# Asymetrické konflikty a hybridní válka

Bc. Jakub Březina

Diplomová práce
2021

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

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

Akademický rok: 2020/2021

# ZADÁNÍ DIPLOMOVÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

| | |
|---|---|
| Jméno a příjmení: | **Bc. Jakub Březina** |
| Osobní číslo: | **L19719** |
| Studijní program: | **N1032A020002 Bezpečnost společnosti** |
| Studijní obor: | **Ochrana obyvatelstva** |
| Forma studia: | **Kombinovaná** |
| Téma práce: | **Asymetrické konflikty a hybridní válka** |

## Zásady pro vypracování

1. Na základě studia odborné literatury zpracujte literární rešerši s důrazem na monografie, studie a články zabývající se bezpečností České republiky.
2. Teoreticky vymezte základní pojmy a právní ukotvení vztahující se k předmětné problematice.
3. Analyzujte problematiku asymetrických a hybridních hrozeb a vyhodnoťte současnou bezpečnostní situaci v České republice.
4. Na základě zjištěných poznatků navrhněte možná opatření pro větší resilienci České republiky vůči asymetrickým a hybridním hrozbám.

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

Seznam doporučené literatury:


1. KIRCHER, Stefan. *Asymmetric Warfare. A Challenge for International Humanitarian Law?*. Munich: GRIN Verlag, 2015, 12 s. ISBN 9783668112650.
2. KŘÍŽ, Zdeněk, Zinaida BECHNÁ a Peter ŠTEVKOV. *Hybridní válka jako nový fenomén v bezpečnostním prostředí Evropy*. Aktualizované a rozšířené druhé vydání. Praha: Pro Informační centrum o NATO vydalo Jagello 2000, 2016. ISBN 978-80-904850-4-4.
3. SMOLÍK, Josef a Tomáš ŠMÍD. *Vybrané bezpečnostní hrozby a rizika 21. století*. Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2010. ISBN 978-80-210-5288-8.


Další odborná literatura dle doporučení vedoucího diplomové práce.

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

Datum zadání diplomové práce: **1. prosince 2020**
Termín odevzdání diplomové práce: **14. května 2021**

L.S.

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

**prof. Ing. Dušan Vičar, CSc.**
ředitel ústavu

V Uherském Hradišti dne 2. prosince 2020

# PROHLÁŠENÍ AUTORA
# DIPLOMOVÉ PRÁCE

Beru na vědomí, že:

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

**Prohlašuji,**

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

V Uherském Hradišti, dne: 7. 5. 2021

Jméno a příjmení studenta: Jakub Březina

.....
podpis studenta

## ABSTRAKT

Tato diplomová práce se zabývá problematikou asymetrických a hybridních hrozeb, kterým Česká republika momentálně čelí. Primárním cílem práce bylo analyzovat asymetrické a hybridní hrozby a na základě zjištěných skutečností navrhnout možná opatření pro větší resilienci vůči těmto hrozbám. Sekundárním cílem bylo vyhodnotit současnou bezpečnostní situaci v Česku. Analýza hrozeb byla provedena pomocí metody „PNH“ a pro vyhodnocení současné bezpečnostní situace bylo použito dotazníkové šetření, kterého se zúčastnilo 517 respondentů. Výsledky analýzy hrozeb ukazují, že pro Českou republiku představuje největší riziko terorismus, politický extremismus, dezinformace a propaganda, kybernetické útoky a hybridní válka. Podle respondentů představuje pro Česko největší hrozbu Islámský stát, Čína a Rusko. I přesto se ale většina respondentů cítí v České republice bezpečně a Česko nadále patří k nejbezpečnějším zemím na světě. V závěru práce jsou formulovány konkrétní návrhy opatření, které by při implementaci značně posílily obranyschopnost České republiky.



Klíčová slova: hybridní válka, asymetrické a hybridní hrozby, analýza hrozeb



## ABSTRACT

This diploma thesis deals with issues of asymmetric and hybrid threats that the Czech Republic is facing at present. The primary goal of this thesis was to analyse asymmetric and hybrid threats based on detected facts to suggest potential precautions for bigger resilience towards these threats. The secondary aim was to evaluate actual security situation in the Czech Republic. The threats analysis was carried out by using “PNH” method and the interview survey was used for evaluation of actual security situation involving 517 respondents. The results of the threats analysis show that terrorism, political extremism, disinformation, and propaganda, cybernetic attacks and hybrid war represent the biggest risk for the Czech Republic. According to respondents, the Islamic State, China and Russia represent the biggest threat for the Czech Republic. Nevertheless, the majority of respondents feel secure and the Czech Republic belong to the safest countries in the world. In conclusion, there are concrete suggestions of precautions, which would considerably reinforce defence of the Czech Republic during implementation.



Keywords: hybrid warfare, asymmetric and hybrid threats, threat analysis

Rád bych touto cestou poděkoval panu doc. Ing. Jaromíru Novákovi, CSc. za odborné vedení a poskytnutí cenných rad a zkušeností, které mi byly velkým přínosem při zpracovávání mé diplomové práce.

Dále bych rád poděkoval své rodině a přítelkyni za neocenitelnou psychickou podporu během celého studia.

*„Svět je nebezpečné místo k životu, ne kvůli lidem, kteří jsou zlí, ale kvůli lidem, kteří s tím nic neudělají.“*

Albert Einstein

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

# OBSAH

**ÚVOD** ..... **9**
**CÍLE A METODY ZPRACOVÁNÍ** ..... **11**
**I TEORETICKÁ ČÁST** ..... **13**
**1 ASYMETRICKÉ KONFLIKTY** ..... **14**
1.1 ZÁJMY A VŮLE AKTÉRŮ ..... 15
1.2 ASYMETRICKÉ STRATEGIE A TAKTIKY ..... 16
1.3 POVAHY SLABÝCH A SILNÝCH AKTÉRŮ ..... 18
**2 HYBRIDNÍ VÁLKA** ..... **20**
2.1 NÁSTROJE HYBRIDNÍ VÁLKY ..... 21
2.2 FÁZE HYBRIDNÍHO ÚTOKU ..... 23
**3 BEZPEČNOSTNÍ PROSTŘEDÍ ČESKÉ REPUBLIKY** ..... **25**
3.1 BEZPEČNOSTNÍ SYSTÉM ČESKÉ REPUBLIKY ..... 26
3.2 BEZPEČNOSTNÍ LEGISLATIVA ..... 27
3.3 STRATEGICKÉ BEZPEČNOSTNÍ DOKUMENTY ..... 29
3.3.1 Bezpečnostní strategie České republiky ..... 29
3.3.2 Audit národní bezpečnosti ..... 30
3.3.3 Obranná strategie České republiky ..... 31
3.4 VÝROČNÍ ZPRÁVY ZPRAVODAJSKÝCH SLUŽEB ..... 31
3.4.1 Výroční zpráva Bezpečnostní informační služby za rok 2019 ..... 32
3.4.2 Výroční zpráva Vojenského zpravodajství za rok 2019 ..... 33
3.5 ZAJIŠTĚNÍ BEZPEČNOSTI NA MEZINÁRODNÍ ÚROVNI ..... 33
**4 DÍLČÍ ZÁVĚR** ..... **36**
**II PRAKTICKÁ ČÁST** ..... **38**
**5 ANALÝZA ASYMETRICKÝCH A HYBRIDNÍCH HROZEB V ČESKÉ REPUBLICE** ..... **39**
5.1 STANOVENÍ KONTEXTU ..... 39
5.2 IDENTIFIKACE NEBEZPEČÍ ..... 41
5.3 ANALÝZA RIZIK ..... 42
5.4 HODNOCENÍ RIZIK ..... 45
5.5 OŠETŘENÍ RIZIK ..... 46
5.6 BEZPEČNOSTNÍ OPATŘENÍ ..... 47
5.6.1 Terorismus ..... 48
5.6.2 Politický extremismus ..... 49
5.6.3 Kybernetické útoky ..... 50
5.6.4 Dezinformace a propaganda ..... 51
5.6.5 Ozbrojený konflikt ..... 52

**6 DOTAZNÍKOVÉ ŠETŘENÍ K BEZPEČNOSTNÍ SITUACI V ČESKÉ REPUBLICE Z POHLEDU VEŘEJNOSTI ..... 54**
6.1 METODIKA DOTAZNÍKOVÉHO ŠETŘENÍ ..... 54
6.2 VYHODNOCENÍ ODPOVĚDÍ ..... 56
6.3 POSOUZENÍ SOUČASNÉHO STAVU BEZPEČNOSTNÍ SITUACE V ČR ..... 67
**7 NÁVRHY OPATŘENÍ K VĚTŠÍ RESILIENCI PROTI ASYMETRICKÝM A HYBRIDNÍM HROZBÁM ..... 70**
7.1 ZVYŠOVÁNÍ ÚROVNĚ MEDIÁLNÍ GRAMOTNOSTI ..... 70
7.2 VZDĚLÁVÁNÍ A OSVĚTA V OBLASTI ASYMETRICKÝCH A HYBRIDNÍCH HROZEB ..... 71
7.3 IMPLEMENTACE NÁRODNÍ STRATEGIE PRO ČELENÍ HYBRIDNÍMU PŮSOBENÍ ..... 72
7.4 PROHLUBOVÁNÍ A POSILOVÁNÍ SPOJENECKÝCH VZTAHŮ ..... 74
7.5 PODPORA A SPOLUPRÁCE ČESKÉHO OBRANNÉHO PRŮMYSLU ..... 75
7.6 DOSTATEČNÉ FINANCOVÁNÍ OBRANNÉHO ROZPOČTU ..... 77
**ZÁVĚR ..... 78**
**SEZNAM POUŽITÉ LITERATURY ..... 80**
**SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK ..... 88**
**SEZNAM OBRÁZKŮ ..... 89**
**SEZNAM TABULEK ..... 90**
**SEZNAM PŘÍLOH ..... 91**

# ÚVOD

Hybridní hrozby jsou v posledních letech velice skloňovaným tématem, nejenom v České republice, ale i všude ve světě. Bezpečnostní prostředí se z globálního hlediska výrazně mění a to má za následek čím dál více napjaté mezinárodní vztahy. Do popředí se dostávají nové různorodé hrozby, které je těžké identifikovat a předvídat. Vývoj těchto hrozeb nelze odhadnout a v současné době je obtížné definovat protivníky či hranice válečné agrese. S těmito hrozbami se můžeme v dnešní době setkat více méně kdekoliv a kdykoliv. Proto je důležité se o tuto problematiku zajímat a věnovat ji pozornost, abychom věděli, jakým způsobem se máme chovat a co máme dělat, pokud budeme nějaké hybridní hrozbě vystaveni. Už jenom uvážlivé jednání v podobě prověřování zdrojů informací může významným způsobem přispět ke snížení závažného bezpečnostního rizika, jako jsou dezinformace. Neméně důležité také je, aby i stát věděl, jakým způsobem má čelit těmto významným bezpečnostním hrozbám.

Jako téma diplomové práce jsem si vybral Asymetrické konflikty a hybridní válka, a to hned z několika důvodů. Hlavním aspektem pro výběr tohoto tématu je osobní zájem o dané téma. Jelikož jsem příslušník Armády České republiky, není mi tato problematika cizí. Podle mého názoru se jedná bezesporu o aktuální téma, které se týká nás všech, ať už chceme nebo ne. Česká republika momentálně čelí hybridním hrozbám a to především z východu. Dalším důvodem pro výběr tohoto tématu je neustále se měnící bezpečnostní situace, která s sebou přináší nové skutečnosti, o kterých je potřeba zejména pravdivě mluvit a psát.

Tato diplomová práce se bude zabývat problematikou asymetrických a hybridních hrozeb, kterým Česká republika bezpochyby čelí. I když se Česko v aktuální situaci nepotýká s vojenskými hrozbami bezprostředně na svém území, neznamená to, že nečelí hrozbám jiného charakteru, jako jsou například terorismus, informační válka, dezinformace a propaganda, kybernetické útoky, politický extremismus aj. Svoji roli hraje také fakt, že je Česká republika členem EU a NATO, a je tak součástí euroatlantického prostoru. Proto je zapotřebí vnímat bezpečnostní hrozby i u našich spojenců a členů EU. Primárním cílem diplomové práce bude analyzovat problematiku asymetrických a hybridních hrozeb a na základě zjištěných skutečností navrhnout možná opatření pro větší resilienci České republiky vůči těmto hrozbám. Sekundárním cílem bude vyhodnotit současnou bezpečnostní situaci v České republice na základě výsledků z analýzy hrozeb a odpovědí z dotazníkového šetření.

Diplomová práce se bude skládat z teoretické a praktické části. Teoretická část bude obsahovat literární rešerši, vymezení základních pojmů a právní ukotvení vztahující se k řešené problematice. Praktická část bude rozdělena na empiricko-analytickou a aplikační část. V empiricko-analytické části bude provedena analýza hrozeb za pomocí jednoduché bodové polokvantitativní metody „PNH“. Dále bude vyhodnocena současná bezpečnostní situace prostřednictvím odpovědí z dotazníkového šetření a na základě výsledků z analýzy hrozeb. V aplikační části diplomové práce budou navrhnuty konkrétní návrhy opatření k větší resilienci České republiky vůči asymetrickým a hybridním hrozbám.

Přínosem práce by mělo být pochopení důležitosti dané problematiky a kvalifikování nejzávažnějších bezpečnostních hrozeb, kterým Česko momentálně čelí. Dalším přínosem by mělo být zhodnocení, jak veřejnost vnímá bezpečnost České republiky a jaké hrozby jsou pro ně nejvíce zneklidňující. Důležitým přínosem celé práce budou konkrétní návrhy opatření, které budou popsány v závěrečné části. Při jejich implementaci by došlo k značnému posílení obranyschopnosti České republiky. Díky této diplomové práci si každý čtenář může uvědomit důležitost svého jednání a přispět tím k bezpečnějšímu životu nás všech.

# CÍLE A METODY ZPRACOVÁNÍ

Obsahem této kapitoly jsou cíle, které bylo nutné v diplomové práci naplnit a metody, jejichž použitím bylo těchto cílů dosaženo. Primárním cílem diplomové práce je analyzovat problematiku asymetrických a hybridních hrozeb a na základě zjištěných skutečností navrhnout možná opatření pro větší resilienci České republiky vůči těmto hrozbám. Sekundárním cílem je vyhodnotit současnou bezpečnostní situace v České republice na základě výsledků z analýzy hrozeb a odpovědí z dotazníkového šetření. Mezi dílčí cíle patří zpracování literární rešerše, navrhnutí bezpečnostních opatření pro minimalizaci nejzávažnějších rizik a teoretické vymezení základních pojmů k dané problematice.

V praktické části diplomové práce, konkrétně v analyticko-empirické části, jsou použity dvě metody zpracování. První z nich je jednoduchá bodová polokvantitativní metoda „PNH“ používána k hodnocení rizik. Tato metoda je založena na bodovém ohodnocení tří složek – pravděpodobnost vzniku události (P), pravděpodobnost následků (N) a názor hodnotitelů (H). Po bodovém ohodnocení jednotlivých činitelů a jejich následným součinem, je výsledkem samotný ukazatel míry rizika (R). Vzorec pro výpočet rizika je tedy následující: $R = P \times N \times H$. Na základě součinu, který vychází ze vzorce, se určí, do jakého rizikového stupně dané nebezpečí patří, a tím se zjistí míra konkrétního rizika. Pro nepřijatelná (nejzávažnější) rizika jsou poté navrhnuta určitá opatření k jejich minimalizaci. Tato metoda byla vybrána především kvůli zohlednění vlastního názoru hodnotitele, jednoduchému výpočtu míry rizika a přehledné interpretaci výsledků, které jsou uvedeny v tabulce. Pomocí metody „PNH“ jsou tedy klasifikovány nejzávažnější asymetrické a hybridní bezpečnostní hrozby, se kterými se Česká republika v aktuální situaci potýká, a následně jsou navrhnuta opatření pro jejich minimalizaci.

Druhou metodou použitou v praktické části diplomové práci je metoda dotazníkového šetření. Tato metoda se řadí mezi kvantitativní metody, které jsou nejčastěji používány k průzkumům veřejného mínění. Před definitivním zveřejněním dotazníku byl dotazník rozeslán přátelům a rodinným příslušníkům, aby se předešlo špatné a nesrozumitelné formulaci otázek. Při získávaní odpovědí od respondentů byl použit standardizovaný dotazník v elektronické formě a to hned z několika důvodů – komfortnost, srozumitelnost, jednoduchost, vhodnost, časová nenáročnost a anonymita (vysvětlení těchto důvodů je podrobněji popsáno na s. 56). Dotazník byl vytvořen v aplikaci Google Forms, která slouží pro vytváření různých formulářů, anket, dotazníků aj. Sběr dat probíhal ve dnech od 26. 10. 2020 do 26. 12. 2020. Dotazník byl uveřejněn přes různé sociální sítě a rozeslán pomocí

emailů. Dotazník se skládá z 19 uzavřených otázek, z toho jsou tři otázky faktografické. Všechny otázky byly povinné až na poslední výčtovou otázku, kde respondenti nemuseli zaškrtnout žádné políčko. V dotazníku byly použity dichotomické i trichotomické otázky, výběrové a výčtové otázky. Uzavřené otázky byly použity z toho důvodu, aby bylo dosaženo co největšího počtu vyplněných dotazníků. Celkově dotazník vyplnilo 517 respondentů a kompletní dotazník je k nahlédnutí v Příloze P I.

Dotazníkové šetření mělo za cíl zjistit, jestli se veřejnost cítí v Česku bezpečně, jaké hrozby jsou pro respondenty nejvíce zneklidňující a jaký mají názor na dílčí otázky týkající se problematiky bezpečnosti ČR. Celá kapitola se skládá ze tří částí. První část pojednává o metodice prováděného výzkumu, ve druhé části jsou vyhodnoceny a analyzovány odpovědi respondentů a ve třetí části je zhodnocena současná bezpečnostní situace v ČR s přihlédnutím na výsledky z analýzy asymetrických a hybridních bezpečnostních hrozeb metodou PNH a na odpovědi z dotazníkového šetření.

# I. TEORETICKÁ ČÁST

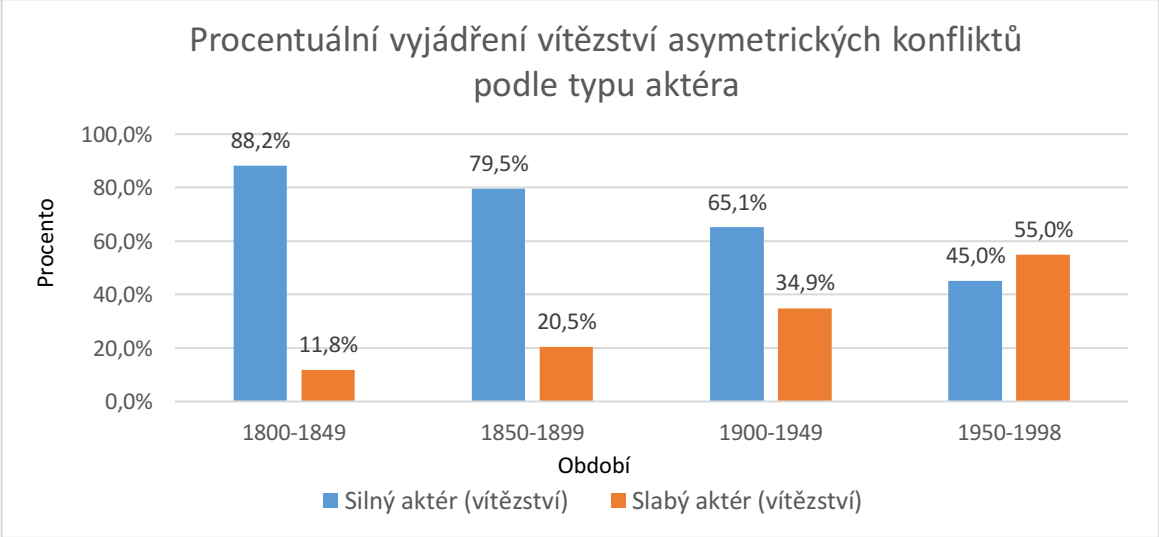
# 1 ASYMETRICKÉ KONFLIKTY

Pojem „asymetrický konflikt“ sahá až do dob počátku samotného lidstva. Už v dávné historii při vytváření nových civilizací, kdy proti sobě v bojích stály rozdílné armády, se dalo mluvit o asymetrických konfliktech. Cassidy (2002, s. 43) ve svém článku zmiňuje, že termín asymetrický konflikt se poprvé objevil již v roce 1974 a použil ho Andrew Mack. Podle Soulemainova (2006, s. 20) se první zmínky o asymetrickém konfliktu objevují až v roce 1995 a to ve dvou amerických dokumentech. První z nich je Doktrína spolupráce mezi druhy vojsk a druhý Národní vojenská strategie. Oba dva dokumenty obsahují definici pojmu asymetrický konflikt, avšak jedná se o naprosto odlišné definice.

Asymetrický konflikt je definován jako *„konflikt protivníků, jejichž prostředky, taktika a strategie jsou obdobné či totožné, nicméně mezi nimi existuje výrazná až zásadní disparita vojenských potenciálů“* (Vojenská strategie, c2008, s. 216). Dle Lele (2014, s. 103) je asymetrický konflikt *„forma války, ve které nestátní aktér používá nekonvenční nástroje a taktiky proti zranitelným místům konkrétního státu, aby dosáhnul neúměrně velkého účinku, s cílem podlomit vůli státu, aby dosáhl svých strategických cílů“*. McKenzie (2000, s. 2) zase definuje asymetrický konflikt jako *„namíření slabšího taktického nebo operačního potenciálu proti slabinám silnějšího oponenta za účelem dosažení disproporčního účinku, jehož cílem je nalomení protivníkova odhodlání, což je v souladu se strategickými cíli asymetrického aktéra“*. I přes všechny zmíněné definice je důležité konstatovat, že pokud hovoříme o asymetrickém konfliktu, hovoříme o strategiích, taktikách, nástrojích, zbraních a zejména lidech, kteří mění průběh a podobu válčení, tak aby minimalizovali výhodu druhé strany (Lele, 2014, s. 102).

Při různých ozbrojených konfliktech často platilo nepsané pravidlo, kdo má větší a modernější vyzbrojenou armádu, má také větší šanci v daném konfliktu dojít do zdárného konce. Jenomže po zkušenostech z minulých let se ukázalo, že tomu tak vždycky není. Převážně konflikty po druhé světové válce a v období studené války, popřípadě konflikty z 21. století ukazují na fakt, že i supervelmoci, které disponují obrovskými finančními prostředky, pumpující stovky miliard dolarů do obrany státu, nestačí na to, aby přemohli relativně slabšího protivníka. Dokonce i v některých konfliktech, se podařilo aktérům s výraznou vojenskou disparitou vyhrát a to se jednalo o aktéry nestátního charakteru. Pravdou však je, že téměř ve všech dosavadních konfliktech v celé historii lidstva docházelo k přinejmenším k mírné silové asymetrii, jinak by nebylo vítězů ani poražených (Krásný, 2003, s. 78).

V asymetrických konfliktech hrají významnou roli nejenom vojenské síly. Zejména nestátní aktéři konfliktů využívají ve svůj prospěch všechny dostupné prostředky, aby dosáhli vytouženého vítězství. Jak píše Mack (1975, s. 175), v konfliktu nezáleží pouze na technologické a vojenské vyspělosti a nadřazenosti, tyto aspekty neznamenají zaručené vítezství. Se zajímavým zjištěním přišel Arreguín-Toft (2001, s. 97), který analyzoval výsledky válek od roku 1800 až do roku 1998. Z grafu (viz obr. 1) je na první pohled patrné, že asymetrie v konfliktech hraje čím dál větší roli. Během bezmála dvou seti let je vidět rapidní nárůst vítězství slabších aktérů v různých konfliktech. Například konflikty mezi lety 1950 a 1998 vyhrál z 55 % slabší aktér, což potvrzuje i tvrzení od Krásného. Arreguín-Toft (2001, s. 96) také zdůvodňuje, čím se toto tvrzení vysvětluje. Hlavním důvodem, proč slabší aktéři častěji vyhrávají války je ten, že silní aktéři nemají na těchto konfliktech veliký zájem a případná prohra pro ně nepředstavuje existenční hrozbu. Na druhé straně slabý aktér je v takovém konfliktu ohrožen samotnou existencí a prohra by pro něj měla s největší pravděpodobností fatální dopad. Podle Arreguína-Tofty (2001, s. 98) může být tento trend častějších vítězství slabších aktérů zapříčiněn demokracií. Demokracie neumožňuje použití vysoké úrovně násilí a brutality na obyvatelstvu i za cenu vítězství.




Obrázek 1: Procentuální vyjádření vítězství asymetrických konfliktů podle typu aktéra ve čtyřech padesátiletých obdobích (Arreguín-Toft, 2001, s. 97; vlastní zpracování).

## 1.1 Zájmy a vůle aktérů

K samotným konfliktům dochází zpravidla, kvůli nějaké příčině. Příčin může být celá řada, ať už vymyšlených nebo reálných. Pravdou je, že definovat hlavní příčinu určitého konfliktu není zdaleka lehké. Někdy se také může jednat pouze o záminky k vyvolání konfliktu, aby následná agrese byla odůvodnitelná. Podle Smolíka a Šmída (2010, s. 32) lze rozdělit

konflikty z hlediska jejich příčin na konflikt zájmů a konflikt hodnot. Pokud se jedná o konflikt zájmů, hovoříme především o těchto konfliktech:

- konflikt o území (pouze pokud území přináší nějaký ekonomický nebo zahraničněpolitický profit, má-li území pouze symbolickou hodnotu, spadá do konfliktu hodnot),
- ekonomický konflikt (konflikt o surovinové zdroje, konflikt o přístup na trhy),
- politický konflikt (prosazování politických cílů, geopolitická nadvláda) (Smolík a Šmíd, 2010, s. 33).

Na druhé straně konflikt hodnot znamená střet o něco méně hmatatelné. V rámci konfliktu hodnot hovoříme:

- o etnických konfliktech,
- o náboženských konfliktech
- a o ideologických konfliktech (Smolík a Šmíd, 2010, s. 33).

*„Kde je vůle, tam je cesta.“* Pro někoho možná klišé, jenže v konfliktech, kde proti sobě stojí výrazně asymetričtí protivníci je právě vůle hnací sílou a motivací, která rozhoduje o úspěchu a neúspěchu účastníka konfliktu. S jistotou se dá říct, že vůle slabého aktéra se přímo odráží v jeho odhodlání a obětavosti přijímat možné vysoké ztráty za cenu vítězství. Kdežto na druhé straně, silný aktér, pro kterého je asymetrický konflikt jakousi omezenou válkou je nepřípustné přijímat jakékoliv oběti. Tato skutečnost je dle Cassidyho (2002, s. 47) významným důvodem, proč slabší aktéři bývají v těchto konfliktech úspěšnější i když čelí znatelně silnějšímu nepříteli. Další významnou roli v asymetrickém konfliktu hraje motivace aktérů. Slabší aktér je motivován především ohrožením své budoucí existence. Do bojů vstupuje slabší aktér se sebeobětováním, které může ovlivnit průběh války natolik, že samotnou válku vyhraje nebo přinutí silnějšího protivníka se stáhnout (Soulemainov, 2006, s. 28). Mezi takové konflikty patří například Válka ve Vietnamu nebo Sovětská válka v Afghánistánu.

