienty, jeden z nich následně zraněním podlehl. Střelec po činu odmítl vypovídat, policie ho poslala do vazby a začala trestně stíhat. Koncem dubna pachatel zemřel v pankrácké věznici. V lednu 2020 napadl pacient ve slánské nemocnici personál. Zde zasáhla ochranka a postřelila pacienta do nohy (ČTK, 2019b; Juna a Burýsek, 2019; Lachtinová, 2019; Nový, 2020).

10. prosince 2019 zaútočil pachatel v čekárně na traumatologickém oddělení ve Fakultní nemocnici Ostrava. Střílel z těsné blízkosti do oblasti hlavy. Nemocnice byla okamžitě uzavřena a zaměstnanci nemohli vycházet. Celkem zraněním podlehl 7 obětí, přičemž 2 z těchto obětí byli příslušníci Vězeňské služby a 2 oběti byli zdravotníci. Po několika hodinách byl pachatel nalezen mrtvý. V reakci na tento útok v pražském Institutu klinické a experimentální medicíny testují software, který by mohl odhalit útočníka se zbraní (Batkovský, 2019; Friedmannová, 2021).

S rozvojem informačních technologií jsou v současnosti nebezpečné i kyberteroristické útoky, kterých neustále přibývá. Hackeři si vybírají nemocnice z důvodu předpokladu nižšího zabezpečení. Síť v nemocnici bývá často propojená a snadněji dostupná. Nezřídka chybí zkušenosti IT pracovníci. Pro útok stačí, když zaměstnanec otevře přílohu u emailu. Od roku 2011 se zvýšil počet kyberútoků více než pětinasobně. Skutečné číslo útoků k roku 2022 není známo, z důvodu snahy o utajení napadenými subjekty. V červnu 2018 napadl hacker počítačovou síť v nemocnici v Janově na Rokycansku. Použil taktiku zašifrování dat, za které požadoval výkupné, které však nemocnice odmítla zaplatit a obnovila data ze záloh. Lékaři však neměli několik dní přístup ke kartotéce (Fišer, 2021; Wildová, 2020).

V roce 2019 se odehrálo 6 útoků na nemocnice v ČR. K nejzávažnějšímu došlo v prosinci roku 2019, proti systémům Nemocnice Rudolfa a Stefanie v Benešově, která funguje jako spádová až pro 400 tisíc lidí. Útočníci zašifrovali data na nemocničních serverech, přístrojích i pracovních stanicích a za dešifrování požadovali výkupné. Následky byly velmi vážné. V ambulancích nebylo možné ošetřovat pacienty, plánované operační výkony musely být zrušeny a pacienti, kteří byli hospitalizováni jak na standardních odděleních, tak na jednotkách intenzivní péče (JIP) musely být přeloženi do okolních nemocnic. Provoz v nemocnici se obnovoval téměř měsíc a následky útoku měli nominální škodu cca 50 milionů korun. Celkem se za rok 2020 odehrálo 16 úspěšných kybernetických útoků na nemocnice. Ten nejzávažnější se stal 13. března 2020 ve Fakultní nemocnici Brno. Zde se jedná o mnohem větší komplex pracovišť. Nemocnice musela zrušit operační výkony a přeložit pacienty do jiných nemocnic. Tento útok zasáhl i pracoviště Zdravotnické záchranné služby (ZZS). Nemocnici vznikla škoda za několik milionů korun. 30. března se odehrál v Psychiatrické nemocnici Kosmonosy kyberútok, s jehož následky se nemocnice vyrovnávala téměř měsíc. 17. dubna se hackeři pokusili zaútočit na Ostravskou a Olomouckou nemocnici, také na nemocnice Pardubického kraje a na Karlovarskou krajskou nemocnici. Naštěstí tyto pokusy byly úspěšně odrazeny (Fišer, 2021; Novotná, 2021a).

1.5 Boj proti terorismu

Základní principy boje proti terorismu v podmínkách ČR jsou zpracovány v dokumentu Strategie ČR pro boj proti terorismu od roku 2013 (Ministerstvo vnitra České republiky, 2013). Tento dokument, který vymezuje základní opatření zaměřené na minimalizaci rizik a dopadů potenciálních teroristických útoků na území ČR a proti jejím zájmům

v zahraničí, vychází ze Strategie boje proti terorismu pro léta 2010-2012 (Ministerstvo vnitra České republiky, 2010) a z Bezpečnostní strategie ČR (BS), (Bezpečnostní strategie ČR, 2015) jako střežového strategického dokumentu (Šín *et al.*, 2017).

Strategie ČR pro boj proti terorismu se zaměřuje na pět oblastí:

1. Zlepšení komunikace a spolupráce mezi subjekty zapojenými do boje proti terorismu a zkvalitňování podmínek pro výkon jejich činnosti, v rámci této činnosti byl zřízen Národní kontaktní bod pro terorismus při Útvaru pro odhalování organizovaného zločinu Služby kriminální policie a vyšetřování Policie České republiky.
2. Ochrana obyvatelstva, kritické infrastruktury a jiných cílů potencionálně zranitelných teroristických útokem. V tomto bodě se BS zabývá vymezením kompetencí a koordinační a metodickou úlohou Policie ČR a následky teroristických útoků mimo jiné v oblasti kybernetické bezpečnosti.
3. Bezpečnostní výzkum, vzdělávání a informování veřejnosti ve vztahu ke konkrétním aspektům boje proti terorismu.
4. Prevence radikalizace ve společnosti a boj proti rekrutování do teroristických struktur.
5. Legislativní a mezinárodně smluvní otázky (Ministerstvo vnitra České republiky, 2013; Bezpečnostní strategie ČR, 2015).

Do boje proti terorismu je zapojeno velké množství státních institucí, konkrétně Ministerstvo vnitra se spoluprací ostatních ministerstev, Policie ČR, Armáda ČR, Bezpečnostní informační služba (dále BIS), Úřad pro zahraniční styky a informace, Vojenské zpravodajství, IZS a Národní bezpečnostní úřad. Každá instituce se angažuje jiným způsobem a v jiné fázi. Fáze teroristického útoku jsou: prevence, bezprostřední působení v průběhu útoku a reakce po teroristickém útoku (Filipec, 2017).

Ve fázi prevence teroristického útoku jsou důležité zpravodajské služby, které analyzují a získávají informace o podezřelých. Díky získaným informacím iniciují preventivní opatření a eliminují hrozbu dalších teroristických aktivit. Veřejnost není o aktivitách zpravodajských služeb informována, neboť jsou přísně tajné. Z tohoto důvodu nelze jejich efektivitu zhodnotit. Během útoku zasahují protiteroristické speciální jednotky. V ČR je hlavní organizací připravovanou na boj s terorismem Policie České republiky (PČR) a zejména její Útvar rychlého nasazení (URNA). Další organizací, která napomáhá

při řešení teroristického útoku, je Armáda ČR a její speciální jednotky (Řehák *et al.*, 2008).

1.6 Boj proti terorismu na nadnárodní úrovni

ČR se rovněž angažuje v boji proti terorismu na nadnárodní, evropské úrovni, a to zejména v mezinárodních organizacích: Rada Evropy, Evropská unie (EU), Severoatlantická aliance (NATO), Organizace spojených národů (OSN) a Organizace pro bezpečnost a spolupráci v Evropě (OBSE) (Filipec, 2017).

OSN (logo na obrázku č. 2) se pokouší potírat terorismus již od 30. let 20. století. Po útocích spáchaných 11. 9. 2001 byla přijata rezoluce 1373 (United Nations, 2001), která zavazuje členské státy k tomu, aby obvinily státy nebo jednotlivce podporující terorismus. Zároveň s přijetím této rezoluce byl zřízen Protiteroristický výbor (Counter-Terrorism Committee – CTC) (Řehák *et al.*, 2008).



Obrázek 2. Logo OSN Zdroj: <https://www.un.org/>

V rámci NATO (logo na obrázku č. 3) byl zřízen Zvláštní výbor NATO, který je tvořen kontrarozvědnými službami, jako je například Bezpečnostní informační služba ČR (BIS). Každoročně se také pořádá konference na téma boje proti terorismu (Řehák *et al.*, 2008).



Obrázek 3. Logo NATO Zdroj: https://www.nato.int/nato-welcome/index_cz.html

OBSE (logo na obrázku č. 4) působí aktivně v policejním výcviku a monitorování pohraničního pásma. Svou zkušeností s prevencí konfliktu a krizovým managementem významně podporuje snahu v boji proti terorismu. Rada Evropy se zabývá bojem proti terorismu po útoku na olympiádě v Mnichově v roce 1972. Její odpověď na útoky

11. 9. 2001 byla také okamžitá. Podnikla několik politických kroků a závazků ke zvýšení účinnosti existujících nástrojů boje proti terorismu.

Rada Evropy také pozoruje úroveň protiteroristických opatření členských zemí (Řehák *et al.*, 2008).



Obrázek 4. logo OBSE Zdroj: <https://www.osce.org>

V rámci spolupráce na úrovni EU jsou dále vybrány následující organizace:

Rada Evropské Unie (logo na obr. č. 5), také Rada ministrů, reprezentuje členské státy a její složení se mění dle tématu schůzí. Má také stanovené speciální pracovní skupiny pro boj s terorismem. V roce 2004 byla v souvislosti s teroristickými útoky v Madridu zřízena funkce Protiteroristický koordinátor EU, který se volí na 5 let a momentálně je to Ilkka Salmi (Council of the European Union, 2009; Rada Evropské unie, 2021). Ten má za úkol rozpoznat slabiny jednotlivých států i EU jako celku a navrhuje jejich řešení. V roce 2005 byla vydána Strategie Evropské unie pro boj proti terorismu, která má za cíl představit protiteroristickou politiku. Má čtyři hlavní témata: prevence, ochrana, stíhání a reakce (Presidency and CT Co-ordinator, 2005; Řehák *et al.*, 2008).



Obrázek 5. Rada Evropské Unie Zdroj: <https://www.consilium.europa.eu/en/council-eu/>

Evropská komise (logo na obrázku č. 6) projednává a připravuje mimo jiné legislativní návrhy v oblasti terorismu, které poté zasílá ke schválení Radě EU a Evropskému parlamentu (Řehák *et al.*, 2008).



Obrázek 6. Logo Evropské komise Zdroj: https://ec.europa.eu/info/index_cs

EUROJUST (logo na obrázku č. 7), jinak také Evropské jednotky pro soudní spolupráci EU, je orgán zabezpečující větší efektivitu národních orgánů, které jsou zmocněny k vyšetřování závažných organizovaných trestných činů s mezinárodním přesahem (např. zástupci policie, prokurátoři, soudci či státní zástupci) (EUROJUST, 2021; Řehák et al., 2008).



Obrázek 7. Logo EUROJUST Zdroj: <https://www.eurojust.europa.eu/>

EUROPOL (logo na obrázku č. 8), od roku 2017 působí jako agentura EU v oblasti prosazování práva a jejím cílem je pomoc a vzájemná podpora členských států EU v boji proti závažné mezinárodní organizované trestné činnosti. Její činnost tkví především v pravidelném vyhodnocování hrozeb prostřednictvím obsáhlých analýz trestné činnosti v rámci EU, na kterém spolupracuje rozsáhlá síť analytiků a zástupci národních orgánů činných v trestním řízení (EUROPOL, 2021; Řehák *et al.*, 2008).



Obrázek 8 Logo EUROPOL Zdroj: <https://european-union.europa.eu/>

INTERPOL (logo na obrázku č. 9), neboli Mezinárodní organizace kriminální policie, je největší policejní organizací sdružující 194 států z celého světa. Velkou výhodou je čistě apolitické postavení této organizace, díky němuž dochází k policejní spolupráci i mezi státy, kde diplomatické vztahy příliš nefungují. Jejím úkolem je zabezpečení policejní spolupráce a koordinace vyšetřovacích činností při odhalování a prevenci všech forem závažné zločinné činnosti. Členské země mají při odhalování a pátrání po pachatelích trestných činů možnost přístupu k 17 policejním databázím Interpolu, které shromažďují údaje o trestných činech a zločincích, jejich otisky prstů, seznamy odcizených pasů atd.

Zaměřuje se také na zabezpečení kyberprostoru a na identifikaci hrozeb plynoucích z trestné činnosti mezinárodních zločineckých sítí (INTERPOL, 2021; Řehák *et al.*, 2008).



Obrázek 9 Logo INTERPOL Zdroj: <https://www.interpol.int/>

MONEYVAL (logo na obrázku č. 10), je výbor expertů pro hodnocení opatření proti praní špinavých peněz a financování terorismu je institut založený za účelem jednotného systému napříč členskými státy EU, který sjednocuje způsoby financování terorismu a boje proti praní špinavých peněz. Jedná se o kontrolní mechanismus Rady Evropy a jednoho z přidružených členských uskupení organizace FATF, Finančního akčního výboru, na mezivládní spolupráci, která má podstatný celosvětový vliv na podobu přijímaných standardů a opatření financování terorismu a boje proti praní špinavých peněz (FATF 2021, Moneyval 2021).



Obrázek 10. Logo MONEYVAL Zdroj: <https://www.afa.ad/en/press-room/communicats-de-premsa/moneyval-publishes-the-andorra2019s-second-follow-up-report>

Na globální úrovni ČR rovněž spolupracuje v rámci G20 a Globálního fóra proti terorismu (Filipec, 2017).

1.7 Ochrana kritické infrastruktury zdravotnictví

Podle zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (dále jen „zákon o zdrav. službách“), se zdravotnickým zařízením (ZZ) rozumí prostory určené pro poskytování zdravotních služeb (§ 4 zákona o zdrav. službách). Kritickou infrastrukturou (KI) chápeme, podle z. č. 240/2000 Sb., krizový zákon (dále jen krizový zákon“), „*prvek kritické infrastruktury nebo systém prvků kritické infrastruktury, narušení jehož funkce by mělo značný dopad na bezpečnost státu, zabezpečení základních*

životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu a ochranou kritické infrastruktury opatření, orientovaná na snížení rizika narušení funkce prvku kritické infrastruktury“ (§ 2 krizového zákona).

Zdravotní péče a ochrana veřejného zdraví byla v roce 2004 zařazena mezi vytipované oblasti KI ČR. Ministerstva a jiné ústřední správní úřady pro ochranu kritické infrastruktury spadající do jejich působnosti navrhují odvětvová kritéria a předkládají je Ministerstvu vnitra. Ministerstvo zdravotnictví (MZ) stanovilo odvětvová kritéria v oblasti své působnosti na základě analýzy rizik posuzovaných nezbytných služeb (Kolektiv autorů, 2011).

1.8 Legislativa související s terorismem

V České republice není terorismus obsažený v samostatném právním předpisu, ale je součástí trestního zákoníku, tedy zákona č. 40/2009 Sb., trestní zákoník, dále jen „TZ“. V tomto zákoně se nachází hlava IX., která je označena jako „Trestné činy proti České republice, cizímu státu a mezinárodní organizaci“, díl 1 s názvem „Trestné činy proti základům České republiky, cizího státu a mezinárodní organizace“. V této hlavě se nachází 14 skutkových podstat trestných činů, které ohrožují základy České republiky, cizího státu nebo mezinárodní organizace a jejich bezpečnost příp. obranu. Mezi nimi je i trestný čin „teroristický útok“ (§ 311 TZ), který je řazen mezi zvlášť závažné zločiny. V českém právu má hned dvě základní skutkové podstaty. Podle první se trestného činu teroristického útoku dopustí ten, „*kdo v úmyslu poškodit ústavní zřízení nebo obranyschopnost České republiky, narušit nebo zničit základní politickou, hospodářskou nebo sociální strukturu České republiky nebo mezinárodní organizace, závažným způsobem zastrašit obyvatelstvo nebo protiprávně přinutit vládu nebo jiný orgán veřejné moci nebo mezinárodní organizaci, aby něco konala, opomíjela nebo trpěla...*“ (§ 311 odst. 1 TZ).

Dále jsou pod písm. a) až e) zmíněné různé situace tzv. alternativní skutkové podstaty, např. zničení či poškození veřejného prostranství, dopravního nebo telekomunikačního systému, energetických, vodárenských, zdravotnických a jiných důležitých zařízení, počítačových systémů, jakož i zmocnění se letadla, lodi, jiného prostředku osobní či nákladní dopravy. Je uzákoněno pravidlo, že tyto skutky musí způsobit škodu velkého rozsahu, což je podle § 138 TZ škoda nejméně 10 000 000 Kč. Pro účely této práce je zdůrazněno písm. a), kde se mluví o zničení zdravotnického zařízení nebo poškození ve větší míře. Dále je nutno upozornit na alternativní skutkovou podstatu nacházející se pod

písm. e), kde způsobená škoda musí být značného rozsahu, což je podle § 38 TZ škoda alespoň 500 000 Kč. Dopustí se jí ten, kdo „*vložením dat do počítačového systému nebo na nosič informací anebo vymazáním nebo jiným zničením, poškozením, změněním nebo potlačením dat uložených v počítačovém systému nebo na nosiči informací, snížením jejich kvality nebo učiněním jich neupotřebitelnými provede útok proti počítačovému systému, jehož narušení by mělo závažný dopad na fungování státu, zdraví osob, bezpečnost, hospodářství nebo zajištění základních životních potřeb obyvatel, útok s dopadem na větší počet počítačových systémů s využitím počítačového programu vytvořeného nebo přizpůsobeného pro takový útok anebo útok*“ (§ 311 odst. 1 písm. e) TZ).

Pro upřesnění je zde uvedena i druhá základní skutková podstata, podle které se zvláště závažného zločinu teroristického útoku dopustí ten, „*kdo v úmyslu poškodit ústavní zřízení nebo obranyschopnost České republiky, narušit nebo zničit základní politickou, hospodářskou nebo sociální strukturu České republiky nebo mezinárodní organizace, závažným způsobem zastrašit obyvatelstvo nebo protiprávně přinutit vládu nebo jiný orgán veřejné moci nebo mezinárodní organizaci, aby něco konala, opomínila nebo trpěla, ...*“ (§ 311 odst. 2 TZ). Pod písm. a) až g) jsou opět alternativní skutkové podstaty, které jsou zcela totožné s předcházejícím odstavcem 1. Pod písm. c) se opět nachází zničení zdravotnických zařízení nebo poškození ve větší míře.

Novelou č. 455/2016 Sb., která je nazývána jako „Protiteroristická novela“, došlo k výrazné trestněprávní úpravě terorismu v českém právním řádu. Představovalo to změnu právní úpravy nejen v samotném TZ, ale rovněž i v souvisejících právních předpisech (Jelínek, 2017a). Účelem novely je zefektivnění boje proti terorismu a splnění závazků ČR, které vyplývají z opatření orgánů EU, mezinárodní organizace FATF a výborem Moneyval, což je Výbor expertů pro hodnocení opatření proti praní špinavých peněz a financování terorismu (viz kapitola 1.5 *Boj proti terorismu*).

Touto novelou vznikl nový institut „teroristická skupina“, což je označení pro „*...společnosti nejméně tři trestně odpovědných osob, které má trvalejší charakter, je v něm provedena dělba činností mezi jeho jednotlivé členy, jeho činnost se vyznačuje plánovitostí a koordinovaností a je zaměřená na páčání trestného činu vlastizrady spáchané formou teroristického útoku nebo teroru* (§ 309), *trestného činu teroristického útoku* (§ 311) ...“ (§ 129a TZ). S tím je spojený i vznik nového trestného činu „Účast na teroristické skupině“, kterého se dopustí ten, „*kdo založí teroristickou skupinu nebo kdo se činnosti*

teroristické skupiny účastní“ (§ 312 odst. 1 TZ). Orgány činné v trestním řízení stíhají založení teroristické skupiny, účast na činnosti teroristické skupiny, což může být poskytování služeb, opatření určitých záležitostí, právní poradenství či jiná aktivita podporující činnost teroristické skupiny (Jelínek, 2017b).

Jako na beztrestného může být pohlíženo na toho, kdo „*plní úkoly jako agent podle jiného právního předpisu (dále jen „agent“), který se účastní činnosti teroristické skupiny, není pro trestný čin účasti na teroristické skupině podle § 312a trestný, jestliže se takového činu dopustil s cílem odhalit pachatele trestné činnosti spáchané členy teroristické skupiny, ve spojení s teroristickou skupinou nebo ve prospěch teroristické skupiny anebo jejímu spáchání předejít,*“ (§ 312c odst. 1 TZ) nebo na toho, kdo „*spáchá čin uvedený v § 312a, není trestný, učinil-li o teroristické skupině oznámení státnímu zástupci nebo policejnímu orgánu v době, kdy nebezpečí, které vzniklo zájmu chráněnému tímto zákonem z jiného činu teroristické skupiny, než je uveden v § 312a, mohlo být ještě odstraněno.*“ (§ 312b TZ).

Co se týká financování terorismu, je ukotveno již na mezinárodní úrovni, a to především v Mezinárodní úmluvě o potlačování financování terorismu. V českém TZ byl výše zmíněnou novelou vložen trestný čin Financování terorismu, kterého se dopustí ten, kdo „*sám nebo prostřednictvím jiného finančně nebo materiálně podporuje teroristickou skupinu, jejího člena, teroristu nebo spáchání teroristického trestného činu, trestného činu podpory a propagace terorismu (§ 312e) nebo vyhrožování teroristickým trestným činem (§ 312f) anebo shromažďuje finanční prostředky nebo jiné věci v úmyslu, aby jich bylo takto užito...*“ (§ 312d odst. 1 TZ). Přičemž se může jednat o podporu finanční, ale i materiální.

Dalším novým trestným činem v českém právu je „Podpora a propagace terorismu“, která je obsažena ve třech skutkových podstatách. Tohoto trestného činu se dopustí ten, kdo „*veřejně podněcuje ke spáchání teroristického trestného činu, nebo kdo veřejně schvaluje spáchaný teroristický trestný čin nebo pro něj veřejně vychvaluje jeho pachatele...*“ (§ 312 e TZ odst. 1). Pro trestní odpovědnost nezáleží na formě projevu, způsobu provedení nebo skutečnosti, že k vyvolání zamýšleného rozhodnutí nedošlo (Jelínek, 2017b). Dále se tohoto trestného činu dopustí ten, a) kdo „*ke spáchání teroristického trestného činu nebo trestného činu účasti na teroristické skupině (§ 312a) zjedná jiného,*“ b) „*kdo jinému poskytne informace nebo výcvik týkající se výroby nebo používání výbušnin,*

zbraní, nebezpečných látek anebo jiných obdobných metod nebo technik pro účely spáchání teroristického trestného činu,“ c) „kdo získá informace nebo si osvojí dovednosti týkající se výroby nebo používání výbušnin, zbraní, nebezpečných látek anebo jiných obdobných metod nebo technik za účelem spáchání teroristického trestného činu,“ nebo d) „kdo sám nebo prostřednictvím jiného za spáchání teroristického trestného činu poskytne nebo slíbí odměnu nebo odškodnění jinému nebo pro jiného anebo na takovou odměnu nebo odškodnění pořádá sbírku.“ (§ 312e odst. 2 TZ).

Třetí základní skutkovou podstatu naplní ten a) *„kdo cestuje do jiného státu nebo do České republiky za účelem spáchání teroristického trestného činu, trestného činu účasti na teroristické skupině (§ 312a), vyhrožování teroristickým trestným činem (§ 312f) nebo trestného činu uvedeného v odstavci 2 písm. b) nebo c), nebo b) „kdo pro jiného takové cestování organizuje, jiného k němu navádí anebo jinému umožní nebo usnadní takto cestovat.“ (§312e odst. 3 TZ)* Tato úprava je reakcí na problém mezinárodního terorismu v rámci tzv. Schengenského prostoru, resp. volného pohybu osob. Zahraniční následovníci radikálního extrémismu jsou připraveni za ozbrojenými konflikty do zahraničí cestovat. Označují se jako „zahraniční bojovníci“ („foreign terrorist fighters“). Veřejného podněcování ke spáchání teroristického trestného činu nebo poskytnutí informací, výcviku či zbraní se lze dopustit i filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí (Jelínek, 2017b).

Posledním trestným činem, který je nutné zmínit, je „Vyhrožování teroristickým trestným činem“ (§ 312f TZ). Vyhrožováním se míní hrozba jakýmkoli teroristickým trestným činem. Přičemž nezáleží na tom, zda jsou takové výhrůžky myšleny vážně, či nikoli.

Další důležitý zákon, který s terorismem souvisí, je zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, dále jen „zákon č. 253/2008 Sb.“ *„Tento zákon upravuje některá opatření proti legalizaci výnosů z trestné činnosti a financování terorismu, některá práva a povinnosti fyzických a právnických osob při uplatňování opatření proti legalizaci výnosů z trestné činnosti a financování terorismu, a to za účelem zabránění zneužívání finančního systému k legalizaci výnosů z trestné činnosti a k financování terorismu a vytvoření podmínek pro odhalování takového jednání“ (§1 zákona č. 253/2008 Sb.).*

Dalším zákonem je zákon č. 153/1994 Sb., o zpravodajských službách ČR. Bezpečnostní informační služba (BIS) *„zabezpečuje informace týkající se organizovaného zločinu*

a terorismu“ (§ 5 odst. 1 písm. e). Vláda závazně určila BIS „jako ústřední zpravodajskou službu odpovědnou za zpracování veškerých analytických a operativních informací týkajících se bezpečnosti ČR, především pak v souvislosti s bojem proti terorismu“ (Usnesení vlády č. 1060/2006). BIS se zaměřuje též na nábor či získávání peněžní či jiné logistické podpory terorismu a šíření radikálních interpretací ideologií či náboženství podporujících teroristickou činnost (BIS, 2021) .

2 Cíle práce a výzkumná otázka

V této kapitole bude formulován problém, který je důvodem k provedení výzkumu. Dále budou uvedeny cíle práce, související s ochranou zdravotnických zařízení před terorismem a zformulovány výzkumné otázky, podle kterých bude vytvořen dotazník pomocí kterého bude proveden výzkum.

2.1 Formulace problému

Zabezpečení měkkých cílů proti terorismu je velmi složitý proces, který komplikuje řada faktorů, např. nedostatečná dokumentace, nedostatek financí, nejistota hrozby. Jistou roli zastupuje i absence dat o zabezpečení jednotlivých nemocnic a jejich ohrožení terorismem. Komplikací je též neznalost nadřízených, jak instruovat své podřízené při probíhajícím teroristickém útoku na měkké cíle. V případě útoku je neznalost instrukcí značný problém. Česká republika v rámci EU řeší tento problém jiným způsobem, než je řešen např. v arabských zemích. To, jak je tento problém řešen v ostatních státech mimo EU, je také otázka, která souvisí s cílem práce.

2.2 Cíle práce

- 1) Analýza zabezpečení vybraných zdravotnických zařízení a jejich zkušeností s teroristickými a kyberteroristickými útoky.
- 2) Analýza rozdílů v ohrožení a zabezpečení zdravotnických zařízení v České republice a vybraných zahraničních státech.

2.3 Výzkumné otázky

- 1) Je zabezpečen vstup do zdravotnického zařízení?
- 2) Jaké jsou zkušenosti zdravotnického zařízení s teroristickými nebo kyberteroristickými útoky?
- 3) Zúčastnili se zaměstnanci zdravotnického zařízení školení na nácvik reakce na teroristický útok?

3 Operacionalizace pojmů použitých v cíli práce

Zdravotnické zařízení – podle zákona o zdravotních službách a podmínkách jejich poskytování č. 372/2001 Sb. se Zdravotnickým zařízením (ZZ) rozumí prostory určené pro poskytování zdravotních služeb (§4 z. č. 372/2001 Sb. O zdravotních službách a podmínkách jejich poskytování).

Teroristický útok – plánované, promyšlené a politicky motivované násilí, zaměřené proti nezúčastněným osobám, sloužící k dosažení vytyčených cílů (Ministerstvo vnitra ČR, 2016a).

Kyberteroristický útok – „*Kyberterorismus zahrnuje agresivní a excesivní jednání, které je prováděno se záměrem vyvolat strach ve společnosti, a jehož prostřednictvím je dosaženo politických, náboženských nebo ideologických cílů. Za využití kyberprostoru a informačních a komunikačních technologií ohrožuje chod státu, jeho ústavní zřízení nebo obranyschopnost mimo jiné cílením na kritickou informační infrastrukturu a významné informační systémy*“ (Ministerstvo vnitra České republiky, 2016b).

Měkké cíle – místa, objekty, prostory nebo akce s vysokou koncentrací osob a nízkou úrovní zabezpečení proti násilným útokům (Ministerstvo vnitra ČR, 2021).

4 Metodika

Diplomová práce je tvořena teoretickou a praktickou částí. Teoretická část diplomové práce je zpracována pomocí odborné rešerše, analýzy právních norem České republiky a odborných článků dané problematiky. Analýzou těchto zdrojů a jejich následnou syntézou byly získány informace použité v této diplomové práci. Problematika ochrany zdravotnických zařízení byla přiblížena a charakterizována prostřednictvím využití stávající literatury používané v oblasti krizové připravenosti zdravotnictví. Kvůli nedostatku zdrojů na téma ochrany zdravotnických zařízení proti terorismu bylo nakonec přistoupeno k odbornému přiblížení a podrobnější charakteristice pojmu terorismus, a to prostřednictvím využití odborných pojmů a termínů používaných v oblasti ochrany obyvatelstva.

Pro potvrzení či vyvrácení stanovených cílů a předpokladů byla zvolena metoda výzkumu v podobě dotazníků, kterých se účastnili respondenti z řad zaměstnanců nemocnic v ČR a jako doplňující byla zvolena kvalitativní metoda výzkumu v podobě polostrukturovaných rozhovorů, kterých se zúčastnili respondenti, kteří byli na stáži/misi v zemích Afriky, Asie a Evropy.

Praktická část diplomové práce obsahuje dotazníkové šetření, respondenti byli osloveni anonymně z řad zaměstnanců nemocnic v České republice. Z důvodu zaručení anonymizace nemocnic nebudou uvedeny jejich názvy. Dotazník bude vyhodnocen pomocí přehledných grafů. Hlavním východiskem k zodpovězení výzkumných otázek byl právě tento dotazník. Další výzkum bude proveden pomocí 10 polostrukturovaných rozhovorů se zaměstnanci zdravotnických zařízení, kteří absolvovali odbornou stáž v zahraničí ve státech Afriky, Asie a východní Evropy. Rozhovory budou přepsány, porovnány, analyzovány a dále graficky znázorněny.

Hlavním východiskem k zodpovězení výzkumných otázek „*Je zabezpečen vstup do zdravotnického zařízení?*“, „*Jaké jsou zkušenosti zdravotnického zařízení s teroristickými nebo kyberteroristickými útoky?*“, „*Zúčastnili se zaměstnanci zdravotnického zařízení školení na nácvik reakce na teroristický útok?*“ bylo dotazníkové šetření.