## 1.2 Asymetrické strategie a taktiky

Asymetrické strategie a taktiky jsou využívány podle Thortona (2007, s. 3) obvykle u slabších aktérů, avšak není to pravidlem. V aktuálních asymetrických konfliktech stojí proti sobě nejčastěji státní a nestátní aktéři. Mezi nejčastější asymetrické taktiky patří bezpochyby terorismus, partyzánský způsob boje (guerilla), barbarismus, nepravidelné válčení aj. (Lele, 2014, s. 102). Asymetrické strategie jsou jednou z nejdůležitějších nástrojů

slabších aktérů při vedení asymetrického boje a mají veliký vliv na výsledky konfliktů. Podle Arreguína-Tofty (2001, s. 38) je také důležité jaké strategie zvolí všichni účastníci konfliktu. Arreguín-Toft (2001, s. 38-39) popisuje různé druhy strategií, které dělí na ofenzivní a defenzivní. U ofenzivních strategií je řeč o konvenčním útoku a barbarismu, kdežto u defenzivních strategií je řeč o konvenční obraně a guerille. Ofenzivní strategie jsou zpravidla využívány silnými aktéry, naopak defenzivní strategii využívají nejčastěji slabší „nestátní" aktéři.

Další dělení typů strategií podle Arreguína-Tofty (2001, s. 101-105) je rozdělení na strategie přímé a nepřímé. Odlišnosti v těchto typech strategií jsou na první pohled jednoznačné. U přímých strategií je cílem aktéra zničit ozbrojené fyzické síly protivníka, kdežto u nepřímé strategie jde aktérovy o narušení protivníkovy vůle bojovat. Mezi přímé strategie patří konvenční útok a konvenční obrana, zatímco do nepřímých strategií patří terorismus, barbarismus nebo guerilla. Výrazný vliv na výsledek konfliktu má zvolená strategie boje. Pokud aktéři zvolí stejnou strategii, čili přímá – přímá nebo nepřímá – nepřímá, tak podle Arreguína-Tofty (2001, s. 106-107) dochází ve většině případů k vítězství silnějšího aktéra, jelikož disponuje větší vojenskou silou a není ničím potlačen. Při volbě rozdílných strategií, čili přímá – nepřímá nebo nepřímá – přímá dochází k potlačení vojenské síly na straně silnějšího aktéra a ve většině případů zpravidla vyhrává slabší aktér. Pro lepší objasnění těchto interakcí mezi strategiemi asymetrických konfliktů vytvořil Arreguín-Toft (2001, s. 107-108) tabulku (viz tab. 1).

Tabulka 1: Očekávané účinky strategické interakce na výsledky konfliktů (očekávaní výherci v buňkách) (Arreguín-Toft, 2001, s. 108; vlastní zpracování).

| | | **Slabý aktér Strategický přístup** | |
|---|---|---|---|
| | | Přímý | Nepřímý |
| **Silný aktér Strategický přístup** | Přímý | Silný aktér | Slabý aktér |
| | Nepřímý | Slabý aktér | Silný aktér |

Dle Kirchera (2015, s. 8) armády států na celém světě čím dál častěji čelí nepřátelským silám, které používají taktiky a strategie asymetrické války. Tyto nepřátelské síly opakovaně

porušují mezinárodní humanitární právo, a to způsobem jako například schováváním se v civilním obyvatelstvu, útočením na civilní obyvatele, kteří poskytují informace druhým stranám a mnoho dalších. Po teroristických útocích 11. září 2001 na Světové obchodní centrum ve Spojených státech amerických se mnoho zemí po celém světě rozhodlo, že upraví svoje dosavadní politiky obrany. Tímto krokem se také terorismus definitivně zařadil mezi asymetrické hrozby. McKenzie (2000, s. 52) identifikoval moderní hrozby, mezi které patří především zbraně hromadného ničení, informační válka, terorismus aj.

## 1.3 Povahy slabých a silných aktérů

Jak je zmíněno v předešlé podkapitole, v aktuálních asymetrických konfliktech mezi sebou nejčastěji stojí státní a nestátní aktéři. Někteří autoři, jako například Lele (2014, s. 103) a Osinga (2002, s. 267-269), označují zpravidla státní aktéry za silnější a nestátní aktéry za slabší. Hlavním prvkem asymetrického konfliktu mezi aktéry musí byt bezesporu asymetrie. V asymetrických konfliktech je slabší aktér brán jako ten, kdo má nižší počet vojenské síly či techniky. Dále je za něj považován ten, kdo používá jako strategii boje terorismus, barbarství či partyzánství. Dalším znakem slabších aktérů je schopnost využití všech možných výhod, jako například využití geografie na bitevním poli ve svůj prospěch (těžká identifikace útoků) nebo využití různých útočných praktik.

Slabší aktér útočí, když to silnější aktér nejméně čeká a kdekoliv je-li to možné, aby silnějšího aktéra překvapil a způsobil mu, co největší ztráty (Volner, 2007, s. 24-26). Podle Krásného (2003, s. 83) se snaží slabší aktéři kompenzovat své technologické a vojenské nedostatky zejména tím, že odmítají přistupovat na pravidla boje silnějších aktérů a vnucují jim svá vlastní pravidla boje. Slabší aktéři se při obraně soustřeďují na použití nekonvenčních praktik, při kterých se zaměřují na slabiny protivníka (Lele, 2014, s. 99). Slabší aktéři používají např. při zabírání území nehumánní praktiky, jako jsou etnické čistky, šíření strachu a teroru na civilním obyvatelstvu a atentáty na vrcholné představitele protivníků či státníky (Osinga, 2002, s. 269). Cílem slabších „nestátních“ aktérů je dosáhnout takové situace, kdy silnější „státní“ aktér sice nemá takové výrazné ztráty na vojenské síle, ale už nemá vůli dále bojovat, jelikož není schopen nebo nemůže přistoupit na nepřímou strategii boje.

Silnější aktéři bývají zpravidla ti státní, kteří mají vyspělou techniku, moderní zbraně, vycvičené vojáky a především organizovanou strukturu velení a řízení. Jenomže ani tyto výhody častokrát nejsou rozhodujícím znakem v boji. Pokud chtějí silnější aktéři vyhrávat

konflikty, je zapotřebí pochopit způsoby vedení asymetrické války a umět na ně rychle a přirozeně reagovat. Silný aktér musí být během konfliktu flexibilní a dokázat se přizpůsobit asymetrických strategiím svého nepřítele (Krásný, 2003, s. 78).

Jak uvádí Metz a Johnson (2001, s. 15), klíčovým by měly být různé výzkumy a experimenty, které se soustřeďují na asymetrické výzvy. Pomocí těchto experimentů se můžou nestátní silnější aktéři více přizpůsobit slabším aktérům. Jedná se o vytvoření nových vojenských strategií, které budou brát v potaz asymetrický typ boje jako je např. guerilla. Vojáci by tak měli být připraveni na neočekáváné útoky a přizpůsobit tomu své chování a myšlení a využívat všech možných prostředků k odrazení útoku. Pokud vojáci silnějších aktérů budou umět předvídat a rychle reagovat na obtížné situace a pochopí strategie a taktiky slabších aktérů, budou tyto strategie a taktiky neúčinné (Metz a Johnson, 2001, s. 15-16). Silnější aktér ve většině případů disponuje kvalitnějšími prostředky. Při střetech se slabými aktéry častokrát nevyužívá své absolutní síly, jelikož nepovažuje slabšího nepřítele za radikální hrozbu. Tyto boje se ve většině případů odehrávají na území slabších aktéru, a proto není přímo ohrožena existence státu silného aktéra. Tato skutečnost má za následek menší zájem silnějších aktérů a dochází proto k prodlužování konfliktů až do doby, kdy to silnější aktér vůbec nepředpokládal nebo do doby, kdy je nucen své síly stáhnout (Cassidy, 2002, s. 42).

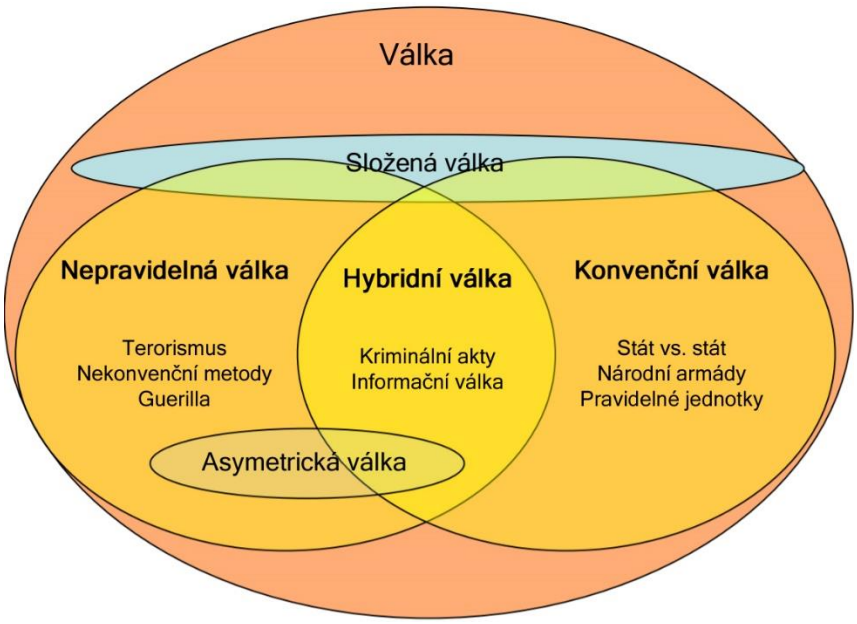
# 2 HYBRIDNÍ VÁLKA

Aby mohl být pochopen pojem hybridní válka, je dobré si připomenout, co představuje pojem obecná válka. S jistotou může být konstatováno, že nejznámější definicí tohoto pojmu je výrok pruského generála Carla Philippa Gottlieba von Clausewitze (1976, s. 87), jehož životním dílem byla kniha *„Vom Kriege“* (O válce), kde je pojem vysvětlen takto *„Válka je jen pokračování politiky jinými prostředky.“* S tímto tvrzením se dá souhlasit, avšak válka nemusí být jen pokračováním politiky, může být také jejím důsledkem. Trochu z obsáhlejšího hlediska je válka vnímána dle McCulloha a Johnsona (2013, s. 6) jako *„organizovaný konflikt mezi ozbrojenými státy, národy nebo jinými stranami v určitém období, za účelem dosažení požadovaného politického/ideologického konečného stavu“*. Podle mého názoru je válka akt násilí, při kterém jsou použity především vojenské prostředky k dosažení určitých cílů a zároveň jsou dodržovány mezinárodní úmluvy. Kdo první použil pojem hybridní válka, není zcela jasné. Frank G. Hoffman (2007, s. 9) tvrdí, že první, kdo použil termín hybridní válka je Robert G. Walker, který tento pojem použil ve své diplomové práci *„Spec Fi: The United States Marine Corps and Special Operation“*.

Velice specifickou definici pro hybridní válku použili Kříž, Bechná a Stevkov, kdy hybridní válku popisují takto: *„Hybridní válka je ozbrojený konflikt vedený kombinací nevojenských a vojenských prostředků s cílem jejich synergickým efektem přinutit protivníka k učinění takových kroků, které by sám o sobě neučinil. Alespoň jednou stranou konfliktu je stát. Hlavní roli při dosažení cílů války hrají nevojenské prostředky v podobě psychologických operací a propagandy, ekonomických sankcí, embarg, kriminálních aktivit, teroristických aktivit a jiných subverzivních aktivit obdobného charakteru“* (Kříž, Bechná a Stevkov, 2016, s. 10).

Hybridní válka slouží ke stejnému účelu jako obecná válka, tedy k dosažení politických/ideologických cílů, nicméně se v některých ohledech liší. Slabina hybridní války spočívá zejména v nejednoznačných demarkačních kritériích válčení. Právě použité prostředky ve válkách, které slouží k dosažení cílů, nám pomáhají pochopit, o jaký typ války se jedná. Jak uvádí ve své publikaci Kříž, Bechná a Stevkov (2016, s. 10) *„Pro hybridní válčení je důležité, že nevojenské prostředky subverzivní povahy mají sehrát hlavní roli.“* V optimálním případě při hybridní válce není využita žádná vojenská síla. Cílem aktéra je použít především osvědčené nástroje, kterými jsou psychologické operace (propaganda), zastrašování terorem, informační válka, kybernetické útoky aj.

Při použití výše zmíněných prostředků a nástrojů hybridní války je samozřejmě těžší prokázat, zda se jedná o válku jako takovou, kdy její výhodou je především popíratelnost. Při relativním míru může agresivní stát provádět hybridní operace, aniž by si toho napadený stát všiml. Je také složité definovat, kdy válka začala a kdy skončí, jelikož útoky můžou být nepravidelné a nepředvídatelné. Tyto všechny aspekty dávají hybridní válce nový rozměr – válka není časově ani prostorově ohraničena, tak jak ji známe. Hybridní válka je prezentována v prostředí ostatních typů válek zhruba tak, jak načrtl ve své práci kapitán Huovinen (2011, s. 9).

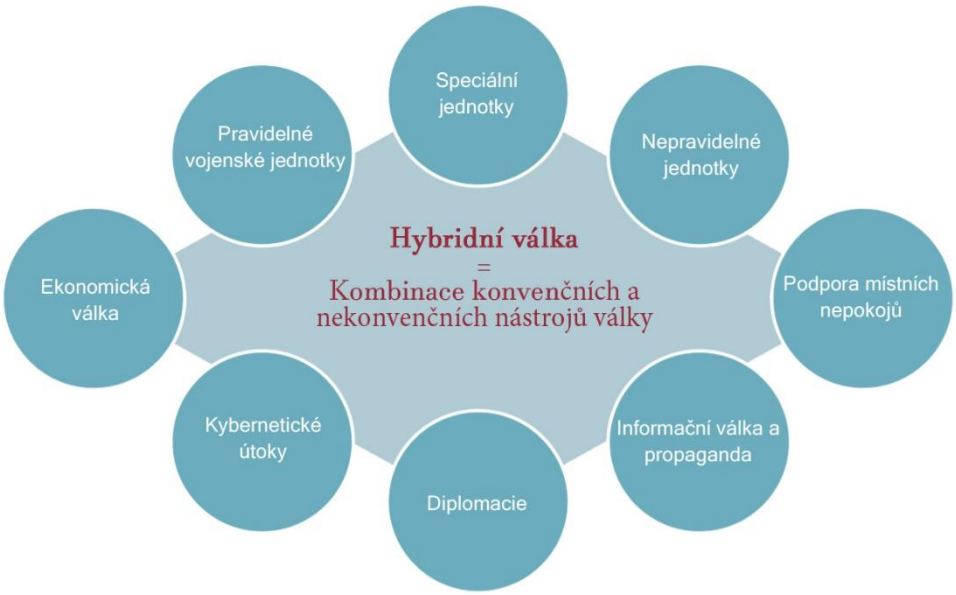



Obrázek 2: Hybridní válka v kontextu s jinými formami války
(Houvinen, 2011, s. 9; vlastní zpracování).

## 2.1 Nástroje hybridní války

Hybridní válka obsahuje široké spektrum nástrojů a změnu pravidel samotné války. Role nevojenských prostředků k dosažení politických a strategických cílů vzrostly a v mnoha případech překročily ve své účinnosti sílu konvenčních zbraní. Ve veliké míře se využívají nástroje zejména politické, ekonomické, humanitární, informační a ostatní nástroje nevojenského charakteru (Munich Security Report 2015, 2015, s. 35). Při vedení hybridní války se používají metody vedení bojů, které spočívají v morálním potlačení nepřítele pomocí různých nástrojů. Zejména informační válka je považována za jeden z nejdůležitějších nástrojů hybridního prostředí. S rapidním rozvojem počítačových technologií a informačních sítí nelze brát tuto stránku věci na lehkou váhu. Je na místě si uvědomit, že informace a data jsou důležitými prvky informační války.

V publikaci Munich Security Report 2015 vyšel přehledný obrázek (viz obr. 4), který stručně a výstižně popisuje všechny složky hybridní války. Mezi hlavní složky hybridní války patří tedy speciální jednotky, nepravidelné jednotky, podpora místních nepokojů (protesty, demonstrace), informační válka (prostřednictvím médií a informačních sítí), propaganda (dezinformační weby, fake news), diplomacie (politický nátlak, využití opozice daného státu), kybernetické útoky (kyberterorismus, útoky hackerů, malware, ransomware aj.), ekonomická válka (uvalení sankcí a cel) a pravidelné vojenské jednotky (Munich Security Report 2015, 2015, s. 35).




Obrázek 3: Hlavní složky hybridní války (Munich Security Report 2015, 2015, s. 35; vlastní zpracování).

Informační válka a propaganda patří v posledních letech mezi stěžejní nástroje hybridní války. Na základě informační války jsou vedeny tzv. informační operace. Řehka (2017, s. 142) tyto informační operace definuje jako *„proces, který integruje účinky jednotlivých vojenských informačních aktivit k dosažení požadovaných informačních cílů“*. Mezi další nepostradatelný nástroj patří propaganda. Podle Řehky dělíme propagandu na bílou, šedou a černou. Bílá propaganda neskrývá svůj skutečný zdroj a obsahuje zejména pravdivé a přesné informace Šedá propaganda neuvádí žádný zdroj a černá propaganda uvádí schválně falešný nebo nepřesný zdroj a obsahuje podvratné a nepravdivé informace (Řehka, 2017, s. 64-64). Neméně důležitá je i tzv. dezinformační kampaň, která je použita pomocí sdělovacích prostředků, zejména internetu (sociální sítě.) Dle TDKIV (Kučerová, 2003) je dezinformace definována takto: *„Záměrně nepravdivá (falešná, lživá, nesprávná, zkreslená)*

*informace sdělovaná s cílem uvést v omyl a ovlivnit příjemce tím, že ji bude považovat za pravdivou a důvěryhodnou.“*

Kybernetické útoky patří také k primárním nástrojům hybridních válek. V kybernetickém prostoru je stále víc a víc citlivých informaci, jak už z prostředí státní infrastruktury, bankovního prostředí ale i sociálních síti. V tomto ohledu mohou být data a informace neoprávněně odcizeny a použity útočníkem pro získání politické, ekonomické a jiné výhody. Pro získávání a zneužívání těchto dat a informací jsou používány především kybernetické útoky typu malware (Jirásek, Novák a Požár, 2013, s. 58-59).

## 2.2 Fáze hybridního útoku

I když fáze hybridního útoku nejsou jasně mezinárodně terminologicky definovány, v dokumentu Background Report 2015 je popsán stručný popis jednotlivých fází hybridního útoku, který je z pohledu autorů považován za přínosný (Hybrid Threats, 2015, s. 8). Podle Ženevského centra pro bezpečnostní politiku se hybridní útok děli na přípravnou fázi, útočnou fázi a následnou fázi. Podobný názor má i finský výzkumný pracovník András Rácz, který ve své publikaci definuje fáze hybridního útoku na přípravnou, útočnou a stabilizační (2015, s. 58).

Přípravná fáze hybridního útoku spočívá v konkrétních krocích a rozhodnutích, které jsou přijaty a uskutečněny ještě před samotným provedením útoku. Tato fáze obsahuje různorodé kroky ve smyslu přípravy moci v ekonomickém, vojenském a soukromém sektoru, získání politického mandátu, hraní diplomatických her a především přijímání kroků v domácí politice za účelem získání podpory společnosti se záměrem nastolení kontroly médií a ovlivňování sociálních sítí. V této fázi je potřeba sledovat všechny podezřelé aktivity a včas reagovat na varovné signály, které by mohly mít pro západní společnost a NATO neblahé následky (Hybrid Threats, 2015, s. 8-9).

Fáze útoku bývá zpravidla nejkratší fází. Zahrnuje především kombinaci dostupných útoků, vojenského a nevojenského charakteru. Obvykle se jedná o vojenské operace, operace polovojenských a speciálních jednotek, politické a diplomatické kroky, teroristické a kybernetické hrozby a útoky s domácí podporou, která je zajištěna dezinformacemi a propagandou. V některých případech je těžké identifikovat, kde je hranice začátku hybridní války a rozlišit tak o jakou válku se jedná nebo v jaké fázi se útok nachází (Hybrid Threats, 2015, s. 9).

Poslední fází hybridního útoku je následná neboli stabilizační fáze, která má za cíl zajistit uskutečnění stanovených ideálů hybridního útoku a častokrát obsahuje politické, diplomatické a vojenské kroky v reakci na aktuální situaci. Tato fáze přichází po samotném útoku a z tohoto důvodu je velice obtížné ji identifikovat. Bývá často přirovnávána k diplomatické šachové hře, která má za úkol uvolnit cestu k vítězství (Hybrid Threats, 2015, s. 9). Aby bylo vůbec možné zahájit a vést hybridní válku, musí být naplněny stanovené podmínky. Podle Rácze se jedná o tyto podmínky:

- převaha útočníků v konvenčních prostředcích,
- chatrná a nízká úroveň vlády v cílené zemi,
- dlouhodobě špatná legitimita centrální vlády v určitém regionu cílené země,
- přesvědčivá a silná mediální podpora,
- přítomnost ozbrojených sil nebo společné hranice s cílenou zemí.

Pokud nejsou z větší části naplněny tyto podmínky, hybridní útok nemusí být úspěšný (Rácz, 2015, s. 73-82).

# 3 BEZPEČNOSTNÍ PROSTŘEDÍ ČESKÉ REPUBLIKY

Z globálního hlediska dochází v posledních letech v bezpečnostním prostředí k výrazným změnám. Po několikaleté stabilizaci přicházejí dynamické proměny bezpečnostního prostředí. Aspekty ovlivňující mezinárodní vztahy jsou dnes více rizikové a komplikované, než před dvěma desetiletími. Do popředí se dostávají nové různorodé hrozby, které je těžké identifikovat a předvídat. Vývoj těchto hrozeb nelze odhadnout a v současné době se dostáváme do situací, při kterých je obtížné definovat i protivníky či hranice válečné agrese. Česká republika se v aktuální situaci nepotýká s vojenskými hrozbami bezprostředně na svém území, to však neznamená, že nečelí hrozbám jiného charakteru. Česká republika jako plnohodnotný člen Severoatlantické aliance (NATO), musí plnit závazky jako ostatní spojenci a zejména se musí podílet na udržování a rozvíjení svojí individuální a kolektivní schopnosti odolat ozbrojenému konfliktu, jak je zmíněno v 3. článku Washingtonské smlouvy (Stojar, 2018, s. 3-5).

Stojar tvrdí, že Česká republika se v aktuální situaci nepotýká s vojenskými hrozbami bezprostředně na svém území a podobné tvrzení uvádí i Bezpečnostní strategie České republiky z roku 2015. Doslova je v dokumentu uvedeno *„Pravděpodobnost přímého ohrožení území ČR masivním vojenským útokem je nízká“* (Kolektiv autorů, 2015, s. 8). Podle mého názoru je tato informace v roce 2021 pořád aktuální. Na druhou stranu je důležité zmínit, že ne všechny státy Evropské unie (EU) a NATO jsou na tom stejně jako my. Podle Bezpečnostní strategie ČR se bezpečnost a stabilita v hraničních státech Evropy (zejména pobaltské státy, Ukrajina) a v oblastech sousedící s Evropou výrazně snižují. Z tohoto hlediska nelze zcela vyloučit možné přímé ohrožení některého z členských států EU či NATO. Ohrožení může mít tradiční vojenskou povahu nebo může být použita forma tzv. hybridního válčení. Pro Českou republiku je proto důležitým prvkem, ke snížení těchto rizik, členství v EU a NATO, ale také dobré vztahy se sousedními státy.

Podle Bezpečnostní strategie ČR 2015 patří mezi hlavní zdroje hrozeb zejména *„vyhrocené postoje vůči hodnotovým základům naší společnosti, ohrožující koncept demokratického právního státu a popírající základní lidská práva a svobody“* (Kolektiv autorů, 2015, s. 8). Tyto postoje mohou mít jak státy, tak i různé organizace či nestátní aktéři. Mezi další zdroje hrozeb patří také mocenské úmysly některých států a velmocí, které nerespektují mezinárodní uspořádání a základní principy mezinárodního práva (Kolektiv autorů, 2015, s. 8).

## 3.1 Bezpečnostní systém České republiky

Primárním nástrojem k zajištění vnější i vnitřní bezpečnosti České republiky je bezpečnostním systém ČR. Jde o komplexní uspořádaný systém, který díky svým vzájemným vazbám, napříč všemi jednotlivými zainteresovanými orgány, může rychle reagovat na krizové a mimořádné situace, jak vojenského, tak i nevojenského charakteru. Také slouží k prevenci a přípravě na možné krizové situace a zajišťuje i jejich včasnou identifikaci a varování (Kolektiv autorů, 2015, s. 23). Podle Balabána a Pernici je základní funkcí bezpečnostního systému ČR *„řízení a koordinace činnosti jednotlivých složek odpovědných za zajišťování bezpečnostních zájmů ČR"* (2015, s. 91). Jelikož je Česká republika vystavena stále novým a nepředvídatelným hrozbám, je zapotřebí, aby bezpečnostní systém ČR včasně reagoval na měnící se podmínky a změny v bezpečnostním prostředí. Právě toto je důvod, proč je vnímán bezpečnostní systém České republiky jako otevřený, jenž se postupně přizpůsobuje neustále se vyvíjející bezpečnostní situaci v ČR a ve světě (Balabán a Pernica, 2015, s. 91).

Dle Šestáka a kolektivu je bezpečnostní systém tvořen z mnoha prvků, zejména ze zákonodárné, výkonné a soudní moci, prvků územní samosprávy, ale i z právnických a fyzických osob. Mezi prvky bezpečnostního systému České republiky řadíme:

- orgány moci zákonodárné (Parlament ČR – Poslanecká sněmovna a Senát),
- orgány moci výkonné (Prezident republiky, vláda, ministerstva, ústřední orgány státní správy, další správní úřady s celostátní působností),
- orgány moci soudní (Ústavní soud, Nejvyšší soud, Vrchní soud aj.),
- orgány ustavené v souladu s ústavou ČR (Česká národní banka a Nejvyšší kontrolní úřad aj.),
- ozbrojené síly České republiky (Armáda ČR, Hradní stráž, Vojenská kancelář Prezidenta republiky),
- ozbrojené bezpečnostní sbory (Policie ČR, Vězeňská služba aj.),
- zpravodajské služby (Bezpečnostní informační služba, Vojenské zpravodajství, Úřad pro zahraniční styky a informace),
- záchranné sbory a služby (Hasičský záchranný sbor ČR, Zdravotnická záchranná služba, Báňská záchranná služba a Letecká pátrací a záchranná služba),
- instituce a orgány s územní působností – krajská úroveň,
- instituce a orgány s územní působností – obce s rozšířenou působností,

- instituce a orgány s územní působností – obecní a místní úroveň,
- právnické a fyzické osoby (Šesták et al., 2015, s. 33-42).

Dle ústavního zákona o bezpečnosti České republiky, bezpečnost ČR *„zajišťují ozbrojené síly, ozbrojené bezpečnostní sbory, záchranné sbory a havarijní služby. Státní orgány, orgány územních samosprávných celků a právnické a fyzické osoby jsou povinny se podílet na zajišťování bezpečnosti České republiky. Rozsah povinností a další podrobnosti stanoví zákon“* (Česko, 1998).

## 3.2 Bezpečnostní legislativa

Bezpečnostní legislativa podle Balabána a Stejskala *„nastavuje legislativní prostředí, které umožňuje a zároveň omezuje realizaci konkrétní bezpečnostní politiky“* (2010, s. 75). K zajištění bezpečnosti státu patří neodmyslitelně legislativa zabývající se bezpečností České republiky, jež je zakotvena v českém právním řádu.

Tabulka 2: Postavení bezpečnostní legislativy v právním řádu ČR (Balabán a Stejskal, 2010, s. 71; vlastní zpracování).

| **Právní řád ČR**<br>(včetně nelegislativních materiálů)<br>↓ |
|---|
| **Ústavní pořádek ČR**<br>(zejména Ústava, Listina základních práv a svobod, ústavní zákon o bezpečnosti ČR)<br>↓<br>**Mezinárodní smlouvy**<br>(ve smyslu čl. 10 a násl. Ústavy)<br>↓<br>**Zákony**<br>(krizový zákon, zákon o IZS, zákon o ozbrojených silách)<br>↓<br>**Prováděcí právní předpisy**<br>(vyhlášky a nařízení vlády)<br>↓<br>**Dokumenty schválené usnesením vlády České republiky**<br>(nelegislativní povahy – například strategie i legislativní povahy – usnesení vlády)<br>↓<br>**Ostatní materiály**<br>(podpůrné výklady, názory, odborné materiály) |

Na základě bezpečnostních dokumentů přijatých vládou České republiky, ale i mezinárodních dokumentů přijatých v rámci NATO a EU, je postavena tzv. krizová a branná legislativa, která slouží ke správnému fungování všech zainteresovaných složek při

vzniku krizové situace nebo mimořádné události. Mezi hlavní zákony branné a krizové legislativy patří zejména ústavní zákon č. 1/1993 Sb., Ústava České republiky a ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky (Šesták et al., 2015, s. 4-5). Do tohoto bezpečnostního balíčku právních předpisů patří mnoho dalších zákonů, nařízení, vyhlášek a směrnic, ale mezi ty nejdůležitější řadíme zákony, viz níže.

**Ústavní a klíčové zákony:**

- ústavní zákon č. 1/1993 Sb., Ústava České republiky, ve znění pozdějších předpisů,
- ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky, ve znění ústavního zákona č. 300/2000 Sb.,
- ústavní zákon č. 23/1991 Sb., kterým se uvozuje LISTINA ZÁKLADNÍCH PRÁV A SVOBOD jako ústavní zákon Federálního shromáždění České a Slovenské Federativní Republiky,
- zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů,
- zákon č. 241/2000 Sb., o hospodářských opatřeních pro krizové stavy a o změně některých souvisejících zákonů, ve znění pozdějších předpisů,
- zákon č. 222/1999 Sb., o zajišťování obrany ČR, ve znění pozdějších předpisů,
- zákon č. 585/2004 Sb., o branné povinnosti a jejím zajišťování (branný zákon), ve znění pozdějších předpisů (Ochrana obyvatelstva a krizové řízení, 2015, s. 92-93).

**Další zákony:**

- zákon č. 239/2000 Sb., o integrovaném záchranném systému a o změně některých zákonů, ve znění pozdějších předpisů,
- zákon č. 320/2015 Sb., o Hasičském záchranném sboru České republiky a o změně některých zákonů, ve znění pozdějších předpisů,
- zákon č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů,
- zákon č 219/1999 Sb., o ozbrojených silách České republiky, ve znění pozdějších předpisů,
- zákon č 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů,
- zákon č. 129/2000 Sb., o krajích (krajské zřízení), ve znění pozdějších předpisů,
- zákon č. 128/2000 Sb., o obcích (obecní zřízení), ve znění pozdějších předpisů (Ochrana obyvatelstva a krizové řízení, 2015, s. 92-93).

## 3.3 Strategické bezpečnostní dokumenty

Strategické bezpečnostní dokumenty jsou nezbytnou součástí bezpečnostní legislativy České republiky a vycházejí právě ze strategického vládnutí. Jedná se v podstatě o výstupy strategického cyklu. V takovém strategickém cyklu jsou identifikovány aktivity a určeny tak i optimální strategické bezpečnostní dokumenty (Balabán a Stejskal, 2010, s. 77). Mezi zásadní strategické bezpečnostní dokumenty patří zejména:

- Bílá kniha o obraně z roku 2011,
- Koncepce ochrany obyvatelstva do roku 2020 s výhledem do roku 2030 z roku 2013,
- Bezpečnostní strategie České republiky z roku 2015,
- Audit národní bezpečnosti z roku 2016,
- Obranná strategie České republiky z roku 2017,
- Koncepce výstavby Armády České republiky 2030 z roku 2019,
- Koncepce přípravy občanů k obraně státu 2019–2024 z roku 2019.

### 3.3.1 Bezpečnostní strategie České republiky

Jako primární strategický bezpečnostní dokument České republiky bezesporu patří Bezpečnostní strategie ČR z roku 2015, na který navazují další strategie a koncepce. Z pohledu obsahu této strategie, se jedná o dokument, který navazuje na své předešlé verze z roku 2003 a 2011. Schválení této strategie přišlo ve správnou chvíli, jelikož tehdejší mezinárodní bezpečnostní prostředí se rapidně zhoršilo, a to zejména v roce 2014. Podle Komentáře think-tanku Evropské hodnoty autoři Bezpečnostní strategie *„opět zvolili metodu exaktního popisu a analýzy jednotlivých fenoménů, vyhýbají se však pojmenování jednotlivých nositelů hrozeb“* (2015, s. 1). Bezpečnostní strategie reaguje a popisuje stav bezpečnostního prostředí včetně klíčových hrozeb v euroatlantickém prostoru. Hlavním cílem Bezpečnostní strategie *„je zajistit systémový a koordinovaný rámec prosazování bezpečnostních zájmů ČR, přispět k efektivnímu využívání jednotlivých multilaterálních, bilaterálních i národních nástrojů a poskytnout vodítko pro odpovídající alokaci zdrojů pro účely bezpečnostní a obranné politiky“* (Kolektiv autorů, 2015, s. 5).

Dokument Bezpečnostní strategie je rozdělen do několika částí. Jedná se o východiska bezpečnostní politiky ČR, bezpečnostní zájmy ČR, bezpečnostní prostředí a strategie prosazování bezpečnostních zájmů ČR. Kapitola o východiscích bezpečnostní politiky ČR pojednává o úkolech vlády a orgánů všech územních samosprávních celků, o klíčovém významu politické a hospodářské stability EU, o principech bezpečnosti ČR apod. V další

kapitole jsou rozebrány bezpečnostní zájmy ČR, které se dělí na životní, strategické a další významné. Důležitou částí dokumentu je strategický kontext bezpečnostního prostředí ČR, kde je definováno, jakým způsobem máme vnímat možnou hrozbu vůči České republice a jak tyto hrozby eliminovat (Kolektiv autorů, 2015, s. 8).

I když se v dokumentu neobjevují konkrétní jména aktérů, dle Komentáře think-tanku Evropské hodnoty jsou těmito aktéry myšleni zejména Islámsky stát, který používá tzv. zahraniční bojovníky a Rusko, které je označeno za asymetrickou hrozbu, kvůli zneužívání pozice výhradního dodavatele strategických surovin (2015, s. 2). Dále jsou ve strategii dle Komentáře think-tanku Evropské hodnoty přehodnoceny bezpečnostní hrozby a na prvním místě se již nenachází terorismus, ale Rusko, jenž se snaží revidovat mezinárodní uspořádání za pomocí hybridního válčení (2015, s. 3). Mezi další významné hrozby patří nestabilita a regionální konflikty v euroatlantickém prostoru a jeho okolí, terorismus, šíření zbraní hromadného ničení a jejich nosičů, kybernetické útoky, negativní aspekty mezinárodní organizace, extremismus aj. (Kolektiv autorů, 2015, s. 11-12).

### 3.3.2 Audit národní bezpečnosti

Dalším důležitým materiálem v oblasti bezpečnosti České republiky je Audit národní bezpečnosti, který byl schválen vládou České republiky 14. 12. 2016. Hlavním cílem auditu bylo zjistit, jestli je ČR schopná identifikovat konkrétní hrozby a jakým způsobem je schopná čelit těmto závažným bezpečnostním hrozbám. Audit si kladl také za cíl ověřit nastavenou bezpečnostní legislativu a fungování bezpečnostního systému. Na auditu se podílelo více než 100 odborníků rozdělených do skupin podle své kvalifikace. Audit se podrobně zaměřuje celkem na 11 zásadních bezpečnostních témat. Každé téma se skládá z popisu a evaluace hrozby a rizik, výčtu odpovědných institucí a základních nástrojů pro eliminaci hrozeb, SWOT analýzy dané oblasti a konkrétních doporučení pro vládu k posílení odolnosti (Audit národní bezpečnosti, 2016, s. 2-9).

Jelikož má audit více než 140 stran, zmíním z mého pohledu jen ty nejdůležitější pasáže. Například v kapitole Působení cizí moci je definováno, že na základě informací od zpravodajských služeb a od jiných zdrojů je Ruská federace, Čínská lidová republika a Islámský stát hrozbou pro Českou republiku. Další zajímavou kapitolou je Hybridní hrozby a jejich vliv na bezpečnost občanů ČR, kde je zmíněna Ruská federace a Islámský stát jako možní aktéři konfliktů používající nástroje hybridní války (Audit národní bezpečnosti, 2016, s. 50 a 128).

### 3.3.3 Obranná strategie České republiky

Obranná strategie České republiky schválená vládou ČR v roce 2017 je aktualizací své předešlé verze z roku 2012, a to vzhledem k vývoji mezinárodního bezpečnostního prostředí. Podle bývalého ministra obrany pana Martina Stropnického je Obranná strategie ČR jedním z řady systémových opatření k posílení zajišťování obranyschopnosti České republiky. *„Obranná strategie vymezuje přístup vlády České republiky k zajišťování obrany České republiky. Určuje způsob naplňování hlavních úkolů ozbrojených sil České republiky a představuje základní zadání pro navazující plánovací proces“* (Obranná strategie České republiky, 2017, s. 6).

Obranná strategie vychází z platných právních předpisů, mezinárodních smluv a souvisejících zákonů. Navazuje na Bezpečnostní strategii České republiky a bere v potaz i dokumenty vycházející z NATO a EU, např. Strategická koncepce NATO a Globální strategie EU. Strategie má základ na tzv. třech pilířích obrany – stát, ozbrojené síly a občan. První pilíř stojí na zodpovědném přístupu státu k obraně České republiky a spojeneckým závazkům, druhý pilíř stojí na akceschopných ozbrojených silách a třetí pilíř se opírá o občanskou povinnost k obraně státu (Obranná strategie České republiky, 2017, s. 6-14). Mezi důležité poznatky vyplývající ze strategie patří například záměr, že Vláda ČR zajistí postupné navyšování zdrojů na obranu, aby v roce 2020 dosáhla úrovně 1,4 % HDP. Tento záměr nebyl naplněn, jelikož za rok 2020 výdaje na obranu činily 1,28 % HDP (viz Příloha P II). Nicméně je chvályhodné, že křivka v posledních letech má rostoucí tendenci (Černochová, 2017).

Na straně č. 7 jsou dále zmíněny hrozby pro země EU a NATO ve formě Ruské federace, která otevřeně realizuje své mocenské ambice a to především pomocí hybridních kampaní, včetně cílených dezinformačních aktivit a kybernetických útoků. Ve strategii je také uveden Islámský stát, který může ohrožovat zejména slabé a hroutící se státy nastolením nestability země, prostřednictvím extremistických radikalizovaných skupin, terorismu a zvyšováním ilegální migrace (Obranná strategie České republiky, 2017, s. 7).

## 3.4 Výroční zprávy zpravodajských služeb

V České republice působí aktuálně tři zpravodajské služby, Bezpečnostní informační služba (BIS), Vojenské zpravodajství (VZ) a Úřad pro zahraniční styky a informace (ÚZSI). Jejich postavení, působnost, koordinaci, spolupráci a kontrolu upravuje zákon č. 153/1994 Sb., o zpravodajských službách České republiky, ve znění zákona č. 227/2019 Sb. V roli české

kontrarozvědky působí BIS, v roli české rozvědky působí ÚZSI a Vojenské zpravodajství využívá rozvědné i kontrarozvědné činnosti (Česko, 1994a). Zpravodajské služby, kromě ÚZSI, vydávají každoročně výroční zprávy, které informují veřejnost o možných hrozbách a činnostech, které mohou ohrozit bezpečnost nebo významné ekonomické zájmy ČR, dále pojednávají o aktivitách zahraničních zpravodajských služeb působících na našem území apod. Nevýhoda těchto výročních zpráv spočívá v jejich uveřejňování, které je téměř s ročním zpožděním. BIS i VZ uveřejnilo výroční zprávy za rok 2019 ve stejný den a to 10. 11. 2020.

### 3.4.1 Výroční zpráva Bezpečnostní informační služby za rok 2019

Primární úkol BIS je získávat, shromažďovat a vyhodnocovat informace důležité pro bezpečnost, ochranu ústavního zřízení, demokratických principů a významných ekonomických zájmů ČR. V zákoně o BIS je definováno, že *„Postavení a působnost Bezpečnostní informační služby a její spolupráci s ostatními zpravodajskými službami České republiky upravuje zvláštní zákon“* (Česko, 1994b). Tímto zákonem se zde myslí zákon č. 153/1994 Sb., o zpravodajských službách České republiky, ve znění zákona č. 227/2019 Sb. (Česko, 1994b).

Samotná výroční zpráva BIS upozorňuje v kapitole „Zpravodajská činnost a zpravodajské poznatky“ na čínské zpravodajské služby, které při své činnosti v roce 2019 využívaly otevřenosti českého prostředí k nabídce čínských investic. Dále zpráva dodává, že intenzita čínských zpravodajských aktivit nezaostává za ruskými. Důležité je také zmínit, že Rusko usiluje o destabilizaci a rozklad svých protihráčů, kdežto Číně jde o vybudování sinocentrické globální komunity, kde ostatní národy uznávají legitimitu čínských zájmů a přiznávají Číně respekt, který ji náleží (Výroční zpráva BIS za rok 2019, 2020, s. 8-10). Dále je ve zprávě uvedeno, že se čínští zpravodajci intenzivně angažovali v české akademické sféře. Zájem těchto zpravodajců cílil na technologická témata, zejména vojenství, bezpečnost, zdravotnictví, ekonomiku a témata mezinárodní a domácí politiky. BIS reagovala na Čínské zpravodajské služby takto: *„Na území ČR byli v roce 2019 aktivní zejména příslušníci civilní rozvědky Ministerstva státní bezpečnosti (MSS) a vojenské rozvědky (MID)“* (Výroční zpráva BIS za rok 2019, 2020, s. 10).

Ve zprávě je také podrobně popsána činnost Ruské zpravodajské služby. BIS například vidí riziko v proruských aktivistech, kteří intenzivně vystupují proti politickému uspořádání Česka a členství v Evropské unii a NATO. BIS se zaměřila i na ostatní zpravodajské služby

působící na území České republiky, kdy jde především o severokorejskou a íránskou činnost (Výroční zpráva BIS za rok 2019, 2020, s. 3). Mluvčí BIS pan Ladislav Šticha uvedl, že *„BIS označuje za rizikové země ty, které mají nedemokratický systém, a které aktivně působí proti České republice, proti Severoatlantické alianci nebo Evropské unii“* (Čínské zpravodajské služby využívají…, 2002).

### 3.4.2 Výroční zpráva Vojenského zpravodajství za rok 2019

VZ má za úkol zabezpečovat informace o možném vojenském ohrožení ČR, o činnostech namířených proti obraně ČR a o činnostech ohrožujících utajované skutečnosti v oblasti obrany ČR (Kdo jsme, ©2020). V zákoně o VZ je definováno, že postavení a působnost VZ a jeho spolupráci se složkami upravuje zákon č. 153/1994 Sb., o zpravodajských službách České republiky, ve znění zákona č. 227/2019 Sb. (Česko, 2005).

Zpráva se zaměřuje na vybrané problematiky, které jsou podle VZ důležité především z hlediska současného a budoucího vývoje. Hned v první pasáži je uvedeno, že napětí mezi globálními rivaly (USA, Čína a Rusko) rapidně vzrostlo. Zpravodajci se domnívají, že reálnou hrozbou je válka, jež se nachází v první fázi, avšak pořád není pozdě tuto hrozbu zvrátit. Co se týká konkrétních hrozeb, zpravodajci varují před kybernetickými útoky, špionáží a kyberzločinem. Dodávají, že ve většině případů jsou útočníci nedohledatelní. Možnými cíli útoku jsou podle výroční zprávy telefony nebo chytré domácnosti. Riziko těchto hrozeb také roste s nízkou kybernetickou gramotností uživatelů, kteří podceňují základní bezpečnostní pravidla (Výroční zpráva VZ za rok 2019, 2020, s. 4-7).

Podle výroční zprávy je velikým rizikem k teroristickým útokům zneužiti bezpilotních prostředků, díky jejich snadné dostupnosti i v Česku. Těmito technologiemi by mohla být napadena např. veřejná shromáždění, dopravní prostředky nebo prvky kritické infrastruktury. Podle VZ bude hrozba zneužití bezpilotních prostředků proti civilním cílům růst a tato hrozba nesmí být podceňována nebo bagatelizována (Výroční zpráva VZ za rok 2019, 2020, s. 11-13).

## 3.5 Zajištění bezpečnosti na mezinárodní úrovni

Bezpečnost České republiky je z pohledu mezinárodní úrovně zajišťována především multilaterálními mechanismy v rámci NATO a EU. Severoatlantická aliance a funkční systém kolektivní obrany jsou zásadními pilíři v garanci bezpečnosti České republiky. Pokud chceme brát, musíme i dávat a v tomto případě to platí dvojnásob, a proto musí být

Česká republika schopná plnit spojenecké závazky, ke kterým se zavázala. Jelikož se stále více oslabují mechanismy kooperativní bezpečnosti i politických a mezinárodněprávních závazků v oblasti bezpečnosti, stejně tak roste nestabilita v některých spojeneckých zemích a zvyšuje se riziko regionálních konfliktů, je zapotřebí tyto hrozby zmírňovat nebo eliminovat. Česká republika k tomu využívá jak bilaterální vztahy, tak alianční a unijní nástroje, Organizaci spojených národů (OSN) a Organizaci pro bezpečnost a spolupráci v Evropě (OBSE) (Kolektiv autorů, 2015, s. 3 a 15).

NATO neboli Severoatlantická aliance, někdy také Organizace severoatlantické smlouvy, byla založena v roce 1949 a k 1. 1. 2021 má 30 členů. Její hlavní úlohou je zajišťovat svobodu a bezpečnost členským zemím politickými a vojenskými prostředky. NATO nedisponuje velikým množství vlastních stálých vojenských sil, avšak členové se po vzájemné dohodě zapojují do operací dobrovolně. Nejvyšším politickým rozhodovacím orgánem v rámci NATO je Severoatlantická rada, která přijímá všechna rozhodnutí konsensem. Funguje také spolupráce s nečlenskými státy a organizacemi na základě různých partnerství, např. Partnerství pro mír, Euroatlantická rada partnerství, Středomořský dialog, Istanbulská iniciativa spolupráce, spolupráce s OSN, EU nebo OBSE aj. Česká republika je členem NATO od 12. března 1999 (NATO, ©2020).

Bývalý druhý generální tajemník OSN, v letech 1953 až 1961, Dag Hammarskjöld jednou pronesl, že *„OSN nebyla založena proto, aby dovedla lidstvo do nebe, ale aby ho zachránila před peklem“* (Vše o OSN, 2014, s. 2). Podle mého názoru jde o velice výstižný citát, který jasně definuje roli OSN v rámci celého světa. OSN vznikla 24. října 1945 a u zrodu stálo 51 států, včetně bývalého Československa. Dnes má OSN 193 členů. *„OSN je mezinárodní organizací sdružující nezávislé státy, jejichž společným cílem je ochrana míru a bezpečnosti a zlepšování podmínek pro život lidí na celém světě“* (Vše o OSN, 2014, s. 5).

Každý stát, který vstoupí do OSN, musí přijmout cíle a pravidla Charty OSN – jedná se o soubor pravidel, práv a povinností, kterými se členské státy musí řídit. OSN má šest orgánů zodpovědných za zajištění světového míru a bezpečnosti. Nejdůležitější orgán je Rada bezpečnosti OSN, jelikož usnesení ostatních orgánů jsou pouze doporučující, kdežto rozhodnuti Rady bezpečnosti OSN je závazné a Rada si může jejich splnění vynucovat silou (Česko, 1947).

Rada je složena z 15 členů, kdy nejvýznamnější postavení má pět stálých členů, kterým náleží právo veta. Nejvíce tohoto práva využívá Rusko a na druhé příčce se umísťují Spojené státy americké (USA). I právě proto chtějí někteří členové OSN reformovat Radu

bezpečnosti OSN, ovšem k tomu potřebují souhlas nejméně dvou třetin členských zemí a souhlas všech pěti stálých členů (Veto List, ©2020). Členství České republiky v OSN umožňuje aktivně prosazovat politické, ale i ekonomické zájmy a posilovat mezinárodní prestiž země (Česká republika v OSN, ©2020).

Další organizací, jež je Česko součástí se nazývá Organizace pro bezpečnost a spolupráci v Evropě, která hraje důležitou roli v předcházení konfliktů, prohlubování stability apod. Podle Bezpečnostní strategie jsou jejími nástroji *„volební pozorovací mise, mechanismy na podporu svobody médií, opatření na zvýšení transparentnosti v oblasti kontroly konvenčního zbrojení či mise na pomoc politické a demokratické transformace v zemích regionu OBSE“* (Kolektiv autorů, 2015, s. 14). Všechny tyto nástroje zajišťují posilování důvěry a bezpečnosti v euroatlantickém a euroasijském prostoru. Neméně důležité je také členství v Evropské unii. Evropská unie je politická a ekonomická unie, které si klade za cíl mimo jiné podporovat mír, své hodnoty a blahobyt obyvatel. Cílem je také posilovat Společnou bezpečnostní a obrannou politiku (SBOP), tak aby byla spolehlivým a účinným nástrojem v oblasti bezpečnosti EU (Balabán a Stejskal, 2010, s. 328-329). Na zhoršující se mezinárodní bezpečnostní prostředí reaguje Evropská unie rozvojem civilních i vojenských schopností SBOP, posilováním schopností třetích zemí a regionálních organizací řešit samostatně krizové situace cestou poskytování výcviku a dodávek výzbroje (Kolektiv autorů, 2015, s. 10).

# 4 DÍLČÍ ZÁVĚR

Teoretická část diplomové práce je základnou, na které jsou postavena východiska praktické části. Teoretická část slouží především k vymezení pojmů, které jsou pro vypracování diplomové práce nezbytné a které byly doposud zjištěny. Informace byly čerpány především z knižních a internetových zdrojů jak od českých, tak od zahraničních autorů. Z rešerše české a zahraniční literatury na danou problematiku vycházejí jednoznačné závěry, které budou popsány v následujících odstavcích. První dvě kapitoly obsahují hlavní teoretická východiska k termínům asymetrický konflikt a hybridní válka, pocházející především od zahraničních autorů. Třetí kapitola teoretické části nesoucí název Bezpečnostní prostředí České republiky je založena na poznatcích zejména od tuzemských autorů.

V první kapitole je popsán samotný pojem asymetrický konflikt, který dodnes nemá přesnou definici, avšak mnoho zahraničních autorů se více méně shoduje v jeho formulaci. Tyto formulace vycházejí od autorů publikací, jako jsou Cassidy, Soulemainov, Lele či McKenzie. V této kapitole jsou také popsány zájmy a vůle aktérů, asymetrické strategie a taktiky a povahy slabých a silných aktérů, které jsou nejlépe popsány a definovány v publikacích od autorů, jako jsou Smolík a Šmíd, Soulemainov, Thorton, Lele, Arreguín-Toft, Kircher, McKenzie, Osinga, Volner, Krásný aj. Z první kapitoly vycházejí jasná teoretická východiska, například: definice asymetrického konfliktu, slabí aktéři v asymetrických konfliktech v posledních letech častěji vyhrávají konflikty, slabí aktéři se snaží podlomit vůli silných aktérů, o výhře s veliké části rozhoduje strategický přístup aktérů.

Druhá kapitola pojednává o hybridní válce jako takové, o nástrojích hybridní války a o fázích hybridního útoku. I když podle některých pochází pojem hybridní válka z posledních let, podle dostupných informací byl tento pojem poprvé použit již v roce 1998. Pojem hybridní válka výstižně definovali autoři Kříž, Bechná a Stevkov. V této kapitole je také definována hybridní válka v kontextu s jinými formami války. Důležitými podkapitolami jsou již zmíněné nástroje hybridní války a fáze hybridního útoku, které jsou podrobně popsány v různých internetových a knižních publikacích od autorů Řehka, Rácz, Jirásek, Novák a Požár. Z druhé kapitoly vycházejí teoretická východiska kupříkladu: definice hybridní války, chápání hybridní války v kontextu s různými formami války, nejdůležitější nástroje hybridní války, tři fáze hybridního útoku (přípravná, útočná a následná fáze) a podmínky pro vedení hybridní války.

Ve třetí kapitole teoretické části je podrobně popsáno bezpečnostní prostředí České republiky. Tato část se skládá z několika podkapitol, které se sebou navzájem souvisejí. Jelikož je tato kapitola závislá na aktuálních informacích, byly použity především internetové zdroje. V počátku je stručně popsána bezpečnostní situace ČR v posledních letech a její vývoj. Kapitola následně přechází na definici bezpečnostního systému ČR a jeho hlavní funkce a součásti. Poté je popsána bezpečnostní legislativa, která je z velké části postavena na tzv. krizové a branné legislativě obsahující ústavní a další zákony, nařízení, vyhlášky a směrnice. Důležitou podkapitolou jsou strategické bezpečnostní dokumenty, které jsou významnou součástí bezpečnostní legislativy ČR a vycházejí ze strategického vládnutí. Jsou zde důkladně rozebrány dokumenty Bezpečnostní strategie ČR, Audit národní bezpečnosti a Obranná strategie ČR.