Hlavním východiskem k zodpovězení výzkumných otázek, „*Jaké jsou zkušenosti zdravotnického zařízení s teroristickými nebo kyberteroristickými útoky?*“, „*Zúčastnili se zaměstnanci zdravotnického zařízení školení na nácvik reakce na teroristický útok?*“ týkajících se zahraničí a porovnání s ČR bylo šetření formou polostrukturovaného rozhovoru.

Výzkumný soubor pro potřeby této práce se skládá ze zaměstnanců nemocnic v České republice, respondenti byli osloveni anonymně přes internet, byl odeslán dotazník do osmnácti nemocnic. Zamítavá odpověď přišla ze čtyř nemocnic. Další oslovené nemocnice ponechaly dotaz bez odpovědi.

Před zahájením rozdání dotazníků respondentům byl s ohledem na určené cíle práce vytvořena nejprve osnova otázek a zkušební dotazník. Ten byl předložen 10 respondentům ke zkušebnímu vyplnění. Poté byl vytvořen dotazník pomocí otázek a několika možností odpovědí.

V dotazníkovém šetření bylo osloveno 742 respondentů a 321 respondentů dotazník vyplnilo. Úspěšnost vyplnění je 43,3 %. Respondenti byli oslovováni z řad zaměstnanců nemocnic v České republice anonymně. Po nasbírání dostatečného počtu responzí (321) byly dotazníky vyříděny dle správnosti odpovědí. Bylo vyřazeno 121 dotazníků pro nedostatečná data, nepřesné odpovědi nebo špatně zvolené odpovědi (např. pokud se respondenti nesetkali s teroristickým útokem a pokračovali na upřesňující otázky). 200 responzí odpovídalo filtru a byly zpracovány do grafů. Tato metoda výzkumu byla zvolena z důvodu získání velkého množství odpovědí pro potřeby zjištění názoru většiny respondentů.

V polostrukturovaných rozhovorech byly dále dopodrobna rozebrány otázky týkající se cíle práce analyzovat rozdíly v ohrožení a zabezpečení zdravotnických zařízení v České republice a vybraných zahraničních státech.

Výzkumný soubor byl utvořen původně z 12, poté z 10 respondentů. Z důvodu neúplnosti informací a krátké zkušenosti respondentů s praxí v určité oblasti byly dva rozhovory vyřazeny. Těchto 10 vybraných respondentů muselo splňovat kritérium orientace a znalosti tématiky. 3 respondenti byli vybráni z důvodu vojenské mise. Jedna z těchto misí byla podniknuta v době bojového klidu (Pákistán).

Před zahájením rozhovorů byly s ohledem na cíl práce a výzkumné otázky vytvořeny osnovy polostrukturovaného rozhovoru podle vytvořených dotazníků. Byly provedeny zkušební rozhovory, které pomáhaly seskupit lépe osnovu otázek. Cílem otázek bylo, aby se prolínaly a podobaly s otázkám, položeným v dotazníkovém šetření. Se zpracováním rozhovoru a jeho použitím každý dotazovaný souhlasil.

Rozhovory byly provedeny pomocí osobního kontaktu s respondenty. Celkem se pokládalo třináct otázek, z nichž byly tři úvodní. Úvodní otázky zjišťují pracovní zařazení osob a délku a místo jejich působení v zahraničí. Hlavní otázky se týkají výzkumných otázek a jsou uvedeny níže. Ze získaných dat dle jednotlivých otázek bylo pomocí programu Inkscape utvořeno grafické znázornění odpovědí. Podrobné a zajímavé části rozhovorů jsou doplněny k myšlenkové mapě.

Tato metoda doplňujícího výzkumu byla zvolena z důvodu potřeby hlubšího pochopení souvislostí spojených s výzkumnými otázkami, možnosti položení doplňujících otázek k problematice a vyslechnutí osobního zážitku a názoru respondenta na tuto problematiku.

5 Výsledky

Výzkum byl proveden pomocí dotazníkového šetření a polostrukturovaných rozhovorů. Z důvodu pochopení struktury, zabezpečení a zalidnění předpokládaných zkoumaných subjektů (okresní, krajské a fakultní nemocnice) zde bude podrobněji popsáno současné zabezpečení nemocnic v ČR z pohledu a zkušeností autorky.

5.1 *Současné zabezpečení a struktura nemocnic*

Okresní typy nemocnic v České republice jsou koncipovány do komplexů budov. Zpravidla jsou oploceny a mají k dispozici služební vchody, které jdou otevřít pomocí čipu, karty či klíče, které má k dispozici jen zaměstnanec. Mimo těchto vchodů je k dispozici i hlavní vchod pro pacienty či jejich návštěvy, který je otevřen veřejnosti v určitých časových úsecích. Tento vchod je zpravidla monitorován kamerami nebo hlídán ostrahou. Ta hlídá ve většině případů hlavní vjezdy a výjezdy pro vozidla a sanitní vozy. Na parkovištích a u hlavních vjezdů jsou pak nainstalovány kamerové systémy. Některé nemocnice mají konstrukčně oddělené prádelny, kotelny a další technické budovy, ale tato struktura někde není z kompozičních důvodů možná. Krajské a fakultní nemocnice jsou mnohdy velmi komplikovaný a rozlehlý komplex budov s více než jedním vstupním terminálem a vchodem pro veřejnost. Kamerové systémy zde mají svou nezastupitelnou roli, stejně jako ochranka. Oblastní nebo městské nemocnice se skládají většinou jen z jedné nebo dvou budov. Z logiky věci vyplývá, že do prostor nemocnice je možno se dostat poměrně snadno. Problematickým aspektem je kontrola příchozích, z důvodu frekventovaného pohybu osob. Především jakkoliv držené zbraně, nepodléhají kontrole, jsou těžko zjištělné a lze je snadno zamaskovat. Pro účely této práce bude znázorněna modelové nemocnice.

Okresní nemocnice se skládá z mnoha oddělení. Po příchodu do nemocnice bývá jako první zpravidla strukturovaný centrální příjem nebo odborné ambulance – chirurgie a ortopedie, spolu s lůžkovými standardními odděleními a většinou zde má zastoupení i několik lůžek jednotky intenzivní péče (JIP). V současné době některé okresní nemocnice, pokud již není v provozu, dostavují urgentní příjem, který slouží k příjmu a selektování pacientů. V rámci chirurgické kliniky zde doplňuje specializaci otorhinolaryngologické (ušní, nosní, krční) (ORL) oddělení, rehabilitační oddělení s lůžky, kam se přeloží pacienti po operacích s potřebou rehabilitace, anesteziologicko-resuscitační oddělení (ARO) s ambulantní a lůžkovou částí, Interna s ambulancí, dialyzační nelůžkové oddělení, JIP

a v rámci JIP i kardiologické specializované oddělení. V rámci interní části je přítomna i gastroenterologická ambulance. Dále se zde nacházejí operační sály, počet záleží na velikosti nemocnice a umístění. V tomto případě hovoříme o 5 operačních sálech a 1 porodním sále. Dalšími odděleními jsou gynekologie, lůžková část s JIP a porodnice s porodním sálem a několika lůžky, dětské oddělení a novorozenecké oddělení s lůžky pro nedonošené novorozence, infekční oddělení se standardními lůžky, neurologické oddělení s JIP, oddělení následné péče s JIP, Sociální lůžka, urologické oddělení – standardní lůžka, plicní, onkologická a oční ambulance, laboratoře a radiodiagnostika, oddělení patologie, lékárna a oddělení spirituální péče. U některých okresních, krajských i městských nemocnic je přidružena stanice zdravotnické záchranné služby. Provoz nemocnice zajišťuje také jídelna, prádelna, technické a IT oddělení, budova ředitelství a sekretariát. Tato modelová nemocnice má k dispozici přibližně 400 lůžek pro pacienty a je zde zaměstnáno přibližně 750 osob. K tomuto číslu je nutno připočítat také ambulantní pacienty, návštěvy a rodiče, kteří mohou pobývat v nemocnici se svými dětmi.

V případě fakultních nemocnic se jedná i o dva a více komplexů budov a jedná se o velmi rozlehlý areál. V některých případech jsou budovy rozmístěny na více místech ve městě – nejsou tedy propojeny. Ve fakultních nemocnicích jsou komplexy rozšířeny o více specializovaných klinik např. dermatovenerologická klinika, gastroenterologická klinika, psychiatrická klinika, onkologická klinika, imunologie a alergologie, oční klinika, stomatologie, plastická chirurgie, pracovní lékařství, traumatologie, metabolická jednotka a řada dalších klinik. Lůžkové oddělení a JIP mají vyšší počet lůžek než okresní nemocnice. Mimo těchto oddělení je zde přidruženo emergency jako vysoko prahový urgentní příjem (příjem pro pacienty ve vážném stavu). Kromě emergency jsou zde specializační centra jako kardiocentrum a neurologické centrum (iktové centrum) zaměřené na příjem pacientů s mozkovou mrtvicí (iktem). Tato centra pro příjem velkého počtu pacientů jsou mnohdy snadno přístupná.

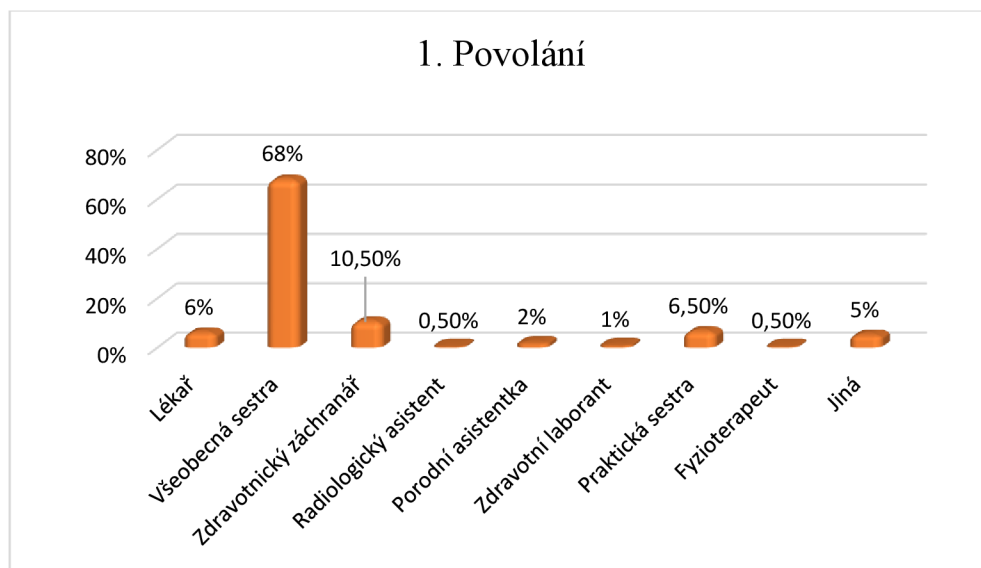
Fakultní nemocnice jsou zpravidla velmi dobře zabezpečeny pomocí kamerových zařízení. Ochrana zde také zajišťuje bezpečí, což je však vzhledem k rozloze nemocnic velmi náročné. U každé velké organizace je najata bezpečnostní agentura, která zajišťuje fyzickou ostrahu objektu, a to hlavně formou obchůzkové služby. Je zde mnohem vyšší koncentrace osob než v nemocnici okresního typu. Co se týče zaměstnanců, je jich v této modelové nemocnici fakultního typu přibližně 5 000. Počet lůžek je přibližně 1750.

K tomuto číslu je nutné ještě připočíst ambulantní pacienty, často s doprovodem, návštěvy a studenty.

Předpokládejme, že pokud by terorista uvažoval o útoku na nemocnici, navštívil by ji jako běžný občan. Svůj útok bude pravděpodobně plánovat a do areálu pronikne z důvodu potřeby lékařského ošetření nebo ze záminky návštěvy. V době moderních technologií a rozvinuté IT technologie se lze dobře připravit. Prakticky každá nemocnice má na svých internetových stránkách zveřejněnou mapu areálu s popisem oddělení, kterou si může útočník v pohodlí domova prostudovat. Tato mapa se zpravidla nachází v každém areálu nemocnice, aby usnadnila návštěvníkům orientaci. Do areálu nemocnice je přístup jednoduchý. Na některá oddělení se cizí osoba nemůže dostat snadno, neboť je zabezpečeno vchodem s čipovým systémem. K čipu mají přístup pouze zaměstnanci konkrétního oddělení. Pro cizí osoby je potřeba zazvonit, identifikovat se a sdělit důvod příchodu na oddělení. Ne vždy je však tato identifikace nutná, některá oddělení otevírají všem bez nutnosti informací. Nejvíce pacientů však najdeme v čekárnách před ambulancemi, kde je přístup neomezený. Bohužel tyto prostory byly již několikrát prostředím, ve kterém se odehrál útok na měkké cíle.

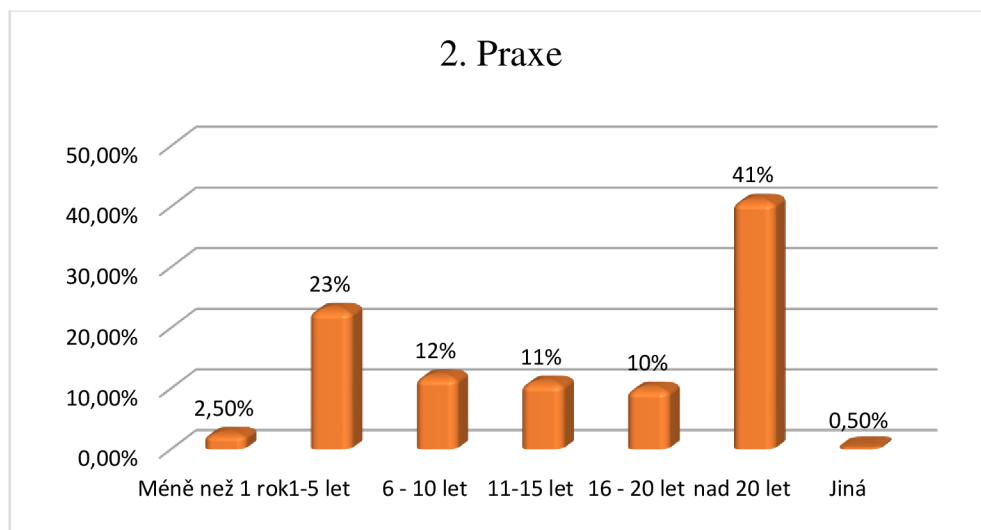
5.2 Výsledky dotazníků

Sběr odpovědí k dotazníkům probíhal od září 2021 do března 2022. Celkem bylo rozdáno 421 dotazníků, z toho bylo vyplněno 321 a následně bylo 121 odpovědí vyřazeno pro neumožnost hodnocení z důvodu neoznačení nebo špatných označení odpovědí. Výsledný výzkumný vzorek je 200 respondentů. První dvě otázky jsou úvodní a zjišťují povolání a délku praxí respondentů. Předpokladem bylo, že nejčastěji budou dotazník vyplňovat všeobecné sestry s délkou praxe více než 20 let.



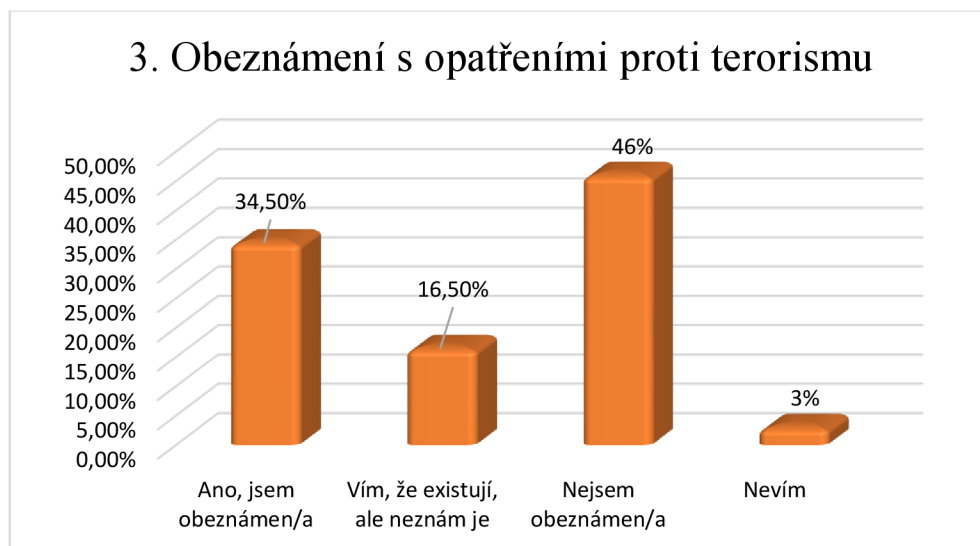
Obrázek 11. Povolání respondentů Zdroj: Vlastní

První otázka zní: „*Na jaké pozici pracujete?*“ Nejvíce odpovědí dle grafu na obrázku č. 11 zastává pozice „*Všeobecná sestra*“, a to 68 % (135). Druhé největší zastoupení má pozice „*Zdravotnický záchranář*“ s 10,5 % (21) responzemi. „*Praktická sestra*“ je zastoupena 6,5 % (13) respondentů. O jednu odpověď méně má pozice „*Lékař*“. Jako „*Jiná*“ s 10 responzemi (5,5 %) byly označené pozice pečovatelka, ergoterapeut, dětská sestra, zubní lékař, referent, dentální hygienistka, 2× sanitář a 2× administrativní pracovník (10 odpovědí). „*Porodní asistentka*“ zde má zastoupení 4 (2 %) hlasů. O polovinu méně, tj. 2 hlasy (1 %) má pozice „*Zdravotní laborant*“. Stejný a nejmenší počet responzí má pozice „*Radiologický asistent*“ a „*Fyzioterapeut*“, a to 1 responzi (0,5 %).



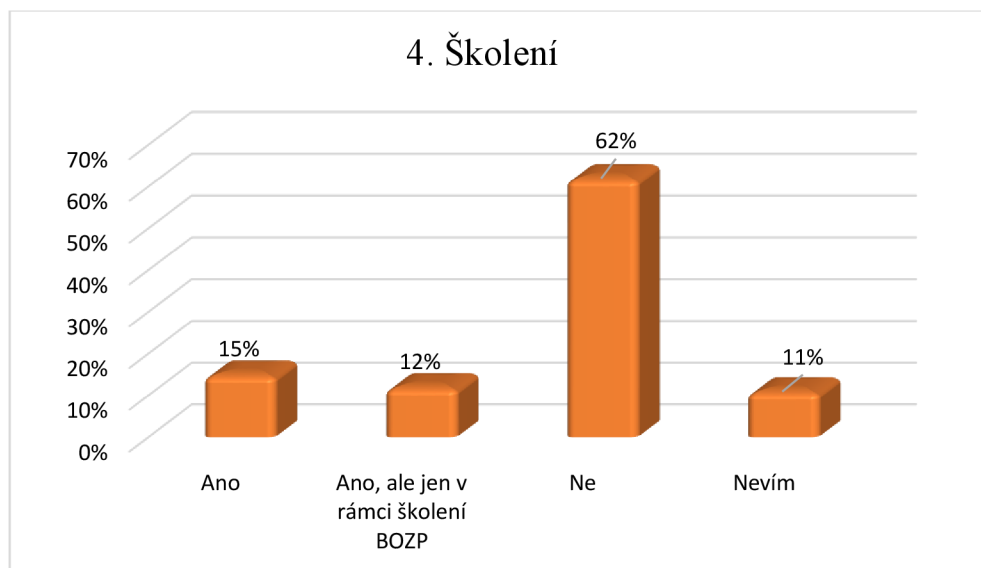
Obrázek 12. Délka praxe respondentů Zdroj: *Vlastní*

Otázka č. 2 zní: „*Jak dlouhá je Vaše praxe ve zdravotnictví?*“ Z grafu na obrázku č. 12 vyplývá, že největší zastoupení respondentů (41 % neboli 82 respondentů) je s délkou praxe nad 20 let. 23 % (46 respondentů) zvolilo odpověď „1–5 let“. Odpověď „6–10 let“ zvolilo 12 % (24) respondentů. O něco méně respondentů zvolilo odpověď „11–15 let“, a to 11 % (22) respondentů. Odpověď „16–20 let“ zvolilo 20 respondentů (10 %). Nejkratší praxi, tedy méně než 1 rok, vybralo 5 respondentů (2,5 %). Mezi odpovědi „*Jiná*“ (0,5 % neboli 1 responze) patří 0 let, která je přiřazena k pozici administrativního pracovníka.



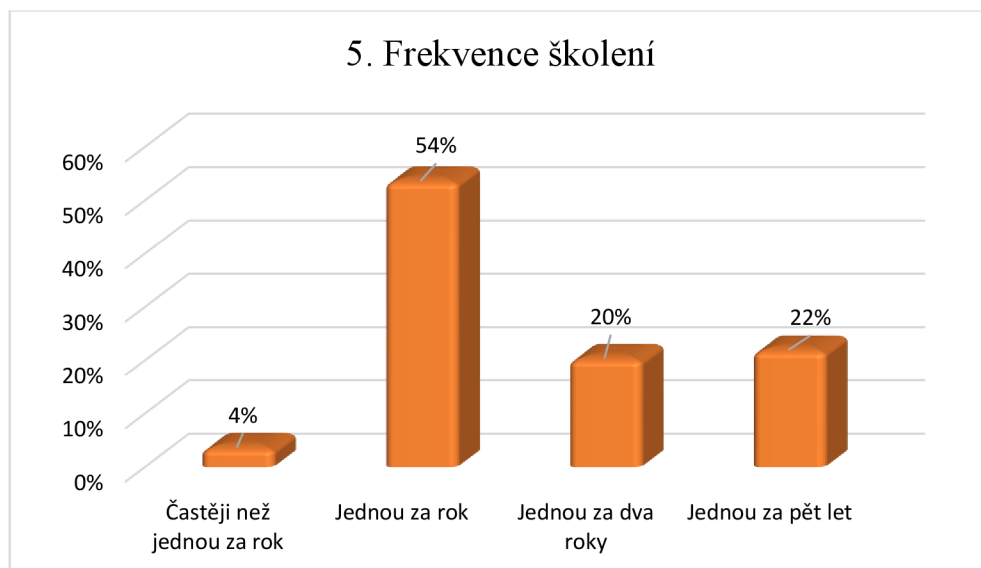
Obrázek 13. Obeznamení s opatřeními proti terorismu Zdroj: Vlastní

Otázka č. 3 zní: „*Jste obeznámen/a s opatřeními proti terorismu od Vašeho zaměstnavatele?*“ Z grafu na obrázku č. 13 vyplývá, že většina respondentů, tedy 92 (46 %), není obeznámena s opatřeními proti terorismu. S odpovědí „*Ano, jsem obeznámen/a*“ však již není tak velký rozdíl (11,5 %), jelikož ji zvolilo 34,5 % (69) respondentů. Odpověď „*Vím, že existují, ale neznám je*“ čítá 16,5 % (33) responzí. Nejméně responzí má odpověď „*Nevím*“, a to 3 % (6) respondentů.



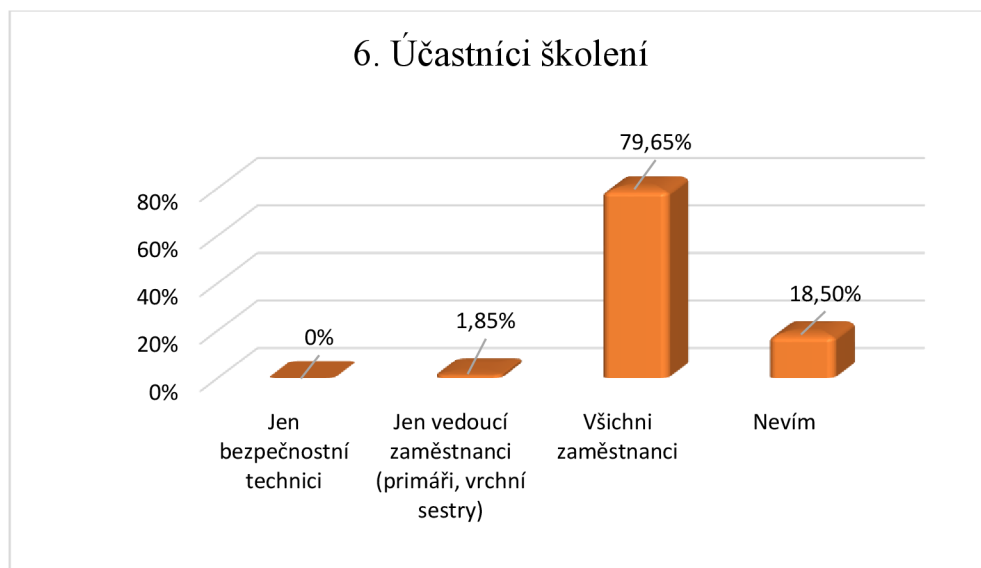
Obrázek 14. Školení Zdroj: *Vlastní*

Z grafu na obrázku č. 14, týkající se otázky č. 4: „*Probíhá na Vašem pracovišti školení na nácvik reakce na teroristický útok?*“ lze určit, že na většině pracovišť školení neprobíhá a to v 62 %, tj. 124 odpovědí. V 15 %, tj. 30 odpovědí školení probíhá a ve 12 %, tj. 24 odpovědí probíhá v rámci školení BOZP. Těchto 27 % (54 respondentů) pokračovalo na další otázky týkající se podrobností o tomto školení. Odpověď „*Nevím*“ zvolilo 11 % tj. 22 respondentů.



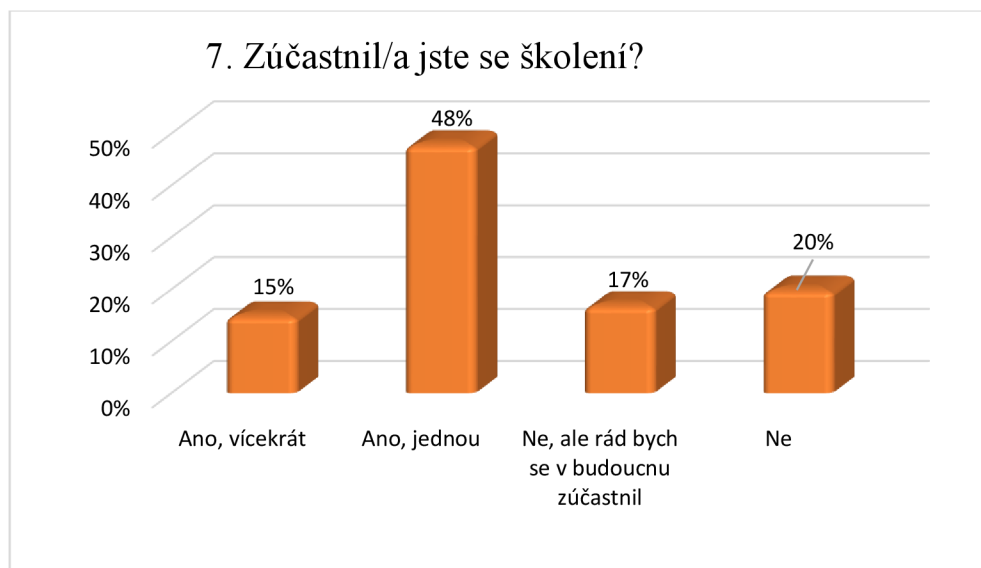
Obrázek 15. Frekvence školení Zdroj: *Vlastní*

Otázka č. 5 zní: „*Jak často probíhá školení na nácvik reakce na teroristický útok?*“ Nejvíce respondentů, a to 54 % (29) dle grafu na obrázku č. 15 odpovědělo, že školení je pořádáno 1× do roka. Odpověď „*Jednou za pět let*“ zvolilo 22 % (12) respondentů. O 2 % méně, tedy 20 % (11) respondentů, zvolilo odpověď „*Jednou za dva roky*“. Podle 2 respondentů (4 %), probíhá školení častěji než jednou za rok.



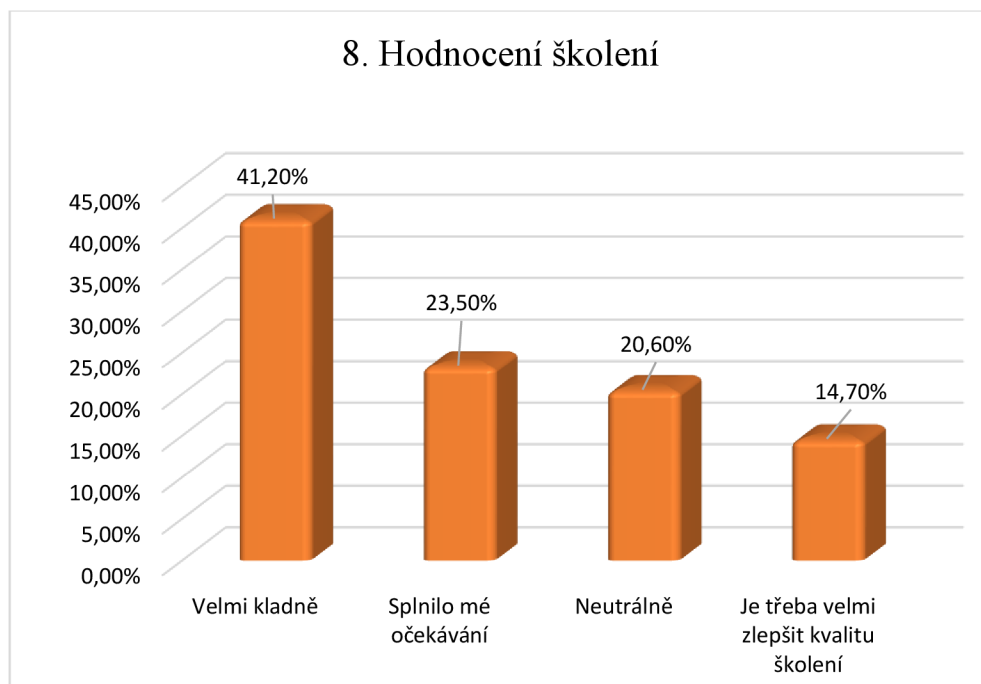
Obrázek 16. Účastníci školení Zdroj: *Vlastní*

Otázka č. 6 zní: „Kdo se může tohoto školení účastnit?“ Na obrázku č. 16 pozorujeme, že většina respondentů, 79,65 % (43 respondentů) zvolila možnost „Všichni zaměstnanci“. Možnost „Nevím“ zvolilo 18,5 % (10 respondentů). Jen 1,85 % (1 respondent) zvolil možnost „Vedoucí zaměstnanci“ Další možnost, a to „Jen bezpečnostní technici“ zůstala bez odpovědí.