Další důležitou podkapitolou je Výroční zprávy zpravodajských služeb. Tyto zprávy byly vydány 10. 11. 2020, jedná se tedy o nejaktuálnější výroční zprávy, ze kterých lze čerpat podstatné informace, týkající se bezpečnosti ČR. Poslední podkapitolou je Zajištění bezpečnosti na mezinárodní úrovni, jenž zahrnuje NATO, OSN, OBSE a EU. Z kapitoly Bezpečnostní prostředí České republiky vycházejí jednoznačné závěry, které jsou obsaženy především v podkapitole Výroční zprávy zpravodajských služeb. Jsou zde popsány možné hrozby a rizika pro ČR, jak konkrétní příklady, tak obecné hrozby vedené ze strany Číny, Ruska, Islámského státu, Severní Koreje či Iránu. Kapitola využívá informace z publikací od autorů, jako jsou Stojar, Balabán, Pernica, Šesták, Stejskal a z internetových zdrojů ve formě výročních zpráv zpravodajských služeb, strategických dokumentů, zákonů a webových stránek. Celkově na teoretickou část diplomové práce bylo použito 49 relevantních zdrojů, z toho je 18 zahraničních.

# II. PRAKTICKÁ ČÁST

# 5 ANALÝZA ASYMETRICKÝCH A HYBRIDNÍCH HROZEB V ČESKÉ REPUBLICE

V posledních letech prochází bezpečnostní prostředí jak ve světě, tak i v České republice, výraznými změnami. Bezpečnostní prostředí je ovlivňováno především tradičními bezpečnostními hrozbami, ale i relativně novými hrozbami, jako jsou například informační válka, kybernetické útoky, šíření dezinformací aj. Aktuální asymetrické a hybridní bezpečnostní hrozby jsou podmíněny mnoha faktory. Tím, že je České republika členem EU a NATO, a je tak součástí euroatlantického prostoru, je zapotřebí vnímat bezpečnostní hrozby i u našich spojenců a členů EU. Na bezpečnostní hrozby je upozorňováno v různých strategických dokumentech (Bezpečnostní strategie České republiky, Audit národní bezpečnosti, Analýza hrozeb pro Českou republiku), které identifikují aktuální hrozby, popřípadě navrhují různá opatření nebo hodnotí, jakým způsobem je ČR schopná čelit těmto hrozbám.

## 5.1 Stanovení kontextu

V této kapitole budou analyzovány vybrané asymetrické a hybridní bezpečnostní hrozby antropogenního charakteru. Cílem analýzy bude klasifikovat nejzávažnější bezpečnostní hrozby s nepřijatelným (nejvyšším) rizikem, kterým Česká republika v současné době čelí. Po zjištění nejzávažnějších rizik budou navrhnuta stručná opatření pro jejich minimalizaci. Pro hodnocení rizik je možné využít mnoho různých metod, v tomto případě se bude jednat o jednoduchou bodovou polokvantitativní metodu „PNH“. Tato metoda hodnocení rizik byla vybrána na základě její vhodnosti a jednoduchosti. Vhodností se v tomto případě myslí zejména zohlednění vlastního názoru hodnotitele, jednoduchost pak spočívá ve výpočtu samotné míry rizika, která vychází ze vzorce $R = P \times N \times H$ a jednoduché interpretaci výsledků, jež jsou uvedeny v hodnotící tabulce. Jednoduchá bodová polokvantitativní metoda „PNH“ je založena na bodovém ohodnocení tří složek, jenž obsahuje stupnici od 1 do 5. Pomocí metody „PNH“ se vyhodnocuje riziko s ohledem:

- na pravděpodobnost vzniku – P,
- pravděpodobnost následků – N
- a názor hodnotitelů – H (Koudelka a Vrána, 2006, s. 9).

Pravděpodobnost vzniku (P) představuje ve vzorci odhad pravděpodobnosti, se kterou může uvažované nebezpečí nastat. Je stanovena pomocí stupnice od 1 do 5, kde číslo 5 vyjadřuje nejvyšší pravděpodobnost vzniku a existence nebezpečí. Stejným způsobem je ohodnocena

pravděpodobnost následků (N), kde číslo 5 představuje nejvyšší možné následky ohrožení. Názor hodnotitelů (H) zohledňuje různé aspekty, které můžou přímo ovlivnit míru konečného rizika. Názor hodnotitele by měl obsahovat míru závažnosti ohrožení, počet ohrožených osob, rozsah ohrožení životního prostředí, čas působení ohrožení, dynamičnost rizika, možnost zajištění první pomoci a další vlivy potencující riziko (Koudelka a Vrána, 2006, s. 9).

V položkách P a N jsou zohledněny všechny okolnosti, které jsou pak vyjádřeny bodovým ohodnocením. Vychází se z dostupných informací ze strategických dokumentů a výročních zpráv zpravodajských služeb, informací z veřejných médií, dat ze zpráv o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území ČR, dat a informací z uskutečněných útoků proti ČR různého charakteru z předešlých let.

Tabulka 3: Pravděpodobnost vzniku a existence nebezpečí (Koudelka a Vrána, 2006, s. 10; vlastní zpracování).

| **P** – Pravděpodobnost vzniku a existence nebezpečí | |
|---|---|
| Nahodilá | 1 |
| Méně pravděpodobná | 2 |
| Pravděpodobná | 3 |
| Velmi pravděpodobná | 4 |
| Jistá | 5 |

Tabulka 4: Možné následky ohrožení (Koudelka a Vrána, 2006, s. 10; vlastní zpracování).

| **N** – Možné následky ohrožení | |
|---|---|
| Nízké | 1 |
| Méně významné | 2 |
| Významné | 3 |
| Velmi významné | 4 |
| Katastrofální | 5 |

Tabulka 5: Názor hodnotitelů (Koudelka a Vrána, 2006, s. 10; vlastní zpracování).

| **H** – Názor hodnotitelů | |
|---|---|
| Zanedbatelný vliv na míru nebezpečí a ohrožení | 1 |
| Malý vliv na míru nebezpečí a ohrožení | 2 |
| Větší, nezanedbatelný vliv na míru ohrožení a nebezpečí | 3 |
| Velký a významný vliv na míru ohrožení a nebezpečí | 4 |
| Více významných a nepříznivých vlivů na závažnost a následky ohrožení a nebezpečí | 5 |

Pro posouzení a vyhodnocení rizik bude použito následující specifikace, která se zaznamená do tabulky pod sloupce pojmenované P, N a H. Celkové hodnocení rizika získáme po stanovení jednotlivých činitelů a jejich následným součinem, jehož výsledkem bude samotný ukazatel míry rizika – R. Z terminologického hlediska představuje riziko míru budoucího ohrožení, které je vyjádřeno jako odhadovaná škoda v penězích nebo v jiných jednotkách (Tichý, 2006, s. 15).

$$\mathbf{R = P \times N \times H}$$

Tabulka 6: Míra rizika vyjádřena bodovou metodou PNH (Koudelka a Vrána, 2006, s. 10; vlastní zpracování).

| Rizikový stupeň | Hodnota R | Míra rizika |
|---|---|---|
| I. | ≥ 100 | Nepřijatelné riziko |
| II. | 51 ÷ 99 | Nežádoucí riziko |
| III | 11 ÷ 50 | Mírné riziko |
| IV. | 4 ÷ 10 | Přijatelné riziko |
| V. | ≤ 3 | Bezvýznamné riziko |

Na základě součinu, který vyjde ze vzorce R = P × N × H určíme, do jakého rizikového stupně dané nebezpečí patří, a tím zjistíme míru konkrétního rizika. Celkově budeme moct nebezpečí zařadit do pěti rizikových stupňů. Pro každý rizikový stupeň budou určeny odlišné úkoly přijatých opatření ke snížení rizika a pro všechna nepřijatelná rizika budou navrhnuta určitá opatření k jejich eliminaci (Šefčík, 2009, s. 63).

## 5.2 Identifikace nebezpečí

Jednou z klíčových aktivit při posuzování rizik je bezesporu identifikace nebezpečí. Samotná činnost spočívá v identifikování všech závažných zdrojů nebezpečí vztahující se k prováděným činnostem. Je řešeno, co nebo kdo může být poškozen a jakým způsobem (Paulus et al., 2015, s. 4). Termín nebezpečí představuje, podle terminologického slovníku z oblasti krizového řízení, *„zdroj potenciálního poškození, újmy například na životech, zdraví, majetku nebo životního prostředí a bývá zdrojem rizika“* (Terminologický slovník pojmů…, 2016, s. 44).

Na základě aktuální bezpečnostní situace v ČR jsou identifikovány různé typy nebezpečí. Při určování samotných typů nebezpečí se vychází ze základních strategických dokumentů, mezi které patří Bezpečnostní strategie České republiky z roku 2015, Analýza hrozeb pro Českou republiku z roku 2015, Audit národní bezpečnosti z roku 2016, Obranná strategie České republiky z roku 2017 a Koncepce výstavby Armády České republiky 2030 z roku

2019. Dále jsou použity informace z výročních zpráv zpravodajských služeb za rok 2019, informace ze Zprávy o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území České republiky v roce 2019 a v neposlední řadě poznatky samotného autora této diplomové práce. Celkově bylo identifikováno 38 typů nebezpečí z 9 zdrojů rizik. Mezi hlavní zdroje rizik patří:

- terorismus,
- nelegální migrace,
- organizovaný zločin,
- politický extremismus,
- kybernetické útoky,
- šíření zbraní hromadného ničení a jejich nosičů,
- dezinformace a propaganda,
- ozbrojený konflikt a
- přerušení dodávek strategických surovin nebo elektrické energie.

Důležitým krokem je také definovat si primární aktiva, která mají pro Českou republiku jako stát vysokou hodnotu. Podle terminologického slovníku (2016. s. 2) se aktivem „*označuje vše, co má pro organizaci či společnost hodnotu, která může být zmenšena působením hrozby"*. Aktiva se dělí na hmotná, např. lidé, nemovitosti nebo peníze a nehmotná, do kterých patří informace a data, autorské práva aj. (Terminologický slovník pojmů…, 2016, s. 2). Pro stát jsou primárním aktivem zejména životy a zdraví osob, různé prvky kritické infrastruktury, důležitý movitý i nemovitý majetek, životní prostředí, peníze, data a informace, území, nerostné suroviny apod.

## 5.3 Analýza rizik

Dalším důležitým krokem v posuzování rizik je jejich analýza. Výstupem analýzy rizik bude určení míry rizika, tzn. určení veličiny vyjadřující, že s určitou pravděpodobností dojde k uskutečnění konkrétního typu nebezpečí a uplatnění jeho destruktivního potenciálu. Určení míry rizika bude zjištěno za pomocí vzorce $R = P \times N \times H$. Do příslušné tabulky budou vloženy všechny podstatné informace a hodnoceny tři složky v pětibodových škálách. Součin těchto hodnot se bude rovnat míry rizika u daného typu nebezpečí. Na základě provedené analýzy budou všechny typy nebezpečí spadající do I. rizikového stupně (nepřijatelné riziko) ošetřeny.

Tabulka 7: Bezpečnostní rizika vyhodnocená metodou „PNH“ (Koudelka a Vrána, 2006, s. 13-16; vlastní zpracování).

| Zdroj rizika | Identifikace nebezpečí | VYHODNOCENÍ ZÁVAŽNOSTI RIZIKA | | | | Míra rizika |
|---|---|---|---|---|---|---|
| | | P | N | H | R | |
| **Terorismus** | Střelba, použití sečných a bodných zbraní | 4 | 5 | 5 | 100 | Nepřijatelné riziko |
| | Výbuchy pum sami o sobě | 4 | 5 | 5 | 100 | Nepřijatelné riziko |
| | Výbuchy iniciující další ničivou činnost | 3 | 5 | 4 | 60 | Nežádoucí riziko |
| | Únosy, braní rukojmí | 4 | 5 | 3 | 60 | Nežádoucí riziko |
| | Dopisní bomby | 2 | 2 | 2 | 8 | Přijatelné riziko |
| **Nelegální migrace** | Nelegální migrace (vstup, pobyt a vycestování osoby na/z území ČR) | 4 | 3 | 4 | 48 | Mírné riziko |
| | Tranzitní nelegální migrace na území ČR | 5 | 3 | 4 | 60 | Nežádoucí riziko |
| **Organizovaný zločin** | Výroba, pašování a distribuce drog | 3 | 3 | 2 | 18 | Mírné riziko |
| | Daňové podvody, útok na státní majetek | 5 | 4 | 3 | 60 | Nežádoucí riziko |
| | Organizovaná prostituce a obchod s lidmi | 4 | 3 | 3 | 36 | Mírné riziko |
| | Organizování nelegální migrace | 4 | 4 | 4 | 64 | Nežádoucí riziko |
| | Padělání měny, zboží a porušování autorských práv | 2 | 2 | 1 | 4 | Přijatelné riziko |
| | Praní špinavých peněz, vydírání a korupce | 4 | 3 | 5 | 60 | Nežádoucí riziko |
| | Mezinárodní obchod se zbraněmi a výbušninami | 3 | 5 | 4 | 60 | Nežádoucí riziko |
| | Organizované krádeže automobilů a loupeže | 3 | 3 | 4 | 36 | Mírné riziko |
| **Politický extremismus** | Narušování veřejného pořádku | 3 | 3 | 3 | 27 | Mírné riziko |

| Zdroj rizika | Identifikace nebezpečí | VYHODNOCENÍ ZÁVAŽNOSTI RIZIKA | | | | Míra rizika |
|---|---|---|---|---|---|---|
| | | P | N | H | R | |
| | Cílené šíření strachu | 4 | 5 | 3 | 60 | Nežádoucí riziko |
| | Oslabování demokracie a nerespektování základních lidských práv | 4 | 5 | 5 | 100 | Nepřijatelné riziko |
| | Používání populistických a propagandistických praktik | 3 | 3 | 2 | 18 | Mírné riziko |
| | Násilné činy z nenávisti | 3 | 4 | 3 | 36 | Mírné riziko |
| **Kybernetické útoky** | Poškození nebo vniknutí do počítačového systému pomocí malware (spyware, adware, ransomware) | 4 | 5 | 5 | 100 | Nepřijatelné riziko |
| | Získávání citlivých údajů (phishing) | 5 | 4 | 4 | 80 | Nežádoucí riziko |
| | Získávání osobních a citlivých dat z databází (SQL Injection a Cross-site scripting) | 5 | 4 | 4 | 80 | Nežádoucí riziko |
| | Znepřístupnění webových stránek ostatním uživatelům (DoS) | 3 | 3 | 3 | 27 | Mírné riziko |
| | Špehování internetové komunikace (Man-in-the-Middle a hijacking) | 4 | 4 | 4 | 64 | Nežádoucí riziko |
| **Šíření zbraní hromadného ničení a jejich nosičů** | Použití ZHN na území ČR | 1 | 4 | 2 | 8 | Přijatelné riziko |
| | Zakoupení komponentů pro ZHN na území ČR | 3 | 3 | 1 | 9 | Přijatelné riziko |
| **Dezinformace a propaganda** | Využívání propagandy k šíření mocenského vlivu (dezinformační kampaně) | 5 | 5 | 5 | 125 | Nepřijatelné riziko |
| | Šíření fake news a hoaxů | 5 | 4 | 4 | 80 | Nežádoucí riziko |
| | Používání dezinformačních webů | 5 | 4 | 4 | 80 | Nežádoucí riziko |

| Zdroj rizika | Identifikace nebezpečí | VYHODNOCENÍ ZÁVAŽNOSTI RIZIKA | | | | Míra rizika |
|---|---|---|---|---|---|---|
| | | P | N | H | R | |
| **Ozbrojený konflikt** | Ozbrojený konflikt na území ČR | 1 | 3 | 1 | 3 | Bezvýznamné riziko |
| | Regionální konflikty v euroatlantickém prostoru a jeho okolí | 3 | 4 | 5 | 60 | Nežádoucí riziko |
| | Ozbrojený konflikt vedený se státním aktérem | 3 | 4 | 2 | 24 | Mírné riziko |
| | Ozbrojený konflikt vedený s nestátním aktérem | 3 | 4 | 3 | 36 | Mírné riziko |
| | Ozbrojený konflikt ve formě hybridní války | 4 | 5 | 5 | 100 | Nepřijatelné riziko |
| **Přerušení dodávek strategických surovin nebo elektrické energie** | Přerušení dodávek ropy | 3 | 3 | 3 | 27 | Mírné riziko |
| | Přerušení dodávek plynu | 3 | 3 | 3 | 27 | Mírné riziko |
| | Přerušení dodávek elektrické energie | 2 | 3 | 1 | 6 | Přijatelné riziko |

## 5.4 Hodnocení rizik

Posledním krokem v posuzování rizik je jejich hodnocení. Z analýzy rizik jasně vyplývá, jaká nebezpečí představují pro ČR vysoké riziko a jaká naopak představují bezvýznamné či přijatelné riziko. Celkově bylo tedy identifikováno 9 zdrojů rizik a 38 typů nebezpečí. Vhodné je také dodat, že všechny zdroje rizik jsou antropogenního charakteru. Z celkového počtu hodnocených typů nebezpečí je kategorizace míry rizika následující:

- bezvýznamná rizika – 1 (3 %),
- přijatelná rizika – 5 (13 %),
- mírná rizika – 12 (31 %),
- nežádoucí rizika – 14 (37 %),
- nepřijatelná rizika – 6 (16 %).

Smyslem hodnocení rizik je identifikace prioritních (nejzávažnějších) rizik, kterým je potřeba nadále věnovat pozornost. Na začátku analýzy rizik byly stanoveny limitní hodnoty úrovně rizika, podle kterých bylo dále rozlišeno pět základních kategorií rizik, viz tabulka

č. 6. Pro lepší znázornění nepřijatelných rizik jsou tato rizika interpretována v přehledné tabulce č. 8.

Tabulka 8: Identifikace prioritních rizik (vlastní zpracování).

| Zdroj rizika | Identifikace nebezpečí | Hodnota rizika | Míra rizika |
|---|---|---|---|
| **Terorismus** | Střelba, použití sečných a bodných zbraní | 100 | Nepřijatelné riziko |
| | Výbuchy pum sami o sobě | 100 | Nepřijatelné riziko |
| **Politický extremismus** | Oslabování demokracie a nerespektování základních lidských práv | 100 | Nepřijatelné riziko |
| **Kybernetické útoky** | Poškození nebo vniknutí do počítačového systému pomocí malware (spyware, adware, ransomware) | 100 | Nepřijatelné riziko |
| **Dezinformace a propaganda** | Využívání propagandy k šíření mocenského vlivu (dezinformační kampaně) | 125 | Nepřijatelné riziko |
| **Ozbrojený konflikt** | Ozbrojený konflikt ve formě hybridní války | 100 | Nepřijatelné riziko |

## 5.5 Ošetření rizik

Mezi další důležitý prvek řízení rizik patří jejich ošetření. Jedná se o proces, při kterém jsou různými způsoby ošetřena nejzávažnější rizika. Není praktické ani efektivní řešit všechna identifikovaná rizika, naopak je žádoucí se zabývat pouze riziky, které mají fatální dopad. Ošetření rizik probíhá obvykle ve dvou fázích. V první fázi ošetření rizik je potřeba navrhnout, jakým způsobem budou rizika ošetřena s ohledem na poměr nákladů na ošetření rizik a získaných přínosů. Ve druhé fázi probíhá samotná implementace navrhnutého protiopatření k redukci rizik (Korecký a Trkovský, 2011, s. 83).

Existuje více způsobů, jimiž lze riziko zmírnit. Zapotřebí je průběžně aktualizovat a zpracovávat plány opatření na redukci rizik. Hlavní nástroje na redukci rizik jsou klasifikovány do čtyř základních kategorií:

- transfer rizika,

- retence rizika,
- prevence a redukce rizika,
- vyhnutí se riziku nebo také eliminace rizika (Božek, 2015, s. 108).

Výběr konkrétního způsobu zmírnění rizika by měl zahrnovat, čeho má být docíleno, jaká bude jeho efektivita a nákladovost implementace opatření, jeho technickou realizovatelnost a účinnost a v neposlední řadě jeho sociální a politickou přijatelnost. Vybrat optimální řešení bývá z veliké části velice složité a vždy záleží na konkrétní situaci. Existují však jisté zásady s ohledem na výši pravděpodobnosti projevu nebezpečí a úrovni jeho dopadu, viz tabulka č. 9 (Božek, 2015, s. 111).

Tabulka 9: Doporučené způsoby minimalizace rizika (Božek, 2015, s. 111; vlastní zpracování).

| | **Vysoká pravděpodobnost výskytu** | **Nízká pravděpodobnost výskytu** |
|---|---|---|
| **Vysoká úroveň dopadu** | Vyhnutí se riziku nebo redukce rizika | Transfer rizika |
| **Nízká úroveň dopadu** | Redukce nebo retence rizika | Retence rizika |

Na základě vysokých hodnot (pravděpodobnost vzniku nebezpečí a možné následky ohrožení), které vycházejí z tabulky č. 7 a doporučeného způsobu minimalizace rizik, dle tabulky č. 9 bylo rozhodnuto, že nejvhodnějším způsobem pro minimalizaci nepřijatelných rizik bude prevence a redukce rizika. Podle Smejkala a Raise (c2010, s. 129-130) se k prevenci a redukci rizika v praxi užívají v zásadě čtyři základní způsoby:

- prevence a redukce rizika u zdroje,
- zdokonalení organizace a prostředků zásahu a záchrany,
- zvyšování informovanosti zaměstnanců a veřejnosti,
- územní rozvoj.

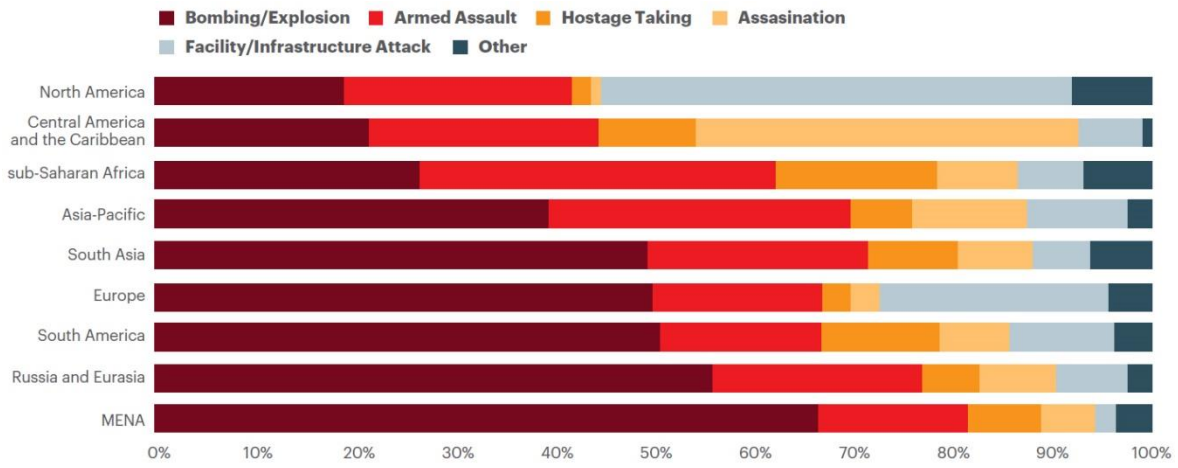
## 5.6 Bezpečnostní opatření

Na základě vyhodnocení nejzávažnějších rizik, kterým Česká republika v současné době čelí, budou v následujících oddílech navrhnuty bezpečnostní opatření pro jejich minimalizaci. V předešlé podkapitole byl vybrán nejvhodnější způsob pro minimalizaci rizik a to prevence a redukce rizika. Ke každému nebezpečí budou nevržena konkrétní bezpečnostní opatření, které mohou svojí implementací zmírnit následky způsobené mimořádnými událostmi nebo eliminovat samotnou míru rizika.

### 5.6.1 Terorismus

Jak je i v teoretické části diplomové práce zmíněno, terorismus se řadí mezi moderní asymetrické hrozby a ve většině případů jej používají slabí aktéři konfliktů. Terorismus bývá nejčastěji použit proti nezúčastněným osobám (civilistům) nebo se zaměřením na konkrétní osoby a jeho primárním cílem je vyvolat strach, jehož prostřednictvím mají být splněny politické, náboženské nebo ideologické požadavky (Terminologický slovník…, 2016, s. 85).

Podle Globálního indexu terorismu z roku 2020 (Global Terrorism Index – GTI) patří Česká republika do oblasti s velmi nízkým dopadem terorismu. Celkově se nachází na 111. místě z celkových 138 míst a polepšila si od roku 2018 o 10 příček (GTI z roku 2020 hodnotí situaci za rok 2019). Mohlo by se tedy zdát, že terorismus nepatří mezi aktuální hrozby ČR, avšak opak je pravdou. Například takové Rakousko se nachází na 91. příčce a i přesto došlo ve Vídni dne 2. listopadu 2020 k závažnému teroristickému útoku, který si vyžádal 4 oběti a několik vážně zraněných. K teroristickému útoku se přihlásil Islámský stát. GTI uvádí ve své výroční zprávě další zajímavé informace, například typy útoků podle regionu (Global Terrorism Index 2020, 2020, s. 93).




Obrázek 4: Typy útoků podle regionu od roku 2000 do roku 2019 (Global Terrorism Index 2020, 2020, s. 44).

Z obrázku vyplývá, že k nejčastějším typům útoků používaných při teroristických činech v Evropě patří bombové a ozbrojené útoky a s tím spojené útoky na důležitou infrastrukturu. Při snaze navrhnout a zavést taková opatření, která povedou k minimalizaci rizika teroristických útoků v ČR je zapotřebí myslet na to, odkud pochází zdroj tohoto rizika. Lidé, páchající tyto hrůzné zločiny, patří nejčastěji k radikálním islamistům, kteří se musejí do dané země dostat, mít finance a prostředky ke spáchání takového činu. Proto je vhodné ze

začátku navrhnout taková opatření, která zamezí vstup podezřelých osob do Evropy. Mezi navrhovaná bezpečnostní opatření vůči teroristickým činům na území ČR tedy patří:

- zavedení přísnějších kontrol při nabývání a držení palných zbraní,
- zabezpečení vnějších hranic EU, které zahrnuje:
  - od roku 2021 zavedení Evropského systému pro cestovní povolení (ETIAS),
  - posílení Evropské pobřežní a pohraniční stráže,
  - zavedení systematických kontrol všech osob překračující vnější hranice, za použití příslušných databází,
- zavedení interoperability databází od roku 2023 – sdílení informací mezi státy EU,
- zablokování zdrojů příjmů a narušení logistiky,
- odstranění teroristických obsahů ze sociálních sítí jako je YouTube a Facebook do jedné hodiny od vyzvání od příslušných orgánů,
- monitorování nenávistných kazatelů na úrovni EU a předcházení radikalizace ve vězení,
- předcházení radikalizace a rekrutování – imámové zneužívající svého postavení k šíření extremistických výkladů islámu,
- omezování dostupnosti prostředků a chemikálií, ze kterých je možné vyrobit bomby (Jak zastavit terorismus: opatření EU, 2018),
- pokračování v procvičování pořádkové policie v akcích typu AMOK (útok aktivního střelce),
- posilování ochrany kritické infrastruktury a věnování pozornosti problematice ochrany měkkých cílů (posílení jejich zabezpečení, vycvičení personálu, spolupráce státu s veřejnou sférou apod.) (Audit národní bezpečnosti, 2016, s. 26).

### 5.6.2 Politický extremismus

Politický extremismus definuje Backas a Jesse jako *„antitezi k demokratickému ústavnímu státu a týká se antidemokratického smýšlení a úsilí. To je takové, které odmítá ústavní stát a jeho základní hodnoty a pravidla“* (Backes a Jesse, 1993 cit. podle Vejvodová, 2012, s. 1). Političtí extremisté jsou přesvědčeni, že právě oni jsou v právu, a to oslabuje respekt k jiným názorům. Mezi typické prvky politického extremismu patří intolerance, nesnášenlivost a odmítání platných právních a morálních norem. Za účelem dosažení svého politického cíle jsou schopni tito extremisté použít jakýchkoliv prostředků, v některých

vyhrocených případech můžou použít i terorismus. V České republice řadíme politický extremismus na dva typy: pravicový a levicový (Vejvodová, 2012, s. 1-2).

V ČR je zastoupena spíše početnější skupina pravicových extremistů, která soucítí s hodnotami a názory politických stran a hnutí jako je Dělnická strana sociální spravedlnosti (DSSS), jež vychází z rozpuštěné Dělnické strany nebo Svoboda a přímá demokracie (SPD). Právě druhé zmíněné politické hnutí je nepřímo odpovědné za vůbec první teroristický čin spáchaný na území ČR. Sympatizant hnutí SPD Jaromír Balda v roce 2017 pokácel dva stromy na vlakové koleje a způsobil tím dvě nehody vlaků, při nichž se jen shodou náhod nikdo nezranil. Tyto skutky chtěl posléze svést na muslimské migranty a vyvolat tak ve společnosti strach z migrační vlny. Za tento trestný čin byl Balda pravomocně odsouzen na čtyři roky odnětí svobody (Balda spáchal teroristický čin…, 2019).

Právě proto, aby občané nepodlehli dezinformacím pocházejícím od představitelů různých pravicových stran, je zapotřebí bojovat proti tomuto jednání. Opatření proti politickému extremismu v ČR by mělo spočívat v:

- efektivnějším monitoringu a zaznamenávání nenávistných projevů s důrazem na nenávistné projevy na internetu,
- pokračování v projektu „Místo pro všechny“ (2020 - 2023), který zahrnuje:
    - komunikaci o problematice ohrožených menšin v masmédiích a na sociálních sítích,
    - řešení konfliktů ve školských zařízeních,
    - prezentaci opatření podporující členy sociálně vyloučených komunit na komunální úrovni,
- informování veřejnosti o extremistické scéně a o protiextremistických aktivitách,
- vzdělávání občanů – prostřednictvím vzdělání si lidé dokáží sami vytvořit obranné mechanismy proti přijímání extrémních názorů,
- poskytování integračních aktivit pro cizince a menšiny,
- poskytování ochrany a pomoci potencionálním obětem trestné činnosti (Zpráva o situaci…, 2020, s. 55-56).

### 5.6.3 Kybernetické útoky

Kybernetické útoky jako primární nástroj hybridní války jsou už zmíněny v teoretické části diplomové práce na s. 22. Kybernetický útok je podle Koloucha a Bašty *„jakékoli úmyslné jednání útočníka v kyberprostoru, které směřuje proti zájmům jiné osoby“* (2019,

s. 82). Aktuální situace napovídá, že kybernetické útoky budou stále častějším jevem. V minulých letech byly útoky zaměřeny zejména na nemocnice, letiště ale i běžné uživatele internetu a momentálně tomu není jinak. Velice známé jsou útoky spáchané v roce 2020 na nemocnice v Benešově a Brně, kde byl použit tzv. ransomware – „vyděračský software". Škody těchto kybernetických útoku šplhají k desítkám miliónů korun, avšak nemocnice v ČR výkupné zatím nikdy nezaplatily, což je z mého pohledu správná volba.

Další často používanou metodou v oblasti kybernetických útoků je tzv. phishing. Jde o metodu, kdy se útočník vydává za důvěryhodnou autoritu, s cílem získat citlivá data konkrétního uživatele. Nejznámější způsob takového útoku spočívá v rozesílání podvodných e-mailů s požadavkem na zadání údajů o bankovní kartě nebo hesla k internetovému bankovnictví. V tomto případě se útočník vydává za banku a chce vylákat od své oběti citlivé informace k jejich následnému zneužití (Phishing, ©2021). Mezi primární opatření proti těmto útokům patří:

- personální posílení bezpečnostních složek, které se zabývají problematikou kybernetické bezpečnosti, kybernetické kriminality a kybernetické obrany,
- finanční posílení bezpečnostních složek na podporu nových bezpečnostních projektů (vytváření nových osvětových a vzdělávacích akcí),
- novelizace zákonů – začít řešit otázku anonymity uživatelů na internetu,
- rozšíření výuky kybernetické bezpečnosti na základních, středních a vysokých školách (Audit národní bezpečnosti, 2016, s. 108-109),
- pokračování v projektu „No More Ransom!", který má za cíl pomoct obětem ransomware získat zpět jejich zašifrovaná data, bez nutnosti platit výkupné zločincům,
- zálohování dat, používání silného antivirového software a řádné aktualizování software (O projektu, ©2021).

### 5.6.4 Dezinformace a propaganda

Dezinformace a propaganda jsou stejně jako kybernetické útoky hlavními nástroji hybridní války, ale používají se i v dobách relativního míru. Mezi dezinformacemi a propagandou panuje určitý vztah, který by se dal vyjádřit tak, že propaganda využívá fake news (žurnalistický útvar) ve svůj prospěch, přičemž dezinformace (záměrně nepravdivá informace) je stavebním prvkem fake news (Cakl, 2019).

Dezinformace jsou bezesporu taktickým krokem, kdežto na druhé straně samotná propaganda je daleko širší strategické rozhodnutí. Propaganda má jasné vlastnosti, podle kterých je zcela rozpoznatelná. Hlavními předpoklady pro úspěšné šíření propagandy jsou: záměrná manipulace čtenáře či diváka, prezentace jediného názoru jako absolutní pravdy a využití psychologické manipulace a přesvědčování svých diváků, že cíl propagandy a jejich tužby jsou jedno a to samé (Babayeva a Garcia, 2020).

Není žádným tajemstvím, že Rusko a Čína se opakovaně pokouší v České republice ovlivňovat veřejné mínění, šířit propagandu a budovat pozitivní obraz svých zemí prostřednictvím mediálního obsahu (Čínské zpravodajské služby využívají…, 2002). Proti těmto praktikám je zapotřebí aplikovat zejména tato opatření:

- zavedení odpovědnosti provozovatelů internetových služeb – společnosti by měly být zodpovědné za rychlé odstraňování falešných zpráv; odpovědné orgány by měly mít možnost odhalit totožnost autorů a sponzorů politického obsahu,
- pokračování v projektu „EUvsDisinfo“, který má na starosti pracovní skupina East StratCom (ESCTF – East StratCom Task Force) – ESCTF předpovídá, řeší a reaguje na probíhající dezinformační kampaně Ruské federace ovlivňující EU a země východního partnerství (Arménie, Ázerbájdžán, Bělorusko, Gruzie, Moldavsko a Ukrajina) (About, ©2021),
- posílení občanského vzdělávání na školách (mediální gramotnost),
- propagování různých naučných materiálů sloužících k ověřování informací, propagování vzdělávacích webů typu: www.bezpecne-online.ncbi.cz, www.esafetylabel.eu.

### 5.6.5 Ozbrojený konflikt

Podle dostupných informací z Výroční zprávy VZ za rok 2019 jasně vyplývá, že se svět přiblížil ke globálnímu konfliktu z důvodu narůstající polarizace zájmů, názorů a rozdílných postojů, prohlubující se multipolarity a úpadku principů mezinárodního práva. Napětí narostlo především mezi globálními rivaly, jako jsou Spojené státy americké, Čínská lidová republika a Ruská federace (Výroční zpráva VZ za rok 2019, 2020, s. 4).

České republice momentálně ozbrojený konflikt bezprostředně na svém území nehrozí, to ale neznamená, že nečelí hrozbám jiného charakteru (Stojar, 2018, s. 3-4 a Kolektiv autorů, 2015, s. 8). Jak je v teoretické části diplomové práce uvedeno, aby mohla být zahájena a vedena hybridní válka, je zapotřebí splnit určité podmínky, které Česká republika naštěstí

nesplňuje. V první řadě se jedná o nesplnění přítomnosti cizích vojsk na území ČR a společných hranic s útočící zemí. Tím se ale nevyvrací fakt, že ČR čelí vlivovým operacím a jsou proti ní používány nástroje hybridní války, zejména ze strany Ruska a Číny. Těmto vlivovým operacím a hybridním hrozbám se dá předcházet opatřeními typu:

- pokračování a podporování činnosti think tanků jako jsou Evropské hodnoty, Prague Security Studies Institute aj.,
- pokračování činnosti zpravodajských služeb, Centra proti terorismu a hybridním hrozbám a Národního centra kybernetické a informační bezpečnosti,
- zapojení neziskových a nestátních aktérů ke komunikaci s veřejností,
- vyhodnocení dopadů při dostavbě nového bloku jaderné elektrárny Dukovany a 5G sítě – riziko získání vlivu Ruska či Číny (Kovanda, 2018),
- implementování Národní strategie pro čelení hybridnímu působení (schválena Vládou ČR dne 29. 4. 2021),
- vytvoření systému varovných indikátorů, s jejichž pomocí budou různé instituce schopny zachycovat informace, které mohou přispět k odhalení probíhající hybridní kampaně,
- definování strategického přístupu České republiky, jak čelit hybridní kampani vedené proti ČR nebo proti jinému státu NATO či EU,
- posílení občanského vzdělávání na školách (základní hodnoty, mediální gramotnost, jednání v krizových situacích) (Audit národní bezpečnosti, 2016, s. 138-139).

# 6 DOTAZNÍKOVÉ ŠETŘENÍ K BEZPEČNOSTNÍ SITUACI V ČESKÉ REPUBLICE Z POHLEDU VEŘEJNOSTI

Základním předpokladem pro rozvoj země a zvyšování prosperity obyvatel je zajištění bezpečnosti. Je známo, že země čelící různým vojenským konfliktům, trpí nedostatkem bezpečnosti, zničenou infrastrukturou, sociálními nejistotami, chudobou, zvýšenou kriminalitou a omezenou hospodářkou činností. Bezpečnost bezesporu patří mezi stěžejní kvalitativní parametr lidského života (Gerhát, 2018, s. 18). Česká republika zajišťuje svou bezpečnost prostřednictvím prosazování svých bezpečnostních zájmů. Mezi životní bezpečnostní zájmy České republiky patří *„zajištění suverenity, územní celistvosti a politické nezávislosti ČR, zachování všech náležitostí demokratického právního státu včetně záruky a ochrany základních lidských práv a svobod obyvatel“* (Kolektiv autorů, 2015, s. 7).

I když by se mohlo zdát, že za zajištění obrany odpovídá pouze vláda, není tomu tak. Díl odpovědnosti nesou kromě institucí státní správy a územní samosprávy také samotní občané. Tato odpovědnost je ukotvena v zákoně č. 222/1999 Sb., o zajišťování obrany České republiky. Už v teoretické části diplomové práce je zmíněna Obranná strategie ČR z roku 2017, která jasně deklaruje tři pilíře obrany ČR, kdy jedním z oněch tří pilířů je právě občanská povinnost k obraně státu (Gerhát, 2018, s. 18).

V této kapitole budou vyhodnoceny a analyzovány odpovědi týkající se bezpečnostní situace v České republice během posledních let z pohledu veřejnosti. Primárním cílem této kapitoly bude zjistit, jestli se veřejnost cítí v ČR bezpečně, jaké hrozby jsou pro ně nejvíce zneklidňující a jaký má názor na dílčí otázky z problematiky bezpečnosti ČR. Kapitola se bude skládat z několika částí, v první podkapitole bude popsána metodika prováděného výzkumu, ve druhé podkapitole budou vyhodnoceny a analyzovány odpovědi na konkrétní otázky, kde budou výsledky graficky znázorněny. Ve třetí podkapitole bude zhodnocena současná bezpečnostní situace v ČR s přihlédnutím na výsledky z analýzy asymetrických a hybridních bezpečnostních hrozeb metodou PNH a na odpovědi z dotazníkového šetření.

## 6.1 Metodika dotazníkového šetření

Dotazníkové šetření je jedna z kvantitativních metod výzkumu veřejného mínění, dle Kohoutka (©2021) se jedná o způsob psaného řízeného rozhovoru. Dotazník se řadí mezi subjektivní metody, protože vyšetřovaný může různým způsobem ovlivňovat své výpovědi

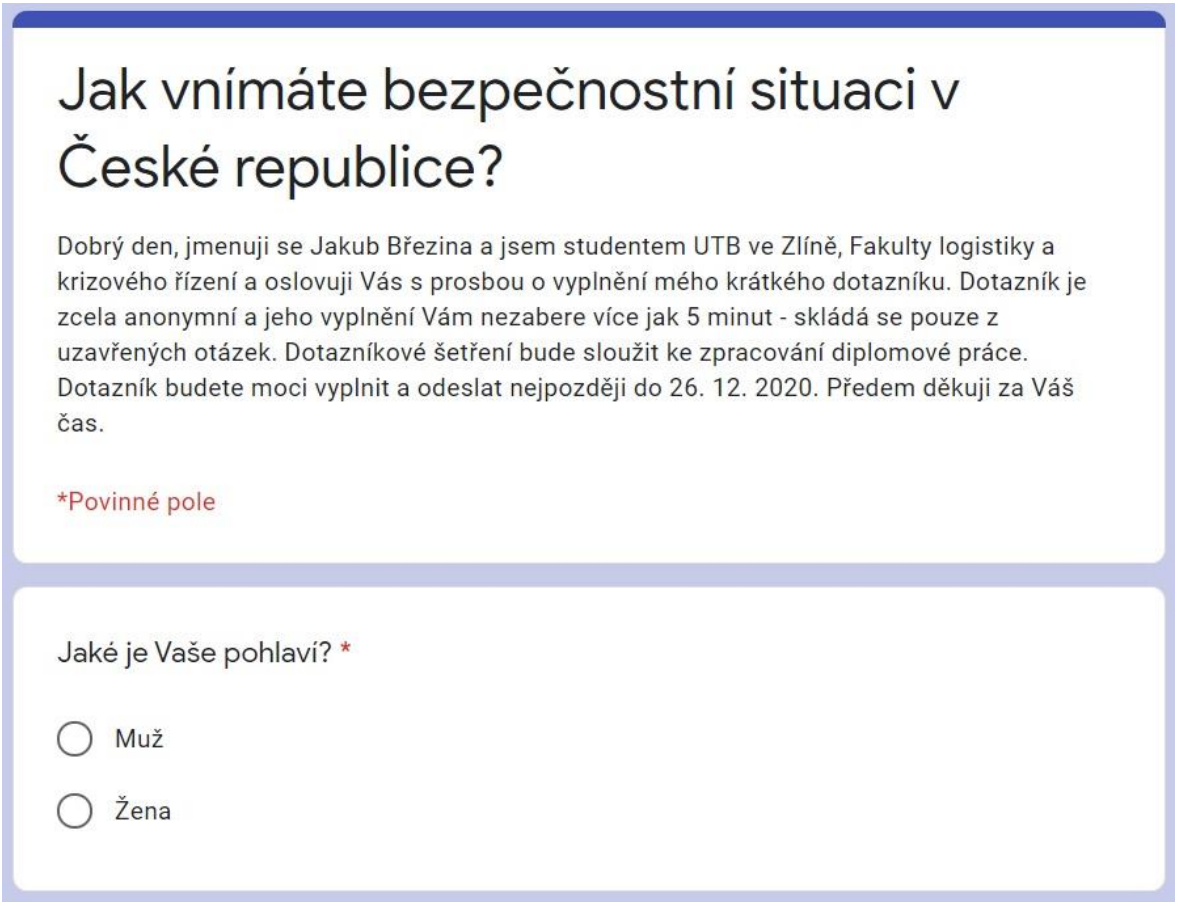
(Kohoutek, ©2021). Jelikož je dotazník anonymní, je vyšší šance, že odpovědi budou upřímnější a tím méně zkreslené. Při sestavování dotazníku byl brán zřetel na jednoduchost a srozumitelnost otázek. Před definitivním zveřejněním dotazníku byl dotazník rozeslán rodinným příslušníkům a známým (v řádu desítek respondentů), aby se předešlo špatné a nesrozumitelné formulaci otázek. Z různých typů dotazníků byl vybrán právě standardizovaný dotazník v elektronické formě a to z důvodů:

- komfortnosti – respondent pouze klikne na odkaz, který ho přesměruje na elektronický dotazník a může ho tak vyplnit kdekoliv, pokud má přístup k internetu,
- srozumitelnosti – dotazovaný odpovídá na uzavřené otázky, kdy stačí pouze zaškrtnout odpověď na danou otázku, popřípadě zaškrtnout políčko *„Nevím“* nebo napsat odpověď vlastními slovy po zaškrtnutí políčka *„Jiná…“*,
- jednoduchosti – s dotazníkem se setkal více méně každý, jak ve škole, tak i v práci či ve volném čase; k vyplnění dotazníku nemusí mít dotazovaný účet na žádné sociální síti,
- vhodnosti – dotazníkové šetření ve formě standardizovaného dotazníku je vhodné zejména kvůli zpracování většího počtu informací,
- časové nenáročnosti – dotazník je strukturovaný proto, aby jeho vyplnění nezabralo respondentovi více jak pět minut, a následně nedošlo k nevyplnění pro jeho časovou náročnost,
- anonymnosti – díky anonymitě dotazníku mohou respondenti vyjádřit svůj názor bez obav s uveřejněním svých odpovědí.

Pro tvorbu dotazníku byla použita jednoduchá aplikace Google Forms, která slouží pro vytváření různých formulářů, anket, dotazníků apod. Tato aplikace byla vybrána především kvůli její jednoduchosti, rychlosti vytvoření dotazníku, bezplatného používání, rychlosti sběru a uložení velkého množství dat a grafického znázornění odpovědí. Konečná verze dotazníku byla vyhotovena 26. 10. 2020 a ten den byla také elektronicky rozeslána přes e-mail a sdílena přes různé sociální sítě (Facebook, Instagram aj.). Sběr dat probíhal ve dnech od 26. 10. 2020 do 26. 12. 2020.

Dotazník se celkově skládá z 19 uzavřených otázek, z toho tři faktografické. U některých otázek, pokud si respondent nevybral z nabízených možností, bylo možné odpovědět vlastními slovy. Na začátku dotazníku byly umístěny faktografické otázky, které podávají informace o respondentovi z hlediska pohlaví, věku a nejvyššího dosaženého vzdělání. Ostatní otázky už se zaměřovaly na samotnou problematiku. Všechny otázky byly povinné

až na poslední výčtovou otázku, kde respondent nemusel zaškrtnout žádné políčko. Byly použity dichotomické i trichotomické otázky, výběrové a výčtové otázky. U výčtových otázek byly zařazeny varianty odpovědi *„Nevím“* popřípadě *„Jiná…“,* aby nedocházelo ke zkreslení dat, pokud respondent odpověď nezná. Uzavřené otázky byly zvoleny pro jednoduché vyplnění odpovědí, aby bylo dosaženo, co největšího počtu vyplněných dotazníků, což se podařilo. Celkově dotazník vyplnilo 517 respondentů a celý dotazník je k dispozici k nahlédnutí v Příloze P I.




Obrázek 5: Grafické znázornění záhlaví dotazníkového šetření v Google Forms (Formuláře, ©2021; vlastní zpracování).

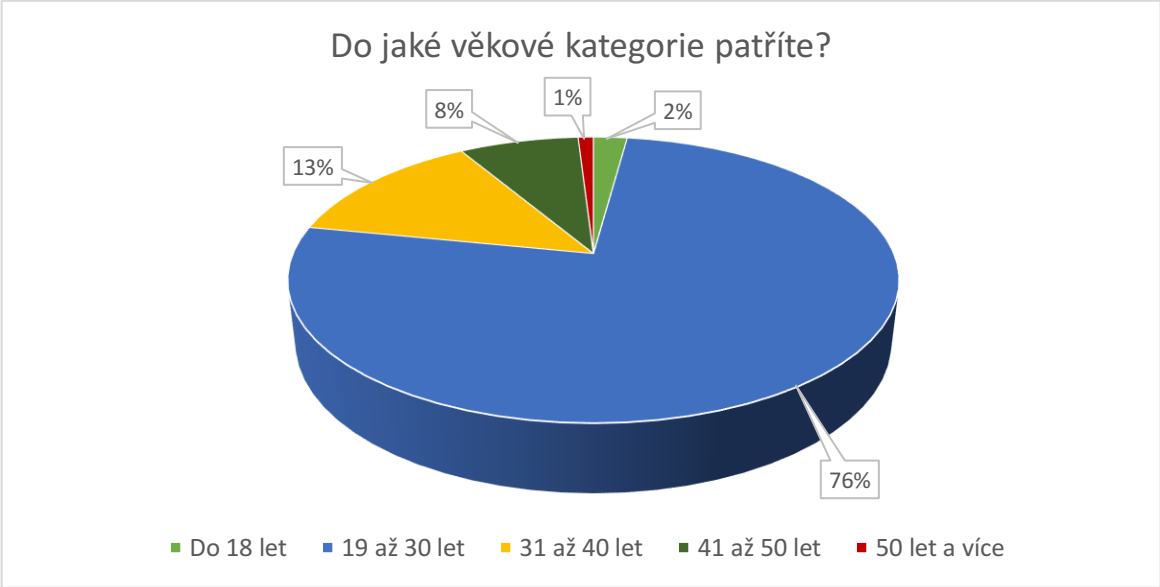
## 6.2 Vyhodnocení odpovědí

Jak už bylo zmíněno v předchozí podkapitole, celkově se dotazník skládá z 19 otázek, z toho se první tři otázky zaměřují na informace o respondentovi. Faktografické otázky zjišťují pohlaví, věk a nejvyšší dosažené vzdělání. Další otázky už se týkají dané problematiky. Pro lepší představu budou odpovědi některých otázek znázorněny formou grafu. Odpovědi jsou zpracovány od 517 respondentů. Ve třech výčtových otázkách se objevuje možnost vybrat z několika nabízených alternativ, proto je součet odpovědí u těchto otázek vyšší, než

je počet respondentů. Do celkového počtu vyplněných dotazníků se započítávají pouze kompletně vyplněné dotazníky, nebylo tedy možné dotazník z poloviny vyplnit a odeslat.

Dotazník vyplnilo celkově 517 osob, z toho bylo 70 % žen a 30 % mužů. Převaha žen převládá nejspíše z toho důvodů, že ženy jsou podle průzkumů na sociálních sítích více aktivní, častěji sdílí různé příspěvky a více používají tlačítko *„To se mi líbí“*. Jelikož byl dotazník sdílen přes sociální sítě a rozeslán přes e-mail, tak jej častěji vyplňovali lidé, kteří tyto sítě používají, tudíž mladší skupina lidí. Celkem 76 % respondentů patří do věkové kategorie 19 až 30 let, druhá nejobsáhlejší skupina činící 13 %, patří do věkové kategorie 31 až 40 let. Úplné věkově složení respondentů, kteří dotazník vyplnili, je vyobrazeno na obrázku č. 6.

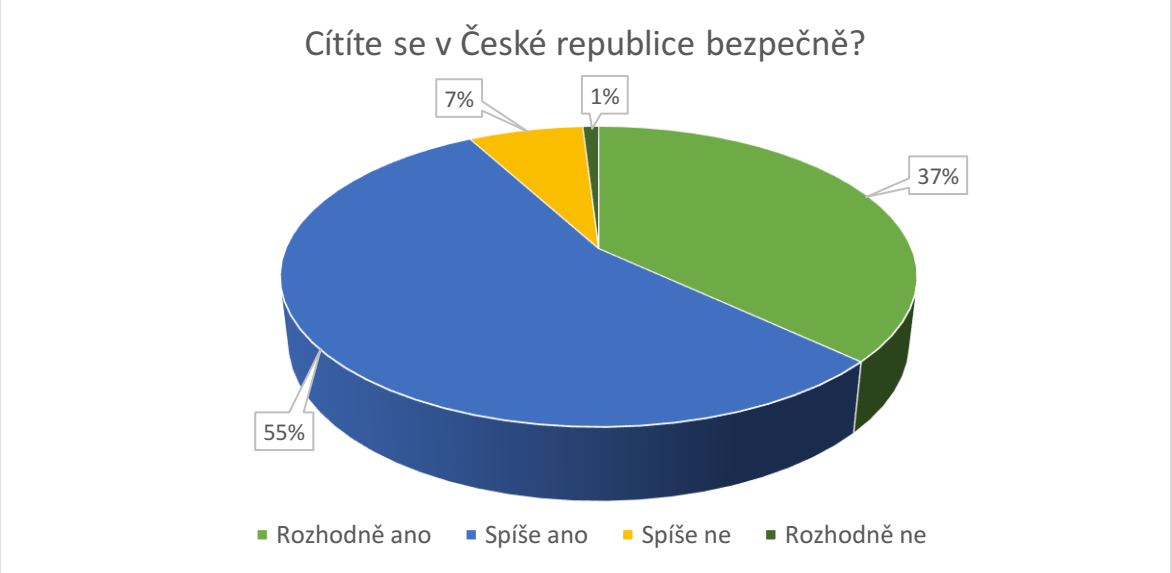
U složení respondentů podle nejvyššího dosaženého stupně vzdělání převládají především dvě kategorie, a to lidé s vysokoškolským vzděláním a středním vzděláním s maturitou. Celkové složení respondentů podle vzdělání je následující: 54 % má vysokoškolské vzdělání, 2 % má vyšší odborné vzdělání, 39 % má středoškolské vzdělání s maturitou, 3 % má středoškolské vzdělání bez maturity a 2 % mají základní vzdělání. Převaha respondentů s vysokoškolským vzděláním se dá vysvětlit především tím, že dotazník byl vložen do školních facebookových skupin UTB, kde jsou z větší části absolventi bakalářských a magisterských programů.