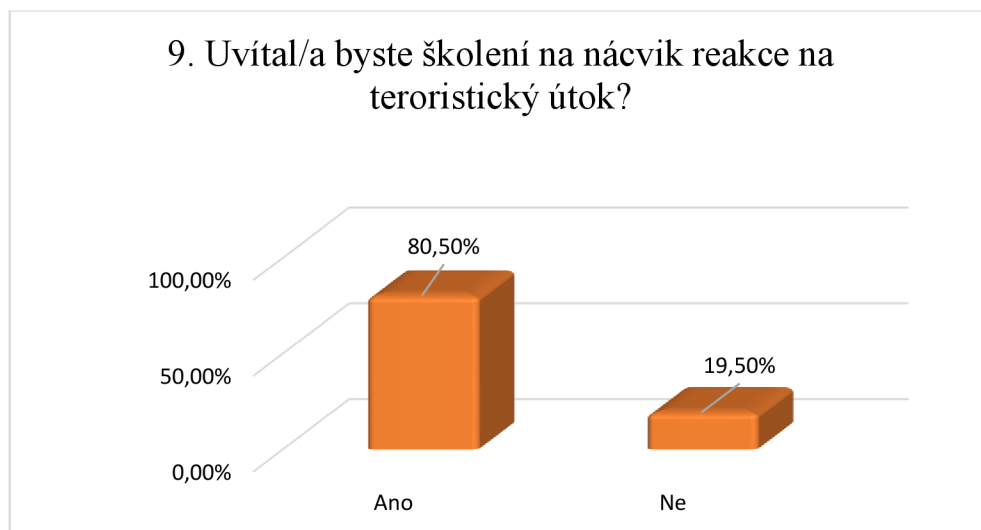
Obrázek 17. Účast na školení Zdroj: *Vlastní*

Otázka č. 7 zní: „Zúčastnili jste se školení na nácvik reakce na teroristický útok?“ Z grafu na obrázku č. 17 vyplývá, že nejvíce respondentů se školení zúčastnilo jen jednou, a to 48 % (26). Vícekrát se zúčastnilo 15 % (8 respondentů). Těchto 63 % (34) respondentů pokračovalo na další otázku. Zbýlých 17 % (9 respondentů) by se rádo zúčastnilo v budoucnosti a 20 % (11 respondentů) se neúčastnilo školení.



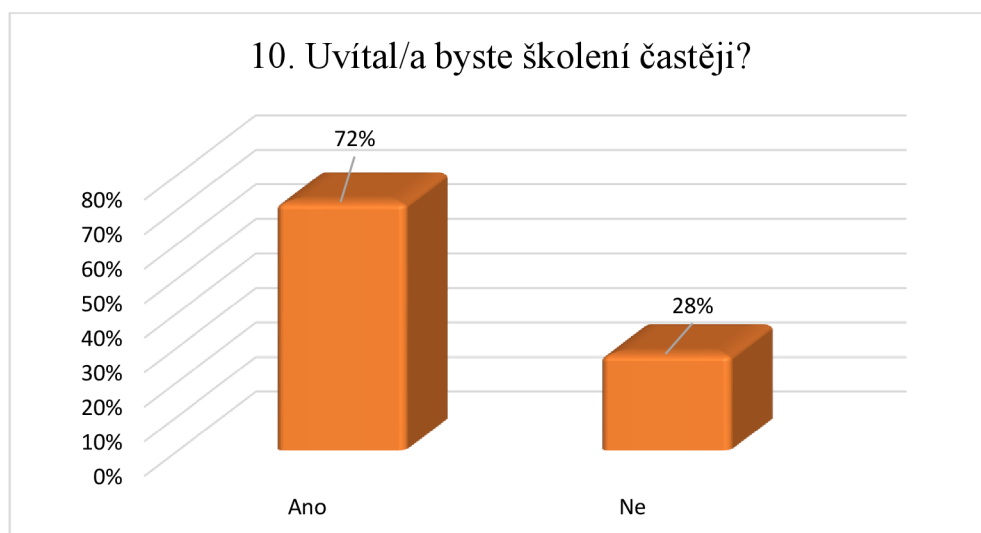
Obrázek 18. Hodnocení školení Zdroj: *Vlastní*

Otázka č. 8 zní: „*Jak školení na nácvik reakce na teroristický útok hodnotíte?*“ Vzhledem k tomu, že velká část respondentů v předchozí otázce uvedla, že se školení účastnila, navazující otázka zkoumala hodnocení školení. Odpovídali jen ti, co se zúčastnili. To ovšem zužuje počet respondentů z 54 na 34. Z grafu na obrázku č. 18 vyplývá, že nejvíce respondentů, tj. 41,2 % (14), hodnotí školení velmi kladně. Podle 8 respondentů (23,5 %) školení splnilo jejich očekávání. Neutrálně hodnotí školení 20,6 % (7) respondentů. Podle 14,7 % (5) respondentů, je třeba velmi zlepšit kvalitu školení.



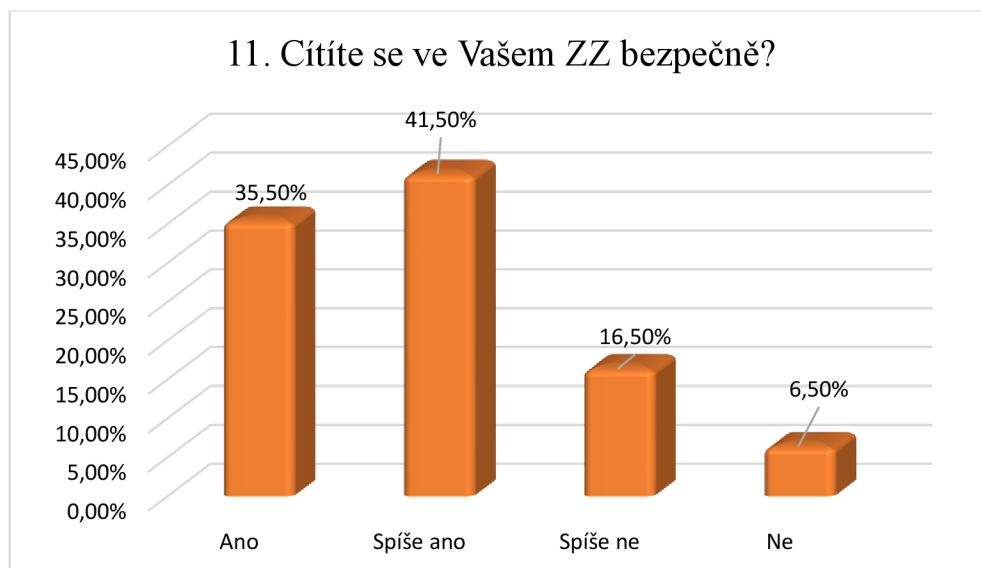
Obrázek 19. Uvítal/a byste školení na nácvik reakce na teroristický útok? Zdroj: Vlastní

Otázka č. 9 zní: „Uvítal/a byste školení na nácvik reakce na teroristický útok?“ Zde opět odpovídalo všech 200 respondentů, přičemž z grafu na obrázku č. 19 vyplývá, že většina respondentů (80,5 %), tj. 161 respondentů by školení uvítala. Zbylých 19,5 % tj. 39 respondentů by školení neuvítala.



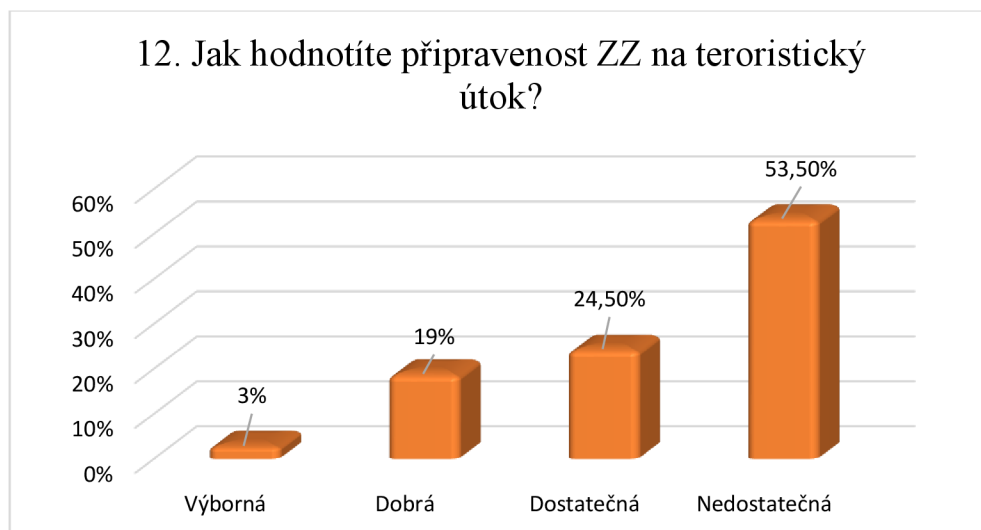
Obrázek 20. Častější pořádání školení Zdroj: Vlastní

Otázka č. 10 zní: „V případě, že byste školení uvítal/a, nebo jste se zúčastnil/a, bylo by vhodné pořádat jej častěji?“ Zde se vzorek respondentů opět třídil a to na 161 z předchozí otázky, kteří by školení uvítali nebo se školení účastnili. Graf na obrázku č. 20 ukazuje, že z těchto 161 respondentů by 72 % tj. 116 respondentů uvítala školení častěji a 28 %, tj. 45 respondentů by jej uvítala méně často.



Obrázek 21. Pocit bezpečí Zdroj: *Vlastní*

Na otázku č. 11-14 již odpovídal plný počet respondentů. Ta zní: „*Cítíte se ve Vašem zařízení bezpečně?*“ Z grafu na obrázku č. 21 vyplývá, že většina z nich, tj. 41,5 % (83) se odpověděli „*Spíše ano*“. Druhou nejvyšší hodnotu získala odpověď „*Ano*“ a to 35,5 % (71 hlasů). Zbýlých 16,5 % (33) respondentů se spíše necítí bezpečně a 6,5 % (13 respondentů) se necítí bezpečně.



Obrázek 22. Připravenost na teroristický útok Zdroj: *Vlastní*

Otázka č. 12 zní: „*Jak hodnotíte připravenost zdravotnického zařízení na případný teroristický útok?*“ Z grafu na obrázku č. 22 vyplývá, že 53,5 %, tj. 107 respondentů uvedlo, že dle jejich názoru je ZZ nedostatečně připraveno na teroristický útok. Dostatečně je ZZ připraveno podle 24,5 %, tj. 49 respondentů. Jako dobrou připravenost hodnotí v dotazníku 38 respondentů (19 %). A nejmenší zastoupení zde má odpověď „*Výborná*“, a to jen 6 osob z celkových 200 respondentů, tj. 3 %.

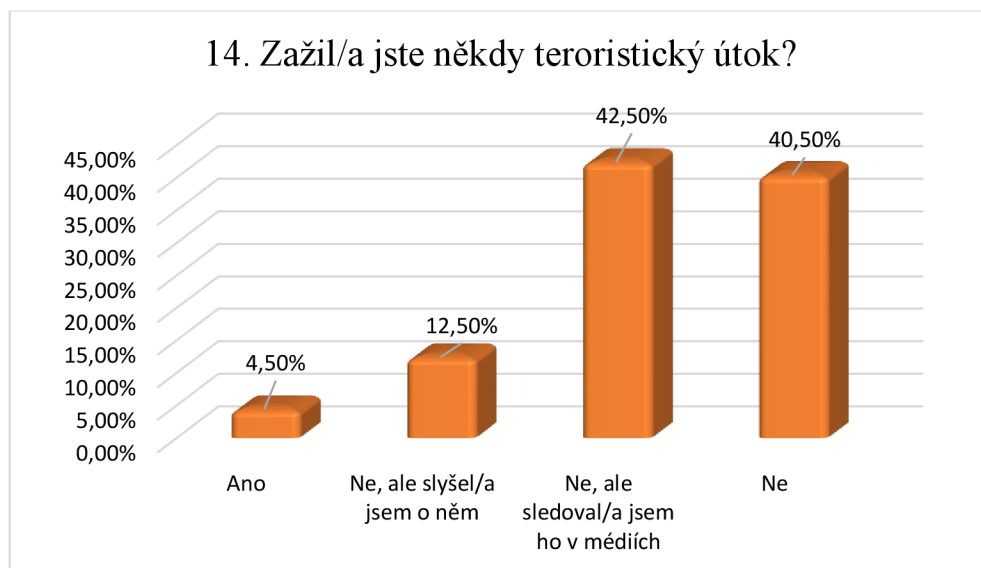


Obrázek 23. Co dělat v případě nastání teroristického útoku Zdroj: Vlastní

Otázka č. 13. zní: „*Jak se zachovat v případě teroristického útoku?*“ Tato otázka měla za úkol zmapovat, zda jsou si zaměstnanci vědomi toho, jak se zachovat v případě ohrožení jejich ZZ teroristickým útokem. Do této otázky by se dal zahrnout i útok na měkké cíle jako velmi podobný teroristickému útokem. Graf na obrázku č. 23 znázorňuje, že největší zastoupení respondentů, tedy 69 % (138 respondentů) uvedlo, že by dbali na svou bezpečnost, kontaktovali svého nadřízeného a řídili se jeho instrukcemi. Odpověď: „*Nevím*“ uvedlo 17,5 %, tedy 35 respondentů. Příručka, podle které by zaměstnanci měli vědět, jak se zachovat v případě teroristického útoku nebo ohrožení ZZ se nachází v 6,5 %, tj. u 13 respondentů. Zbýlých 7 %, tedy 14 respondentů uvedlo „*Jinou*“ odpověď. V tomto případě byla sestavena tabulka č. I pro přehled odpovědí, které byly uvedeny v odpovědi „*Jiná*“.

Tabulka I. Odpověď jiná na otázku č. 13 Zdroj: Vlastní

Jiná...	Počet
Záleží na spoustě okolností, zda se dá utéct, schovat, útočit	1
Svá bezpečnost na prvním místě, dovolání silových složek na místo	1
Utéct	1
Schovat se	1
Záleželo by asi na povaze útoku a na jeho rozsahu	1
Moje bezpečnost je zásadní, rozhodně se nebudu řídit pokyny nadřízených, nemají moc potuchy o této problematice	1
Dbát na vlastní bezpečnost	2
Pokud možno kontaktovat dispečink 158. Řídit se jejich pokyny. Dbát na své bezpečí jako při jiných napadeních agresorem.	2
Dle cvičení – útek, úkryt, boj	4



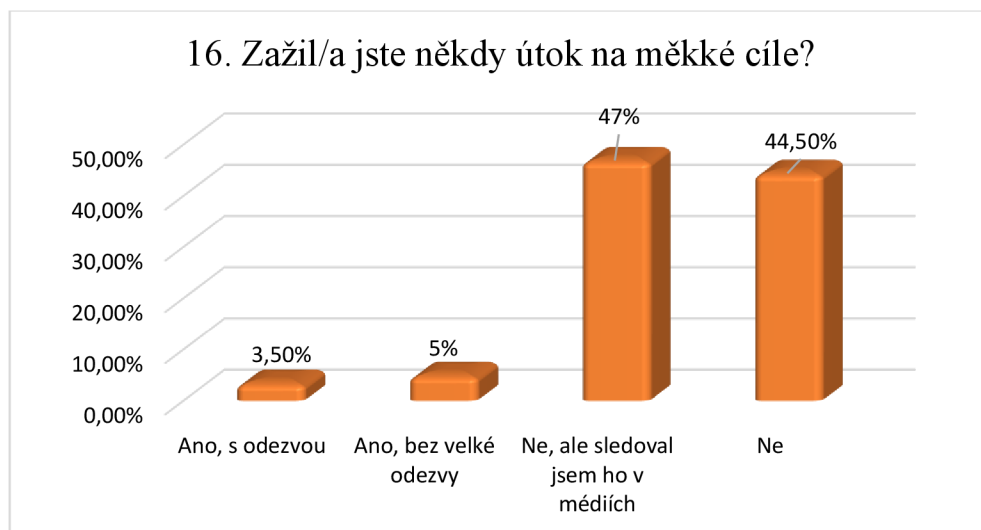
Obrázek 24. Teroristický útok Zdroj: *Vlastní*

Otázka č. 14 zní: „Zažil/a jste někdy teroristický útok? (jako teroristický útok je definováno plánované, promyšlené a politicky motivované násilí, zaměřené proti nezúčastněným osobám, sloužící k dosažení vytyčených cílů.)“ Touto otázkou bylo zjištěno množství teroristických útoků na nemocnice z pohledu respondentů. Z důvodu předpokladu minimálního množství odpovědi „Ano“ byly přidány možnosti „Ne, ale slyšel/a jsem o něm“ a „Ne, ale sledoval/a jsem ho v médiích.“ Z grafu na obrázku č. 24 vyplývá, že nejvíce respondentů (42,5 %) tj. 85, zvolilo možnost „Ne, ale sledoval/a jsem ho v médiích.“ Odpověď „Ne“ zvolilo 40,50 %, tj. 81 respondentů. Odpověď „Ne, ale slyšel/a jsem o něm“ zvolilo 12,5 %, tj. 25 respondentů. Zbýlých 9 respondentů (4,5 %) zvolilo možnost „Ano“. 119 respondentů, kteří se nějakým způsobem setkali s teroristickým útokem, ať osobně, či v médiích, pokračovali na další otázku.



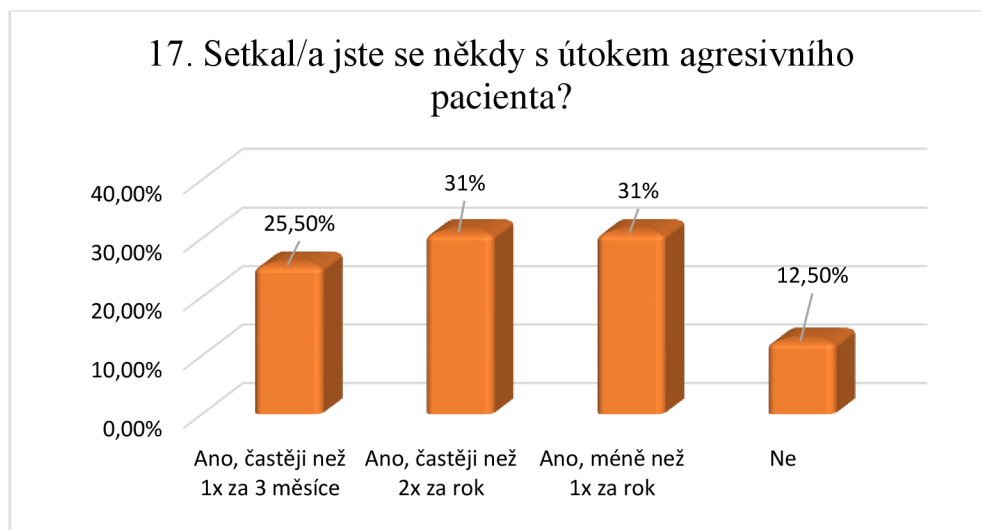
Obrázek 25. Odezva na teroristický útok Zdroj: *Vlastní*

Otázka č. 15 zní: „*Jak probíhala odezva na teroristický útok?*“ V tomto případě odpovídalo 119 respondentů, kteří byli vyčleněni předchozí otázkou. Graf na obrázku č. 25 znázorňuje, že nejvíce respondentů, tedy 51,3 % (61) odpovědělo „*Nevím*“. Druhá nejhojnější odpověď je „*Zlepšilo se zabezpečení ZZ*“, tu zvolilo 31,1 % respondentů (37). Dle 16,8 % (20) respondentů neproběhla žádná odezva. V jednom případě (0,8 %) bohužel došlo ke zhoršení zabezpečení ZZ.



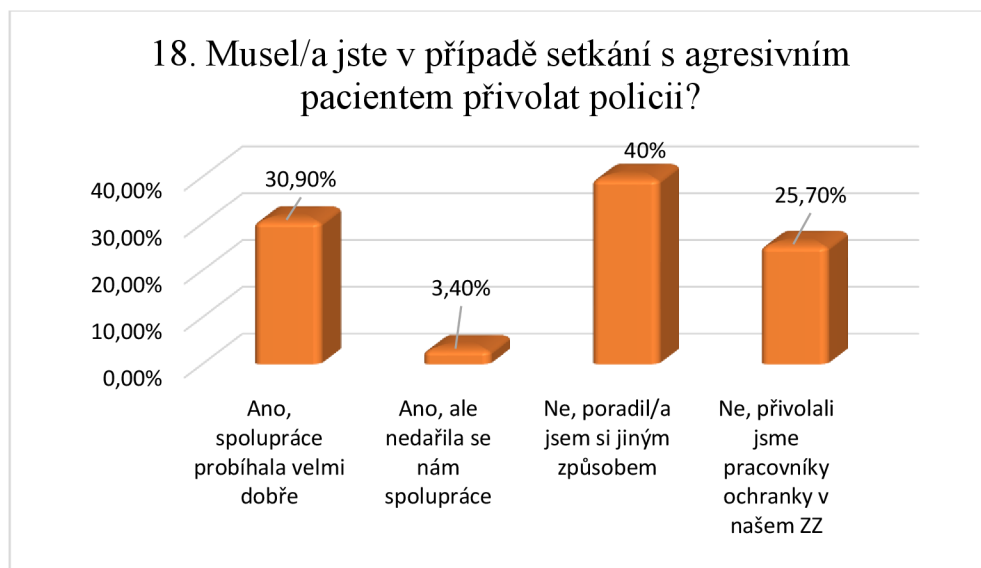
Obrázek 26. Útok na měkké cíle Zdroj: *Vlastní*

Otázka č. 16 zní: „Zažil/a jste někdy útok na měkké cíle? (všechny útoky kromě teroristického, na místa – objekty a prostory s vysokou koncentrací osob a nízkou úrovní zabezpečení proti násilným útokům.)“ Z důvodu malého počtu odpovědí u otázky týkající se zkušeností s teroristickým útokem byl dotazník doplněn mimo jiné otázkou, která zjišťuje zkušenost respondentů s útokem na měkké cíle. Zde se však respondenti s útokem v mnoha případech také naštěstí nesetkali. Graf na obrázku č. 26 znázorňuje, že nejvíce respondentů, tj. 94 (47 %) označilo odpověď „Ne, ale sledoval jsem ho v médiích“. Odpověď „Ne“, je druhá nejčastější, zvolilo ji 44,5 % (89) respondentů. Obdobně, jako u otázky na teroristický útok, nejmenší zastoupení, a to 5 % (10) respondentů měla odpověď „Ano, bez velké odezvy“ a 3,5 % (7) respondentů odpověď „Ano, s odezvou“.



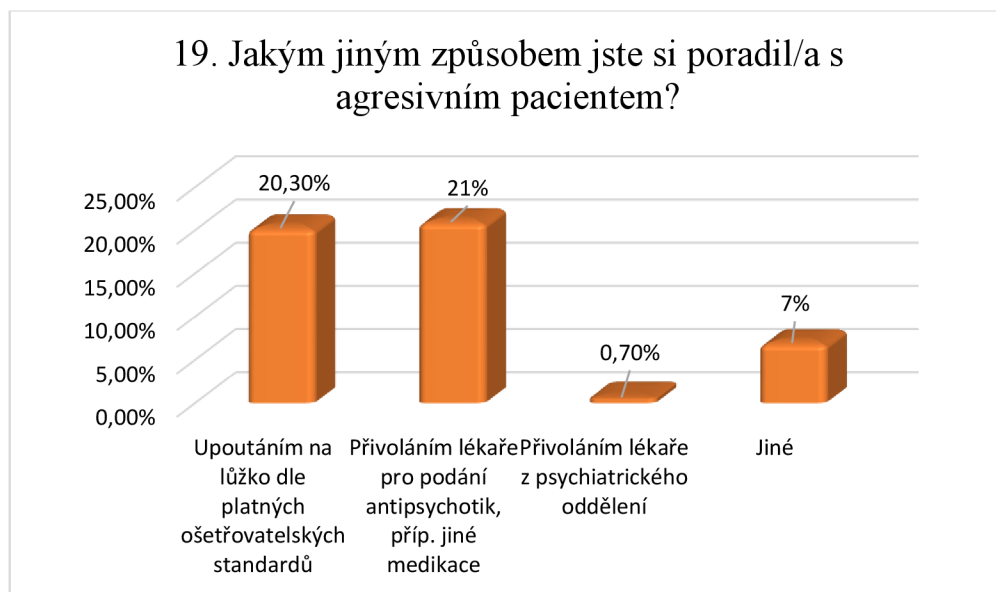
Obrázek 27. Agresivní pacient Zdroj: *Vlastní*

Z důvodu předpokladu nízkého počtu kladných odpovědí na otázky týkající se zkušenosti s teroristickým útokem nebo útokem na měkké cíle byla přidána série otázek dotazujících se na setkání respondentů s agresivním pacientem. Respondenti, kteří odpověděli na tu to otázku „Ano“, pokračují na další otázky a vyčleňuje se tedy menší výzkumný soubor. Otázka č. 17 zní: „Setkal/a jste se někdy s útokem agresivního pacienta?“ Na tuto otázku již byl nasbíráán větší počet „pozitivních“ responzí. Z grafu na obrázku č. 27 vyplývá, že odpovědi „Ano, častěji než 2× za rok“ a „Ano, méně než 1× za rok“ čítají stejný počet a to 31 % (62) respondentů. O něco méně responzí má odpověď „Ano, častěji než 1× za 3 měsíce“, a to 25,5 % (51). Nejméně respondentů, 12,5 % (25) zvolilo odpověď „Ne“.



Obrázek 28. Přivolání PČR Zdroj: Vlastní

Respondenti, kteří v předchozí otázce zvolili možnost „Ano“ (175), pokračovali na otázku č. 18, která zní: „Musel/a jste v případě setkání s agresivním pacientem přivolat policii?“ Graf na obrázku č. 28 znázorňuje, že největší zastoupení má odpověď: „Ne, poradil/a jsem si jiným způsobem“, a to 40 %, tj. 70 respondentů. K upřesnění této odpovědi tito respondenti pokračovali na další otázku (otázka č. 19). 30,9 %, tj. 54 respondentů uvedlo, že přivolali PČR a spolupráce probíhala velmi dobře. 25,7 % (45) respondentů přivolali pracovníky ochranky v jejich ZZ. Zbylých 6 respondentů (3,4 %) uvedlo, že se jim s přivolanou PČR nedařila spolupráce.

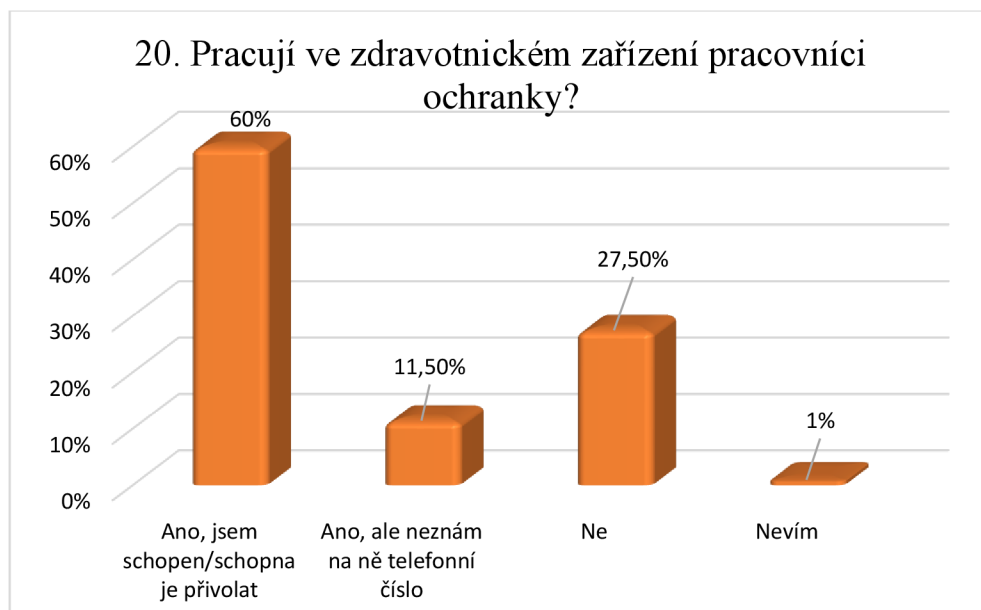


Obrázek 29. Jiný způsob vypořádání s agresivním pacientem Zdroj: Vlastní

Otázka č. 19 zní: „*Jakým jiným způsobem jste si poradil/a s agresivním pacientem?*“ Tato otázka upřesňuje odpověď z předchozí otázky „*Ne, poradil/a jsem si jiným způsobem*“, na kterou odpovídalo celkem 70 respondentů. Z grafu na obrázku č. 29 vyplývá, že nejvíce respondentů, tj. 21 % (30) si poradilo přivoláním lékaře pro podání antipsychotik, či jiné medikace. Odpověď „*Upoutáním na lůžko dle platných ošetrovatelských standardů*“ zvolilo o jednoho méně, tj. 20,3 % (29) respondentů. 7 % (10) respondentů uvedlo jinou odpověď. Jiné odpovědi jsou znázorněny v tabulce č. II. V jednom případě (0,7 %) si poradili přivoláním lékaře z psychiatrického oddělení.