Obrázek 6: Věkové složení respondentů (Březina, 2021; vlastní zpracování).

***Cítíte se v České republice bezpečně?***

První otázka se týkala pocitu bezpečí v České republice. Přesně 92 % respondentů odpovědělo kladně (rozhodně ano a spíše ano), naopak zbylých 8 % je spíše opačného názoru. Existuje mnoho faktorů, které můžou ovlivnit odpověď na tuto otázku. Pocit bezpečí vnímáme každý jinak. Někdo se může cítit v ČR bezpečně, jelikož jsme součástí NATO a EU, anebo díky relativně fungujícímu právnímu systému a bezpečnostním sborům odvádějícím výbornou práci. Na druhé straně se lidé nemusí v ČR cítit bezpečně opět z několika důvodů, například kvůli stálému nárůstu hybridních hrozeb, používání propagandistických kampaní ze strany Ruska či jiné země anebo kvůli aktuální covidové situaci. Faktem zůstává, že podle Globálního indexu míru, který vychází z různých indikátorů hodnocení (zdravotnictví, vzdělávání, bezpečnost, pracovní a sociální život aj.), byla Česká republika v roce 2020 8. nejbezpečnější zemí světa (Global Peace Index 2020, 2020, s. 15).




Obrázek 7: Cítíte se v ČR bezpečně? (Březina, 2021; vlastní zpracování).

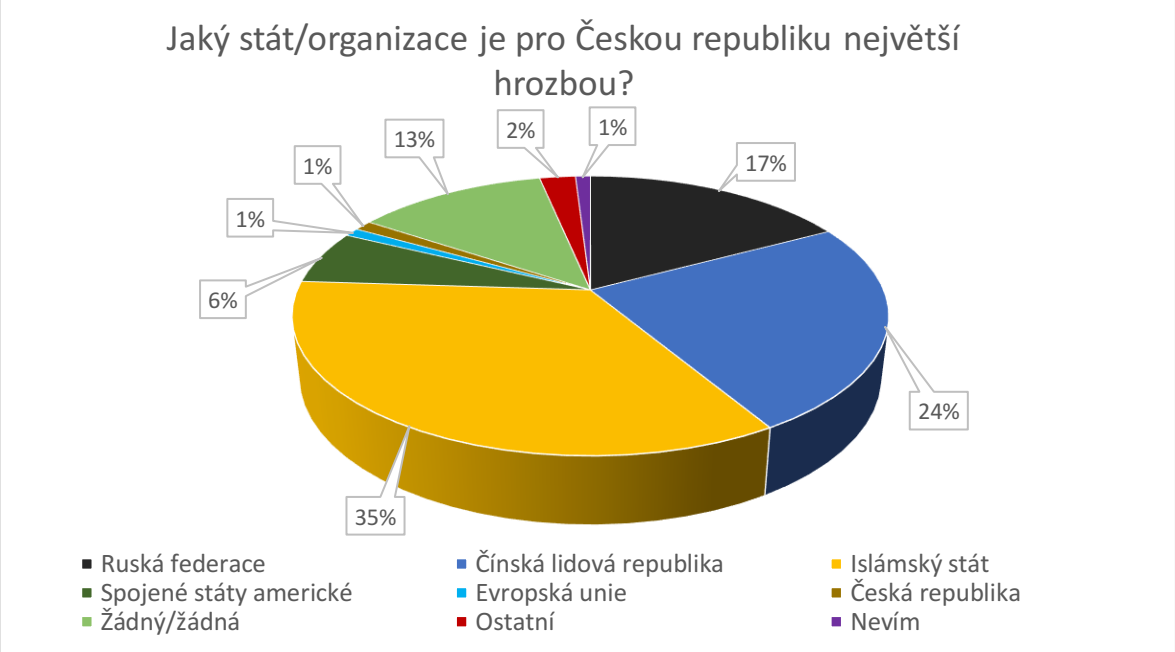
***Myslíte si, že se bezpečnostní situace v České republice v posledních pěti letech zhoršila?***

Na tuto otázku už tak jednoznačná odpověď, jako v předchozí otázce nebyla. Celkem 6 % respondentů je přesvědčeno, že rozhodně ano, 28 % respondentů zaškrtlo spíše ano, 56 % respondentů si myslí, že spíše ne a 10 % respondentů vybralo odpověď rozhodně ne. Tedy zhruba dvě třetiny respondentů si myslí, že se bezpečnostní situace nezhoršila, zbylá jedna třetina je opačného názoru. Důvodem může být horšící se situace v posledních letech na Blízkém východě nebo i v samotné Evropě. Také za tím můžou stát teroristické útoky, které se v posledních letech odehrávají v zemích EU. Za zmínku stojí nedávný teroristický útok,

který se stal 2. listopadu 2020 ve Vídni, jenž si vyžádal 4 lidské životy. Jelikož se tento čin odehrál necelých 100 km od českých hranic, někteří občané můžou mít strach, že se takový čin stane v nejbližší době i v ČR.

***Jaký stát/organizace je pro Českou republiku největší hrozbou?***

Zajímavým zjištěním pro mě bylo, jaké státy/organizace představuji pro ČR největší hrozbu z pohledu veřejnosti. Respondenti měli v dotazníku na výběr ze šesti možností a to: Ruská federace, Čínská lidová republika, Islámský stát, Spojené státy americké, žádný/žádná a jiná. Nakonec se ale výsledný graf skládá celkově z devíti odpovědí. Největší hrozbou z pohledu veřejnosti je organizace Islámský stát s 35 %, na druhém místě je Čínská lidová republika s 24 % a třetí místo zaujímá Ruská federace s 17 %. Všechny tyto zmíněné hrozby jsou bezesporu odůvodnitelné. Už jenom z výročních zpráv zpravodajských služeb se dá dočíst o různých akcích, které vedou jak Rusko, tak Čína, popřípadě Islámský stát, ať už se jedná o propagandu, dezinformační kampaně, kybernetické útoky či terorismus. 13 % respondentů si myslí, že pro ČR není hrozbou žádný stát či organizace a pouze 6 % respondentů označilo jako hrozbu Spojené státy americké. Někteří se domnívají, že hrozbou je EU (1 %) a dokonce i Česká republika sama sobě (1 %).

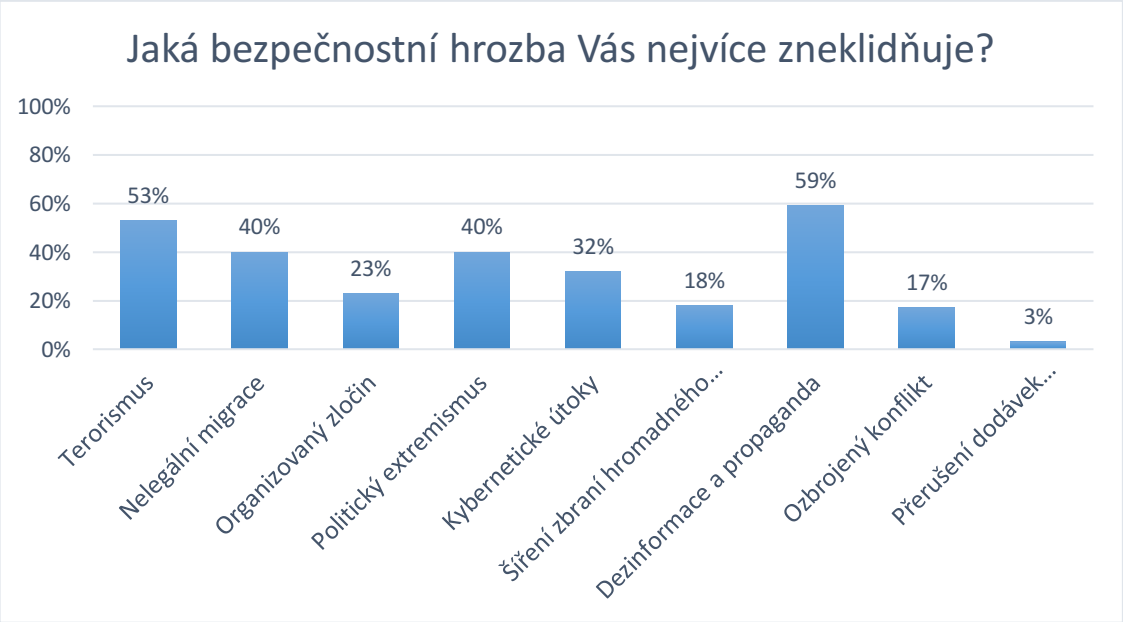



Obrázek 8: Jaký stát/organizace je pro Českou republiku největší hrozbou? (Březina, 2021; vlastní zpracování).

***Jaká bezpečnostní hrozba Vás nejvíce zneklidňuje?***

Tato otázka úzce souvisí s tou předcházející, jelikož za bezpečnostními hrozbami z velké části stojí nějaký stát či organizace. U této otázky mohli respondenti vybrat maximálně tři odpovědi, tím pádem součet všech odpovědí je vyšší než samotný počet respondentů. Velikým překvapením je výsledný graf, ze kterého je patrné, jaké hrozby jsou pro občany ČR zneklidňující. Celkem pro 59 % dotázaných představuje největší hrozbu dezinformace a propaganda. Mezi další významné hrozby podle výsledků patří terorismus, který označilo 53 % respondentů, téměř každý druhý. Nelegální migrace a politický extrémismu označilo 40 % respondentů. Procentuální vyjádření všech hrozeb je k nahlédnutí viz níže.

Pozitivní informací je, že lidé vnímají moderní hrozby, především ty hybridní. S dezinformacemi a propagandou se lidé setkávají na internetu dennodenně, jak na různých zpravodajských webech, tak i na sociálních sítích. I teď během covidové pandemie se fake news šíří rychleji než kdy jindy. Proto je důležité si informace ověřovat a zjišťovat si jejich původní zdroje. Terorismus už je jakým si evergreenem mezi hrozbami, ale není možné ho akceptovat. Bojovat proti němu musí zejména vláda, armáda, policie, zpravodajské služby, ale i soukromé subjekty. Ať už s některými výroky prezidenta Miloše Zemana souhlasíme nebo ne, v jednom z nich má rozhodně pravdu *„S teroristy se nevyjednává, s teroristy se bojuje“*.

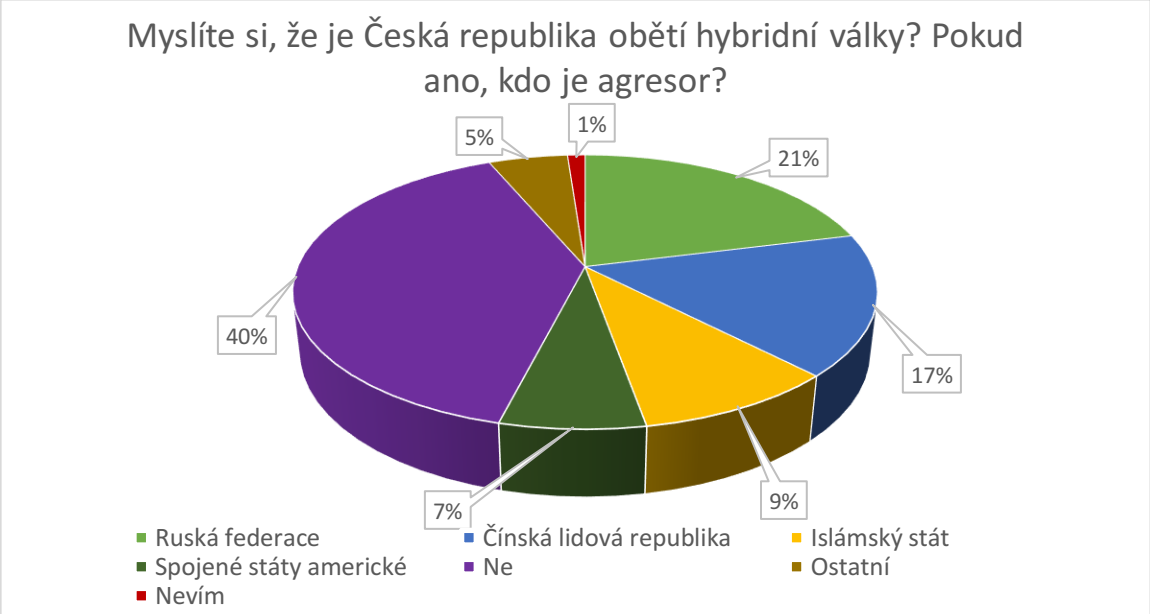



Obrázek 9: Jaká bezpečnostní hrozba Vás nejvíce zneklidňuje? (Březina, 2021; vlastní zpracování).

***Myslíte si, že je Česká republika obětí hybridní války? Pokud ano, kdo je agresor?***

V teoretické části jsou popsané podmínky, kdy je možné mluvit o hybridní válce a Česká republika tyto podmínky naštěstí momentálně nesplňuje. Pravdou však zůstává, že jsou proti ČR používány nástroje hybridní války, které mají za úkol například ovlivnit veřejné mínění, destabilizovat zemi, šířit dezinformace apod. Mezi tyto nástroje patří i informační válka a podle ředitele NÚKIB Karla Řehky se ČR právě v takové formě války nachází (Golis, 2018).

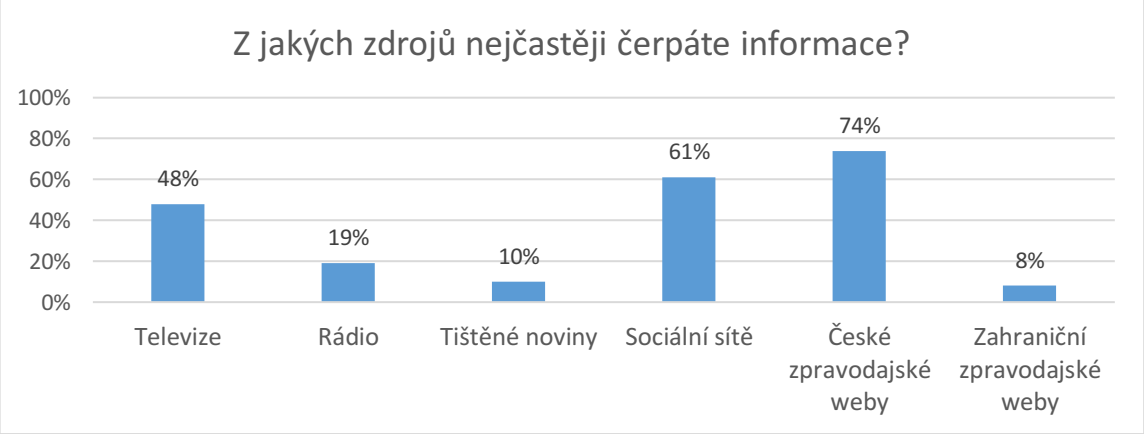
Celkem 40 % respondentů si myslí, že ČR není obětí hybridní války, na druhé straně 54 % respondentů je přesvědčeno o opaku. Respondenti označili za největšího agresora Ruskou federaci s 21 %, pak Čínskou lidovou republiku se 17 %, Islámský stát s 9 % a Spojené státy americké se 7 %. Podle ředitele Bezpečnostní informační služby Michala Koudelky je Rusko a Čína hlavními aktéry, co se týče používání vlivových nástrojů. Podle Koudelky je Rusko i Čína *„připraveny nasadit kompletní vlivový arsenál, otevřenými aktivitami počínaje a utajovanými zpravodajskými konče“* (ČTK, 2020). Spojené státy mají s Českou republikou nadstandartní vztahy i tak ale musí být ČR obezřetná a hájit si svoje strategické zájmy. Poslední menší výhružka ve formě obchodní války ze strany USA zazněla na začátku roku 2020, kdy Česko chtělo zavést digitální daň ve výši 7 %, k tomu ale nakonec nedošlo.




Obrázek 10: Myslíte si, že je Česká republika obětí hybridní války? Pokud ano, kdo je agresor? (Březina, 2021; vlastní zpracování).

***Z jakých zdrojů nejčastěji čerpáte informace?***

Další otázka se zaměřovala na to, z jakých zdrojů respondenti čerpají informace. Mohlo by se zdát, že to není až tak důležité, ale opak je pravdou. Média jsou v dnešní době podle mého názoru dobrý sluha ale zlý pán. Pokud nám média prezentují informace podložené fakty, tak je vše v pořádku, pokud jsou ale informace vymyšlené nebo překroucené, jedná se o tzv. dezinformace. Dezinformace jsou často jakým si stavebním kamenem fake news (falešných zpráv), které mají za cíl ovlivnit či zmanipulovat příjemce této zprávy. Proto je potřeba si informace ověřovat a to především na internetu. To spočívá v zjištění zdroje informace, z jakého primárního zdroje daný web čerpal, ověření si zda nejde o hoax a v neposlední řadě ověření si pravosti fotek či obrázků. Z vyhodnocených dat jasně vyplývá, že 74 % dotázaných čerpá informace nejvíce z českých zpravodajských webů, mezi které patří i weby dezinformační, jakou jsou například Aeronet, AC24, Protiproud, Parlamentní listy a mnoho dalších.




Obrázek 11: Z jakých zdrojů nejčastěji čerpáte informace? (Březina, 2021; vlastní zpracování).

***Byli jste někdy v minulosti obětí kybernetického útoku?***

Následující čtyři otázky se zaměřují na dva primární nástroje hybridní války, a to kybernetické útoky a dezinformace a propaganda. Z předešlé otázky vyplývá, že více než polovina respondentů si myslí, že je Česká republika obětí hybridní války. Z odpovědí je patrné, že se 67 % respondentů nestalo obětí kybernetického útoku, naopak tuto zkušenost má 18 % dotazovaných a 15 % respondentů neví, jestli se někdy stalo obětí kybernetického útoků. Otázkou zůstává, jakého charakteru byly dané útoky a jaký účel plnily. Jisté ale je, že těchto útoků přibývá a nebude tomu jinak, proto bude zapotřebí si svá data pečlivě chránit, zálohovat či šifrovat.

***Víte, jakým způsobem čelit kybernetickým útokům?***

Více než polovina, přesně 53 %, dotázaných je přesvědčena, že ví, jakým způsobem se mají bránit proti kybernetickým útokům. Ostatních 47 % to netuší, což je 241 respondentů. Proti kybernetickým útokům hraje velkou roli obrana a z větší části se na ní podílí lidský faktor. Právě onen lidský faktor z veliké části představuje nejslabší článek kybernetické bezpečnosti. Proto je vhodné se v této oblasti vzdělávat a používat základní bezpečnostní pravidla. I proto experti z NÚKIB, Národní agentury pro komunikační a informační technologie (NAKIT) a Ministerstva vnitra spojili síly a připravili dokument s názvem *„Minimální bezpečnostní standart"*. Tento dokument si klade za cíl pomoc s kybernetickou bezpečností především organizacím, kde je žádoucí aby pracovníci znali a respektovali základní pravidla ochrany před hrozbami kyberprostoru. NÚKIB vydává i další podpůrné materiály, které poskytují informace o kybernetické bezpečnosti (Houser, 2020).

***Setkali jste se někdy v minulosti s dezinformacemi (fake news) či propagandou?***

Tato otázka úzce souvisí s otázkou *„Jaká bezpečnostní hrozba Vás nejvíce zneklidňuje?"*. Respondenti s překvapením odpověděli, že je nejvíce zneklidňují právě dezinformace a propaganda. U této otázky odpovědělo kladně 96 % respondentů, záporně 2 % respondentů a možnost nevím zvolily 2 % respondentů. Dezinformace a propaganda se stávají fenoménem dnešní doby a setkáváme se s nimi téměř všude. Dezinformace se nacházejí zejména na dezinformačních webech, které mají za úkol zmanipulovat čtenáře či diváka a přesvědčit ho o tom, že uváděné informace jsou pravdivé. Proto je důležité si tyto informace ověřovat a zjišťovat původní zdroj takové informace. Také je důležité zvyšovat mediální gramotnost žáků základních a středních škol, u kterých je mediální gramotnosti dlouhodobě na velmi nízké úrovni.

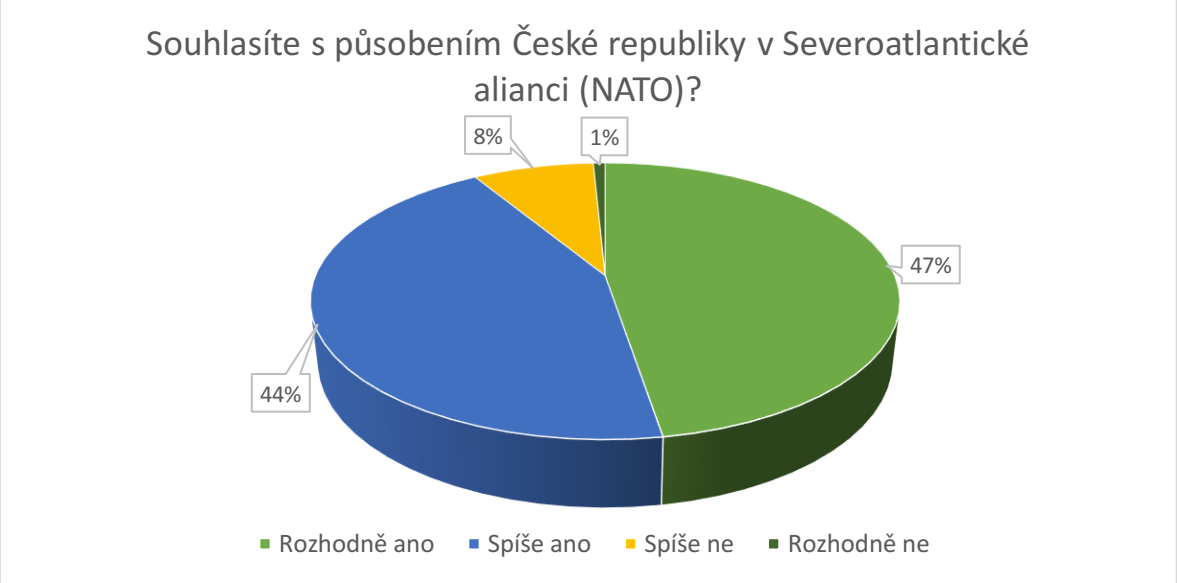
***Víte, jakým způsobem čelit dezinformacím (fake news) a propagandě?***

Více než tři čtvrtiny respondentů, přesně 76 % ví, jak čelit dezinformacím a propagandě, ostatních 24 % respondentů to neví. Dá se konstatovat, že je to dobrá zpráva, jelikož většina dotázaných je schopna si informace jakkoli ověřovat. Na různých webech, které se snaží dezinformacím předcházet, je k dispozici mnoho materiálů, které nám mohou s touto aktuální hrozbou pomoci. Nejznámější je *„RESIST: příručka pro boj s dezinformacemi"*, která je podle mého názoru hodně obsáhlá, místy nepřehledná a čtenář se v ní může snadno ztratit. Originální anglická verze má 72 stran, přeložená česká verze má stran 24. Ale například na webu www.bezpecne-online.cz jsou k dispozici stručnější metodické pomůcky,

které dobře poslouží, jak učitelům, tak i dětem nebo seniorům. Určitě je vhodné se v této oblasti vzdělávat a vést k tomu i děti a seniory, kteří jsou daleko náchylnější k uvěření hoaxům a fake news na internetu.

***Souhlasíte s působením České republiky v Severoatlantické alianci (NATO)?***

Rok 1999 byl pro Českou republiku z pohledu bezpečnosti důležitým milníkem. Česká republika se připojila k NATO a zavázala se tak k plnění určitých závazků. I dnes převládají u veřejnosti názory, že bychom měli z NATO vystoupit, že je pro nás členství nevýhodné, ale z dotazníkového šetření jasně vyplývá, že je více lidí opačného názoru. Celkem 91 % respondentů souhlasí s působením ČR v NATO, zbylých 9 % je proti. Podle mého názoru je NATO z pohledu ČR zárukou bezpečí. Česká republika momentálně není schopná se sama bránit proti případnému napadení, proto je nutností být rovnocenným partnerem v NATO. V rámci smlouvy se všechny členské státy zavazují ke kolektivní obraně, a proto je útok na jakýkoliv členský stát brán, jako útok proti všem. Této skutečnosti bylo využito v reakci na teroristické útoky 11. září 2001 spáchané ve Spojených státech amerických.




Obrázek 12: Souhlasíte s působením České republiky v Severoatlantické alianci (NATO)? (Březina, 2021; vlastní zpracování).

***Myslíte si, že je prezident České republiky politicky orientovaný spíše na:***

I když by se mohlo zdát, že tato otázka nijak nesouvisí s bezpečností ČR, opak je pravdou. Prezident ČR má reprezentovat stát navenek, má pravomoc jmenovat a povyšovat generály a je také vrchním velitelem ozbrojených sil. Nejenom kvůli těmto pravomocem je důležité, jaké prohlášení prezident vydává, ale také jaké má politické názory a jakým směrem

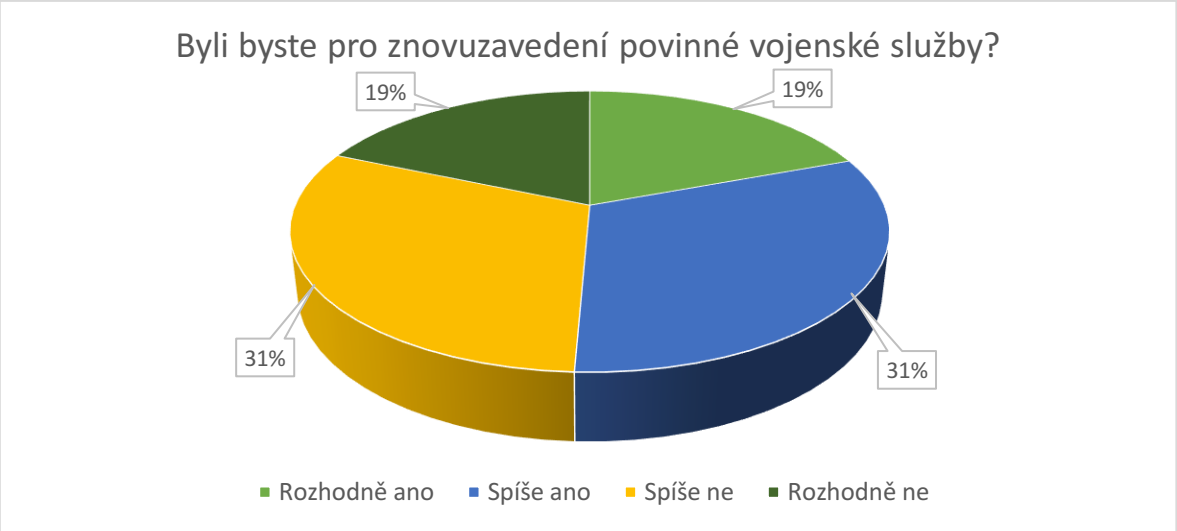
politicky smýšlí. Celkem 91 % respondentů je přesvědčeno, že prezident České republiky Miloš Zeman je politicky orientovaný spíše na východ, ostatních 9 % se domnívá, že je prezident orientovaný spíše na západ. Prezident České republiky Miloš Zeman je označován za loutku a trojského koně Ruska a Číny. Prezident za své funkční období nebyl ani jednou pozván do Bílého domu, naopak s představiteli Ruska a Číny má velmi vřelé vztahy. Miloš Zeman je také proti vylučování Ruska a Číny z tendru na Dukovany a opakovaně nechce povýšit ředitele BIS Michala Koudelku do hodnosti generála a takto by se dalo pokračovat dál. Není tedy pochyb, že Miloš Zeman je politicky orientovaný spíše na východ a otázkou zůstává, do jaké míry to může být pro ČR nevýhodné nebo nebezpečné.

***Souhlasíte se zahraničními misemi Armády České republiky?***

Účast na zahraničních misích vychází především ze zákona č. 219/1999 Sb., o ozbrojených silách České republiky. Zejména pak z paragrafu 9, který hovoří o úkolech vyplívajících z mezinárodních smluvních závazků o společné obraně proti napadení a paragrafu 10, který uvádí mezinárodní spolupráci s cizími ozbrojenými silami ve prospěch míru a bezpečnosti (Česko, 1999). Armáda ČR se zúčastňuje zahraničních operací na základě smluvních závazků k mezinárodním organizacím. Jedná se zejména o NATO, EU, OSN a OBSE, popřípadě na základě bilaterálních dohod. Celkem 76 % respondentů je pro zúčastňování se takovýchto misí, zbylých 24 % je proti. Podle mého názoru je nezbytné se zahraničních misí zúčastňovat nejenom proto, abychom dostáli svým závazkům a byly tak rovnocennými členy mezinárodních organizací, ale také pro bezpečnost všech občanů Česka. Edmund Burke to vystihuje ve svém citátu: *„Zlu k vítězství stačí, když dobří lidé nedělají nic.“* (Edmund Burke, ©2021).

***Byli byste pro znovuzavedení povinné vojenské služby?***

Povinná vojenská služba byla v České republice zrušena v roce 2005, kdy zároveň došlo k profesionalizaci Armády České republiky. Zároveň pořád platí branná povinnost, která by byla vyžadována při ohrožení státu nebo při válečném stavu. Při této otázce došlo překvapivě k nejednotné odpovědi, polovina respondentů by byla pro znovuzavedení povinné vojenské služby a polovina by byla proti. Někteří poslanci a senátoři jsou toho názoru, že by se povinná vojenská služba měla zavést. Na druhé straně převládají i opačné názory, že zavedení povinné vojenské služby by byl krok zpět. Podle mého názoru se ČR vydala tím nejlepším směrem – profesionalizace Armády ČR, možnost připojit se k aktivním zálohám nebo možnost zúčastnit se dobrovolného vojenského 6 týdenního cvičení.




Obrázek 13: Byli byste pro znovuzavedení povinné vojenské služby? (Březina, 2021; vlastní zpracování).

***Měly by se ve školách vyučovat předměty o bezpečnosti České republiky?***

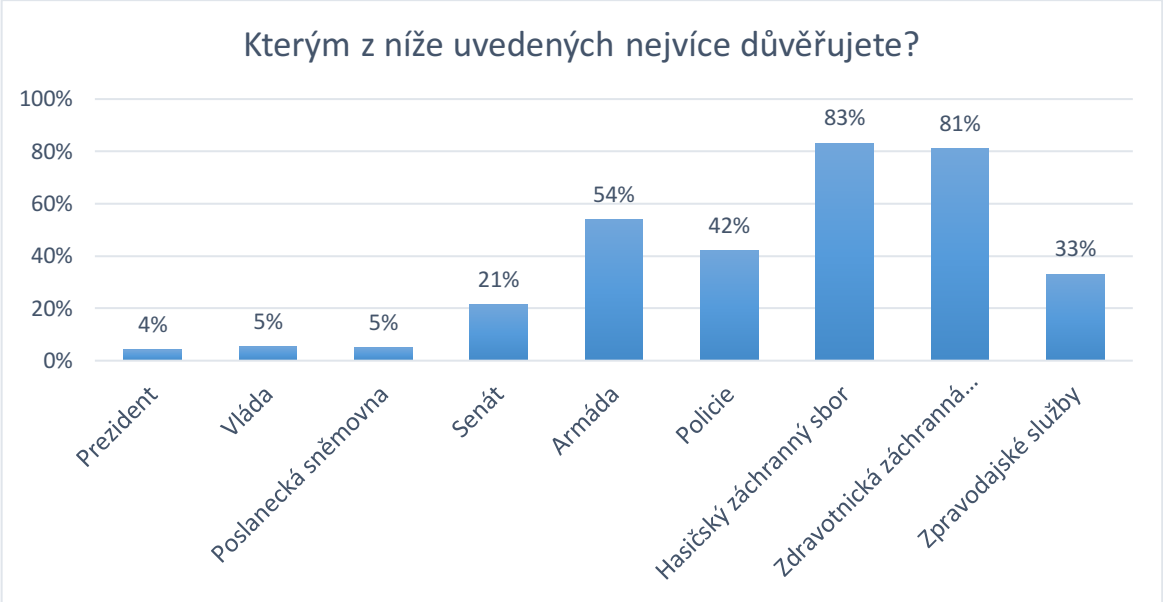
Vzdělávání v oblasti bezpečnosti České republiky je na základních a středních školách momentálně zajišťováno prostřednictvím Přípravy občanů k obraně státu (dále jen POKOS). Aktuálně je platná Koncepce POKOS 2019-2024, která navazuje na Koncepci POKOS 2013-2018. Celkem 84 % respondentů by bylo pro zavedení předmětů o bezpečnosti ČR na školách, zbylých 16 % tento názor nesdílí. Hlavním cílem Koncepce POKOS 2019-2024 je *„dosáhnout takového stavu, aby každý občan cítil svou stálou spoluodpovědnost za zajišťování obrany státu a byl k obraně státu připraven“* (Koncepce přípravy…, 2019). Podle mého názoru je nezbytné, aby se děti seznamovaly s touto problematikou již na základních či středních školách. Pokud se budou občané v této oblasti vzdělávat, napomůže to minimalizovat případné ztráty na životech a majetku při vyhlášení stavu ohrožení nebo válečného stavu a při mimořádných událostech či při krizových situacích nevojenského charakteru (Koncepce přípravy…, 2019).

***Kterým z níže uvedených nejvíce důvěřujete?***

Poslední otázka z dotazníkového šetření měla za cíl zjistit, jakou důvěrou se těší dané orgány. Respondenti mohli označit i více orgánů, kterým důvěřují, ale zároveň nemuseli zaškrtnout žádného z nabízených. Tuto možnost využilo 19 z 517 respondentů, kteří uvedeným orgánům buď nedůvěřují, nebo na otázku nechtěli odpovědět. Nejnižší důvěře z pohledu veřejnosti se těší prezident a vláda. Prezidentovi důvěřují 4 % respondentů a vládě 5 % respondentů. Nízká důvěra v Prezidenta České republiky Miloše Zemana může být způsobena jeho arogantním chováním a někdy kontroverzními výroky. Někteří státníci se

domnívají, že prezident spíše společnost rozděluje, než aby ji sjednocoval. To může být taky jedním z důvodu, proč prezidentovi důvěřuje tolik málo lidí. V Česku momentálně působí menšinová vláda složená z koalice ANO a ČSSD tolerovaná KSČM. Poslední dobou se vláda netěší veliké oblíbenosti z mnoha důvodů, kdy jeden z nich je pravděpodobně tolerance KSČM. Dalším důvodem může být ne moc dobré zvládání covidové situace. O moc líp na tom není ani poslanecká sněmovna, které důvěřuje také pouze 5 % respondentů.

Trochu lépe hodnocený je až senát s 21 %. Senát je označován jako pojistka demokracie, jeho schopnost se projevila například při úpravě daňového balíčku, který poslanci poslali do senátu v minulém roce. Někteří lidé se však domnívají, že tento orgán je zbytečný a měl by být zrušen. Třetina respondentů důvěřuje zpravodajským službám, policii důvěřuje 42 % respondentů a armádě důvěřuje 54 % respondentů. Nejvyšší oblíbenosti a důvěře se těší zdravotnická záchranná služba (ZZS) a hasičský záchranný sbor (HZS). ZZS důvěřuje 81 % respondentů, nejspíš díky její kvalitní a rychlé péči, kterou denně využívá několik tisíc občanů. HZS se těší takové důvěry nejspíše kvůli obětavému a vstřícnému přístupu hasičů, kteří každý den nasazují své životy při řešení různých mimořádných událostí.




Obrázek 14: Kterým z níže uvedených nejvíce důvěřujete? (Březina, 2021; vlastní zpracování).

## 6.3 Posouzení současného stavu bezpečnostní situace v ČR

Jednotné stanovisko reflektující současnou bezpečnostní situaci v ČR není lehké deklarovat. V posledních letech dochází ke změně bezpečnostního prostředí, jež sebou přináší moderní asymetrické a hybridní hrozby, kterým ČR bezesporu také čelí. Mezi tyto moderní hrozby

patří především informační válka, kybernetické útoky, šíření dezinformací, používání propagandy aj. Moderní hrozby jdou ruku v ruce s novými technologiemi. Předpokládá se, že konflikty v budoucnosti se budou odehrávat více méně jen v kyberprostoru, avšak podle mého názoru se jedná o nereálné předpovědi a i z tohoto důvodu si myslím, že lidé, technika a výzbroj budou mít v konfliktech pořád velké zastoupení. ČR se momentálně nenachází v situaci, kdy by byla ohrožena vojenským konfliktem bezprostředně na svém území. To však neznamená, že nečelí hrozbám jiného charakteru.

V první kapitole praktické části diplomové práce byla provedena analýza asymetrických a hybridních bezpečnostních hrozeb. Cílem analýzy bylo klasifikovat nejzávažnější bezpečnostní hrozby s nepřijatelným rizikem a navrhnout opatření k jejich minimalizaci. Z analýzy vyplývá, že nejzávažnějšími zdroji rizika jsou terorismus, politický extremismus, dezinformace a propaganda, kybernetické útoky a ozbrojený konflikt ve formě hybridní války. I když některým hrozbám už ČR čelí, jiným se zatím vyhýbá. Hybridní válka a teroristický čin v podobě bombového útoku jsou naštěstí zatím jenom hrozby, o kterých se píše a snad tomu tak zůstane i nadále.

Ve druhé kapitole praktické části diplomové práce byly vyhodnoceny a analyzovány odpovědi týkající se bezpečnostní situace v ČR během posledních let z pohledu veřejnosti. Cílem dotazníkového šetření bylo zjistit, jestli se veřejnost cítí v ČR bezpečně, jaké hrozby jsou pro dotazované nejvíce zneklidňující a jaký názor mají na dílčí otázky z problematiky bezpečnosti ČR. Z dotazníkového šetření vyplývá několik skutečností. Přes 90 % respondentů se cítí v České republice bezpečně, na druhé straně třetina dotázaných si myslí, že se bezpečnostní situace za posledních pět let zhoršila. Přes třetinu respondentů označilo za největší hrozbu Islámský stát, druhou příčku obsadila Čína a třetí Rusko. Mezi konkrétní hrozby, které veřejnost zneklidňují, patří dezinformace a propaganda, terorismus, politický extremismus a nelegální migrace. Dílčí otázky dopadly zhruba podle očekávání, až na dvě. Překvapujících odpovědí se dostalo u otázky o znovuzavedení povinné vojenské služby, kde bylo 50 % pro a 50 % proti a dále u otázky týkající se důvěryhodnosti daných orgánů, kde nejhůře dopadli prezident, poslanecká sněmovna a vláda.

Institut pro ekonomiku a mír (Institute for Economics and Peace – IEP) vydává každoročně od roku 2007 publikaci, ve které je vyhodnocena mimo jiné také mírumilovnost daného státu. Index vyhodnocuje tři hlavní témata, jedná se o úroveň bezpečnosti ve společnosti, rozsah domácích a mezinárodních konfliktů a míru militarizace. Podle Globálního indexu míru (Global Peace Index – GPI) z roku 2019 se Česká republika celosvětově umístila na

10. místě. V roce 2020 se ČR umístila celosvětově na 8. místě a celoevropsky se umístila dokonce na 5. místě, čili v celkovém hodnocení si o dvě příčky polepšila (Global Peace Index 2020, 2020, s. 15). IEP vydává každoročně také dokument, kde je vyhodnocena míra ohrožení terorismem. Podle Globálního indexu terorismu (Global Terrorism Index – GTI) z roku 2020, patří ČR do oblasti s velmi nízkým dopadem terorismu a celkově se nachází na 111. místě z celkových 138 příček. Ze zprávy také vyplývá, že ČR si oproti minulému roku polepšila celkem o 10 příček. I z těchto dvou indexů lze usuzovat, že Česká republika je stále jednou z nejbezpečnějších zemí, jak v Evropě, tak i ve světě (Global Terrorism Index 2020, 2020, s. 93).

Na základě výsledků z analýzy asymetrických a hybridních bezpečnostních hrozeb metodou PNH, na základě vyhodnocení a analýzy dotazníkového šetření týkající se bezpečnostní situace v ČR a z dostupných informací se dá konstatovat, že Česká republika nadále patří mezi jednu z nejbezpečnějších zemí na světě. Určitě je vhodné věnovat pozornost hybridním a asymetrickým hrozbám, které jsou v posledních letech na vzestupu. Celková připravenost ČR čelit těmto hrozbám je na dobré úrovni, avšak existují oblasti, ve kterých by bylo vhodné se zdokonalovat.

# 7 NÁVRHY OPATŘENÍ K VĚTŠÍ RESILIENCI PROTI ASYMETRICKÝM A HYBRIDNÍM HROZBÁM

Bezpečnost občanů by měla být jednou z hlavních priorit jakéhokoliv státu. V posledních letech, s příchodem moderních hrozeb je tato priorita čím dál více narušována. Zranitelná místa i hrozby se neustále vyvíjejí, čemuž se musí Česká republika přizpůsobovat. Každý den jsou občané ČR závislí na nejrůznějších službách, jako je energetika, doprava, zdravotnictví či finance. Tyto služby využívají fyzickou a digitální infrastrukturu, což zvyšuje jejich zranitelnost i potenciál narušení. Ruku v ruce s bezpečností občanů jde i bezpečnost státu, která je podle zákona zajišťována ozbrojenými silami, ozbrojenými bezpečnostními sbory, záchrannými sbory a havarijními službami. Dále jsou povinni se na ni podílet státní orgány, orgány územních samosprávných celků a právnické osoby a fyzické osoby (Sdělení komise…, 2020, s. 2-3).

Fenoménem moderních hrozeb jsou bezesporu kybernetické útoky. Tyto útoky páchají velké škody jak v domácnostech, tak i v bankách, finančních službách, zdravotnických zařízeních, malých a velkých podnicích. K nejpoužívanějším metodám patří škodlivý software, krádeže osobních či obchodních dat hackery a phishing. Tyto útoky můžou mít fatální následky, například jako tomu bylo v roce 2020 ve Fakultní nemocnici Brno, kdy byl použit ransomware (vyděračský software). Na vzestupu jsou i tzv. hybridní hrozby ze stran státních a nestátních aktérů, do kterých patří právě kybernetické útoky, ale i dezinformační kampaně, propaganda a teroristické útoky. I když v roce 2019 došlo k mírnému poklesu teroristických útoků, hrozba těchto útoků ze strany islamistických teroristů je stále vysoká. Rostoucí tendenci má i politický extremismus, především ten pravicový. Znepokojující jsou pak útoky motivované rasistickou ideologií. Mezi další bezpečnostní hrozbu patří i nelegální migrace, konkrétně pak tranzitní nelegální migrace (Sdělení komise…, 2020, s. 11-12).

V této kapitole budou navrhnuta možná opatření k větší resilienci České republiky vůči asymetrickým a hybridním hrozbám. Opatření vycházejí z aktuální bezpečnostní situace a jejich implementací by Česká republika alespoň vyrovnala své bezpečnostní deficity v některých důležitých oblastech a dosáhla by tak k posílení své obranyschopnosti.

## 7.1 Zvyšování úrovně mediální gramotnosti

Mediální gramotnost je v posledních letech velmi skloňovaným tématem. Častou definicí tohoto pojmu jsou slova prof. Jana Jiráka, ten dodává: *„Tento pojem by měl sdružovat*

*základní schopnosti – vyhledávání informací, vyhledávání obsahů, porozumění všech jejich významů, schopnosti sdělení analyzovat a porovnávat s dosavadními zkušenostmi, schopnost kriticky hodnotit.“* (Smekalová, 2021). Mediální gramotnost je potřeba zvyšovat nejenom kvůli častěji se šířícím dezinformacím v mediálním prostoru, ale také z důvodů využívání propagandistických kampaní k šíření mocenského vlivu ze stran velmocí.

Mediální gramotnost by měli lidé získávat už na základních, popřípadě středních školách v rámci tzv. mediální výchovy. To se ale podle posledních plošných průzkumů neděje. V letech 2017 až 2018 proběhlo hned několik průzkumů, které měly za cíl zjistit, na jaké úrovni mediální gramotnosti se nachází populace v České republice. Průzkumy byly provedeny organizacemi Česká televize, agentura STEM/MARK, Česká školní inspekce, think tank Evropské hodnoty a Člověk v tísni. Ze všech průzkumů vyplývají shodné závěry, avšak interpretované výsledky vycházejí z průzkumu od agentury STEM/MARK ve spolupráci s Českou televizí. Vysoké úrovně mediální gramotnosti dosahují především muži (31 % z nich), lidé ve věku 30-44 let (31 %) a respondenti s vysokoškolským vzděláním (46 %). Naopak nízkou mediální gramotnost vykazují častěji ženy (32 % z nich), lidé starší 60 let (36 %) a ti, kteří nemají maturitu (38 %). Další průzkum provedený agenturou MEDIAN ve spolupráci s organizací Člověk v tísni se zaměřila především na středoškolské studenty. Z průzkumu vychází, že nejvyšší mediální gramotností se pyšní studenti na gymnáziích ale celková mediální gramotnost středoškoláků je nízká (Smekalová, 2021).

Na základě výše uvedených výsledků průzkumů by bylo vhodné zařadit mediální výchovu do Rámcového vzdělávacího programu pro základní vzdělávání jako samostatný předmět, který by se vyučoval na všech základních školách. Výhodou by byly stejné podmínky pro výuku jako u ostatních povinných předmětů, dané hodinovou dotací zakotvenou v rozvrhu, vedení výuky podle výukového plánu, způsob přípravy učitelů aj. Aktuálně si školy můžou vybrat, v jaké formě budou mediální výchovu vyučovat a to prostřednictvím projektů, integrací do jiného vyučovacího předmětu nebo vytvořením samostatného předmětu. Vzdělávání seniorů by bylo vhodné realizovat pomocí různých vzdělávacích kurzů, v rámci univerzity Třetího věku nebo pomocí elektronických výukových materiálů (Obrátil, 2013).

## 7.2 Vzdělávání a osvěta v oblasti asymetrických a hybridních hrozeb

Důležitým nástrojem v boji proti asymetrickým a hybridním hrozbám by mohla být osvětová činnost, která by pojednávala o tom, co to vlastně asymetrické a hybridní hrozby jsou, jaký mají dopad na společnost, jaké nástroje jsou používány a jakým způsobem jim lze čelit. Proto

je také důležitá komunikace s lidmi. Je nezbytné vysvětlit pojmy jako je hybridní a informační válka, propaganda, dezinformace, kybernetické útoky apod. Osvětová činnost by mohla spočívat v různých kampaních, které by měly za cíl seznámit veřejnost s danou problematikou a doporučit konkrétní bezpečnostní opatření, popřípadě odkázat na různé vzdělávací materiály prostřednictvím webových stránek jako jsou www.e-bezpeci.cz, www.esafetylabel.eu, www.ncbi.cz, www.bezpecne-online.ncbi.cz, www.jsns.cz aj. Osvětová kampaň by měla být otevřená a přátelská, zaměřená na zájmy občanů, nemělo by se v žádném případě jednat o hloupou propagandu. Do kampaně by se mohly zapojit známé a důvěryhodné osobnosti (Kříž, Bechná a Stevkov, 2016, s. 16-17).

Na internetu se momentálně nachází spousta různých vzdělávacích materiálů, jak ve formě elektronických dokumentů, tak i ve formě videí a online seminářů. Před koronakrizí byly velice populární i vzdělávací akce, které sloužily především pro žáky základních a středních škol, učitele a rodiče. K dispozici byly i vzdělávací akce pro firemní zaměstnance a ostatní cílové skupiny, jako jsou například senioři. Mezi kvalitní materiály v oblasti vzdělávání o hrozbách na internetu patří:

- **RESIST: Příručka pro boj s dezinformacemi** od Vládní komunikační služby ve Velké Británii (přeložilo Centrum proti terorismu a hybridním hrozbám),
- **Jak čelit informačním vlivovým aktivitám** od Švédské agentury pro civilní pohotovost (přeložilo Centrum proti terorismu a hybridním hrozbám),
- **Dezinformační dezinfekce** od Člověka v tísni, o. p. s. (vzdělávací program JSNS),
- **Podoby ruské propagandy** od Člověka v tísni, o. p. s. (vzdělávací program JSNS),
- **V digitálním světě** od Člověka v tísni, o. p. s. (vzdělávací program JSNS),
- **Surfařův průvodce po internetu** od Zvol si info z.s.,
- **Rozšifruj zprávy** od Zvol si info z.s.,
- **Průvodce po sociálních sítích** od Zvol si info z.s.,
- **Pravda a lež na internetu** od O2 Czech Republic a.s. (projekt Chytrá škola),
- **Příručka pro vyvracení nepravdivých informací 2020** od Stephana Lewandovskyho a kolektivu autorů.

## 7.3 Implementace Národní strategie pro čelení hybridnímu působení

Bezpečnostní strategický dokument, který by jasně pojmenoval to, co je nazýváno hybridní hrozbou, uváděl by konkrétní důsledky působení hybridních hrozeb a stanovil by, čeho má Česká republika v oblasti hybridního působení dosáhnout, doposud chyběl. Na základě

Akčního plánu Auditu národní bezpečnosti z roku 2016 bylo pověřeno Ministerstvo obrany ČR, aby vypracovalo strategii pro boj s hybridními hrozbami. Po více než čtyřech letech se tak stalo a Národní strategie pro čelení hybridnímu působení byla Vládou České republiky dne 29. 4. 2021 schválena. Velkou zásluhu na konečném vyhotovení tohoto dokument má náměstek pro řízení sekce obranné politiky a strategie ministerstva obrany Jan Havránek, který si dokončení této strategie vzal jako jednu ze svých hlavních priorit (Magdoňová, 2020).

Dokument je pro širší veřejnost přístupný od 29. 4. 2021, avšak podle dostupných informací je materiál zásadní ve dvou ohledech. *„Jde o vůbec první dokument, jenž s vahou státní autority hybridní hrozby výslovně pojmenovává, zevrubně je vsazuje do aktuálního kontextu a uvádí konkrétní důsledky jejich působení. Dokument současně přichází s uceleným plánem, jak takovým hrozbám čelit.“* (Horák, 2021). V dokumentu je uvedeno, že největší dopad má hybridní aktivita státního původu, i když strategie konkrétní není. Podle dlouhodobých upozornění kontrarozvědky se jedná o Rusko a Čínu (Horák, 2021).

Národní strategie pro čelení hybridnímu působení si vytyčila tři strategické cíle, o které by mělo Česko v boji proti hybridním hrozbám usilovat. Prvním cílem je odolná společnost, odolný stát, odolná kritická infrastruktura. Jedná se o schopnost státu a společnosti se rychle a bez významných negativních dopadů vypořádat s intenzivním hybridním působením a v případě způsobených škod tyto škody bez prodlení napravit a obnovit plně funkční stav. Druhým cílem je systémový a celostní přístup v rámci České republiky. Ten spočívá v posílení meziresortní spolupráce a nadresortní koordinace. Česko bude pravidelně prověřovat akceschopnost svého bezpečnostního systému čelit hybridnímu působení prostřednictvím národních a mezinárodních cvičení. Výstupy z těchto cvičení budou využívány k dalšímu systematickému zkvalitňování bezpečnostního systému ČR.

Třetím cílem je schopnost adekvátní a včasné reakce. Poslední cíl bude spočívat v pokračování spolupráce se členy NATO a EU. Podle strategie je členství v těchto organizacích klíčovým nástrojem odstrašování původců hybridního působení. Solidarita a vzájemná podpora členských zemí NATO a EU představuje účinný nástroj prevence hybridního působení i reakce na jeho konkrétní projevy (Národní strategie pro čelení hybridnímu působení, 2021). Ve strategii je doslova napsáno, že *„ČR je připravena na nepřátelskou hybridní činnost reagovat odvetnými opatřeními (včetně sankcí) a dalšími nástroji svými i nástroji mezinárodních organizací, jichž je členem. Součástí adekvátní*

*reakce bude i rozvoj schopnosti vyhodnocovat její účinnost, což bude sloužit jako zpětná vazba pro další postup.“* (Národní strategie pro čelení hybridnímu působení, 2021).

V závěru dokumentu je popsán stručný proces implementace této strategie. Implementace bude pravidelně aktualizována a bude reagovat na neustále se vyvíjející bezpečnostní prostředí. Na strategii bude navazovat akční plán, který bude obsahovat konkrétní opatření a kroky. Plnění akčního plánu bude každoročně vyhodnocováno a dle potřeby bude aktualizováno. Přitom aktualizace plánu je podle mého názoru nezbytná a rozhodující činnost, která povede k efektivnímu výsledku (Národní strategie pro čelení hybridnímu působení, 2021).

## 7.4 Prohlubování a posilování spojeneckých vztahů

V době zhoršující se bezpečnostní situace nejen v Evropě, ale na celém světě, je zapotřebí rozvíjet a budovat spojenecké vztahy s dalšími zeměmi, jako potenciálními cíli hybridní agrese. Výměna zkušeností a větší synergie mezi NATO a EU je v tomto ohledu nezbytná. Neméně důležité je také omezovat diplomatické, hospodářské, vojenské a kulturní vztahy se zeměmi, které by mohli být potencionálními hybridními útočníky (Kříž, Bechná a Stevkov, 2016, s. 16-18).

Prohlubování a posilování spojeneckých vztahů v rámci NATO je podmíněno plněním aliančních závazků vůči ostatním členům. Aby se Česká republika stala rovnocenným členem NATO, je zapotřebí dosáhnout výdajů na armádu ve výši 2 % HDP v co nejbližší době, nejpozději však do roku 2024. Podle dostupných informací je ale patrné, že skoro všechny vládní koalice se této nezbytné investici záměrně dlouhodobě vyhýbají. Například spolupráce v rámci V4 v podobě společných akvizic vojenského materiálu, kvůli restrukturalizaci a obnovy výzbroje by napomohla v plnění aliančních závazků a zároveň by to bylo ekonomicky, politicky i časově výhodné (Daubner et al., 2019, s. 7).