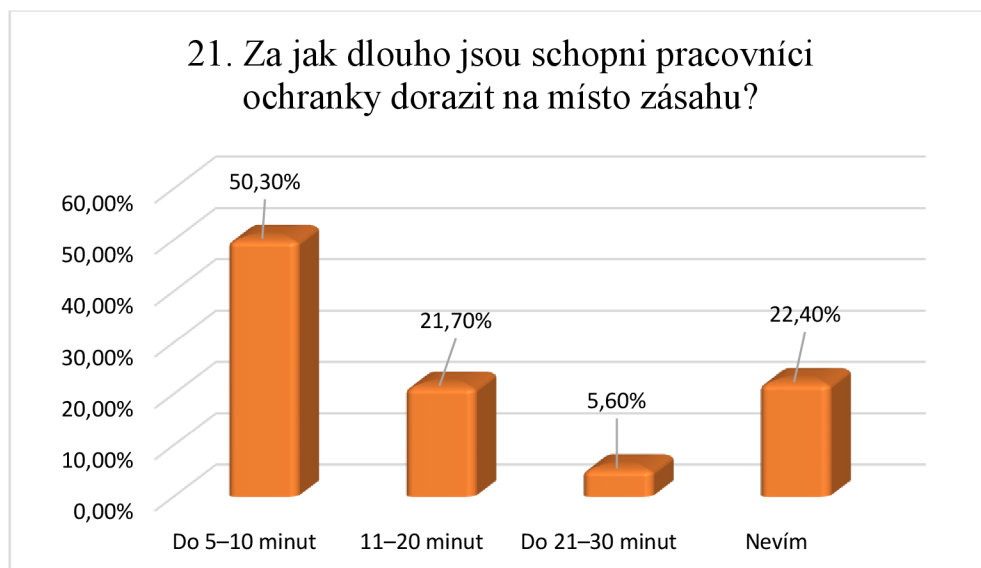
Tabulka II. Odpověď jiná na otázku č. 19 Zdroj: Vlastní

Komunikace, bezpečí všech, lékař ve službě, medikace, kurty	1
Byl zpacifikován, odebral jsem mu nůž a následně přikurtován	1
Deeskalační metody	1
Podle standardů zařízení	1
Uklidňováním, že vše bude v pořádku	1
Ubránili jsme se	1
Komunikací s pacientem	1
Sama jsem je zpacifikovala	2
Napadl mě, poté MUDr. přivolala pomoc z nejbližších oddělení	1



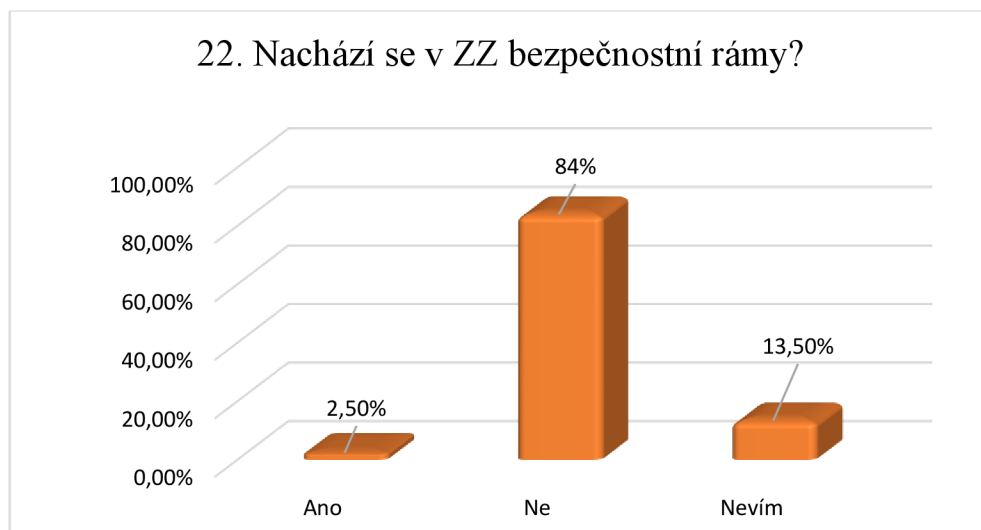
Obrázek 30. Pracovníci ochrany Zdroj: Vlastní

Otázka č. 20 zní: „*Pracují ve zdravotnickém zařízení pracovníci ochrany?*“ Tato otázka zjišťuje, v kolika případech z celkových 200 pracují v ZZ pracovníci ochrany a zda jsou respondenti schopni je přivolat v případě nouze. Z grafu na obrázku č. 30 vyplývá, že v 60 % (120 respondentů) ve ZZ pracují pracovníci ochrany a respondenti jsou schopni je přivolat. Odpověď „*Ne*“ zvolilo 27,5 % (55) respondentů. 11,5 % (23) respondentů uvedlo, že ve ZZ pracují pracovníci ochrany, neznají na ně však telefonní číslo. Ve dvou případech (1 %) respondenti uvedli, že neví.



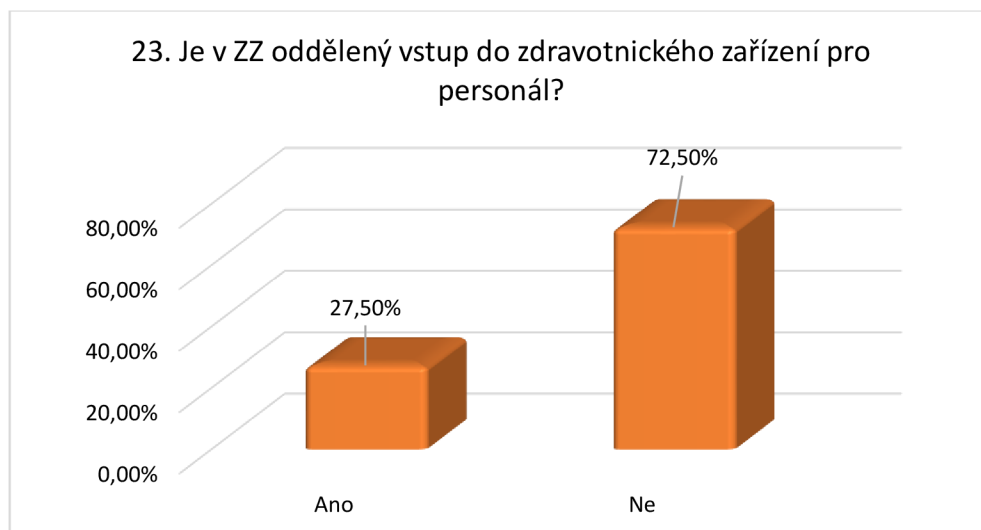
Obrázek 31. Za jak dlouho jsou schopni pracovníci ochranky dorazit na místo zásahu?
Zdroj: *Vlastní*

Otázka č. 21 zní: „Za jak dlouho jsou schopni pracovníci ochranky dorazit na místo zásahu?“ Tato otázka mapuje, za jak dlouho jsou pracovníci ochranky schopni dorazit na místo. Pro tuto otázku byli vyřazeni respondenti, kteří v předchozí otázce odpověděli „Ne“, tj. (55) 27,5 % a „Nevím“ tj. (2) 1 % respondentů. Zbýlých 143 (71,5 %) respondentů odpovídalo na tuto otázku. Graf na obrázku č. 31 znázorňuje, že odpověď „Do 5-10 minut“ zvolilo 72 (50,3 %) respondentů. Druhá nejčastější odpověď je „Nevím“, kterou vybralo 32 (22,4 %) respondentů. O 1 responzi méně má otázka „Do 11–20 minut“ (21,7 %). Nejdélší časový údaj, a to „Do 21–30 minut“ vybralo nejméně, 5,6 % (8) respondentů.



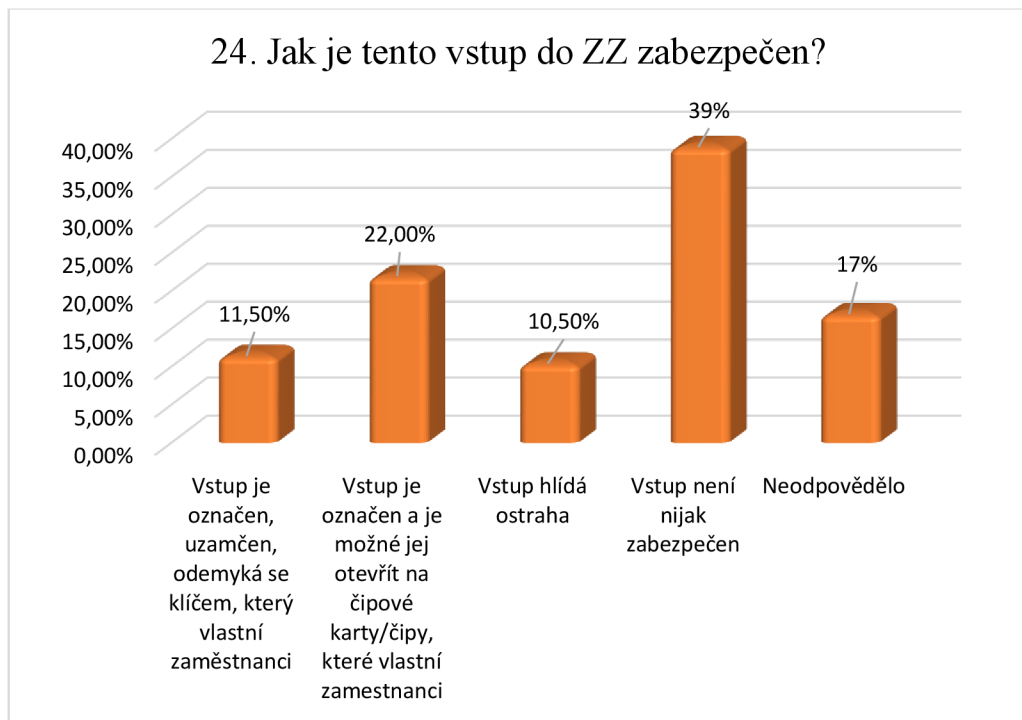
Obrázek 32. Bezpečnostní rámy Zdroj: *Vlastní*

Otázka č. 22 zní: „*Nachází se ve zdravotnickém zařízení bezpečnostní rámy?*“ Tato otázka se týká zabezpečení jednotlivých nemocnic. Bohužel vzhledem k anonymizaci nemocnic nelze určit, v jaké nemocnici se bezpečnostní rámy nachází. Graf na obrázku č. 32 znázorňuje, že nejvíce respondentů, a to 84 % (168) zvolilo odpověď „*Ne*“. Ukázalo se, že se ve většině nemocnic bezpečnostní rámy nenachází. Odpověď „*Nevím*“ zvolilo 13,5 % (27) respondentů. Podle 2,5 % (5) respondentů se bezpečnostní rámy v nemocnici nachází.



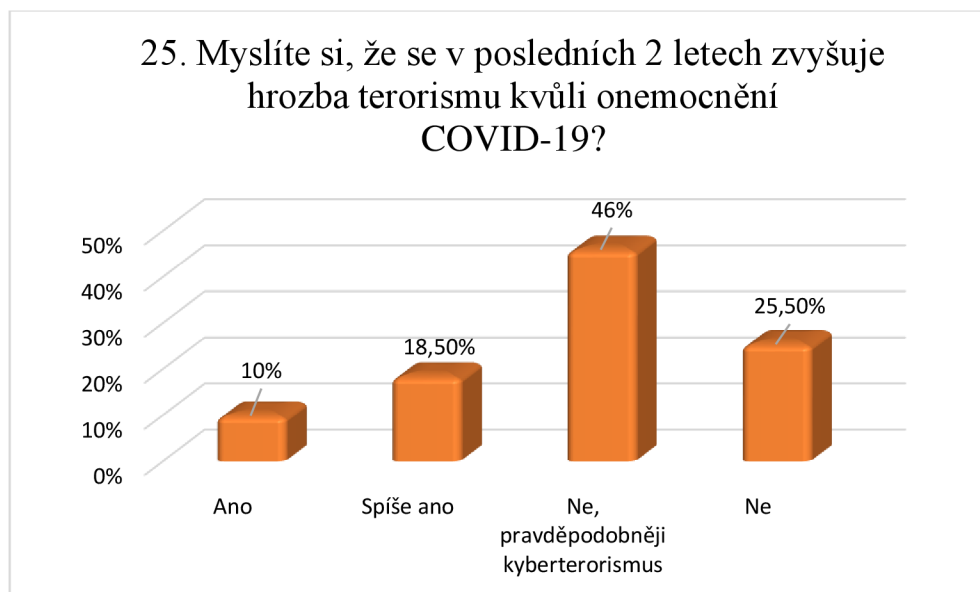
Obrázek 33. Vstup do ZZ Zdroj: *Vlastní*

Otázka č. 23 zní: „*Je ve zdravotnickém zařízení oddělený vstup do zdravotnického zařízení pro personál?*“ Tato otázka má také za úkol zmapovat zabezpečení ZZ. Graf na obrázku č. 33 znázorňuje, že většina respondentů, tedy 72,5 % (145), odpověděla, že ve ZZ není oddělený vstup pro personál. Podle zbylých 27,5 % (55) respondentů je ve ZZ oddělený vstup pro personál.



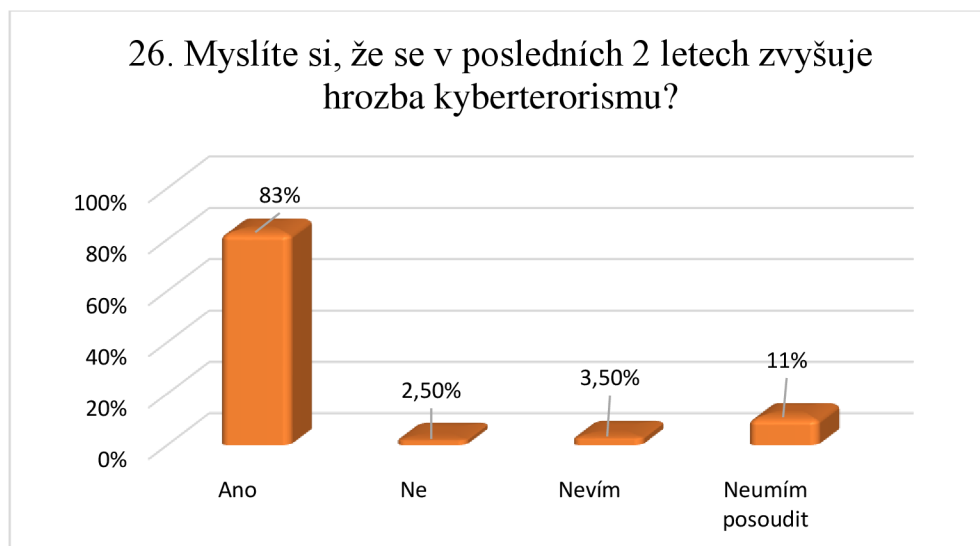
Obrázek 34. Zabezpečení vstupu pro personál Zdroj: *Vlastní*

Další otázka týkající se zabezpečení vstupu do zdravotnického zařízení, otázka č. 24 zní: „*Jak je tento vstup do zdravotnického zařízení zabezpečen?*“ Z grafu na obrázku č. 34 vyplývá, že odpověď s nejvíce responzemi, a to 39 % (78), je: „*Vchod není nijak zabezpečen*“. Vchod, který je označen a lze otevřít pomocí čipové karty, nebo čipu, který vlastní jen zaměstnanci se nachází ve 22 % (44) případech. Bez odpovědi ponechalo otázku 17 % (34) respondentů. Podle 11,5 % (23) respondentů, je vchod označen, uzamčen a odemká se klíčem, který vlastní pouze zaměstnanci. O dvě responze méně, tj. 10,5 % (21), má odpověď „*Vchod hlídá ostraha*“.



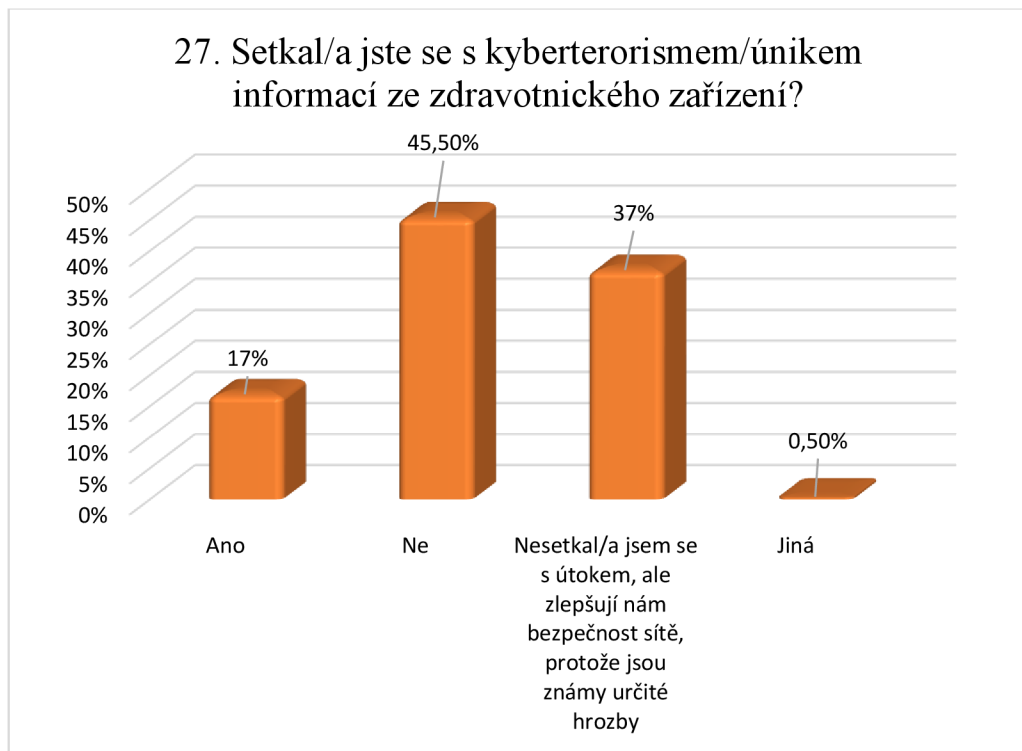
Obrázek 35. Hrozba terorismu Zdroj: *Vlastní*

Otázka č. 25 se týká hrozby terorismu z pohledu respondentů. Ta zní: „*Myslíte si, že se v posledních 2 letech zvyšuje hrozba terorismu kvůli onemocnění COVID-19?*“ Graf na obrázku č. 35 znázorňuje, že nejvíce respondentů, a to 46 % (92) se domnívá, že „*Ne, pravděpodobněji než kvůli COVID-19 se hrozba zvyšuje u kyberterorismu*“. Druhý největší podíl responzí, tj. 25,5 % (51) má odpověď „*Ne*“. Podle 18,5 % (37) respondentů se spíše hrozba zvyšuje a podle 10 % (20) respondentů není větší riziko terorismu z důvodu pandemie COVID-19.



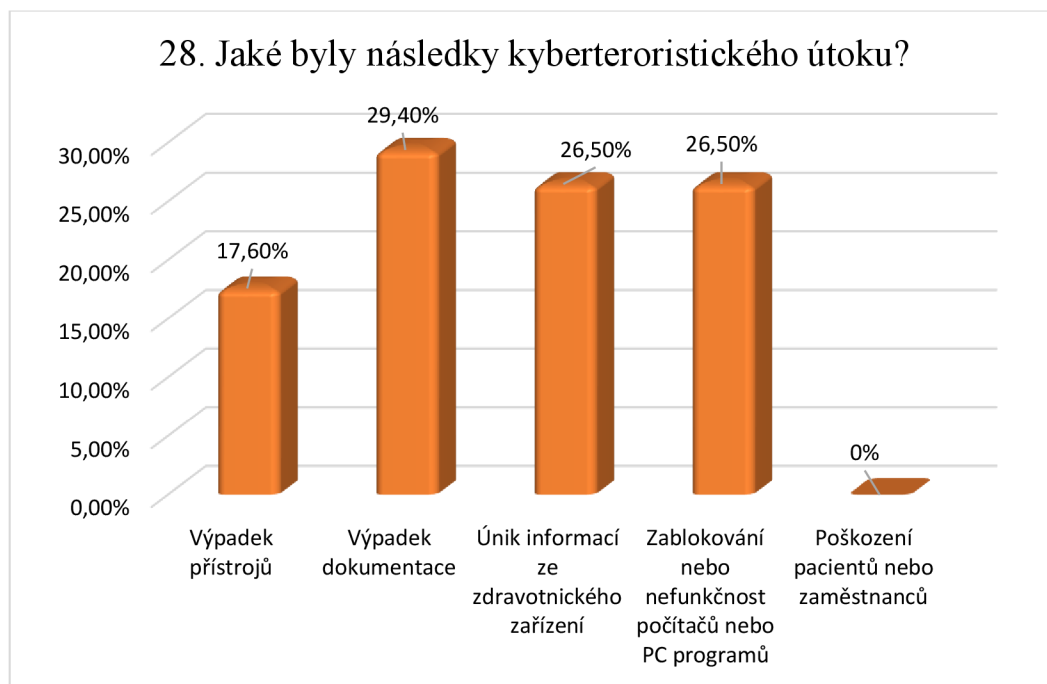
Obrázek 36. Hrozba kyberterorismu Zdroj: *Vlastní*

Otázka č. 26 zní: „Myslíte si, že se v posledních 2 letech zvyšuje hrozba kyberterorismu?“ Tato otázka zjišťuje názor respondentů na hrozbu kyberterorismu. Jelikož v předchozí otázce byla častá odpověď, že je z pohledu respondentů větší hrozba kyberterorismu větší, než hrozba terorismu z důvodu pandemie COVID-19, lze očekávat, že kladná odpověď na tuto otázku bude vysoká. Z grafu na obrázku č. 36 vyplývá, že dle předpokladu odpovědělo nejvíce respondentů, a to 83 % (166), že si myslí, že se hrozba kybernetického útoku v posledních 2 letech stupňuje. Odpověď „*Neumím posoudit*“ zvolilo 11 % (22) respondentů. Možnost „*Nevím*“ má 3,5 % (7) responzí a nejméně responzí má odpověď „*Ne*“, a to 2,5 % (5).



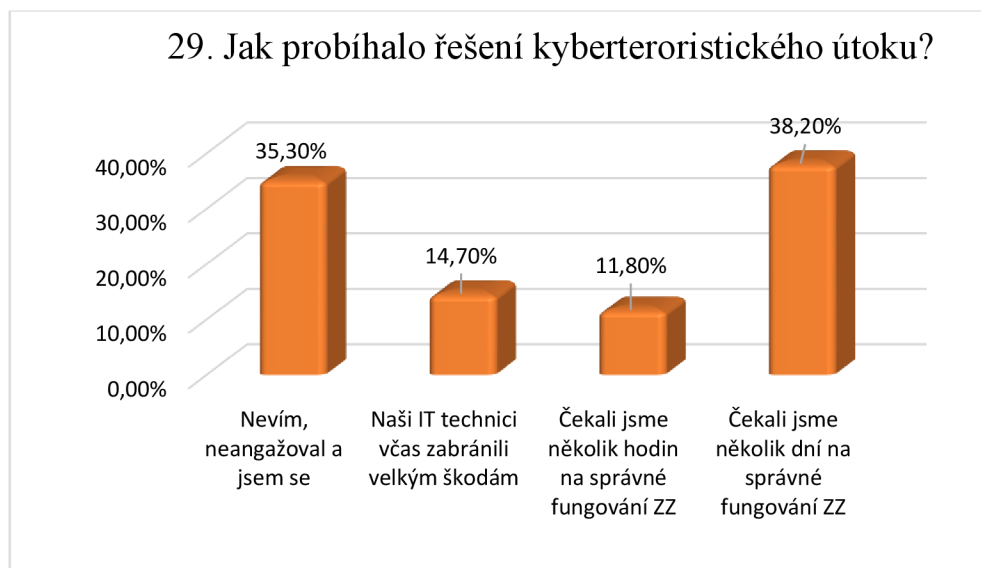
Obrázek 37. Setkání s kyberteroristickým útokem Zdroj: Vlastní

Otázka č. 27 zní: „Setkal/a jste se s kyberterorismem/únikem informací ze zdravotnického zařízení?“ Tato otázka mapuje četnost kyberteroristických útoků na ZZ. Graf na obrázku č. 37 znázorňuje, že nejvíce responzí, a to 45,5 % (91), má naštěstí odpověď „Ne“, tedy většina respondentů se s kyberteroristickým útokem nesešla. Ve 37 % (74) případech se respondenti nesešli s útokem, ale zaregistrovali zlepšování bezpečnosti sítí v jejich ZZ. Odpověď „Ano“ má 17 % (34) responzí. Takové responze vedou k položení dalších otázek pro upřesnění těchto útoků. Z tohoto důvodu byly položeny další, následující otázky. V jednom případě zde byla jako responze označena odpověď „Jiná“, v tomto případě bylo zodpovězeno „Setkala jsem se s kyberteroristickým útokem jen v médiích“.



Obrázek 38. Následky kyberteroristického útoku Zdroj: Vlastní

Otázka č. 28 je upřesňující pro respondenty, kteří se setkali s kyberteroristickým útokem nebo únikem informací ze ZZ. Týká se tedy 34 respondentů. Z grafu na obrázku č. 38 vyplývá, že nejčastějším následkem kyberteroristického útoku je dle respondentů „*Výpadek dokumentace*“. Tato odpověď získala 29,4 % hlasů, tj. 10 respondentů. Stejný počet, tj. 26,5 % (9) respondentů mají odpovědi: „*Únik informací ze zdravotnického zařízení*“ a „*Zablokování nebo nefunkčnost počítačů nebo PC programů*“. Odpověď „*Výpadek přístrojů*“ získala 17,6 % (6) responzí. Žádnou responzi naštěstí nezískal následek „*Poškození pacientů nebo zaměstnanců*“. Všechny tyto následky jsou v zastoupení responzí 1 a více velmi vážné.



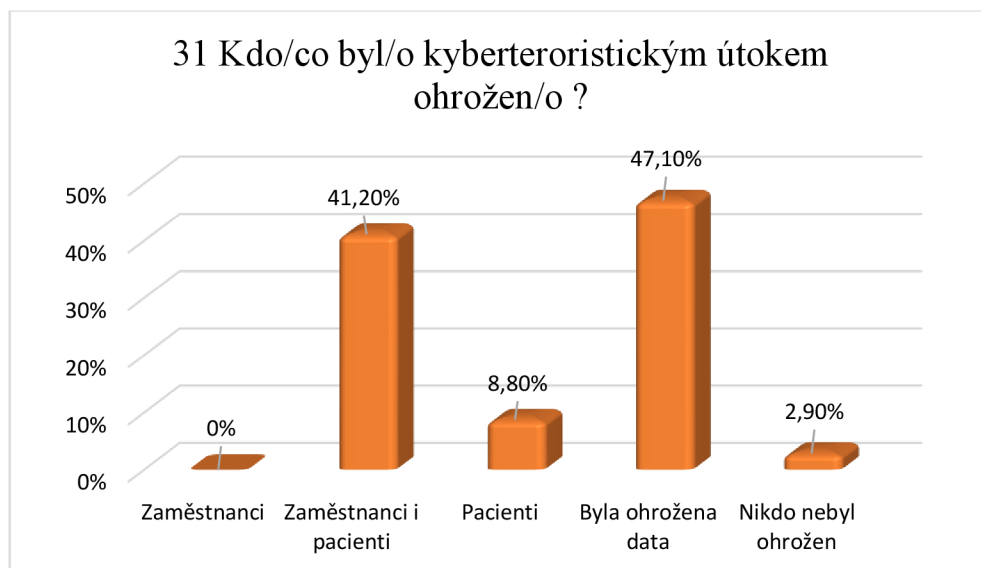
Obrázek 39. Řešení kyberteroristického útoku Zdroj: Vlastní

Otázka č. 29 zjišťuje, jak probíhalo nebo jak dlouho trvalo řešení kyberteroristického útoku. Graf na obrázku č. 39 znázorňuje, že nejvíce responzí, 38,2 % (13), má odpověď „Čekali jsme několik dní na správné fungování ZZ“. Časový údaj v rádech dnů je pro ZZ velmi dlouhá doba na čekání na správné fungování a následky poté mohou být velmi vážné. O něco méně responzí, tj. 35,3 % (12), má odpověď „Nevím, neangažoval/a jsem se“. Včas bylo zabráněno velkým škodám v 14,7 % (5) případech. O jednu responzi méně, tj. 11,8 % (4), má odpověď „Čekali jsme několik hodin na správné fungování ZZ“.



Obrázek 40. Vyrovnání se s kyberteroristickým útokem Zdroj: *Vlastní*

Otázka č. 30 zjišťuje schopnost ZZ obnovit správné fungování a vypořádat se s kyberteroristickým útokem. Z grafu na obrázku č. 40 vyplývá, že v 64,7 % (16 responzí) se ZZ vypořádalo s útokem dobře a neproběhla masivní ztráta dat ani omezení funkčnosti. Ve 23,5 % (8 případech) proběhlo omezení funkčnosti ZZ, které se dlouho nedařilo vyřešit. Ve třech případech (8,9 %) proběhla větší ztráta dat nebo informací. V jednom případě (2,9 %) se ZZ s útokem dlouho nevyrovnalo.



Obrázek 41. Ohrožení kyberteroristickým Zdroj: Vlastní

Poslední otázka (otázka č. 31), která upřesňovala informace o kyberteroristickém útoku, měla za úkol zjistit, kdo byl tímto útokem ohrožen. Graf na obrázku č. 41 znázorňuje, že nejvíce ohrožena byla data, a to ve 47,1 % (16 případech). Odpověď „Zaměstnanci i pacienti“ zvolilo 41,2 % (14) respondentů. 3 responze, tj. 8,8 % má odpověď „Pacienti“ a v jednom případě (2,9 %) nebyl nikdo ohrožen. Pouze zaměstnanci samostatně nebyly ohroženy v žádném případě.

Po rozvaze byla zvolena doplňující otázka, která zní: „*Chcete doplnit nějaké informace k tématu ochrany zdravotnických zařízení?*“, ta měla za úkol získat zajímavé nebo doplňující informace. Nejzajímavější jsou sepsány níže.

R₂₈: „Zvyšování bezpečnosti ZZ je v současné době (pandemie COVID-19, válka na Ukrajině) rozhodně na místě.“

R₉₅: „Většina menších nemocnic nemá ochranku, ale spoléhá se jen na kamerový systém nemocnice a na případnou kooperaci s PČR nebo městskou policií.“

R₁₅₂: „Málo schopná ochranka, složená převážně z částečně invalidních osob.“

R₁₅₃: „Když jsem jednou volala ochranku, že je na oddělení člověk z ambulance, který k nám zabloudil a je slovně agresivní, tak mi řekli že nepřijdou. Bohužel mě nenapadlo poslat stížnost na ředitelství.“

R₁₆₉: „Areál nemáme kompletně oplocený, jsme u lesa. Nemáme v oknech alarmy, nemáme možnost použít nouzového přivolání policie či vedení. Nemáme v případě krize, zejména o noční, plán, jak utéct nebo informovat kolegyně.“

R₁₈₄: „K nácviku útoku na měkké cíle jsme vůbec nedostali od zaměstnavatele zpětnou vazbu, co bylo dobře, co špatně...návrh zlepšení ochrany. Ochranku sice máme, ale jsou to lidé v důchodu, ženy, invalidní důchodci...takže vlastně v případě nutnosti nefunguje jako použitelná ochrana.“

5.3 Výsledky polostrukturovaných rozhovorů

Sbírání polostrukturovaných rozhovorů probíhalo v období od září 2021 do března 2022. Výzkumný soubor se skládal z osob, které byly na stáži/misi v zajímavých oblastech světa. Pro tuto diplomovou práci to znamená, že země je nebo byla potenciálně či reálně ohrožena teroristickým útokem, nebo v ní teroristický útok již proběhl. Výjimkou je zde Spolková republika Německo, která byla vybrána z důvodu odlišnosti ochrany nemocnic od České republiky. V případě rozhovoru z oblasti Saudské Arábie se podařilo získat dva odlišné rozhovory od různých osob v různých časových obdobích. Osoby pro rozhovor jsem selektovala ze svého okolí a z řad zaměstnanců na mém pracovišti v nemocnici, kterou zde nelze uvést z důvodu anonymizace. Všechny osoby souhlasily se zveřejněním rozhovorů. Z důvodu nedostatku informací byl vyřazen rozhovor zdravotnických pracovníků pracujících ve Velké Británii a Spolkové republice Německo.

Pomocí prvních tří otázek v rozhovoru bylo zjištěno, na jaké pozici respondenti pracovali a v jaké oblasti a jak dlouho pracovníci působili. Označení respondentů je zde uvedeno podle zemí působnosti zkratkou. Zjištěné informace jsou zpracovány v tabulce č. III.

Tabulka III. Přehled jednotlivých respondentů Zdroj: Vlastní

Respondent	Země/oblast	Pozice	Doba trvání pobytu
R _{BH}	Bosna a Hercegovina/Mostar	medik	6 měsíců
R _{AFG}	Afghánistán	vedoucí chirurg	2× 9 měsíců
R _{Ir}	Irák/Basra	vedoucí chirurg	2× 9 měsíců
R _{Pá}	Pákistán/Kašmír	vedoucí chirurg	8 měsíců
R _{Rw}	Rwanda	lékař	3 roky
R _{Sú}	Súdán /Chartúm	medik	1 měsíc
R _{SA1}	Království Saúdská Arábie 1	všeobecná sestra Nursing supervi- sior	10 let
R _{SA2}	Království Saúdská Arábie 2 /Rijád	všeobecná sestra	4 roky
R _{SAE}	Spojené arabské emiráty/Abu Dhabí	všeobecná sestra	13 let
R _{SRN}	Spolková republika Ně- mecko/Cham	všeobecná sestra	2 měsíce

Všechny následující otázky souvisí s cílem práce č. 2 – Analýzou rozdílu v ohrožení a zabezpečení ZZ v ČR a v zahraničních státech.

Otázka č. 4 zní „*Jak bylo Vaše působiště zabezpečeno proti možnému teroristickému útoku?*“



Obr. 42. Zabezpečení zdravotnických zařízení dle respondentů Zdroj: Vlastní

Tato otázka souvisí s cílem č.1 Analýza zabezpečení zdravotnických zařízení a s cílem č. 2 Analýza rozdílů v ohrožení a zabezpečení zdravotnických zařízení v České republice a vybraných zahraničních státech.

Z grafického zpracování na obrázku č. 42 vyplývá, že ve státech Bosna a Hercegovina, Afghánistán a Irák se k ochraně nemocnic využívají všechny prostředky, přesto ale nejsou srovnatelné s ochranou nemocnic v ČR. Tyto státy spojuje odpověď „*Oplocení*“. Vojáci střeží ZZ v Pákistánu, Súdánu a Saudské Arábii. V Iráku funguje systém předsunuté kontroly a check-pointů a v druhém případě Saudské Arábie, Spojených arabských emirátech a Spolkové republice Německo spoléhají mimo jiné na ochranka.

V následujícím textu jsou vybrány nejzajímavější odpovědi k tématice.

R_{AFG} : „*Celá ta nemocnice byla součástí vojenské základny, a to je velikosti menšího města, celé je to obehnané a jsou tam předsunuté kontroly a check-pointy. Nebylo to zabezpečené proti tomu, co by mohlo létat ze vzduchu, to se nedá.*“

R_{RW} : „*Standardně byla ostraha objektu, což byli zaměstnanci bezpečnostní služby, kteří byli vyzbrojeni plynovými pistolemi nebo obušky, nicméně lidé, kteří přicházeli do zdravotnického zařízení se nekontrolovali, ostraha byla vyšší před prezidentskými volbami, to se kontrolovali všichni na vstupu do areálu, kontrolovali se lidem batohy, kapsy*

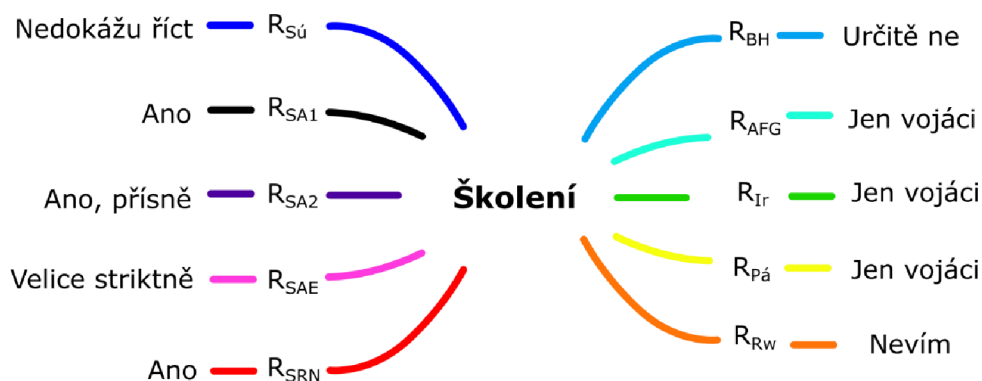
a podobně. Také byla vyšší úroveň ostrahy v době, kdy tam přijel ministr zdravotnictví. Běžně se nic nekontrolovalo.“

R_{SA1}: „V době, kdy ještě nebyl Súdán rozdělen na dva státy (Severní a jižní), vysoké napětí, v hlavním městě byla spousta uprchlíků, nízká bezpečnost, nikdy jsme se nepohybovali sami, byli jsme vždy s někým ze studentů, který nám byl přidělen. V nemocnici při vstupu byli bezpečnostní rámy, byla tam neozbrojená kontrola, v některých místech hlídala armáda s výzbrojí.“

R_{SA2}: „Tak hlavně se tam dbalo na média a internet, čili každé tři měsíce jsme měnili přístupová hesla na všechny weby. To znamená, že jsme všechno dělali přes počítače a veškerá dokumentace se vedla přes počítače, byly tam různé webové stránky jako Surginet a Oracle, ty hlavní stránky a samozřejmě bylo tam různé zabezpečení. Byla jsem tam kolem roku 2001, kdy došlo k útoku v USA, takže tam byla security v každé nemocnici, pak po těch útocích jsme normálně procházeli pásy jako na letišti.“

R_{SAE}: „Tam to bylo takový trošku už otevřený, takže tam byla security, u každých hlavních dveří byla stanice security, čili bezpečnostní technik nebo taková policie místní a ty to kontrolovali. Samozřejmě byly v těchto arabských zemích návštěvy povolené, většinou 24 hodin 7 dní v týdnu, takže pořád. Security, přišli na pomoc na dané místo okamžitě. Potom se z toho samozřejmě dělaly záznamy, vyhodnocovalo se to, ale oni měli pravomoci zpacifikovat ty lidi, samozřejmě nejdřív mluvili, oni na to byli školení, domlouvali jim a případně je zpacifikovali.“

Otázka č. 5 zní: „Školí se místní zaměstnanci na nácvik reakce na teroristický útok?“



Obrázek 43 Školení zahraničních zaměstnanců Zdroj: Vlastní

Tato otázka souvisí s VO č. 3: „Zúčastnili se zaměstnanci zdravotnického zařízení školení na nácvik reakce na teroristický útok?“

Z grafického zpracování na obrázku č. 43 týkající se otázky č. 5 vyplývá, že v Bosně a Hercegovině se zaměstnanci neškolí. V Iráku, Afghánistánu a Pákistánu se jedná o vojenskou misi, tím pádem se personál člení na civilní a vojenský. Vojenský personál se podrobně cvičí, zatímco civilní personál je základně proškolen a jsou mu poskytnuty osobní ochranné pomůcky. Ve Rwandě a Súdánu nemáme o školení žádné informace. V Saudské Arábii je podle obou respondentů školení velmi striktní. Ve Spojených arabských emirátech se zaměstnanci také velmi striktně školí. Ve Spolkové republice Německo probíhá školení společně se základním školením BOZP a je velice stručné.

V následujícím textu jsou vybrány nejzajímavější odpovědi k tématice.

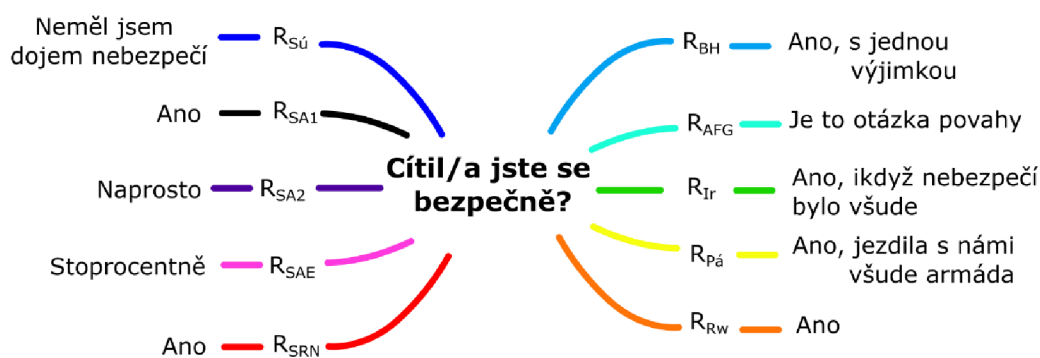
R_{Ir} : „Dělí se to na ten personál civilní a vojenský. Civilní zaměstnanci, např. ekonomové, dovozci zboží, kuchaři apod. se moc neškolí, jsou upozorněni, kam mají běžet do krytu, nějaké ochranné prostředky mají nafasované, přilbu, neprůstřelnou vestu. Vojenští zaměstnanci jsou vycvičení. Já jsem důstojník, čili jsem vycvičen.“

R_{SA1} : „Ano. Prochází základním výcvikem, který se zabývá chováním v život ohrožujících situacích, nácvik sebeobrany a obsluhy AK47.“

R_{SA2} : „Ano. A dost přísně. A velice striktně. My v Saudské Arábii jsme měli přímo nácvik, kdy nám zavolali, vyhlásili black code a my jsme museli zastavit operativu a nevěděli

jsme, jestli to je opravdová situace nebo jestli je to trénink, dostali jsme instrukce, kolik pacientů přijede, s jakým poraněním, a museli jsme s nimi manipulovat, celá nemocnice pracovala v tomhle duchu. Takže my jsme odvezli plánované pacienty zpět na oddělení, kdo mohl být propuštěný, byl propuštěný, to prošlo dokumentací a do toho nám začali vozit namaskované vojáky a my jsme s nimi museli manipulovat jako kdyby ta zranění byla opravdová.“

Otázka č. 6 zní: „Cítil/a jste se v průběhu stáže/mise bezpečně?“



Obrázek 44. Bezpečnost v průběhu stáže/mise Zdroj: *Vlastní*

Z grafického zpracování na obr. č. 44 vyplývá, že se respondenti cítili v průběhu stáže bezpečně na všech místech působení.

R_{BH}: „Ano, kromě potyčky s agresivním pacientem.“

R_{Ir}: „To je otázkou povahy člověka. Bezpečně se tam nemůžete cítit nikdy, protože to nebezpečí je všude, trvá pořád, nemůžete ho nikdy vyloučit. Byli jsme samozřejmě ve větším bezpečí, než je strážní služba nebo průzkumné čety a podobně. Ti trvale vyjíždějí mezi lidi, tak jsou na tom z hlediska bezpečnosti hůř. My jsme jezdili v obrněných autech v obcích nebo ve městě, tam to může vybuchnout kdykoliv a vybuchne to. Kousek od nás vybuchlo auto s atentátníkem, našťástí nás to nezasáhlo, stříleli po nás, proděravěli nám gumu, ale prostřelili pouze vrchní plášť a na vnitřní tvrdé gumě jsme museli dojet. Také jsme se převrátili, protože jsme najeli na minu v blízkosti silnice a museli jsme čekat až nás vysvobodí.“

„Takže ohrožení bylo samozřejmě. Nebo bombardují, v nemocnici operujete a můžou lítat nějaké třaskaviny vzduchem, vy nevíte, co to přesně je a ono to třaská kolem vás, všichni se běží schovat a vy musíte dokončit tu operaci. Podle mě je to otázka povahy, jestli to člověk snese nebo nesnese, já to snášim dobře, mě to nevadí, žádné posttraumatické

stresové poruchy nemám. Někdo to ale nevydýchá a musí být vrácen do České republiky kvůli depresím, protože tam ležet na posteli v těžkých depresích není možné. Já jsem do toho šel dobrovolně, věděl jsem, že budu pořád v ohrožení a vydržím to.“

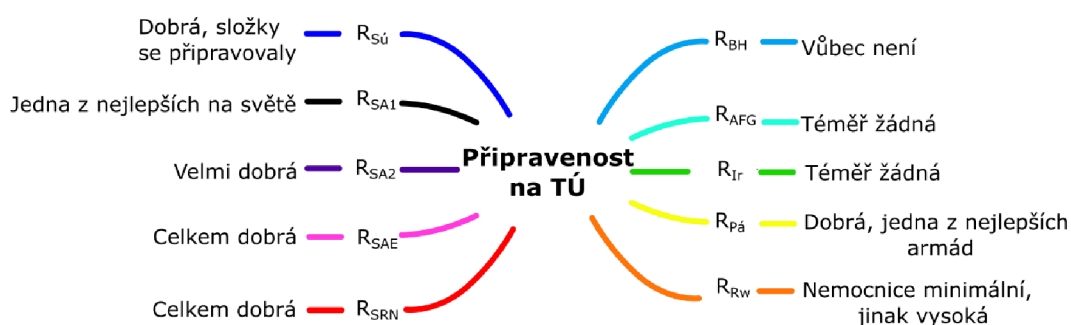
R_{PÁ}: „Když jsme jeli někam do hor na výlet, tak s námi jela jízdní ozbrojená jednotka pákistánské armády. Nemohli nás nechat ohrozit, protože kdyby nás někdo zatkł, tak by nás museli vyměnit za Tálibance, které bylo náročné zajmout. Nesměl si nás ani nikdo fotit.“

R_{SÚ}: „Byla to moje první zkušenost s africkým státem, bylo zakázáno některé objekty fotit, v noci se nesmělo nikam chodit. V některých částech města to nebylo pro Evropany bezpečné a bylo doporučeno se tam nepohybovat. V nemocnici byla všude ostraha, takže v nemocnici jsem neměl dojem nebezpečí.“

R_{SA2}: „Naprostο, viděla jsem, jak je tam ta bezpečnost zajištěná. My jsme zažili bombový útok na rezidenční oblast, kde žili Američani anebo západní cizinci a bylo hodně raněných, tak nám je vozili do nemocnice. Zažili jsme trochu válečnou chirurgii a po tomhle incidentu jsme bydleli u nemocnice v takový vilový čtvrti, kolem dokola byla vysoká zeď, byl tam vjezd bránou, kde stála security, která byla ozbrojená. Po tomhle incidentu oni dokonce k nemocnici nasadili tanky na taková vyvýšená místa, což pro nás bylo trochu jako takové zvláštní, na to jsme nebyli zvyklí, ale bylo to z důvodu naší bezpečnosti. A musím říct, že nikdo si tam vůči nám nic nedovolil nikdy.“

R_{SRN}: „Cítím se bezpečně. Nevnímám větší ohrožení než v jiném veřejném prostoru.“

Otázka č. 7 zní: „*Jak hodnotíte tamní připravenost na teroristický útok?*“



Obrázek 45. Připravenost na TÚ Zdroj: Vlastní

Na grafickém znázornění na obrázku č. 45 lze vidět, že se připravenost na teroristické útoky liší. Tato otázka také záleží na pocitovém vnímání bezpečnosti jednotlivých respondentů, což se může u každého lišit. V Bosně a Hercegovině, Afghánistánu a Iráku není téměř žádná připravenost. Pákistán disponuje jednou z nejlepších armád na světě, lze tedy hodnotit tamní připravenost jako dobrou. Ve Rwandě více dbají na veřejnou bezpečnost než na zabezpečení nemocnic. V Súdánu, Saudské Arábii, Spojených arabských emirátech a Spolkové republice Německo je připravenost hodnocena od „*celkem dobrá*“ až po „*jedna z nejlepších na světě*“.

R_{BH}: „V Bosně a Hercegovině byla občanská válka v 90. letech, byli tam teroristické pseudoútoky, byli tam partyzáni, ale nikdy tam žádný útok nebyl, takže si myslí, že se tam ani nic stát nemůže.“

R_{Pá}: „Připravenost byla dobrá, mají jednu z nejpočetnějších armád - 6 milionů vojáků. Zatýkali tam teroristy a Tálibánce, zavírali je do vězení, mají jízdní jednotku, která dopadala zločince i na koních.“

R_{Rw}: „Obecně jsou ve Rwandě bezpečnostní složky na vysoké úrovni, takže si myslím, že i tajná policie je na vysoké úrovni, takže by byli schopní odhalit bezpečnostní hrozbu s předstihem. A co se týče konkrétně ostrahy jednotlivých objektů – zdravotnických zařízení – bezpečnost byla minimální. Pokud by se někdo rozhodl, že chce provést útok, bez problémů by tam pronesl zbraň. Nemocnice byla oplocená, ostraha tam byla. Středisko je vysoko v horách, na oplocení nebyly peníze.“

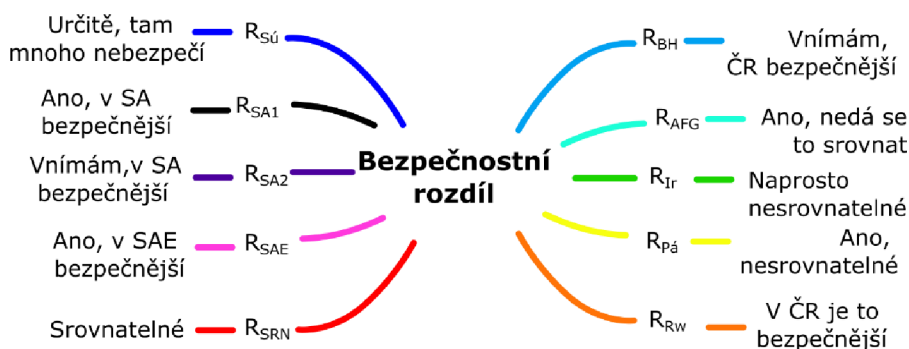
R_{SÚ}: „Súdán byl v té době vojenská diktatura, do armády dostaly velké množství peněz, probíhali tam nepokoje v té době, součástí Súdánu je Dárfúr, taky hodně známé místo

a myslím si, že ta šance na teroristický útok tam byla velmi vysoká i ty složky se na to připravovali, na potlačení nepokojů, ať už protivládních, nebo s lidmi, co byli vnitřně vysídlení.“

R_{SA2} : „Já si myslím, že byli docela dobře připravení. Bohužel se to stalo, ale měli tam americké základny, takže oni dost vizuálně bojovali proti terorismu a jsou proti terorismu i když je to všechno na vážkách. Mají tam teroristické skupiny, které jsou proti Američanům a politické války, ale pokud někoho chytili jako teroristu, tak vzhledem k tomu, že je tam povolen trest smrti, tak se tam provádí veřejné popravy.“

R_{SAE} : „Celkem dobrá. V Abú Dhabí se stalo to, že v jednom obchodním Arabka pobodala Angličanku. Šla do obchodního centra, tam si ji vyhlídla, vůbec jí neznala, šla k ní a protože byla ze západu, byla bílá, tak jí pobodala. Zajímavé bylo to, že okamžitě udělali velikou akci. Všude jsou kamery, takže oni vlastně tu zfanatizovanou Arabku sledovali z obchodního centra, jak nastoupila do svého auta, hned zjistili značku auta, kam jela, to ještě jela dát uměle udělanou bombu ke dveřím doktora Egyptana, který měl americký pas. Všechno to měli zmapované a poté zveřejnili video, jak komando vpadlo do její vily, jak je tam všechny zajistili a během tří, čtyř dnů byla ta útočnice veřejně popravena.“

Otázka č. 8 zní: „Vnímáte významný rozdíl v bezpečnosti v ČR a v místě stáže/mise?“



Obrázek 46. Bezpečnostní rozdíl Zdroj: Vlastní

Z grafického znázornění na obr. č. 46 vyplývá, že respondenti vnímají významný rozdíl v bezpečnosti, kromě R_{SRN} , kde rozdíl v bezpečnosti není tak výrazný.

R_{AFG} : „Nejde to srovnat, nemohu to posoudit, mám zkušenosti z mnoha států i v Africe. V Afghánistánu to ovlivnil Sovětský svaz, když tam dosadili se Sovětským svazem kolaborujícího afghánského komunistu – Nadžibulláha – jako prezidenta, domnívali se, že to bude jednou další stát Sovětského svazu. Když se ale rozpadl v Evropě, stahovali

se odtamtud vojáci. Je jasné, že Talibánci budou vyvážet svoje revoluční snahy ven, tak jako komunisti z Kuby a Severní Ameriky vyváželi ven revoluci. Časem bylo jasné, že tam budou muset zasáhnout mezinárodní síly, které budou zajišťovat pořádek. Řekl bych, že Afghánistán se nijak více nelišil od Iráku.“

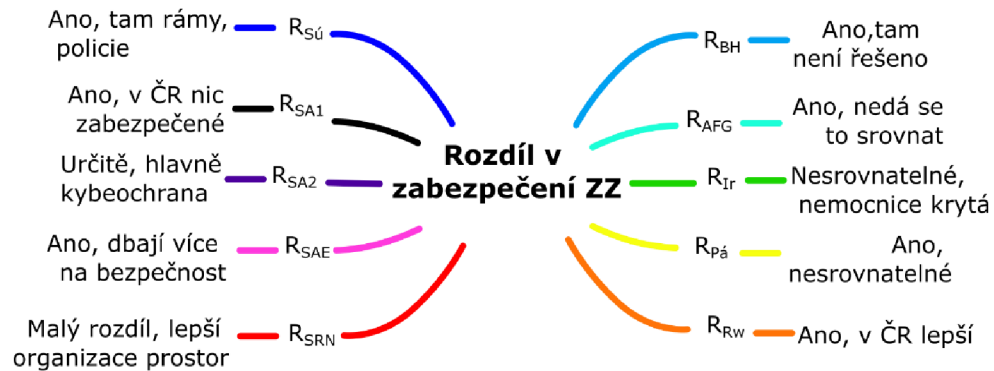
R_{Ir}: „Naprostě nesrovnatelné státy, já to ani nemohu posoudit, protože já trvale jezdím do mnoha států, do Asie, do Afriky od rovníku dolů, tam se nějak nebojuje, značně nebezpečná je Středoafriická republika a Demokratická republika Kongo, tam je to na pováženou. Ty státy jsou neevropské, ale jinak velice bezpečné, nic se tam neděje. A některé státy v Africe jsou velmi proevropské, například Namibie, to je velmi pro euroamerický stát, i ta morálka společnosti je stejná jako u nás. To se ale nedá říct o těchto státech, jako je Irák, ti lidé tam jinak přemýšlejí, mají svou kulturu, která se vyvinula jinak než naše kultura. Pro srovnání Afrika kulturu žádnou nemá, všechno jim tam bylo dodáno z Evropy, čili od rovníku dolů lidi vychovali Evropané. Namibie byla německá, Botswana byla britská, a od toho se to odvíjí. Angola a Mosambik byly portugalské, severní Mosambik tam jsou národně osvojenecké boje, ale jinak jsou to bezpečné státy. A oproti tomu všechny ty arabsko-perské oblasti a afghánské oblasti, tam byl jiný systém. Takže je to něco úplně jiného. Tady buďme rádi za to, kde žijeme, tohle je úžasná země k životu, oproti Iráku, Afghánistánu, tam když pošlete ráno dítě do školy, tak si na padesát procent nejste jistí, jestli se vrátí domů. V některých zemích vůbec nevíte, jestli druhý den budete mít nějaké sousto, jestli vás někdo nezabije. Buďme rádi, lidé tady nadávají, ale to je tím, že si zvykli. Ta účast na misích vám úplně přeskupí hodnoty, máme štěstí na to, v jaké zemi jsme se narodili.“

R_{RW}: „Rwanda sousedí se státy, které mají špatnou bezpečnost, konkrétně demokratická republika Kongo, neustále tam probíhají příhraniční nepokoje, je tam nízká bezpečnost, občas, i v době, kdy jsem tam byl na stáži, tak je tam nějaký bombový útok v hlavním městě, nebo ve větších městech. To se týkalo většinou voleb, souviselo to s opozicí, ale o žádném útoku na zdravotnické zařízení nevím. Co se týče bezpečnosti, rozhodně má Česká republika mnohem vyšší úroveň.“

R_{Sú}: „Určitě. Noční vycházení bylo nebezpečné, některá místa byla nebezpečná. Všude byla přítomnost vojáků a policajtů v mnohem vyšší míře. Byli ozbrojeni, navíc to bylo v době uzákoněné Šarí'a, takže i pro ženy to bylo jiné místo, než jsme zvyklí tady.“

R_{SAE}: „Ano, vnímám. Upřímně vám řeknu, že raději bych šla ve tři hodiny ráno v Emirátech, v Abú Dhabí než tady.“

Otázka č. 9 zní: „Vnímáte rozdíl v zabezpečení zdravotnických zařízení v ČR a v místě stáže/mise? Jaký?“



Obrázek 47. Rozdíl v zabezpečení ZZ v ČR a v místě stáže/mise Zdroj: *Vlastní*

Grafické znázornění na obr. č. 47 ukazuje, že respondenti vnímají rozdíl v zabezpečení ZZ v místě stáže/mise a v ČR.

R_{BH}: „V ČR velmi dobře fungují security, když přijde někdo podivný, tak zavolají policii. Mně přijde, že tam (v Bosně a Hercegovině, pozn. autorky) toto vůbec neřeší.“

R_{SÚ}: „Určitě, tam byli kontroly na vstupu, které se podobaly kontrolám na letišti u nás. Detekční rámy, kontrolovalo se oblečení, kapsy. Na vstupech hlídala policie nebo armáda.“

R_{SA1}: „Ano. V ČR není nic zabezpečené, pokud dojde k pouhému napadení personálu pacientem pomoci se neodvoláte, teroristický útok si vůbec nedovedu představit. Byl by to absolutní masakr.“

Otázka č. 10 zní: „Zažil/a jste teroristický útok? Byla přítomna odezva? Jak probíhala?“



Obrázek 48. Teroristický útok v zahraničí Zdroj: Vlastní

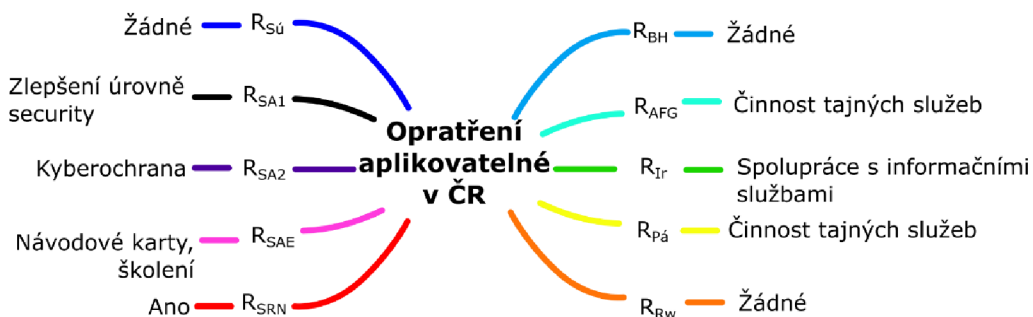
Z grafického znázornění na obr. č. 48 vyplývá, že jen jeden z respondentů zažil teroristický útok, respondenti v Iráku a Afghánistánu však mají zkušenosti s válečnými útoky.

R_{AFG}: „Že by někdo cíleně zaútočil, to ne. Útočili na základnu, rozbili nám vybavení, ale za terorismus to nepovažuji. My jsme zažili útoky a nejsme si jistí, zda to lze považovat za teroristické útoky, protože my jsme nebyli civilní osoby.“

R_{SA1}: „Ano, ostřelování raketami ze vzduchu. Odezva byla okamžitá, dopadla pouze jedna střela, dalších 52 zneškodněno ještě ve vzduchu.“

R_{SA2}: „Na vlastní kůži ne, neviděla jsem nikoho vybuchnout, ale zažila jsem to v nemocnici, kdy nám vozili právě z toho útoku pacienty, takže jsme den a dvě noci operovali lidi, který byli zranění tím útokem.“

Otázka č. 11 zní: „Myslíte si, že nějaké prvky zabezpečení přítomné v místě Vašeho pobytu jsou aplikovatelné i v ČR?“



Obrázek 49. Opatření aplikovatelná v ČR Zdroj: Vlastní

Grafické znázornění na obr. č. 49 ukazuje, že v Bosně a Hercegovině, ve Rwandě a Súdánu nejsou žádné prvky zabezpečení, které by byly aplikovatelné v ČR. Podle

respondentů z Afghánistánu, Iráku a Pákistánu jsou to činnosti tajných služeb a spolupráce s nimi. Podle respondentů ze Saudské Arábie je to zlepšení úrovně security a kyberochrany. Podle respondenta ze Spojených arabských emirátů jsou to školení a návodové karty, podle kterých budou zaměstnanci vědět, jak se zachovat. Podle respondenta ze Spolkové republiky Německo lze nějaké prvky zabezpečení aplikovat v ČR.

R_{BH}: „Nic. Nevím, jestli jako prvek ochrany říct, jak se lidé chovají. Přejde mi, že jsou tam lidé slušnější, mají větší úctu ke zdravotníkům.“

R_{Pá}: „Myslím si, že především je to o činnosti tajných služeb. My jsme museli spolupracovat s Tálibánci i s lidmi, kteří později vytvořili Islámský stát. Po válce někteří lovci nacistů, kteří je chtěli chytit, tak museli spolupracovat s jinými nacisty, kteří jim to prozradili. Je to výhoda, protože o spoustě věcech se dozvíte dopředu. Usáma bin Ládín, když ho chytili, tak jsme si uvědomili, že jsme jezdili kolem jeho domu, měl dům obehnaný dráty, ale to tam má každý druhý. A dopadli ho po spolupráci s podplacenými lidmi. Takle agenturní činnost je skoro nejlepší. Lidé si představují jako nejlepší obranu zeď, dráty, střely namířené, ale já si myslím, že nejdůležitější je vědět o tom dopředu. Izrael díky spolupráci a díky tomu že má všude špičkové odhalí 99 ze 100 hrozcích útoků. To považuji za úplně nejdůležitější. Žádná velká hradba, velká střecha, protiatomová zábrana nefunguje, Je to také samozřejmě důležité.“

R_{SÚ}: „Já si myslím, že Česká republika je mnohem rozvinutější stát a má mnohem propracovanější systém bezpečnosti než Súdán, takže Súdán se pokouší vlastními silami, tak jak je na té úrovni schopen a pro nás by taková bezpečnost smysl neměla. Aby nás kontrolovala armáda kolem areálu a všichni procházeli přes detektor. Myslím si, že se nacházíme na úplně jiné úrovni státní stability, že to není třeba.“

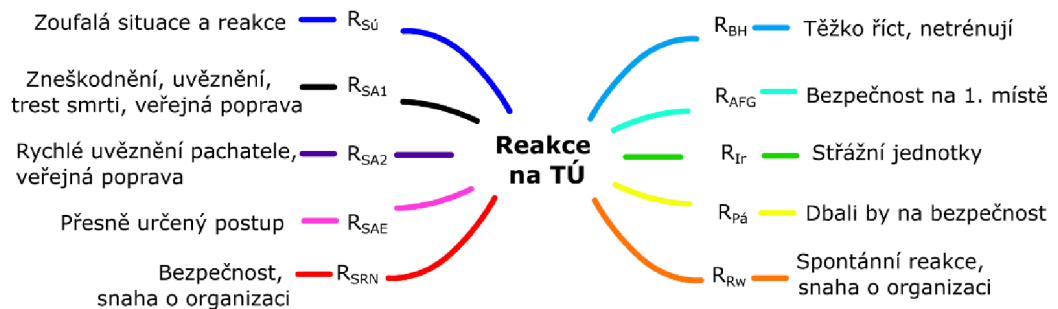
R_{SA1}: „Ano, minimálně pořádná security služba v nemocnici, která je kdykoliv dosažitelná, a hlavně vykonávána lidmi k tomuto zdravotně a fyzicky způsobilými. Stařík na recepci je nedostačující.“

R_{SA2}: „Já teda věřím, že ano, protože si myslím, že kódový systém měl určitě význam, nedokážu si to představit tady, když něco bouchne, protože vždycky vznikne panika a lidi nevědí v tu chvíli, co mají dělat. A tomu právě napomáhaly ty karty, které jsme měli a tam skutečně krok po kroku bylo napsané, jak postupovat, protože pracujeme v kolektivu. Vždy byl určený někdo, kdo vedl skupinu. My jsme fungovali podle amerického systému

a oni mají různé kódy a k nim jsou přesně dané instrukce, jak postupovat, pokud se něco stane. Těch kódů bylo 10. Code black je černý kód v případě bombového útoku v externím teroristickém nebezpečí, takže je krok po kroku popsán na kartě, co se musí dělat, kam se to hlásí, pokud někdo něco zjistí, že je někdo v nějakém nebezpečí nebo je venku nebezpečí. Code blue znamená zástavu krevního oběhu. Když byli na emergency lidé agresivní, tak se zavolal code white na dané telefonní číslo, které bylo všem známé, to spojilo security a ti přišli okamžitě na pomoc na dané místo. Oni měli pravomoci zpacifikovat ty lidi. Nejdřív mluvili, oni na to byli školení a případně je zpacifikovali.... Nedokážu si to představit tady, protože jsem tady třetí rok a nic podobného jsme nezažili a neprobíhá ani školení. Tam jsme se školili každý rok a každý rok to bylo povinné, dělali zápisy a každý zápis měl zaměstnanec ve své složce.“

R_{SRN}: „Ano. Vstup na čip/pouze přes recepci považuji za dobrý prvek. Člověk z venku se dostal dovnitř, buď protože měl kartu zaměstnance nebo si musel zavolat na recepci, představit se a říct, co potřebuje, aby byl vpuštěn do objektu. Na druhou stranu ale šlo o malou kliniku s menší fluktuací příchozích a odchozích. Jako pozitivní také vnímám uspořádání kliniky – nejprve recepce, poté čekárna.“

Otázka č. 12 zní: „Jak by se v místě stáže/mise zachovali v případě teroristického útoku?“



Obrázek 50. Reakce na teroristický útok v zahraničí Zdroj: Vlastní

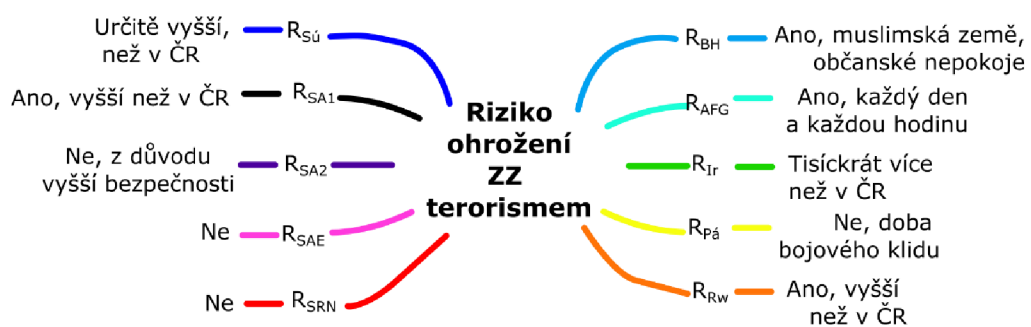
Z grafického znázornění na obr. Č. 50 vyplývá, že v Bosně a Hercegovině, ve Rwandě a v Súdánu by reagovali spontánně, nejsou připraveni na takový útok. V Afghánistánu, Iráku a Pákistánu by dbali hlavně na bezpečnost a vyslali by strážní jednotky k ohledání místa útoku. V Saudské Arábii a Spojených arabských emirátech je známá jasná a rychlá reakce. Ve Spolkové republice Německo není přesně určen postup, ale dle respondenta by se projevila snaha o organizaci zaměstnanců a evakuaci pacientů s ohledem na vlastní bezpečí.

R_{BH} : „Zavolali by policii, utekli by, schovali by se. Těžko říct. Oni tam na to vůbec netré-
mují, neřeší to a trochu se bojím, co by se mohlo stát. Tam mají dvě sanitky na město
o rozměru Plzně, takže tam by ani nebyly prostředky, jak to řešit.“

R_{AFG} : „Tam jsou strážní jednotky tak ty by obšacovaly celou oblast okamžitě, ti, co mají
aktivní službu, by vyjeli do okolí a snažili by se udělat co největší ochranný perimetr,
jinak se to řeší tak, když tam něco bouchne, aby se dbalo na bezpečnost, záchrana lidí
není na prvním místě, důležitější je opatrnost, jestli nehrozí nějaký sekundární potenco-
nální výbuch, takže když někdo vyhodí auto do povětří, to se převrátí a sjedou se tam
armádní jednotky. Když by někoho začali vyprošťovat, tak je možné, že je někdo sleduje
a spustí daleko silnější výbuch, který ohrozí nebo zraní co největší počet lidí. Když je
někde vidět mrtvolu, která zapáchá někde okolo základny, tak musí přijet odminovací vo-
zidlo, to mu zapráhne za nohu řetěz a popojedou a odtáhnou ji, protože je nebezpečí, že
v její blízkosti byla uložena mina nebo bomba. To samé je se zbrani na zemi, nesmí se
toho nikdo dotýkat. Musíme být velice opatrní a počkat až se zabezpečí místo. V první
řadě jezdí pyrotechnici.“

R_{RW} : „V tomhle místě by to probíhalo zcela spontánně, pacienti by se začali evakuovat,
utíkat, mezitím by sestry projevili snahu o organizaci a asistenci těm, kteří nejsou mobilní.
Vedoucí toho zdravotnického střediska byla vrchní sestra, záleželo by na její organizaci.
Když jsem tam pracoval, tak nebyl zpracovaný žádný plán nebo standard, podle kterého
by se postupovalo. Pravděpodobně by byla zachovalá hierarchie vedení, ale bez předem
daného plánu. Pacienti by se evakovali na fotbalové hřiště se stadionem.“

Otázka č. 13 zní: „Bylo zdravotnické zařízení ohroženo teroristickým útokem častěji
než v ČR?“



Obrázek 51. Riziko ohrožení terorismem v porovnání s ČR Zdroj: Vlastní

Z grafického znázornění na obr. č. 51 vyplývá, že v Bosně a Hercegovině, Afghánistánu, Iráku, Rwandě, Súdánu a v Království Saudské Arábii (R_{SA1}) existuje častější ohrožení ZZ než v ČR. V Pákistánu nebylo ZZ ohroženo častěji z důvodu bojového klidu. Dle R_{SA2} není ZZ v Království Saudská Arábie ohroženo teroristickým útokem častěji než v ČR z důvodu vyšší bezpečnosti. Ve Spojených arabských emirátech a Spolkové republice Německo nejsou ZZ ohrožena častěji než v ČR. Odlišná odpověď obou respondentů může být zdůvodněna pobytem v jiném časovém období. R_{SA1} cca 2006–2016 a R_{SA2} cca 2000–2004.

R_{BH}: „Ano, myslím si, že je větší riziko, protože Bosna je muslimská země. Je tam silná enkláva ze Saudské Arábie, začínají se tam stěhovat, protože je tam mnoho mešit. Riziko je tam vyšší také kvůli občanským aspektům, protože jsou tam Srbové, Bosňané a Chorvati, a ti se spolu nesnášejí a stát se to může, že tam dá někdo někomu bombu do auta a podobně.“

R_{Pá}: „Tak tisíckrát více. Každý den a každou hodinu. Těžko rozlišit teroristický útok a útok vojenské napadení v rámci národního boje. Je to jiná situace a nesnese to srovnání s naším státem. V Madridu například byli velmi překvapení, to evropský stát nečeká.“

R_{RW}: „Vzhledem k tomu, že je tam větší politická nestabilita, tak si myslím, že určitě.“

R_{Sú}: „Určitě. Politická nestabilita, diktatura, prezident, který je obviněný u mezinárodního tribunálu. Takže ta šance na teroristický útok je mnohem vyšší.“

6 Diskuse

Současnou situaci v ČR lze považovat za bezpečnou, je však potřeba upozornit, že nikdo a nikde není proti terorismu imunní. Z tohoto důvodu je velmi důležitá prevence a připravenost správně zareagovat. Na místě je otázka: „*Kdy, kde, jak se to stane a co jsme udělali, abychom útoku předešli*“. Již se neptáme, zda se teroristický útok stane (Procházková, 2014). Ve společnosti a v mysli spousty občanů, včetně zdravotníků jsou prevence a zabezpečení často podceňovány, jak bylo zjištěno od respondentů v dotaznících. Opačným názorem je, že dostatečnou připraveností a prevencí lze snížit mnohdy katastrofické následky útoku, a to jak materiálně, tak i ve smyslu počtu obětí a zraněných osob.

Diplomová práce se zabývá kvantitativním způsobem zpracování dat metodou dotazníků a věnuje se analýze zabezpečení zdravotnických zařízení (ZZ) a zkušenosti s útoky. Zabývá se také kvalitativním výzkumem metodou polostrukturovaných rozhovorů a věnuje se analýze rozdílů v zabezpečení ZZ a zkušenosti s útoky v ČR a ve vybraných státech Afriky, Asie a Evropy. Výzkumná část diplomové práce se zabývala zkoumáním odpovědí na dotazníkové šetření ze strany zaměstnanců nemocnic v ČR a zkoumáním odpovědí na polostrukturované rozhovory ze strany zaměstnanců nemocnic v ČR se zkušeností práce v zahraničí. Odpovědi na jednotlivé otázky dotazníkového šetření jsou zpracovány v kapitole 5.2. *Výsledky dotazníků*. Odpovědi na jednotlivé otázky polostrukturovaných rozhovorů jsou rozpracovány v kapitole 5.3. *Výsledky polostrukturovaných rozhovorů*. Celkové zhodnocení získaných dat je popsáno v následujících částech diskuse.

Diskuse je rozdělena do dvou částí. První část diskuse se vztahuje k cíli práce č. 1 Analýza zabezpečení vybraných zdravotnických zařízení a jejich zkušenosti s teroristickými a kyberteroristickými útoky a výzkumným otázkám VO1 „*Je zabezpečen vstup do zdravotnického zařízení?*“ VO2 „*Jaké jsou zkušenosti zdravotnického zařízení s teroristickými a kyberteroristickými útoky?*“ VO3 „*Zúčastnili se zaměstnanci zdravotnického zařízení školení na nácvik reakce na teroristický útok?*“. Druhá část diskuse pojednává o výsledcích vztahujících se k cíli práce č. 2 Analýza rozdílů v ohrožení a zabezpečení zdravotnických zařízení v ČR a vybraných zahraničních státech.

6.1 Diskuse vztahující se k cíli práce č. 1

Prvním cílem diplomové práce je **analýza zabezpečení vybraných zdravotnických zařízení a jejich zkušeností s teroristickými a kyberteroristickými útoky** a zodpovědět na výzkumné otázky **VO1: „Je zabezpečen vstup do zdravotnického zařízení?“ VO2: „Jaké jsou zkušenosti ZZ s teroristickými nebo kyberteroristickými útoky?“ VO3: „Zúčastnili se zaměstnanci zdravotnického zařízení školení na nácvik reakce na teroristický útok?“**. K naplnění tohoto cíle bylo potřeba provést šetření pomocí dotazníků. Z vyhodnocení získaných dat vyplynulo následující.

6.1.1 Zabezpečení vstupu do ZZ

Zabezpečení ZZ souvisí s pocitem bezpečí jednotlivých respondentů, s přítomností efektivní spolupráce s pracovníky ochrany, s přítomností bezpečnostních rámců u hlavního vchodu a u vstupu na oddělení a zabezpečení vstupu pro zaměstnance. Největší počet, tj. 41,5 %, respondentů (83/200) se cítí ve svém ZZ spíše bezpečně, pouze 6,5 % (13/200) respondentů se necítí bezpečně. Ve většině případů, tj. 71,5 % (143/200), pracují ve ZZ pracovníci ochrany, kteří jsou ve většině případů, tj. 50,3 % (72/143) schopni v relativně krátkém časovém úseku (5–10 minut) dorazit na místo zásahu. Neméně důležitá je i znalost telefonního čísla na pracovníky ochrany, kteří mohou zajistit dorážení na místo zásahu a schopnost je v případě nutnosti přivolat. Z respondentů, kteří odpověděli „Ano“ 71,5 % (143/200), většina, tj. 84 % (120/143), je schopná je přivolat. Ve většině ZZ, tj. v případě 84 % (168/200) responzí, se u hlavního vchodu nenachází bezpečnostní rámy. S těmi se setkáváme jen ve 2,5 % případů (5/200).

Vstup pro personál není ve většině případů (72,5 %, tj. 145/200) oddělený od vstupu pro běžné občany a pacienty. Největší počet respondentů uvedl, že vstup do ZZ není nijak zabezpečen, a to 39 % (78/200). Ve 21 případech z 200 (10,5 %) hlídá vchod ostraha. Z předchozí otázky je patrné, že ve většině ZZ se nachází ostraha (71,5 %, 143/200), ale tato otázka ukazuje, že není jejím úkolem ve všech těchto ZZ hlídat vchod, který hlídá pouze v 10,5 % (21/200) případů. Ve 22 % (44/200) responzí je vstup označen a je možné jej otevřít pouze na čipové karty, které vlastní zaměstnanci. Podle 11,5 % (23/200) respondentů je vstup označen a odemyká se klíčem, který vlastní zaměstnanci.

Na **VO1: „Je zabezpečen vstup do zdravotnického zařízení?“** lze odpovědět takto: Ve většině případů není vstup do ZZ zabezpečen a nenachází se u něj bezpečnostní rámy.

Vstup pro personál není ve většině případů oddělen ani zabezpečen. Ve většině ZZ se nachází ochranka, která je schopna v krátkém časovém úseku dorazit na místo zásahu. Úkolem ochranky však není hlídat vchod do ZZ.

Předpoklad zodpovězení VO1 byl, že vstup není zabezpečen pomocí bezpečnostních rámu, ale že jej hlídá ostraha objektu (ochranka). Vstup pro personál by měl být zabezpečen pomocí čipů nebo klíčů. **Předpoklad nebyl z větší části naplněn**, bylo zjištěno, že se ve ZZ nachází ostraha, ale ve většině případů nehlídá vstup. Důvodem nenaplnění předpokladu může být spoléhání se na kamerový systém.

6.1.2 Zkušenosti ZZ s teroristickým nebo kyberteroristickými útokem

Nejdříve bylo zjišťováno hodnocení připravenosti ZZ z pohledu respondentů. Většina respondentů, tj. 53,5 % (107/200) zde uvedla, že připravenost ZZ na teroristický útok je nedostatečná. Podle 24,5 % (49/200) respondentů je dostatečná, podle 19 % (38/200) je dobrá a výborně ji hodnotí pouze 3 % (6/200) respondentů.

Dále bylo zkoumáno, zda respondenti ví, jak se zachovat v případě teroristického útoku. Většina respondentů, tj. 69 % (138/200) uvedla, že by dbala na svou bezpečnost, kontaktovala svého nadřízeného a řídila se jeho instrukcemi. To se dá považovat za správnou odpověď v případě, kdy nadřízený umí zorganizovat činnosti vedoucí ke zvládnutí teroristického útoku. To jest zajistit bezpečí zaměstnanců, kontaktovat PČR a evakuovat ohrožené pacienty a zaměstnance. Evakuační plán by měl být součástí každého ZZ, popř. traumatologického plánu (dokumentace). Kromě těchto dokumentů existují tzv. Soubor typové činnosti (STČ) pro integrovaný záchranný systém (IZS), kde je zpracována problematika „aktivního střelce“ (STČ 14), „Špinavá bomba“ (STČ 1) a „nález nástražného výbušného systému podezřelého předmětu, munice, výbušnin a výbušných předmětů.“ (STČ 3), které s terorismem úzce souvisí. Nejlepším řešením v případě teroristického útoku na ZZ by byla karta s algoritmem, pomocí kterého je popsán seznam úkonů, které se musí provést, aby se zamezilo velkým škodám (podobně jako karty pro velitele u STČ). A to z důvodu, že stresující situace ovlivňují rozhodovací schopnosti a psychický stav lidí. Přičemž i zaměstnanci, kteří nyní ví, jak se zachovat ve chvíli teroristického útoku mohou znejistit a nepodniknout některé důležité kroky. V některých ZZ jsou používány tzv. příručky, jak uvedlo 6,5 % (13/200) respondentů. 17,5 % (35/200) respondentů uvedlo, že neví, jak se zachovat. U této odpovědi byl předpoklad responzí vyšší, vzhledem k nedostatečným zkušenostem s útoky a s malým počtem probíhajících školení

(viz kapitola 6.1.3. *Školení na nácvik reakce na teroristický útok*). V 7 % (14/200) případů zde byla zvolena odpověď „*Jiná*“, v níž respondenti popisovali jiné způsoby, jak se zachovat při probíhajícím teroristickém útoku. V těchto odpovědích se objevilo 2× správně kontaktovat PČR na tel. čísle 158. V jednom případě „*dovolání silových složek na místo*“, předpokládáme, že respondent měl na mysli také PČR. názor, že by bylo vhodné bojovat s útočníkem se zde objevil 2×. Tento názor nelze považovat za vhodné řešení, z důvodu bezpečnostního rizika, pokud daný respondent není odborně způsobilý (příslušník PČR), což vzhledem k výzkumnému vzorku nelze předpokládat.

Setkání respondentů s teroristickým útokem proběhlo podle 4,5 % respondentů (9/200). Pro předpoklad malé zkušenosti setkání s teroristickým útokem byla přidána možnost, týkající se sledování útoků respondenty v médiích, či z doslechu. Teroristický útok v médiích sledovalo 42,5 % (85/200) respondentů. O teroristickém útoku na nemocnici slyšelo 12,5 % (25/200) respondentů. Žádným způsobem se s teroristickým útokem neseťkalo 40,5 % (81/200) respondentů. Dále, na otázku týkající se odezvy na teroristický pokračovalo 59,5 % (119/200) respondentů, kteří se setkali s teroristickým útokem přímo, v médiích nebo o teroristickém útoku „*slyšely*“. Co se týče odezvy na teroristický útok, většina respondentů, tj. 51,3 % (61/119) neví, zda a jak proběhla.

Z důvodu předpokladu malého počtu respondentů, kteří se setkali s teroristickým útokem, bylo zkoumáno jejich setkání s útokem na měkké cíle a s tím související setkání s agresivním pacientem. Útok na měkké cíle zažilo 8,5 % (17/200) respondentů a ve 3,5 % (7/200) byla přítomna odezva.

V souvislosti s teroristickým útokem může jít také o motivaci a psychologický profil útočníka. Toto téma přesahuje rozsah této práce, ale zabývá se jím ve své knize Procházková (2014), dle které je důležitý profil a osobnost teroristy. Hrají zde roli pocity křivdy, zranitelnost a náchylnost k negativním vnějším vlivům a vlivům prostředí. Profilem útočníka se okrajově zabývá i de Cauwer *et al.*, (2017) podle kterého je teroristou pravděpodobněji nečekaný člověk pro lidi s předsudky, který může být i vysoce vzdělaný. Z agresivního člověka se může stát útočník na měkké cíle nebo terorista. Také se v našich podmínkách setkáváme mnohem častěji s agresivním pacientem, než s teroristickým útokem nebo útokem na měkké cíle. Tento může atakovat personál a způsobit i ztráty na životech (viz kapitola 1.4 *Útoky na ZZ v souvislosti s terorismem*). Dvě třetiny útočníků

měli dle výzkumu v USA v minulosti příznaky duševního zdraví, včetně depresivních, sebevražedných a psychotických příznaků. (Department of Homeland Security, 2019)

Z těchto důvodů byla tato výzkumná otázka rozšířena na setkání respondentů s agresivním pacientem. Většina respondentů 87,5 % (175/200) se setkala s agresivním pacientem. Většina responzí ukazovala, že se 31 % (62) respondentů setkalo s agresivním pacientem častěji než 2× za rok. Stejný počet, tedy 31 % (62), respondentů se setkal s agresivním pacientem méně než 1× za rok. Častěji, než 1× za 3 měsíce se s agresivním pacientem setkalo 25,5 % (51) respondentů.

Další otázky zjišťovaly zkušenost s reakcí na setkání s agresivním pacientem. Většina respondentů, tj. 40 % (70/175) uvedlo, že si poradili bez nutnosti přivolání PČR. Tito respondenti poté odpovídali na podrobnější otázku, která zjišťovala, jak si s agresivním pacientem poradili. Většina respondentů, tj. 21 % (30/70) přivolala lékaře pro podání medikace (antipsychotik nebo jiné). Pouze o jednoho respondenta méně (20,3 % 29/70) měla odpověď „*upoutáním na lůžko dle platných ošetrovatelských standardů*“. Tyto standardy se v každé nemocnici liší.

Co se týče kyberteroristického útoku, většina respondentů, 83 % (166/200) se s ním neseťkala. Setkání s kyberteroristickým útokem potvrdilo 17 % (34/200) respondentů. Ti, kteří se s kyberterorismem setkali, pokračovali na upřesňující otázky. Většina respondentů tj. 29,4 % (10/34) uvedla, že následek kyberteroristického útoku byl výpadek dokumentace. Podle většiny respondentů (38,2 %; 13/34) čekalo ZZ na správné fungování několik dní. Dobře a bez velké ztráty dat se s kyberteroristickým útokem vyrovnalo ZZ podle většiny (64,7 %; 16/34) respondentů. Ve většině případech, tj. 47,1 % (16/34) byla ohrožena data.

Na VO2: „*Jaké jsou zkušenosti ZZ s teroristickými nebo kyberteroristickými útoky?*“

lze odpovědět takto: Podle většiny respondentů je ZZ nedostatečně připraveno na teroristický útok, většina respondentů by v případě teroristického útoku kontaktovala nadřízeného a dbala na svou bezpečnost. Většina respondentů se s teroristickým útokem neseťkala, ale sledovala ho v médiích a neví, jak probíhala odezva. Většina respondentů se setkala s agresivním pacientem v různých časových intervalech, nejčastěji méně, než 1× za rok a více než 2× za rok. Většina respondentů se neseťkala s kyberteroristickým útokem. Přesto se s kyberteroristickým útokem setkalo více respondentů než s jiným teroristickým útokem. Ti, co se setkali s kyberteroristickým útokem, uvedli, že nejčastějším

následkem byl výpadek dokumentace, čekali několik dní na správné fungování ZZ, které se nejčastěji s útokem vyrovnalo dobře, bez velké ztráty dat nebo omezení funkčnosti. Nejčastěji byla kyberteroristickým útokem ve ZZ ohrožena data.

Předpoklad zodpovězení VO2 byl, že zařízení je nedostatečně připraveno na teroristický útok z důvodu malých zkušeností s tímto a podobným útokem. Většina respondentů zvolí správný a logický postup v případě události spojených s terorismem. Respondenti se nesetkají s terorismem ani s útokem na měkké cíle, ale pravidelně se budou setkávat s agresivními pacienty nebo občany. Při setkání s agresivním pacientem respondenti přivolají PČR. S kyberteroristickým útokem se respondenti ve většině případů nesetkají, a v případě takových útoků bude většinou cíleno na data. Tento předpoklad **byl z většiny naplněn**. V bodě přivolání PČR respondenty není předpoklad naplněn, a to z případného důvodu dobré funkčnosti medikace agresivních pacientů, pokud lze podat, velké vzdálenosti stanice PČR od nemocnice, dobrého fungování ostrahy nebo špatných zkušeností se spoluprací s PČR.

V roce 2005 a 2006 byl proveden výzkum týkající se zlepšování připravenosti nemocnic na teroristický útok v USA. Týkal se sester a lékařů na pohotovosti (77 účastníků). Účastníci studie důsledně vyjadřovali názor, že ani emergency, ani nemocniční zařízení nejsou dostatečně připraveny na teroristickou událost zahrnující radioaktivní materiály. Klíčové obavy lékařů zahrnovaly možnost zahlcení nemocnice, bezpečnost blízkých, potenciální personální problémy, problémy s připraveností a sebeobranou. Účastníci rovněž vyjádřili potřebu dalších informací, např. rozšíření dokumentace (Becker a Middleton, 2013). Tento výzkum získal podobné výsledky s touto prací.

6.1.3 Školení zaměstnanců na nácvik reakce na teroristický útok

Nejdříve byla zjišťována obeznámenost respondentů s opatřeními proti terorismu, přičemž většina respondentů, tj. 46 % (92/200) obeznámena není. Školení ve většině případů (62 %; 124/200) neprobíhá. V 15 % (30/200) školení probíhá a ve 12 % (24/200) probíhá školení v rámci BOZP (Bezpečnost a ochrana zdraví při práci). Respondenti, v jejichž pracovišti probíhá školení i v rámci BOZP pokračovali na podrobnější otázky 27 % (54/200). Většina respondentů, tj. 54 % (29/54) uvedla, že školení probíhá jednou za rok. Dle většiny respondentů, (79,65 %; 43/54) se školení účastní všichni zaměstnanci. Školení se zúčastnilo 63 % (34/54) respondentů, z nichž 76,5 % (26/34) jednou a 23,5 % (8/34) vícekrát. Těchto 34 respondentů se týkala otázka zkoumající

hodnocení školení. Většina respondentů, tj. 41,2 % (14/34) hodnotí školení velmi kladně. Většina respondentů, tj. 80,5 % (161/200) by školení na nácvik reakce na teroristický útok uvítala. Z těchto 161 respondentů by většina, tj. 72 % (116/161) uvítala školení častěji.

Odpověď na VO3: „*Zúčastnili se zaměstnanci zdravotnického zařízení školení na nácvik reakce na teroristický útok?*“ je: Většina respondentů uvedla, že se u nich na pracovišti školení nekoná a že nejsou obeznámeni s opatřeními proti terorismu od jejich zaměstnavatele. V případech, ve kterých školení probíhá se koná nejčastěji jednou za rok a účastní se jej všichni zaměstnanci. Většina respondentů, která uvedla, že se u nich školení koná, se školení účastnila a hodnotí jej velmi kladně. Většina respondentů by školení na nácvik reakce na teroristický útok uvítala.

Předpoklad zodpovězení VO3 byl, že se v ČR školení na nácvik reakce na teroristický útok nekoná, ale že zaměstnanci jsou obeznámeni s opatřeními proti terorismu od jejich zaměstnavatele – toto opatření je součástí traumatologických a evakuačních plánů. Předpoklad **byl z části naplněn**. Zaměstnanci nejsou obeznámeni s opatřeními proti terorismu z neznámých důvodů.

Školení sester v Izraeli zkoumá práce autorů Ron a Shamai (2014), kteří uvádí, že školení pravidelně probíhá a je pro všechny povinné. To může být z důvodu větší hrozby terorismu nebo válečného útoku v tomto státě. Přípravenost zdravotnických pracovníků v Pákistánu je dle 60 % (120/200) respondentů také nedostatečná a polovina respondentů by si v případě útoku na jejich ZZ poradila. 76 % (152/200) absolvovalo vzdělání v oblasti krizového řízení, ale nevěděli o krizovém plánování. Autoři zde doporučují zlepšit připravenost pomocí vzdělávání a cvičení sester a lékařů (Azeem *et al.*, 2019). Školení, lepší koordinaci a přiřazení jednotlivých úkolů také doporučují v USA, kde se této problematice věnovali z pohledu chemických útoků (Georgopoulos *et al.*, 2004). O upevnění reakce zdravotní péče na terorismus prostřednictvím procesů zmírňování, připravenosti, reakce a zotavení a o výuce „*protiteroristické medicíny*“ uvažují ve své práci Court *et al.*, (2020), kteří usilují o zavedení nového oboru, a to právě „*protiteroristické medicíny*“. Podle výzkumu v USA autorů Ganora a Wernliho (2013) nemá většina zaměstnanců nemocnic dostatečnou kvalifikaci, aby věděla, co dělat v případě teroristického útoku. Z těchto výzkumů vyplývá, že školení sester na tuto problematiku není problémem jen v ČR a v Evropě, ale také v USA, Pákistánu a Izraeli.

6.2 *Diskuse vztahující se k cíli práce č. 2*

Evropské země v této otázce jsou Spolková republika Německo (SRN) a východoevropská Bosna a Hercegovina, k asijským zemím řadíme Afghánistán, Pákistán, Irák, Království Saudská Arábie a Spojené arabské emiráty, mezi africké země pak patří Súdán a Rwanda, menší tropický stát.

Druhým cílem diplomové práce je **analýza rozdílů v ohrožení a zabezpečení ZZ v ČR a vybraných zahraničních státech**. K naplnění tohoto cíle bylo potřeba provést šetření pomocí polostrukturovaných rozhovorů. Z vyhodnocení získaných dat vyplynulo následující.

Podobný systém ochrany jako v ČR se nachází v druhém případě Saudské Arábie, Spojených arabských emirátech a SRN, kde hlavní prvek zabezpečení tvoří ochranka. Horší zabezpečení, a to z dostupných prostředků (oplocení, recepce), se nachází v Bosně a Hercegovině, Afghánistánu, Iráku a Rwandě. Zabezpečení pomocí ozbrojených sil se nachází v prvním případě Saudské Arábie, Súdánu a ve vojenské nemocnici v Pákistánu.

Zaměstnanci se ve většině zemí neškolí. Ve vojenských nemocnicích v Afghánistánu, Iráku a Pákistánu se školí jen vojáci, pro civilisty je zde obsaženo základní poučení o krytech a ochranných pomůckách, které mají k dispozici. V obou rezpozích z Království Saudské Arábie a ve Spojených arabských emirátech se zaměstnanci školí přísně, a to včetně zacházení se zbraněmi. V těchto případech funguje tzv. kódový systém dle USA. Terorismu se v těchto případech týká code Black – bombový útok a code Silver – aktivní střelec. V SRN probíhá školení v rámci BOZP, podobně, jako v ČR.

Všichni respondenti se v průběhu stáže cítili bezpečně, stejně jako se respondenti v ČR cítí bezpečně ve svém ZZ. V Bosně a Hercegovině, Afghánistánu, Iráku a Rwandě je minimální připravenost na teroristický útok. Pákistán, Spojené arabské emiráty a Království Saudské Arábie jsou nejlépe připravené státy na teroristický útok. V ČR je z pohledu zaměstnanců ZZ připravenost na teroristický útok nedostatečná.

Oproti ČR zažil respondent teroristický útok v Království Saudské Arábii, kde byla nemocnice ostřelována raketami, naštěstí z důvodu dobré obrany, a to sestřelováním raket, zabránili škodám. S útoky se také setkali respondenti v Afghánistánu a Iráku, zde se jedná spíše o za válečné útoky, jelikož respondenti nebyli civilní osobou.

Zásadní rozdíl v zabezpečení ZZ vnímají všichni respondenti, kromě respondenta ze SRN. V Bosně a Hercegovině a Rwandě je zabezpečení méně efektivní, než v ČR nebo žádné. V Súdánu, Království Saudské Arábie a Spojených arabských emirátech vnímají respondenti efektivnější zabezpečení ZZ před terorismem.

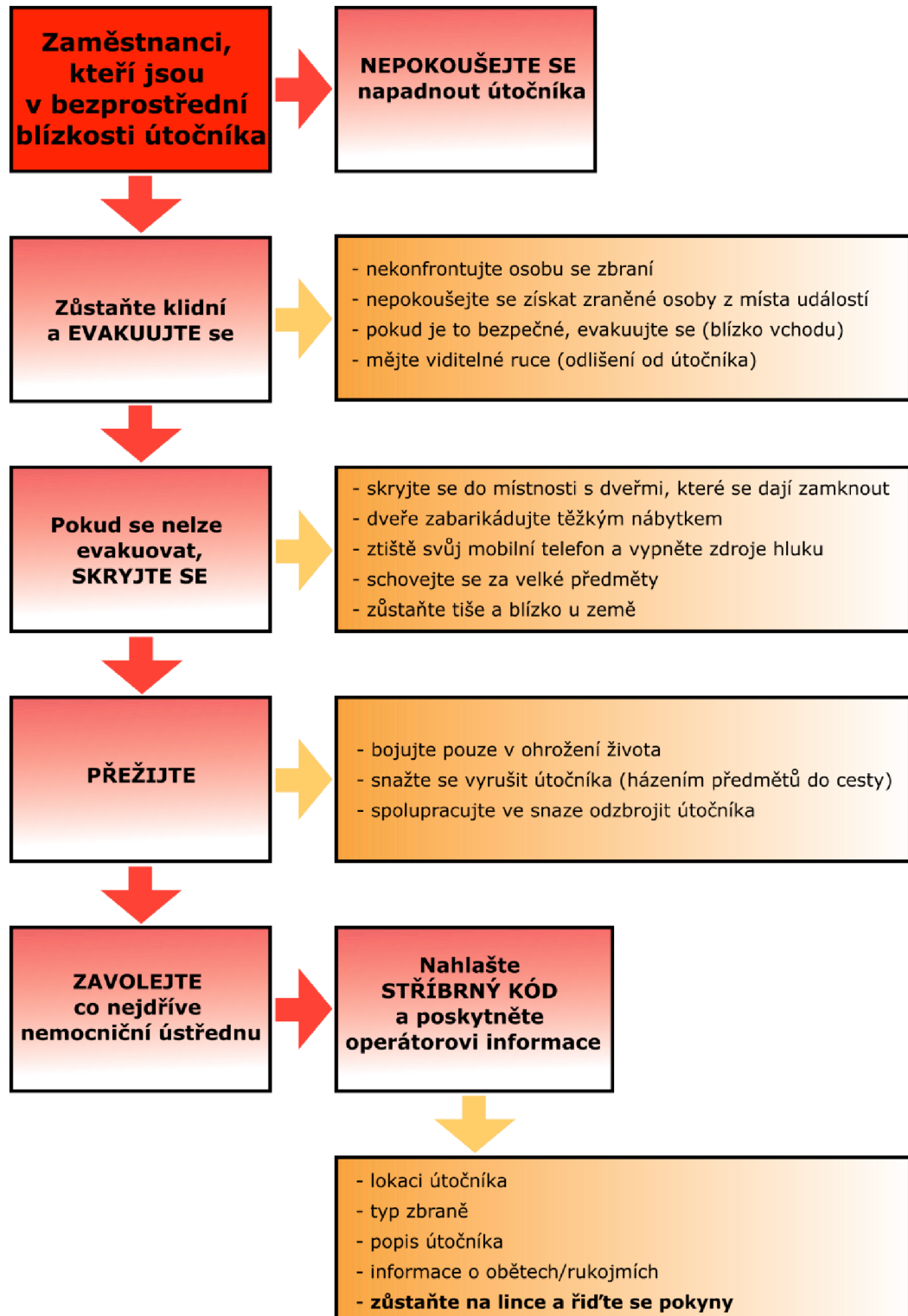
Ohrožení zdravotnického zařízení bylo ve většině případů větší než v ČR. V Pákistánu respondent pobýval v době bojového klidu, nebylo tam tedy vyšší ohrožení než v ČR. Větší riziko nevnímá ani respondent ze SRN. V jednom případě Království Saudské Arábie a ve Spojených arabských emirátech nebylo respondentem vnímáno ohrožení, a to z důvodu vysoké kvality zabezpečení ZZ.

Většina respondentů si myslí, že prvky zabezpečení jsou aplikovatelné v ČR. Doporučují spolupráci s tajnými informačními službami, dle kterých se dají teroristické útoky predikovat a dá se jim i včas zabránit. Zlepšení úrovně ochrany závisí na jednotlivých zařízeních. Zlepšení kyberochrany je velmi dobré doporučení, je však v působnosti IT specialistů a zaměstnanců jednotlivých ZZ. Doporučení školení a návodových karet vychází z kódového systému používaném v USA a Království Saudské Arábie. Tento systém lze připodobnit ke společným typovým činnostem STČ, které v ČR fungují na úrovni IZS a jsou prostředkem, jak spolu mohou jednotlivé složky IZS co nejlépe spolupracovat. Tento prvek lze podrobněji analyzovat a doporučit jeho aplikaci v jednotlivých ZZ.

Kódový systém používaný v USA zahrnuje velké množství událostí. Například požár, evakuaci, hromadné neštěstí, zástavu krevního oběhu, aktivního střelce, bombový útok, hromadný příjem raněných atd. K těmto kódům jsou vytvořeny návodové karty, které jsou dostupné pro všechny zaměstnance a podle kterých jejich držitelé ví, jak se přesně zachovat a koho kontaktovat. Pro využití v připravenosti na teroristický útok a útok na měkké cíle lze nejlépe využít Silver code, aktivní střelec a Black code bombový útok. Code Silver (stříbrný kód) je plánovaná reakce na zajištění bezpečnosti zdravotnických pracovníků, pacientů a návštěvníků v nemocnici, pokud má násilník zbraň a je vyžadována policejní reakce. Code Silver je volán v případě existence hrozby, pokusu nebo při aktivním použití zbraně ke způsobení zranění. Ostatní pracovníci by neměli přicházet na pomoc, aby nebyli zraněni. Jakmile bude zavolán tento kód, bude kontaktována policie.

Zaměstnanec by měl volat stříbrný kód v případě:

- Pokus ublížit nebo zranit osoby jakoukoli zbraní
- Nošení zbraně v areálu nemocnice nebo v jeho blízkosti



Obrázek 52 Postup při stříbrném kódu, upraveno Zdroj: Ontario Hospital Association

Postup zaměstnanců při podezření nebo spatření osoby se zbraní byl přeložen a znázorněn na obrázku č. 52. Pro zaměstnance, kteří nejsou v bezprostřední blízkosti útočníka, by měli okamžitě kontaktovat policii a dále následovat obdobné kroky, které platí pro zaměstnance v blízkosti útočníka. To znamená, že evakuují pacienty a zabraňují dalším osobám vstupu do místa útoku a přesunou se na předem určené místo setkání. Dále jsou v příručce stanoveny pokyny pro vedoucí. Zde jsou pokyny rozšířeny o spočítání zaměstnanců ve svém týmu, pokud je to bezpečné, a podávání instrukcí ostatním (pacientům, návštěvníkům, zaměstnancům). Konec události je hlášen 3× opakovaným oznámením: „*Stříbrný kód, vše čisté*“. Do té doby se zaměstnanci řídí pokyny nadřízených a policie. Dále jsou v příručce popsány kompetence policistů. Příručka se také týká operátorů a jim určených pokynů. V rámci procesu zotavení vedení nemocnice zváží potřeby fyzického a duševního zdraví všech pracovníků a pacientů (OHA, 2016)

Code Black (černý kód) je užít v souvislosti hrozby bombového útoku. Při černém kódu je důležité:

- Zachovat klid
- Brát hovor vážně
- Mluvit normálním hlasem
- Nepřerušovat volajícího
- Dělat si poznámky
- Zaznamenat telefonní číslo
- Zjistit informace a prodlužovat hovor
- Kontaktovat ochranku

Zaměstnanci poté hledají podezřelé předměty, v případě nalezení se tato skutečnost nahlásí vedoucímu. Zaměstnanci se nesmějí dotýkat podezřelého předmětu. V místnosti je nařizeno otevřít okna a zmírnit tak poškození od skla. Dále se musí všichni přítomní co nejrychleji evakuovat do bezpečné vzdálenosti. V příloze příručky je dokumentace k zaznamenání všech podrobností týkajících se této události. Pokud je bomba nahlášena hovorem, jsou zde k dispozici otázky, např.: „*Kdy vybuchne bomba? Kde se nachází bomba? Odkud voláte? Kolik vím o bombě?*“ Dále se zde zaznamenávají podrobnosti o pachateli, pokud jsou známy, např.: hlas volajícího, přízvuk, rychlost řeči a zvuky v pozadí (Emergency Preparedness Committee, 2012).

Předpokladem pro cíl č. 2 bylo, že se setkávání s útoky, zabezpečení i ohrožení ZZ terorismem bude výrazně lišit od České republiky. S výjimkou SRN, která se ve většině bodů shoduje, **byl tento předpoklad naplněn**. S útoky se také země neseťkávali o mnoho častěji, než v ČR a důvodem nenaplnění tohoto předpokladu je malý vzorek respondentů a velká odlišnost.

Závěr

Diplomová práce se věnovala zabezpečení zdravotnických zařízení před terorismem a porovnání zabezpečení ve vybraných zahraničních státech. Prvním cílem práce bylo „*Analyzovat zabezpečení vybraných zdravotnických zařízení a jejich zkušenosti s teroristickými a kyberteroristickými útoky*“. K tomuto cíli byly sestaveny výzkumné otázky „*Je zabezpečen vstup do zdravotnického zařízení?*“, „*Jaké jsou zkušenosti zdravotnického zařízení s teroristickými nebo kyberteroristickými útoky?*“, „*Zúčastnili se zaměstnanci zdravotnického zařízení školení na nácvik reakce na teroristický útok?*“ Druhým cílem práce bylo „*Analyzovat rozdíly v ohrožení a zabezpečení zdravotnických zařízení v České republice a vybraných zahraničních státech*“.

Aby bylo možné zodpovědět na výzkumné otázky a splnit cíle diplomové práce, bylo potřeba kvantitativním způsobem zpracovat data metodou dotazníkového šetření a výsledky zpracovat do grafů a kvalitativním způsobem zpracovat data metodou polostrukturovaných rozhovorů se zaměstnanci se zkušeností ze zahraničí a výsledky následně graficky zpracovat.

Na základě výsledků dotazníkového šetření lze konstatovat, že ve většině zdravotnických zařízení (ZZ) není zabezpečen vstup a nenacházejí se v něm bezpečnostní rámy. Vstup pro zaměstnance není oddělen ani zabezpečen. Ve většině ZZ se nachází fyzická ostraha (security, ochranka), jejím úkolem však není zabezpečovat vstup do ZZ. Tímto byla zodpovězena první výzkumná otázka „*Je zabezpečen vstup do zdravotnického zařízení?*“. Podle většiny respondentů je ZZ nedostatečně připraveno na teroristický útok, většina ZZ se nesetkala s teroristickým útokem, ale setkala se s agresivním pacientem. S kyberteroristickými útokem se též většina ZZ nesetkala, ale zkušenosti s ním měl větší počet respondentů než s teroristickým útokem. Nejčastějším následkem kyberteroristického útoku byl výpadek dokumentace s ohrožením dat, ZZ čekala na obnovu funkce několik dní a vyrovnala se s útokem dobře. Tímto byla zodpovězena druhá výzkumná otázka „*Jaké jsou zkušenosti zdravotnického zařízení s teroristickými nebo kyberteroristickými útoky?*“. Ve většině ZZ se nekoná školení a zaměstnanci nejsou obeznámeni s opatřeními proti terorismu. V některých případech, ve kterých se školení koná je zpřístupněno všem zaměstnancům jednou do roka a účastníci jej hodnotí velmi kladně. Většina respondentů by školení nácvik reakce na terorismus uvítala. Tímto byla zodpovězena třetí výzkumná

otázka *Zúčastnili se zaměstnanci zdravotnického zařízení školení na nácvik reakce na teroristický útok?*⁶. První cíl práce byl splněn.

Z výsledků polostrukturovaných rozhovorů v závislosti s naplněním druhého cíle práce vyplývá, že horší zabezpečení než v ČR se nachází v Bosně a Hercegovině, Afghánistánu, Iráku a Rwandě. Ozbrojené síly zabezpečují zdravotnická zařízení v Království Saudské Arábie, Súdánu a ve vojenské nemocnici v Pákistánu. Ve Spojených arabských emirátech, druhém případě Království Saudské Arábie a SRN je zabezpečení podobné jako v ČR. Zaměstnanci se ve většině zemí neškolí. Všichni respondenti se v průběhu stáže cítili bezpečně, stejně jako se respondenti v ČR cítí bezpečně ve svém ZZ. Oproti ČR zažil respondent teroristický útok v Království Saudské Arábie, bez velkých škod a s výbornou reakcí. Zásadní rozdíl v zabezpečení ZZ vnímají všichni respondenti, kromě respondenta ze SRN. Ohrožení zdravotnického zařízení bylo ve většině případů větší než v ČR. Většina respondentů si myslí, že prvky zabezpečení jsou aplikovatelné v ČR, a to lepší ochranka, spolupráce s tajnými informačními službami, lepší školení a zpracování návodových karet vycházejících z kódového systému, zlepšení kyberochrany. Tímto by splněn cíl práce č.2.

Pro zlepšení ochrany zdravotnických zařízení před terorismem jsou sestavena následující doporučení, která vycházejí z výsledků diplomové práce. Zlepšit nebo zavést školení zaměstnanců zdravotnických zařízení, s možným využitím příručky kódového systému, který lze přepracovat do metodiky nebo standardu pro všechna zdravotnická zařízení na území ČR. Návrh podoby metodiky je znázorněn na obrázku č. 52 (viz kapitola 6.2. *Diskuse vztahující se k cíli práce č. 2*). Zavést nebo zlepšit funkčnost tlačítek, která by v jednotlivých zařízeních sloužila k přivolání ochranky nebo PČR a zjistit jejich efektivitu. Zvážit zaměstnání většího množství pracovníku ochranky. Bezpečnostní rámy, pokud je v zařízení dostatek zaměstnanců k jejich obsluze, se též nabízejí jako možnost, ale může se zdát jako nadbytečný a poměrně komplikovaný systém. Použití systém kamer, které rozpoznají zbraň, tento systém je současně ve fázi vývoje.

Práce může být využita jako vzdělávací materiál pro studenty nebo zdravotníky, kteří mají zájem o studium této problematiky, či jako předloha k vytváření efektivního systému školení pro zaměstnance zdravotnických zařízení. Tato práce může poskytnout návrhy na zlepšení krizové připravenosti zdravotnických zařízení při vzniku mimořádné události s prvky teroristického útoku. Diplomová práce má sloužit jako upozornění

na nedostatečnou připravenost a ochranu zdravotnických zařízení před terorismem, neexistující konkrétních legislativně určených požadavků týkajících se zabezpečení zdravotnických zařízení.

Seznam použitých zdrojů

1. ACKERMAN, G. a H. PETERSON., 2020. Terrorism and COVID-19: Actual and potential impacts. *Perspectives on Terrorism. USA: Terrorism Research Initiative*. 14(3), 59-73. ISSN 2334-3745.
2. AWAN, J. H., et al., 2017. A user friendly security framework for the protection of confidential information. *IJCSNS International Journal of Computer Science and Network Security*. Pakistan. 17(4), 215-223.
3. AZEEM, A. R. et al., 2019. Perception of Preparedness of Health Care Professionals in Case of a Nuclear, Chemical, Biological Attack/Emergency in a Tertiary Care Hospital. *Cureus*. 11(5), 7 ISSN 2168-8184.
4. BASIT, A. et al., 2019. South Asia. *Counter Terrorist Trends and Analyses*. International Centre for Political Violence and Terrorism Research. 11(1), 33-64. ISSN 1098-6596.
5. BATKOVSKÝ, M. 2019 *Střelba v ostravské nemocnici. Zemřelo šest lidí, další jsou zranění. Útočník se zastřelil*. [online]. Reflex [cit. 2022-02-02]. Dostupné z: <https://www.reflex.cz/clanek/zpravy/98840/strelba-v-ostravske-nemocnici-zemrelo-sest-lidi-dalsi-jsou-zraneni-utocnik-se-zastrelil.html>
6. BECKER S. M. a S. MIDDLETON., 2013 Improving Hospital Preparedness for Radiological Terrorism: Perspectives From Emergency Department Physicians and Nurses. *Disaster medicine and Public Health Preparedness*. 10. Dostupné také z: <https://www.cambridge.org/core/journals/disaster-medicine-and-public-health-p>
7. BESHEER, M., 2022 *OSCE Chair: Russian Actions in Ukraine 'State Terrorism'*. *Voice of America English News* [online]. [cit. 2022-04-01]. Dostupné z: https://www.voanews.com/a/osce-chair-russian-actions-in-ukraine-state-terrorism-/6485037.html?fbclid=IwAR2h99djiwtcBWU0v3DBqiPUB4IxyixWMYMOOrF2UB_HO4xNXCYwyPE_Spec
8. BIS. 2021 *Terorismus*. [online]. Bezpečnostní informační služba [cit. 2021-07-04]. Dostupné z: <https://www.bis.cz/terorismus/?fbclid=IwAR0t4duY44C114c0xzL6eWPMbIDg>

9. BONANATE, L., 1997 *Mezinárodní terorismus*. 1. vydání Praha: Columbus. 190 s. ISBN 80-85928-45-0
10. BUCHTELE, T., 2001 Politická situace v Baskicku a její kořeny. *Mezinárodní Politika*. 15(8), 16-19. ISSN 0543-7962
11. COLE, D., 2022 *Russia's strike on Ukraine maternity hospital is part of a terrible wartime tradition*. [online]. NPR [cit. 2022-03-20]. Dostupné z: https://www.npr.org/sections/goatsandsoda/2022/03/16/1086982186/russias-strike-on-ukraine-maternity-hospital-is-part-of-a-terrible-wartime-tradi?t=1647861893117&fbclid=IwAR0rgC3ZyR_mDB1oTMLmJ2g5yQb_QPjtyvxSWU1cqs0B_YK1i_C6712K1fE
12. COUNCIL OF THE EUROPEAN UNION., 2009 European Security Strategy. Belgium: © European Communities. ISBN 978-92-824-2421-6. Dostupné z: doi:10.2860/1402 43str. Dostupné z: <http://www.europa.eu>.
13. COURT, M. et al., 2020 Creating a Medical Initiative Mandated by Escalating Asymmetric Attacks. *Prehospital and Disaster Medicine. Counter-Terrorism Medicine*. 35(6), 595-598. Dostupné z: doi:10.1017/S1049023X2000103X
14. CRAWFORD, S., 2002. *SAS encyklopedie*. 1. vydání. Praha: Svojtka & Co. 588 s. ISBN 80-7237-069-3
15. ČTK., 2011. *Při útoku na nemocnici v Afghánistánu zahynulo 60 lidí*. [online]. Aktuálně.cz [cit. 2021-06-02]. Dostupné z: <https://zpravy.aktualne.cz/zahranici/pri-utoku-na-nemocnici-v-afghanistanu-zahynulo-60-lidi/r~i:article:705304/>
16. ČTK., 2019a. *Útok Tálibánu na nemocnici na jihu Afghánistánu má již 39 obětí*. [online]. Lidovky.cz [cit. 2021-06-21]. Dostupné z: https://www.lidovky.cz/svet/utok-talibanu-na-nemocnici-na-jihu-afghanistanu-ma-jiz-39-obeti.A190920_132624_ln_zahranici_ele
17. ČTK., 2019b *V Praze se střílelo na dvou místech. Jeden vážně zraněný*. [online]. Týden.cz [cit. 2022-01-21]. Dostupné z: https://www.lidovky.cz/svet/utok-talibanu-na-nemocnici-na-jihu-afghanistanu-ma-jiz-39-obeti.A190920_132624_ln_zahranici_ele

19. ČTK., 2021 *K útoku na vojenskou nemocnici v Kábulu se přihlásil Islámský stát*. České noviny [online]. Česká tisková kancelář [cit. 2021-06-14]. Dostupné z: <https://www.ceskenoviny.cz/zpravy/pri-explozich-u-vojenske-nemocnice-v-kabulu-zahynulo-nejmene-15-lidi/2111734>.
20. ČTK., 2022. *Útoky na zdravotnická zařízení se stávají součástí válečné taktiky, varuje WHO* [online]. Zdravotnický deník [cit. 2022-03-29]. Dostupné z: <https://www.zdravotnickydenik.cz/2022/03/utoky-na-zdravotnicka-zarizeni-se-stavaji-soucasti-valecne-taktiky-varuje-who/>
21. DAVID V. a M. MALACKA., 2005 *Fenomén mezinárodního terorismu*. Praha: Linde Praha a.s. 143 s. ISBN 80-7201-524-9
22. DE CAUWER, H., 2017. Hospitals: Soft target for terrorism? *Prehospital and Disaster Medicine*. 32(1), 94-100, doi:10.1017/S1049023X16001217
23. DEPARTMENT OF HOMELAND SECURITY., 2019 Strategic Framework for countering terrorism and targeted violence. USA: Homeland Security. 40 s.
24. DOLLIVER, M. a E. KEARNS., 2019 Is It Terrorism? Public Perceptions, Media, and Labeling the Las Vegas Shooting. *Studies in Conflict & Terrorism*. 1-19. Dostupné z: doi:10.1080/1057610X.2019.1647673
25. DOUCET, L., 2021 *Afghanistan: Biden says Afghans must decide their own future*. [online]. [cit. 2. 7. 2021] Dostupné z: https://www.bbc.com/news/world-asia-57619932?fbclid=IwAR1WfAmZQpZ0zfeqkhPQhPajGyWZ_e_T-CS_96B21duytl3kG8MRGGHt1YQ
26. EMERGENCY PREPAREDNESS COMMITTEE., 2012 North York General Hospital Policy Manual. Dostupné také z: https://www.nygh.on.ca/data/2/rec_docs/1000_code-black.pdf
27. EUROJUST (The European Union's Judicial Cooperation Unit)., 2021. *About Eurojust* [online]. [cit. 2021-07-02] Dostupné z WWW: <http://www.eurojust.europa.eu/Pages/languages/cs.aspx>
28. EUROPOL (European Union Agency for Law Enforcement Cooperation)., 2021. *About Europol* [online] 2021. [cit. 2021-07-02] Dostupné z WWW: <https://www.europol.europa.eu/cs/about-europol>

29. FATF., 2021. *Who we are* [online]. [cit. 2021-07-03] Dostupné z WWW:
<http://www.fatf-gafi.org/about/howweare/>
30. FIALA, T. a V. LUPTÁKOVÁ., 2021. *Biden stáhne vojáky z Afghánistánu do 11. září, odejdou i vojska NATO* [online]. Český Rozhlas Plus [cit. 2022-04-25]. Dostupné z: <https://plus.rozhlas.cz/biden-stahne-vojaky-z-afghanistanu-do-11-zari-odejdou-i-vojska-nato-rozebira-8468043?fbclid=IwAR2JRCQfRzZE9uxO2hHvOAXKFBETXoCpMxDbF4o6QiBk4R-P7dMnYmNBT1k>
31. FILIPEC, O., 2017. *Fenomén terorismus: česká perspektiva*. 1. vydání. Olomouc: Univerzita Palackého v Olomouci. 258 s. ISBN 978-80-244-5040-7
32. FIŠER, M., 2021. *Hackerské útoky nejsou v Česku výjimečné. Čelily jim nemocnice, MZV i volební web* [online]. Novinky.cz [cit. 2021-07-15]. Dostupné z: <https://www.novinky.cz/internet-a-pc/bezpecnost/clanek/hackerske-utoky-nejdou-v-cesku-vyjimecne-celily-jim-nemocnice-mzv-i-volebni-web-40353025>
33. FRIEDMANNOVÁ, S., 2021 *Střelba v nemocnici: policii zburcuje systém vyvinutý v Česku* [online]. Seznam Zprávy [cit. 2021-07-20]. Dostupné z: <https://www.seznamzpravy.cz/clanek/strelba-v-nemocnici-policii-zburcuje-system-vyvinuty-v-cesku-156013>
34. GANOR, B. a M. WERNLI., 2013 Terrorist Attacks against Hospitals. *International Institute for Counter-Terrorism*. 1-32. Dostupné také z: <https://www.ict.org.il/Article/77/Terrorist-Attacks-against-Hospitals-Case-Studies>
35. GEORGOPOULOS, G. P. et al., 2004. Hospital response to chemical terrorism: Personal protective equipment, training, and operations planning. *American Journal of Industrial Medicine*. 46(5), 432-445. Dostupné z: doi:10.1002/ajim.20075
36. GOEL, S., 2020. National Cyber Security Strategy and the Emergence of Strong Digital Borders. *Partnership for Peace Consortium of Defense Academies and Security Studies Institutes*. 19(1), 73-86. Dostupné z: doi:10.11610

37. HAVELKA, M., 2017. *Marxismus-leninismus*. Sociologická encyklopedie [online]. Praha: Sociologický ústav AV ČR, 2017 [cit. 2021-07-09]. Dostupné z: <https://encyklopedie.soc.cas.cz/w/Marxismus-leninismus>
38. HOLE, G., 1998. *Fanatismus: sklon k extrému a jeho psychologické kořeny*. 1. vydání. Praha: Portál. 152 s. ISBN 80-7178-183-5
39. IBÁÑEZ, Luis de La Corte., 2009. *Logika Terorismu*. 1. vydání. Praha: Academia. 322 s. ISBN 978-80-200-1724-6
40. INSTITUTE FOR ECONOMICS & PEACE., 2022. *The Ukraine Russia Crisis: Terrorism Briefing* [online]. [cit. 2022-04-05]. Dostupné z: <http://visionofhumanity.org/resources>
41. INTERPOL (International Criminal Police Organization), 2021. *What is Interpol?* [online] [cit. 2021-07-03] Dostupné z WWW: <https://www.interpol.int/en/Who-we-are/What-is-INTERPOL>
42. JELÍNEK, J., 2017a „Protiteroristická“ novela trestního zákoníku – poznámky k orientačnímu studiu. *Bulletin advokacie*. 17(3), 23-28. ISSN 1805-8280.
43. JELÍNEK, J., 2017b. *Trestní právo hmotné: obecná část, zvláštní část*. 6. vydání. Praha: Leges. 976 s. ISBN 978-80-7502-236-3
44. JEMELKA, P., 2021. *Talibán vyhlásil Islámský emirát Afghánistán*. [online]. Novinky .cz [cit. 2022-02-04]. Dostupné z: <https://www.novinky.cz/zahranicni/svet/clanek/taliban-vyhlasil-islamsky-emirat-afghanistan-40369534>
45. JUNA, P. a J. BURÝSEK., 2019. *Střelba v nemocnici, útok ve škole. Největší tragédie novodobého Česka*. [online]. Seznam zprávy [cit. 2021-07-0]. Dostupné z: <https://www.seznamzpravy.cz/clanek/strelba-v-nemocnici-utok-ve-skole-nejvetsi-tragedie-novodobeho-ceska-84473>
46. Katalog typových činností IZS Amok – útok aktivního střelce STČ 14/IZS, Praha, 2013
47. Katalog typových činností IZS Špinavá bomba STČ 01/IZS, Praha, 2015

48. Katalog typových činností IZS Hrozba použití NVS nebo nález NVS, podezřelého předmětu, munice, výbušnin a výbušných předmětů STČ 03/IZS, Praha, 2015
49. KOLEKTIV AUTORŮ., 2011. *Ochrana kritické infrastruktury*. Praha: Česká asociace bezpečnostních manažerů. 21 s. ISBN 978-80-260-1215-3
50. KOLEKTIV AUTORŮ POD VEDENÍM MINISTERSTVA ZAHRANIČNÍCH VĚCÍ ČR., 2011. *Bezpečnostní strategie České republiky*. Praha: Ministerstvo zahraničních věcí České republiky. 21 s. ISBN 978-80-7441-005-5
51. KRAUS, J., 2014. *Iránský státní terorismus*. 1. vydání. Brno: Centrum pro studium demokracie a kultury. 219 s. ISBN 978-80-7325-342-4
52. KŘOVÁK, J., 2018. *Přes 800 obětí a další stovky zraněných. To je bilance 50 let působení teroristické skupiny ETA*. [online]. Lidovky.cz [cit. 2021-07-15]. Dostupné z: https://www.lidovky.cz/svet/pres-800-obeti-a-dalsi-stovky-zrane-nych-to-je-bilance-50-let-pusobeni-teroristicke-skupiny-eta.A180504_114147_In_zahranici_ele
53. KUBÁTOVÁ, Z., 2020. *Útok na nemocnice je terorismus, říká antivirový miliardář Kasperskij*. [online]. Seznam zprávy [cit. 2021-06-15]. Dostupné z: <https://www.seznamzpravy.cz/clanek/utok-na-nemocnice-je-terorismus-rika-antivirovy-miliardar-kasperskij-113592?msclkid=c4a91ce1bc0911ec95d8d8e60c852718>
54. LACHTINOVÁ, Z., 2019. *Pacient ve vinohradské nemocnici postřelil dva jiné, jeden zemřel*. [online]. Seznam zprávy [cit. 2021-08-04]. Dostupné z: <https://www.seznamzpravy.cz/clanek/pacient-ve-vinohradske-nemocnici-postrelil-dva-lidi-odzbrojily-ho-sestry-67768>
55. MACIAS, A., 2021. *POLITICS Biden plans to withdraw U.S. forces from Afghanistan by Sept. 11, missing May deadline* [online]. [cit. 2022-01-20]. Dostupné z: https://www.cnbc.com/2021/04/13/biden-plans-to-withdraw-us-forces-from-afghanistan-by-sept-11.html?fbclid=IwAR024Je3ax-jQ5JIA1uaD-KYC7CGggYH38IRbV1fi26DX6kaPD_jACz3DHcI
56. MAREŠ, Miroslav., 2005. *Terorismus v ČR*. 1. vydání. Praha: Centrum strategických studií. 476 s. ISBN 80-903333-8-9

57. MILLER, I. a J. MITCHEL., 2009. *21st Century Criminology: A Reference Handbook*. 1. issue. Singapore: SAGE Publications. 915 p. ISBN 978-1-4129-6019-9
58. MINISTERSTVO VNITRA ČR., 2010. *Strategie boje proti terorismu pro léta 2010–2012*. [online]. 29 s. [cit. 2021-07-16]. Dostupné z: <https://www.mvcr.cz/clanek/dokumenty-454055.aspx>
59. MINISTERSTVO VNITRA ČR., 2013. *Strategie České republiky pro boj proti terorismu od r. 2013*. [online]. Praha 29 s. [cit. 2021-07-17]. Dostupné z: <https://www.mvcr.cz/clanek/dokumenty-454055.aspx>
60. MINISTERSTVO VNITRA ČR., 2016a. *Definice terorismu* [online]. [cit. 2021-08-05]. Dostupné z: <https://www.mvcr.cz/cthh/clanek/definice-terorismu.aspx>
61. MINISTERSTVO VNITRA ČR., 2016b. *Kybernetický terorismus, kyberterorismus* [online]. [cit. 2021-09-17] Dostupné z: <https://www.mvcr.cz/clanek/kyberneticky-terorismus-kyberterorismus.aspx>
62. MINISTERSTVO VNITRA ČR., 2021a. *Ochrana měkkých cílů*. [online]. [cit. 2022-02-19]. Dostupné z: <https://www.mvcr.cz/clanek/ochrana-mekkych-cilu.aspx>
63. MINISTERSTVO VNITRA ČR., 2021b. *Stupně ohrožení terorismem*. [online]. [cit. 2022-02-21]. Dostupné z: <https://www.mvcr.cz/cthh/clanek/stupne-ohrozeni-terorismem.aspx>.
64. NEJVYŠŠÍ STÁTNÍ ZASTUPITELSTVÍ ČR., 2021. *Moneyval* [online]. [cit. 2021-07-03]. Dostupné z: <http://www.nsz.cz/index.php/cs/mezinarodni-spoluprace/dali-organizace/moneyval>
65. NEKOLA, D., 2017. *Islám a terorismus*. 1. vydání. Pstruží: Lukáš Lhoťan. 269 s. ISBN 978-80-906030-8-0.
66. NOVOTNÁ, K., 2021a. *Nemocnice jsou pro hackery stále snadným cílem. Útoků přitom přibývá*. [online]. IDnes.cz [cit. 2021-12-07]. Dostupné z: https://www.idnes.cz/zpravy/domaci/kyberneticky-utok-hacker-nemocnice-zabezpeceni.A210203_141638_domaci_knn

67. NOVOTNÁ, K., 2021b *Politici jsou zajedno. Vládu Tálibánu Česko v žádném případě neuzná.* [online]. IDnes.cz [cit. 2021-09-07]. Dostupné z: https://www.idnes.cz/zpravy/domaci/taliban-afghanistan-politici-diplomacie.A210818_102846_domaci_knn
68. NOVÝ, P., 2020. *Útok ve slánské nemocnici: Pacient napadl nožem personál, ochranka ho postřelila.* [online]. Globe24.cz [cit. 2021-10-04]. Dostupné z: <https://globe24.cz/domov/utok-ve-slanske-nemocnici-pacient-napadl-nozem-personal-ochranka-ho-postrelila.f751e888>
69. ONTARIO HOSPITAL ASSOCIATION., 2016. *CODE SILVER : Person with a Weapon* [online]. 6 s. [cit. 2022-04-20]. Dostupné z: <https://www.oha.com/Documents/Code Silver Policy Sample.pdf>
70. PRESIDENCY AND CT CO-ORDINATOR., 2005. *The european union counter-terrorism strategy* [online]. [cit. 2022-02-21]. Dostupné z: <https://www.oha.com/Documents/Code Silver Policy Sample.pdf>
71. PROCHÁZKOVÁ, D., 2014. *BOJ PROTI TERORISMU Projekt EU: Improving Security by Democratic Participation - ISDEP.* 1. vydání. Praha: České vysoké učení technické v Praze, Fakulta dopravní Ústav bezpečnostních technologií a inženýrství. 196 s. ISBN 978-80-01-05568-7.
72. QAZI, S., 2020. *Ghani sworn in as Afghan president, rival holds own inauguration.* [online]. Aljazeera [cit. 2021-05-04]. Dostupné z: <https://www.aljazeera.com/news/2020/3/9/ghani-sworn-in-as-afghan-president-rival-holds-own-inauguration>
73. RADA EU., 2021a. *COVID-19: Rada schválila závěry o dopadech pandemie na vnitřní bezpečnost a hrozbu terorismu* [online]. [cit. 2022-01-18]. Dostupné z: <https://www.consilium.europa.eu/cs/press/press-releases/2021/06/07/covid-19-council-approves-conclusions-on-the-impact-of-the-pandemic-on-internal-security-and-terrorist-threat/?msclid=f3351166bb4111eca8bf0e7d43270b0e>
74. RADA EU., 2021b. *Protiteroristický koordinátor* [online]. [cit. 2022-01-18]. Dostupné z: <https://www.consilium.europa.eu/cs/policies/fight-against-terrorism/counter-terrorism-coordinator/>

75. RASCHID, A., 2001. *Taliban: Militant Islam, Oil, and Fundamentalism in Central Asia*. 2. vydání. London: Yale University Press. 274 p. ISBN 978-0-300-08902-8.
76. RON, P. a SHAMAI, M., 2014. The impact of ongoing national terror on the community of hospital nurses in Israel. *Community Mental Health Journal*. 50(3), 354–361. ISSN 00103853.
77. ROZENFIELD, M. *et al.*, 2019. New Trends in Terrorism-Related Injury Mechanisms: Is There a Difference in Injury Severity? *Annals of Emergency Medicine*. 74(5), 697–705. doi: 10.1016/j.annemergmed.2019.02.034.
78. RUBENSTEIN, L., 2018. 2018 IMPUNITY REMAINS : Attacks on Health Care in 23 Countries in Conflict'. *Safeguarding Health in Conflict*. 1-35.
79. ŘEHÁK, D. *et al.*, 2008. *Vybrané aspekty soudobého terorismu*. Praha: Ministerstvo obrany České republiky - Agentura vojenských informací a služeb. 143 s. ISBN 978-80-7278-443-1
80. SIMON, M.F. *et al.*, 2022. *At least 43 attacks on health-care facilities and patients in Ukraine, WHO says*. [online]. The Washington Post [cit. 2022-03-29]. Dostupné z: <https://www.washingtonpost.com/world/2022/03/17/ukraine-attacks-hospitals-clinics-health-care-russia/?fbclid=IwAR0cCbLH0-3453w50bJvV7QFH5ZxYbvhCl-9vBAocCOb3doN4PFI-zxG0CQ>
81. SOFT TARGETS PROTECTION INSTITUTE., 2016. *ZÁKLADY OCHRANY MĚKKÝCH CÍLŮ – METODIKA* [online]. Praha: Ministerstvo vnitra ČR [cit. 2021-07-12]. Dostupné z: <https://www.mvcr.cz/clanek/ochrana-mekkych-cilu.aspx>
82. STRMISKA, M., 1996. *Politický terorismus. Úvod do studia politického terorismu v demokratických systémech*. Brno: Masarykova univerzita. 104 s. ISBN 80-210-1360-5.

83. SVOBODA, T., 2019. *Trest pro prvního teroristu v Česku platí. Za útok na vlaky stráví ve vězení čtyři roky.* [online]. Seznam zprávy [cit. 2021-07-11]. Dostupné z: https://www.seznamzpravy.cz/clanek/trest-pro-prvniho-teroristu-v-cesku-plati-za-utok-na-vlak-y-stravi-ve-vezeni-ctyri-roky-85201?fbclid=IwAR3mQjsae0X_7m0gXLQfxrQCMsmH7a4c_UP9QrNLRJ0XtxLMoYYxyAUTbxE
84. ŠÍN, R. et al., 2017. *Medicína katastrof.* Praha: Galén. 352 s. ISBN 978-80-7492-295-4.
85. ŠMIGOL, O., 2020. *Za útoky na porodnici a pohřeb v Afghánistánu stojí Islámský stát, tvrdí USA.* [online]. [cit. 2021-08-11]. Dostupné z: <https://echo24.cz/a/SQZ3a/za-utoky-na-porodnici-a-pohreb-v-afghanistanu-stoji-islamsky-stat-tvr-di-usa>
86. UNITED NATIONS., 2001. *Resolution 1373.* Dostupné z: doi: 10.4324/9781315170657-71
87. UNIVERSITY OF MARYLAND., 2022. *GTD, Analysis.* [online]. [cit. 2021-04-18]. Dostupné z: <https://www.start.umd.edu/gtd/analysis/>
88. Usnesení Vlády České republiky 1060/2006 ke koordinaci činnosti zpravodajských služeb České republiky při vyhodnocování informací důležitých pro bezpečnost České republiky se zvláštním zaměřením na boj proti terorismu.
89. WILDOVÁ, O., 2020. *V ČR přibývá hackerských útoků na nemocnice* [online]. *Medicina.cz* [cit. 2021-06-18]. Dostupné z: <https://medicina.cz/clanky/12705/243/V-cR-pribyva-hackerskych-utoku-na-nemocnice/>
90. Zákon číslo 153/1994 Sb.. O zpravodajských službách České republiky, ve znění pozdějších předpisů.
91. Zákon číslo 181/2014 Sb., O kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů.
92. Zákon číslo 240/2000 Sb., O krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů.
93. Zákon číslo 253/2008 Sb., O některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů.

94. Zákon číslo 372/2011 Sb., O zdravotních službách a podmínkách jejich poskytování, ve znění pozdějších předpisů.
95. Zákon číslo 40/2009 Sb., Trestní zákoník, ve znění pozdějších předpisů
96. ZOUHAR, J., 1985. *Místo a úloha jednotek SNB určených k boji proti terorismu*. [online]. Správa pro politickovýchovnou, vzdělávací, kulturní a propagační činnost [cit. 2022-01-25]. Dostupné z: ww.oovbstrnadice.cz/misto-a-uloha-jednotek-snb-urceny-k-boji-proti-teroristickym-a-jinym-ozbrojenym-skupinam-nebezpecnych-pachatelu/

Zdroje obrázků:

1. EUROJUST. *Logo EUROJUST.*, 2022. *European Union Agency for Criminal Justice Cooperation* [online]. [cit. 2022-04-01]. Dostupné z: <https://www.eurojust.europa.eu/>
2. EUROPOL. *Logo EUROPOL.*, 2022. *European Union Agency for Law Enforcement Cooperation (Europol)* [online]. [cit. 2022-04-01]. Dostupné z: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/europol_en
3. Evropská komise. *Logo Evropské komise.*, 2022. [online]. [cit. 2022-04-01]. Dostupné z: https://ec.europa.eu/info/index_cs
4. EXANPRO. *Stupně ohrožení terorismem.*, 2005. [online]. [cit. 2022-04-01]. Dostupné z: http://www.exanpro.cz/images/Threat_levels.png
5. INTERPOL. *Logo INTERPOL.*, 2022. [online]. [cit. 2022-04-01]. Dostupné z: <https://www.interpol.int/>
6. MONEYVAL. *Logo MONEYVAL.*, 2022 *AFA* [online]. [cit. 2022-04-01]. Dostupné z: <https://www.afa.ad/en/press-room/comunicats-de-premsa/moneyval-publishes-the-andorra2019s-second-follow-up-report>
7. NATO. *Logo NATO.*, 2022. [online]. [cit. 2022-04-01]. Dostupné z: https://www.nato.int/nato-welcome/index_cz.html
8. OBCE. *Logo OBSE.*, 2022. [online]. [cit. 2022-04-01]. Dostupné z: <https://www.osce.org/>
9. Ontario Hospital Association. *CODE SILVER : Person with a Weapon* [online] 2016 [cit. 2022-04-03]. Dostupné z: <https://www.oha.com/Documents/Code%20Silver%20Policy%20Sample.pdf>
10. OSN. *Logo OSN.*, 2022. *UN* [online]. [cit. 2022-04-01]. Dostupné z: <https://www.un.org/>
11. Rada Evropské unie. *Logo Rady Evropské unie.*, 2022. [online]. [cit. 2022-04-01]. Dostupné z: <https://www.consilium.europa.eu/cs/european-council/members/>

Seznam obrázků

Obrázek 1. Stupně ohrožení terorismem (<i>podle EXANPRO 2005, upraveno</i>).	23
Obrázek 2. Logo OSN Zdroj: https://www.un.org/	30
Obrázek 3. Logo NATO Zdroj: https://www.nato.int/nato-welcome/index_cz.html ...	30
Obrázek 4. logo OBSE Zdroj: https://www.osce.org	31
Obrázek 5. Rada Evropské Unie Zdroj: https://www.consilium.europa.eu/en/council-eu/	31
Obrázek 6. Logo Evropské komise Zdroj: https://ec.europa.eu/info/index_cs	31
Obrázek 7. Logo EUROJUST Zdroj: https://www.eurojust.europa.eu/	32
Obrázek 8 Logo EUROPOL Zdroj: https://european-union.europa.eu/	32
Obrázek 9 Logo INTERPOL Zdroj: https://www.interpol.int/	33
Obrázek 10. Logo MONEYVAL Zdroj: https://www.afa.ad/en/press-room/comunicats-de-premsa/moneyval-publishes-the-andorra2019s-second-follow-up-report	33
Obrázek 11. Povolání respondentů Zdroj: Vlastní.....	47
Obrázek 12. Délka praxe respondentů Zdroj: Vlastní	48
Obrázek 13. Obeznamení s opatřeními proti terorismu Zdroj: Vlastní.....	49
Obrázek 14. Školení Zdroj: Vlastní	50
Obrázek 15. Frekvence školení Zdroj: Vlastní	51
Obrázek 16. Účastníci školení Zdroj: Vlastní	52
Obrázek 17. Účast na školení Zdroj: Vlastní	53
Obrázek 18. Hodnocení školení Zdroj: Vlastní.....	54
Obrázek 19. Uvítal/a byste školení na nácvik reakce na teroristický útok? Zdroj: Vlastní	55
Obrázek 20. Častější pořádání školení Zdroj: Vlastní	55
Obrázek 21. Pocit bezpečí Zdroj: Vlastní.....	56
Obrázek 22. Připravenost na teroristický útok Zdroj: Vlastní	57
Obrázek 23. Co dělat v případě nastání teroristického útoku Zdroj: Vlastní	58
Obrázek 24. Teroristický útok Zdroj: Vlastní	59
Obrázek 25. Odezva na teroristický útok Zdroj: Vlastní	60
Obrázek 26. Útok na měkké cíle Zdroj: Vlastní	61
Obrázek 27. Agresivní pacient Zdroj: Vlastní	62
Obrázek 28. Přivolání PČR Zdroj: Vlastní	63
Obrázek 29. Jiný způsob vypořádání s agresivním pacientem Zdroj: Vlastní	64

Obrázek 30. Pracovníci ochranky Zdroj: Vlastní.....	65
Obrázek 31. Za jak dlouho jsou schopni pracovníci ochranky dorazit na místo zásahu? Zdroj: Vlastní	66
Obrázek 32. Bezpečnostní rámy Zdroj: Vlastní	67
Obrázek 33. Vstup do ZZ Zdroj: Vlastní	68
Obrázek 34. Zabezpečení vstupu pro personál Zdroj: Vlastní	69
Obrázek 35. Hrozba terorismu Zdroj: Vlastní	70
Obrázek 36. Hrozba kyberterorismu Zdroj: Vlastní	71
Obrázek 37. Setkání s kyberteroristickým útokem Zdroj: Vlastní.....	72
Obrázek 38. Následky kyberteroristického útoku Zdroj: Vlastní	73
Obrázek 39. Řešení kyberteroristického útoku Zdroj: Vlastní	74
Obrázek 40. Vyrovnání se s kyberteroristickým útokem Zdroj: Vlastní	75
Obrázek 41. Ohrožení kyberteroristickým Zdroj: Vlastní.....	76
Obr. 42. Zabezpečení zdravotnických zařízení dle respondentů Zdroj: Vlastní	79
Obrázek 43. Školení zahraničních zaměstnanců Zdroj: Vlastní	81
Obrázek 44. Bezpečnost v průběhu stáže/mise Zdroj: Vlastní	82
Obrázek 45. Připravenost na TÚ Zdroj: Vlastní	84
Obrázek 46. Bezpečnostní rozdíl Zdroj: Vlastní.....	85
Obrázek 47. Rozdíl v zabezpečení ZZ v ČR a v místě stáže/mise Zdroj: Vlastní	87
Obrázek 48. Teroristický útok v zahraničí Zdroj: Vlastní	88
Obrázek 49. Opatření aplikovatelná v ČR Zdroj: Vlastní.....	88
Obrázek 50. Reakce na teroristický útok v zahraničí Zdroj: Vlastní	90
Obrázek 51. Riziko ohrožení terorismem v porovnání s ČR Zdroj: Vlastní	91
Obrázek 52 Postup při stříbrném kódu, upraveno Zdroj: Ontario Hospital Association	102

Seznam tabulek

Tabulka I. Odpověď jiná na otázku č. 13 Zdroj: Vlastní.....	58
Tabulka II. Odpověď jiná na otázku č. 19 Zdroj: Vlastní.....	64
Tabulka III. Přehled jednotlivých respondentů Zdroj: Vlastní.....	78

Seznam příloh

Příloha 1 - Vzor dotazníku

Příloha 2 - Vzor polostrukturovaného rozhovoru

Příloha 1 - Vzor dotazníku

Dobrý den,

jmenuji se Anna Klečková a jsem studentkou Jihočeské univerzity v Českých Budějovicích, kde studuji obor Civilní nouzová připravenost na Zdravotně sociální fakultě. K ukončení tohoto studia zpracovávám diplomovou práci na téma: „**Ochrana vybraných zdravotnických zařízení proti terorismu**“. Tímto bych Vás chtěla požádat o vyplnění tohoto dotazníku. Dotazník je anonymní a informace v něm uvedené budou využity pouze pro zpracování a vyhodnocení dat v mé diplomové práci. **Vámi vybrané odpovědi označte křížkem, vždy je správná pouze jedna odpověď**. Děkuji Vám za spolupráci.

1) Na jaké pozici pracujete?

- Lékař
- Všeobecná sestra
- Zdravotnický záchranář
- Radiologický asistent
- Porodní asistentka
- Zdravotní laborant
- Praktická sestra
- Fyzioterapeut
- Jiná

2) Jak dlouhá je vaše praxe?

- Méně než 1 rok
- 1–5 let
- 6–10 let
- 11–15 let
- 16–20 let
- Nad 20 let

- 3) Jste obeznámen/a s opatřeními proti terorismu od Vašeho zaměstnavatele?
- Ano, jsem obeznámen
 - Vím, že existují, ale neznám je
 - Nejsem obeznámen
 - Nevím
- 4) Probíhá na Vašem pracovišti školení na nácvik reakce na teroristický útok?
- Ano, pokračujte na otázku č. 5
 - Ano, ale jen v rámci školení BOZP
 - Ne, pokračujte na otázku č. 9
 - Nevím
- 5) Jak často probíhá školení na nácvik reakce na teroristický útok?
- Častěji než jednou za rok
 - Jednou za rok
 - Jednou za dva roky
 - Jednou za pět let
- 6) Kdo se může tohoto školení účastnit?
- Jen bezpečnostní technici
 - Jen vedoucí zaměstnanci (primáři, vrchní sestry)
 - Všichni zaměstnanci
 - Nevím
- 7) Zúčastnili jste se školení na nácvik reakce na teroristický útok?
- Ano, vícekrát
 - Ano, jednou
 - Ne, ale rád bych se v budoucnu účastnil
 - Ne

8) Jak školení na nácvik reakce na teroristický útok hodnotíte?

- Velmi kladně
- Splnil mé očekávání
- Neutrálně
- Je třeba velmi zlepšit kvalitu školení

9) Uvítal/a byste školení na nácvik reakce na teroristický útok?

- Ano
- Ne

10) V případě, že byste školení uvítal/a, nebo jste se zúčastnil/a bylo by vhodné pořádat jej častěji?

- Ano
- Ne

11) Cítíte se ve Vašem zdravotnickém zařízení bezpečně?

- Ano
- Spíše ano
- Spíše ne
- Ne

12) Jak hodnotíte připravenost zdravotnického zařízení na případný teroristický útok?

- Výborná
- Dobrá
- Dostatečná
- Nedostatečná

13) Jak se zachovat v případě teroristického útoku?

- Dbát na svou bezpečnost, kontaktovat nadřízeného a řídit se jeho instrukcemi
- Nevím
- Máme ve zdravotnickém zařízení příručku, podle které vím jak se zachovat
- Jiná odpověď

14) Zažil/a jste někdy teroristický útok? (jako teroristický útok je definováno plánované, promyšlené a politicky motivované násilí, zaměřené proti nezúčastněným osobám, sloužící k dosažení vytyčených cílů.)

- Ano
- Ne, ale slyšel/a jsem o něm
- Ne, ale sledoval/a jsem ho v médiích
- Ne

15) Jak probíhala odezva na teroristický útok?

- Nebyla přítomna
- Zlepšilo se zabezpečení zdravotnického zařízení
- Nevím
- Zhoršilo se zabezpečení zdravotnického zařízení

16) Zažil/a jste někdy útok na měkké cíle? (všechny útoky kromě teroristického, na místa – objekty a prostory s vysokou koncentrací osob a nízkou úrovní zabezpečení proti násilným útokům.)

- Ano, s odezvou
- Ano, bez velké odezvy
- Ne, ale sledoval/a jsem ho v médiích
- Ne

17) Setkal/a jste se někdy s útokem agresivního pacientem?

- Ano, častěji než 1× za 3 měsíce
- Ano, častěji než 2× za rok
- Ano, méně než 1× za rok
- Ne

18) Musel/a jste v případě setkání s agresivním pacientem přivolat policii?

- Ano, spolupráce probíhala velmi dobře
- Ano, ale nedařila se nám spolupráce
- Ne, poradil/a jsme si jiným způsobem, pokračujte na otázku č. 19
- Ne, přivolali jsme pracovníky ochranky v našem zdravotnickém zařízení

19) Jakým jiným způsobem jste si poradil/a s agresivním pacientem?

- Upoutáním na lůžko dle platných ošetrovatelských standardů
- Přivoláním lékaře pro podání antipsychotik, případně jiné medicíny
- Přivoláním lékaře z psychiatrického oddělení
- Jiným způsobem, vypište

20) Pracují ve zdravotnickém zařízení pracovníci ochranky?

- Ano, jsem schopen je přivolat
- Ano, ale neznám na ně telefonní číslo
- Ne – pokračujte na otázku č. 22
- Nevím – pokračujte na otázku č. 22

21) Za jak dlouho jsou schopni pracovníci ochranky dorazit na místo zásahu?

- Do 5-10 minut
- Do 11-20 minut
- Do 21-30 minut
- Nevím

22) Nachází se ve zdravotnickém zařízení bezpečnostní rámy?

- Ano
- Ne
- Nevím

23) Je ve zdravotnickém zařízení oddělený vstup do zdravotnického zařízení pro personál?

- Ano
- Ne

24) Jak je tento vstup do zdravotnického zařízení zabezpečen?

- Vstup je označen, uzamčen, odemyká se klíčem, který vlastní zaměstnanci
- Vstup je označen a je možné jej otevřít jen na čipové karty/čipy které vlastní zaměstnanci
- Vstup hlídá ostraha
- Vstup není nijak zabezpečen

25) Myslíte si, že se v posledních 2 letech zvyšuje hrozba terorismu kvůli onemocnění COVID-19

- Ano
- Spíše ano
- Ne, pravděpodobněji než kvůli Covid – 19 se hrozba zvyšuje u kyberterorismu
- Ne

26) Myslíte si, že se v posledních 2 letech zvyšuje hrozba kyberterorismu?

- Ano
- Ne
- Nevím
- Neumím posoudit

27) Setkal/a jste se s kyberterorismem/únikem informací ze zdravotnického zařízení?

- Ano – specifikujte, pokračujte na otázku č. 28
- Ne
- Neseťkal/a jsem se s útokem, ale zlepšují nám bezpečnost sítě, protože jsou známy určité hrozby
- Jiná odpověď

28) Jaké byly následky kyberteroristického útoku?

- Výpadek přístrojů
- Výpadek dokumentace
- Únik informací ze zdravotnického zařízení
- Zablokování nebo nefunkčnost počítačů nebo počítačových programů
- Poškození pacientů nebo zaměstnanců

29) Jak probíhalo řešení kyberteroristického útoku?

- Nevím, neangažoval/a jsem se
- Naši IT technici včas zabránili velkým škodám
- Čekali jsme několik hodin na správné fungování zdravotnického zařízení
- Čekali jsme několik dní na správné fungování zdravotnického zařízení

30) Jak se vaše zdravotnické zařízení s kyberteroristickým útokem vyrovnalo?

- Dobře, neproběhla velká ztráta dat ani omezení funkčnosti
- Proběhla větší ztráta dat nebo informací
- Proběhlo omezení funkčnosti, které trvalo velmi dlouho
- Dosud se zdravotnické zařízení s útokem nevyrovnalo

31) Kdo byl kyberteroristickým útokem ohrožen?

- Zaměstnanci
- Zaměstnanci i pacienti
- Pacienti
- Byla ohrožena ztráta dat
- Nikdo nebyl ohrožen

Příloha 2 - Vzor polostrukturovaného rozhovoru

Dobrý den,

jmenuji se Anna Klečková a jsem studentkou Jihočeské univerzity v Českých Budějovicích, kde studuji obor Civilní nouzová připravenost na Zdravotně sociální fakultě. K ukončení tohoto studia zpracovávám diplomovou práci na téma: „**Ochrana zdravotnických zařízení proti terorismu**“. Tímto Vás žádám o rozhovor na téma ochrany zdravotnických zařízení v zahraničí a v České republice. Rozhovor je anonymní a informace v něm uvedené budou využity pouze pro zpracování a vyhodnocení dat v mé diplomové práci.

Děkuji Vám za spolupráci.

- 1) Na jaké pozici pracujete?
- 2) V jaké lokalitě probíhala vaše mise/stáž?
- 3) Jak dlouho Vaše mise/stáž trvala?
- 4) Jak bylo Vaše působiště zabezpečeno proti možnému teroristickému útoku?
- 5) Školí se místní zaměstnanci na nácvik reakce na teroristický útok?
- 6) Cítil/a jste se v průběhu stáže bezpečně?
 - a. Proč ano?
 - b. Proč ne?
- 7) Jak hodnotíte tamní připravenost na teroristický útok?
- 8) Z jakého důvodu tak hodnotíte?
- 9) Vnímáte významný rozdíl v bezpečnosti v ČR a v místě stáže/mise?
- 10) Vnímáte rozdíl v zabezpečení zdravotnických zařízení v ČR a v místě stáže? Jaký?
- 11) Zažil/a jste teroristický útok?
- 12) Byla přítomna odezva? Jak probíhala?
- 13) Myslíte si, že nějaké prvky zabezpečení přítomné v místě Vašeho pobytu jsou aplikovatelné i v ČR?
 - a. Jaké? Z jakého důvodu?
- 14) Jak by se zachovali v místě stáže v případě teroristického útoku?
- 15) Bylo zdravotnické zařízení ohroženo teroristickým útokem častěji než v ČR?

Seznam zkratek

ARO	Anesteziologicko-resuscitační oddělení
BIS	Bezpečnostní informační služba
BOZP	Bezpečnost a ochrana zdraví při práci
BS	Bezpečnostní strategie
CBRNE	Chemické, biologické, radiologické, nukleární, explozivní (látky)
CTC	Protiteroristický výbor (Counter-Terrorism Committee)
ČR	Česká republika
ETA	Euskadi Ta Askatasuna (Baskicko a svoboda)
EU	Evropská unie
FATF	Finanční akční výbor na mezinárodní spolupráci
FN	Fakultní nemocnice
ICT	Informační a komunikační technologie
IKEM	Institut klinické a experimentální medicíny
ISR	Zpravodajské sledovací a průzkumné činnosti
IT	Informační technologie
IZS	Integrovaný záchranný systém
JIP	Jednotka intenzivní péče
KI	Kritická infrastruktura
MZ	Ministerstvo zdravotnictví
NATO	North Atlantic Treaty Organization (Severoatlantická aliance)
OBSE	Organizace pro bezpečnost a spolupráci v Evropě
OSN	Organizace spojených národů
PČR	Policie České republiky
PETA	People for The Ethical Treatment of Animals (Lidé pro etické zacházení se zvířaty)

SRN	Spolková republika Německo
StB	Státní bezpečnost
STČ	Soubor typové činnosti
TOPO	Zákon o trestní odpovědnosti právnických osob a řízení proti nim
TZ	Trestní zákoník
VDA	Volksbund für Deutschtum im Ausland
ZHN	Zbraně hromadného ničení
ZZ	Zdravotnické zařízení
ZZS	Zdravotnická záchranná služba