Kybernetické útoky jsou jednou z nejpoužívanějších hybridních hrozeb a Česká republika by měla nejen proti této hrozbě spolupracovat s členskými státy NATO a EU. Primárním obranným prvkem proti kybernetickým útokům je prevence. Bylo by vhodné zavést cvičení, která by simulovala různé scénáře kybernetických útoků na území členských států NATO a EU. V rámci těchto cvičení by docházelo k výměně postupů, zkušeností, know-how a zlepšila by se tak mezinárodní připravenost a kooperace v případě kybernetického útoků na více členských států NATO a EU (Daubner et al., 2019, s. 12).

Velikým milníkem v boji proti hybridním hrozbám se stala spolupráce mezi NATO a EU, jež vyústila v založení Evropského centra pro ochranu proti hybridním hrozbám (The European Centre of Excellence for Countering Hybrid Threats – Hybrid CoE) v Helsinkách 11. dubna 2017. Hybrid CoE má momentálně 28 členů a Česko se stalo členem 21. května 2018. Hybrid CoE sídlí v Helsinkách nejspíše z toho důvodů, že skandinávské země jsou velmi schopné čelit dezinformacím. Například ve Finsku je výuka tzv. mediální gramotnosti samozřejmostí a proto jsou lidé zvyklí s informacemi pracovat a ověřovat si jejich zdroje. V centru se školí úředníci a testují se zde některé nápady, které jsou výsledkem diskusí mezi členskými státy. Centrum se také zabývá výzkumem a analýzami, proč jsou lidé náchylnější věřit dezinformacím, proč se dezinformace šíří nebo jaké jsou nejohroženější skupiny. Jedná se o pomyslné strategické centrum, kde se diskutují problémy a členské státy si vyměňují zkušenosti a poznatky. Výsledkem jsou pak obecná jednotná doporučení pro všechny členské země (Fabiánová, 2019).

## 7.5 Podpora a spolupráce českého obranného průmyslu

V době krize se každý stát opírá především o svůj domácí průmysl. Český obranný průmysl je zhruba z 90 % exportní. Tím je dokázáno, že je ve světě o české výrobky a technologie stále velký zájem. Obranný průmysl je klíčovou součástí obranyschopnosti každé země, stejně tak je důležitý i pro ekonomiku, zaměstnanost, technologický rozvoj i prestiž v zahraničí. Český obranný průmysl má více jak stoletou tradici a v mnoha oblastech se řadí mezi světovou špičkou. S vyvíjejícími se technologiemi je potřeba jít s dobou, a proto je důležité podporovat domácí obranný průmysl, který přispívá k rozvíjení obranyschopnosti Ozbrojených sil České republiky, zejména v době míru (Vala, 2020).

Jelikož se bezpečnostní situace ve světě zásadním způsobem zhoršila, je důležité, od koho Ozbrojené síly České republiky pořizují vojenský materiál. Soběstačnost ve výrobě zbraní a munice je předpokladem většího bezpečí. V časech krize se Česká republika musí spoléhat pouze na sebe a na své nejbližší vojensko-politické spojence. Není možné být v oblasti klíčových technologií závislý na potencionálních protivnících ve smyslu zahraničních dodavatelů vojenského materiálu. *„Cílem spolupráce ministerstva s obranným průmyslem ČR je zajištění dodávek vojenského materiálu a služeb k pořízení a udržení provozuschopnosti kritických zbraňových systémů a zabezpečení operačních potřeb OS ČR.“* (Strategie vyzbrojování…, 2016, s. 13).

Na konci roku 2020 začala ze strany Ministerstva obrany ČR kampaň na podporu českého obranného průmyslu, která měla za úkol přiblížit veřejnosti devět klíčových firem. Tyto firmy jsou nezbytnými partnery dodávajícími své produkty mimo jiné také pro Armádu ČR, která se z velké části podílí na boji proti asymetrickým a hybridním hrozbám (Vzdělávací akce, ©2021). Mezi primární strategické dodavatele vojenského materiálu patří především:

- **EGO Zlín, spol. s r. o.,** vyrábějící záchranné systémy, systémy pro imobilní pacienty, systémy biologické ochrany, systémy dekontaminace a stanové systémy,
- **Ray Service, a. s.,** poskytující komplexní řešení v oblasti výroby kabelových svazků, elektromechanických celků, elektronických zařízení a dodávek kabelových komponent,
- **ERA a. s.,** vyvíjející a vyrábějící multilaterační systémy a technologie pro sledování a rozpoznávání cílů na multistatickém principu (světový unikát – pasivní sledovací systém VERA-NG; nastupující technologie v oblasti protivzdušné obrany – sledování bezpilotních prostředků),
- **AERO Vodochody AEROSPACE a. s.,** zaměřující se na konstrukce a výrobu vojenských a civilních letadel L-39/59/159 (ČR patří mezi jednu z devíti zemí na světě, která dokáže kompletně vyvinout a vyrobit vojenský letoun),
- **PBS Group, a. s.,** vyvíjející a vyrábějící leteckou techniku (jediná česká firma vyrábějící proudové motory, zejména pro bezpilotní letouny),
- **Česká zbrojovka a. s.,** vyrábějící služební, lovecké a sportovní palné zbraně (Česká zbrojovka patří mezi pět nejvýznamnějších výrobců ručních palných zbraní na světě; CZ 806 Bren 2 používá například i Francouzská elitní protiteroristická jednotka),
- **Sellier & Bellot a. s.,** vyrábějící lovecká a sportovní střeliva a komponenty pro pistole a revolvery, pušky, brokovnice a okrajový zápal (Sellier & Bellot patří mezi jednu z nejstarších světových firem v muničním a obranném průmyslu),
- **TATRA TRUCKS a. s.,** vyrábějící nákladní automobily (unikátní podvozek dodnes nikým nenapodobený; Tatra je třetí nejstarší existující automobilkou světa s nepřerušenou výrobou automobilů),
- **Meopta – optika, s. r. o.,** poskytující komplexní řešení od návrhu, vývoje, konstrukce, výroby až po montáž optických, optomechanických a optoelektronických systémů (#VIMECOMAME, ©2021).

## 7.6 Dostatečné financování obranného rozpočtu

Spolupráce a podpora obranného průmyslu úzce souvisí s jeho dostatečným financováním, jelikož na pořízení kvalitního vojenského materiálu je zapotřebí dostatek finančních prostředků. A právě problém s finančními prostředky ještě donedávna trápil Ministerstvo obrany České republiky, kterému chybělo 5 mld. Kč. Poslanci za KSČM by na konci roku 2020 nepodpořili státní rozpočet, pokud by nebylo převedeno 10 mld. Kč z rozpočtu ministerstva obrany do rezervy státního rozpočtu. Pokud by nedošlo k navrácení těchto finančních prostředků zpátky do rozpočtu ministerstva obrany, mělo by to zásadní negativní vliv na plánované modernizační projekty, nebylo by možné dodržet závazků našich spojenců a především by mohlo dojít k ohrožení obranyschopnosti České republiky (ČTK, 2021). Naštěstí vláda 29. 3. 2021 splnila slovo a vrátila veškeré finanční prostředky, které na konci minulého roku byly přesunuty do rozpočtové rezervy.

Už tak je ale financování obranného rozpočtu nedostatečné nebo při nejmenším diskutabilní. V Obranné strategii České republiky z roku 2017 se píše o tom, že Česká republika by měla na obranu v roce 2020 vynaložit 1,4 % HDP. Momentálně je jasné, že se tak nestalo, jelikož v roce 2020 činily výdaje na obranu 1,28 % HDP. Na druhé straně z Koncepce výstavby Armády České republiky do roku 2030 z roku 2019 vychází, že v roce 2020 mělo být vynaloženo na obranu 1,28 % HDP, čili podle tohoto dokumentu jde financování Ministerstva obrany ČR podle plánů. Z těchto dostupných informací vyplývá, že je potřeba se řídit nejnovějšími dokumenty, které obsahují reálné hodnoty výdajů určených na obranu a zároveň si přiznat, že Česká republika s největší pravděpodobností nestihne do roku 2024 vynakládat na obranu 2 % HDP. Předpokládaný, ale už teď nejspíše nereálný, vývoj vynaložených finančních prostředků na obranu ČR do roku 2024 je k nahlédnutí v Příloze P II. Nereálný zejména z toho důvodu, že by v letech 2023 a 2024 muselo dojít k rapidnímu navýšení obranného rozpočtu zhruba o desítky miliard Kč (Koncepce výstavby Armády České republiky 2030, 2019, s. 38 a Obranná strategie České republiky, 2017, s. 10).

Pokud by docházelo v budoucích letech ke stagnaci nebo snižování výdajů na obranu, mohlo by to mít fatální následky z důvodu neplnění akvizičních plánů a došlo by k oslabení obranyschopnosti České republiky. Armáda disponuje zastaralou technikou, kterou je potřeba modernizovat. Armáda musí jít s dobou a není možné budovat kvalitní a profesionální armádu se čtyřicet let starou technikou typu UAZ-469, DANA nebo BVP-2.

# ZÁVĚR

Jak už bylo zmíněno v úvodu diplomové práce, bezpečnostní prostředí se neustále vyvíjí a bezpečnostní situace ve světě není nejlepší. S příchodem moderních technologií dochází k ulehčování běžných činností v našich životech, což bylo bezesporu primárním důvodem vývoje těchto technologií. Bohužel jsou i tací, kteří moderní technologie zneužívají ve svůj prospěch a používají je jako nástroje hybridní či informační války, jako tomu bylo a je v mnoha případech konfliktů. Problematika tématu byla zpracovávána jak v teoretické, tak v praktické části diplomové práce. V teoretické části byly rozebrány a definovány základní pojmy vztahující se k dané problematice. V praktické části byly použity metody, jejichž použitím bylo dosaženo naplnění stanovených cílů. V závěru praktické části byly formulovány konkrétní návrhy opatření, které by při implementaci značně posílily obranyschopnost České republiky.

Primárním cílem práce bylo analyzovat problematiku asymetrických a hybridních hrozeb a na základě zjištěných skutečností navrhnout možná opatření pro větší odolnost České republiky vůči těmto bezpečnostním hrozbám. Podlé mého názoru se podařilo cíl naplnit. Pro naplnění primárního cíle bylo učiněno několik kroků. Prvním krokem bylo teoreticky vymezit základní pojmy vztahující se k předmětné problematice. Další krok spočíval v analýze hrozeb, která byla provedena metodou „PNH“. Posledním krokem bylo na základě analýzy hrozeb a dotazníkového šetření navrhnout konkrétní opatření proti těmto bezpečnostním hrozbám. Sekundární cílem bylo vyhodnotit současnou bezpečnostní situaci v České republice. Tento cíl byl také naplněn a to pomocí dotazníkového šetření, které mělo zjistit, jak občané vnímají aktuální bezpečnostní situaci v Česku, jaké hrozby a organizace/státy jsou pro ně nejvíce zneklidňující apod.

V analýze hrozeb pomocí metody „PNH“ bylo celkově identifikováno 38 typů nebezpečí z 9 zdrojů rizik. Z hodnocení hrozeb vyplývá, že nejzávažnějšími zdroji rizika jsou terorismus, politický extremismus, dezinformace a propaganda, kybernetické útoky a ozbrojený konflikt ve formě hybridní války. Na základě vyhodnocení nejzávažnějších rizik, byla navrhnuta bezpečnostní opatření, která mohou svojí implementací zmírnit následky způsobené mimořádnými událostmi nebo eliminovat samotnou míru rizika.

Pro vyhodnocení současné bezpečnostní situace bylo použito dotazníkové šetření, kterého se zúčastnilo 517 respondentů. Respondenty nejvíce zneklidňuje dezinformace a propaganda, terorismus, nelegální migrace a politický extremismus. Co se týče

státu/organizace, tam respondenti vybrali Islámský stát, Rusko a Čínu. I přes tyto odpovědi se ale více než 90 % respondentů cítí v České republice bezpečně. Dalším příznivým zjištěním bylo, že více než 90 % dotázaných souhlasí s působením Česka v NATO. Naopak zneklidňujícím zjištěním bylo, že více jak 95 % respondentů se už někdy setkalo s dezinformacemi či propagandou a navíc necelých 25 % dotázaných neví, jakým způsobem čelit této hrozbě.

Navrhnutá opatření v závěru práce vycházejí z výsledku analýzy hrozeb a dotazníkového šetření. Přihlédnuto bylo také k aktuální bezpečnostní situaci, která se každým dnem mění. Celkem bylo navrhnuto šest konkrétních opatření a každé z nich má své opodstatnění. Mezi ty nejdůležitější patří určitě zvyšování úrovně mediální gramotnosti ve společnosti, vzdělávání a osvěta v oblasti asymetrických a hybridních hrozeb a implementace Národní strategie pro čelení hybridnímu působení, která byla schválena Vládou České republiky dne 19. 4. 2021. Je nezbytné, aby si lidé uvědomili, že čelit hybridnímu působení musíme pouze celospolečenským přístupem, zahrnujícím jak bezpečnostní složky a orgány veřejné správy, tak i součásti mediálního, vzdělávacího a komerčního sektoru.

Na základě zjištěných výsledků z diplomové práce by bylo možné dále pokračovat v bádání předmětné problematiky např. analyzováním dezinformačních webu a jejich vlivem na společnost. Výstupem by mohl být ucelený seznam dezinformačních webů s podrobnými informacemi, popřípadě navrhnutí anti dezinformačního webu, který by prezentoval ověřené zprávy a přispíval by tak k minimalizaci šíření fake news. Dále by web obsahoval vzdělávací materiály ke zvyšování mediální gramotnosti ve společnosti.

Při psaní diplomové práce jsem se ujistil, jak je důležité obezřetně a konstruktivně přistupovat k veřejně dostupným informacím a prověřovat si zdroje těchto informací. Zejména při vypracovávání mé práce a při současné epidemiologické situaci jsem si uvědomil, jakou sílu mají dezinformační kampaně a šíření fake news. Psaní diplomové práce mi přineslo nové poznatky o dané problematice, pochopení důležitosti hybridních hrozeb v novodobých asymetrických konfliktech a především zjištění nových způsobů čelení proti těmto hrozbám.

# SEZNAM POUŽITÉ LITERATURY

About, ©2021. *EUvsDisinfo* [online]. [cit. 2021-01-22]. Dostupné z: https://euvsdisinfo.eu/about/

ARREGUÍN-TOFT, Ivan, 2001. *How the Weak Win Wars: A Theory of Asymmetric Conflict* [online]. Cambridge University Press [cit. 2020-10-28]. ISBN 9780511521645.

Audit národní bezpečnosti, 2016. In: *Vláda České republiky* [online]. Praha: Ministerstvo vnitra ČR, odbor bezpečnostní politiky a prevence kriminality [cit. 2020-11-14]. Dostupné z: https://1url.cz/etEas

ČTK, 2020. Dezinformace i zastrašování politiků. Čína a Rusko se podle Koudelky nejvíc snaží ovlivnit správu v Česku. In: IRozhlas [online]. [cit. 2021-02-04]. Dostupné z: https://1url.cz/az8u2

BABAYEVA, Elnaz a Sebastian GARCIA, 2020. Propaganda v supermoderní době. *Avast blog* [online]. [cit. 2021-01-22]. Dostupné z: https://1url.cz/6zYXr

BALABÁN, Miloš a Bohuslav PERNICA, 2015. *Bezpečnostní systém ČR: problémy a výzvy*. Praha: Univerzita Karlova v Praze, nakladatelství Karolinum. ISBN 978-80-246-3150-9.

BALABÁN, Miloš a Libor STEJSKAL, 2010. *Kapitoly o bezpečnosti*. 2., změn. a dopl. vyd. Praha: Karolinum. ISBN 978-80-246-1863-0.

Balda spáchal teroristický čin. Nejvyšší soud odmítl skutek překvalifikovat, 2019. In: *Česká televize ČT24* [online]. [cit. 2021-01-12]. Dostupné z: https://1url.cz/zzcMX

Bezpečnostní strategie 2015: kvalitní koncepce, které by se politici měli držet, 2015. *Komentář think-tanku Evropské hodnoty* [online]. [cit. 2020-11-13]. Dostupné z: https://1url.cz/2zPfQ

BOŽEK, František, 2015. Řízení rizik. In: *Moodle - Univerzita obrany* [online]. Brno [cit. 2021-01-09]. Dostupné z: https://1url.cz/BzPTV

BŘEZINA, Jakub, 2021. Dotazníkové šetření: Jak vnímáte bezpečností situaci v České republice? In: *Google Forms* [online]. 517 respondentů. Sběr dat 26. 10. - 26. 12. 2020 [cit. 2021-01-31]. Dostupné z: https://forms.gle/4TbZd863BLYmfxzp7

CAKL, Ondřej, 2019. Dezinformace, fake-news, bulvární zpráva. *Transparency international* [online]. [cit. 2021-01-22]. Dostupné z: https://1url.cz/nM6Bv

CASSIDY, Robert M., 2002. Why Great Powers Fight Small Wars Badly. *Military review*. 41-53.

CLAUSEWITZ, Carl von, 1976. *On war*. Ed. and Trans. M. Howard, P. Paret. Princeton University Press. ISBN 9780691018546.

ČERNOCHOVÁ, Jana, 2017. *Aktualizace Obranné strategie ČR a realita* [online]. In: . [cit. 2020-11-14]. Dostupné z: https://1url.cz/SzPfW

Česká republika v OSN, ©2020. In: *Ministerstvo zahraničních věcí ČR* [online]. [cit. 2020-11-17]. Dostupné z: https://1url.cz/0zPfi

ČESKO, 1947. Vyhláška č. 30/1947 Sb., o chartě Spojených národů a statutu Mezinárodního soudního dvora, sjednaných dne 26. června 1945 na konferenci Spojených národů o mezinárodní organisaci, konané v San Francisku. In: *Sbírka zákonů České republiky*. Dostupné také z: https://www.zakonyprolidi.cz/cs/1947-30/zneni-19930119

ČESKO, 1994a. Zákon č. 153/1994 Sb., o zpravodajských službách České republiky. In: *Sbírka zákonů České republiky*. Dostupné také z: https://www.zakonyprolidi.cz/cs/1994-153/zneni-20190906

ČESKO, 1994b. Zákon č. 154/1994 Sb., o bezpečnostní informační službě. In: *Sbírka zákonů České republiky*. Dostupné také z: https://www.zakonyprolidi.cz/cs/1994-154/zneni-20190906

ČESKO, 1998. Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky. In: *Sbírka zákonů České republiky*. Dostupné také z: https://www.zakonyprolidi.cz/cs/1998-110

ČESKO, 1999. Zákon č. 219/1999 Sb., o ozbrojených silách České republiky. In: *Sbírka zákonů České republiky*. Dostupné také z: https://www.zakonyprolidi.cz/cs/1999-219

ČESKO, 2005. Zákon č. 289/2005 Sb., o Vojenském zpravodajství. In: *Sbírka zákonů České republiky*. Dostupné také z: https://www.zakonyprolidi.cz/cs/2005-289/historie

Čínské zpravodajské služby využívají otevřenost Česka, omezit ruské špiony je složité, uvádí BIS, 2020. In: *Česká televize ČT24* [online]. [cit. 2020-11-15]. Dostupné z: https://1url.cz/vzPfN

ČTK, 2021. Výbor pro obranu vyzval vládu, aby vrátila pět miliard Kč armádě. In: *České noviny* [online]. [cit. 2021-02-26]. Dostupné z: https://1url.cz/1zmnA

DAUBNER, David et al., 2019. Bezpečnostní hrozby pro ČR a NATO z pohledu mladé generace. In: *Asociace pro mezinárodní otázky* [online]. [cit. 2021-02-28]. Dostupné z: https://1url.cz/CzyJ6

Edmund Burke, ©2021. In: *Databáze knih* [online]. [cit. 2021-02-12]. Dostupné z: https://www.databazeknih.cz/citaty/edmund-burke-21245

FABIÁNOVÁ, Pavlína, 2019. Evropské centrum proti hybridním hrozbám vede z Helsinek boj proti neviditelnému nepříteli. In: *Česká televize ČT24* [online]. [cit. 2021-02-28]. Dostupné z: https://1url.cz/fzyev

Formuláře, ©2021. *Google* [online]. [cit. 2021-01-31]. Dostupné z: https://www.google.com/forms/about/

GERHÁT, Ivan, 2018. *Příprava občanů k obraně státu: příručka pro učitele základních a středních škol*. 2. vydání. Praha: Ministerstvo obrany České republiky - Vojenský historický ústav Praha. ISBN 978-80-7278-728-9.

*Global Peace Index 2020: Measuring Peace in a Complex World* [online], 2020. The Institute for Economics & Peace, 107 s. [cit. 2020-11-08]. ISBN 978-0-6485327-8-1. Dostupné z: https://1url.cz/yzPfH

*Global Terrorism Index 2020: Measuring the Impact of Terrorism* [online], 2020. The Institute for Economics & Peace [cit. 2021-01-10]. ISBN 978-0-646-81976-1. Dostupné z: https://1url.cz/qzPf2

GOLIS, Ondřej, 2018. V Česku probíhá informační válka, jsme testovací laboratoří Ruska, přiznává brigádní generál Řehka. In: *IRozhlas* [online]. [cit. 2021-02-04]. Dostupné z: https://1url.cz/XzfDH

HOFFMAN, Frank G., 2007. *Conflict in the 21st Century: The Rise of Hybrid Wars*. Potomac Institute for Policy Studies.

HORÁK, Jan, 2021. Veřejně pojmenovat nepřítele a jít do odvety. Česko má strategii pro hybridní válku. In: Aktuálně.cz [online]. [cit. 2021-03-27]. Dostupné z: https://1url.cz/nKzk3

HOUSER, Pavel, 2020. NÚKIB definuje standard pro zabezpečení nemocnic, škol a obecních úřadů. In: *ITbiz* [online]. [cit. 2021-02-11]. Dostupné z: https://1url.cz/8zxq2

HUOVINEN, Petri, 2011. *Hybrid Warfare - Just a Twist of Compound Warfare*. National Defence University, Department of Military History.

Hybrid Threats: NATO, 2015. *Background Report* [online]. Praha: Asociace pro mezinárodní otázky (AMO), (3) [cit. 2020-11-01]. Dostupné z: https://1url.cz/0zPfq

Jak zastavit terorismus: opatření EU, 2018. In: Evropský parlament [online]. [cit. 2021-01-10]. Dostupné z: https://1url.cz/pzPUg

JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR, 2013. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. 2., aktualiz. vyd. Praha: Policejní akademie ČR v Praze. ISBN 978-80-7251-397-0.

Kdo jsme, ©2020. In: *Vojenské zpravodajství* [online]. [cit. 2020-11-16]. Dostupné z: https://www.vzcr.cz/kontakt-45

KIRCHER, Stefan, 2015. *Asymmetric Warfare. A Challenge for International Humanitarian Law?*. Munich: GRIN Verlag, 12 s. ISBN 9783668112650.

Kolektiv autorů, 2015. *Bezpečnostní strategie České republiky* [online]. Praha: Ministerstvo zahraničních věcí České republiky, 24 s. [cit. 2020-11-08]. ISBN 978-80-7441-005-5.

KOHOUTEK, Rudolf, ©2021. Dotazník. In: *Specializační studium výchovného poradenství Pedagogická fakulta Univerzity Karlovy* [online]. [cit. 2021-01-30]. Dostupné z: http://www.ssvp.wz.cz/Texty/dotaznik.html

KOLOUCH, Jan a Pavel BAŠTA, 2019. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o. CZ.NIC. ISBN 978-80-88168-31-7.

*Koncepce výstavby Armády České republiky 2030*, 2019. Praha: Ministerstvo obrany České republiky - VHÚ Praha. ISBN 978-80-7278-789-0.

*Koncepce přípravy občanů k obraně státu 2019–2024*, 2019. In: Ministerstvo obrany České republiky [online]. Praha [cit. 2021-02-13]. Dostupné z: https://1url.cz/rzxg2

KORECKÝ, Michal a Václav TRKOVSKÝ, 2011. *Management rizik projektů: se zaměřením na projekty v průmyslových podnicích*. Praha: Grada. Expert (Grada). ISBN 978-80-247-3221-3.

KOUDELKA, Ctirad a Václav VRÁNA, 2006. *Rizika a jejich analýza* [online]. Ostrava, 17 s. [cit. 2020-12-30]. Dostupné z: https://1url.cz/Cz9iF. Vysoká škola báňská - Technická univerzita Ostrava, Fakulta elektrotechniky a informatiky, Katedra obecné elektrotechniky.

KOVANDA, Ondřej, 2018. Hybridní válka? Buďme s tím označením opatrní, radí experti. In: *IDNES* [online]. [cit. 2021-01-23]. Dostupné z: https://1url.cz/izYPB

KRÁSNÝ, Antonín, 2003. Pohledy na asymetrii v operacích. *Obrana a strategie*. 77-88.

KŘÍŽ, Zdeněk, Zinaida BECHNÁ a Peter ŠTEVKOV, 2016. *Hybridní válka jako nový fenomén v bezpečnostním prostředí Evropy*. Aktualizované a rozšířené druhé vydání. Praha: Pro Informační centrum o NATO vydalo Jagello 2000. ISBN 978-80-904850-4-4.

KUČEROVÁ, Helena, 2003. *Dezinformace: KTD: Česká terminologická databáze knihovnictví a informační vědy (TDKIV)* [online]. Praha: Národní knihovna ČR [cit. 2020-11-01]. Dostupné z: https://1url.cz/fzPfB

LELE, Ajey, 2014. *Asymmetric Warfare: A State vs Non-State Conflict*. OASIS.

MACK, Andrew, 1975. *Why Big Nations Lose Small Wars: The Politics of Asymmetric Conflict*.

MAGDOŇOVÁ, Jana, 2020. Náměstek Havránek: Vytvoření strategie pro boj s hybridními hrozbami je teď hlavní prioritou. In: *iRozhlas* [online]. [cit. 2021-01-23]. Dostupné z: https://1url.cz/JzYPN

MCCULLOH, Timothy a Richard JOHNSON, 2013. *Hybrid Warfare*. JSOU Report. ISBN 978-1-933749-77-8.

MCKENZIE, Kenneth F., 2000. *The Revenge of the Melians: Asymmetric Thre a t s and the Next QDR*. 118 s. Dostupné také z: https://1url.cz/FzPfp

METZ, Steven a Douglas V. JOHNSON, 2001. *Asymmetry and U.S. Military Strategy: Definition, Background, And Strategic Concepts*. 30 s. U.S. Army War College, Strategic Studies Institute.

*Munich Security Report 2015: Collapsing Order, Reluctant Guardians?* [online], 2015. Munich Security Conference Foundation [cit. 2020-10-31]. Dostupné z: https://1url.cz/gzPfG

Národní strategie pro čelení hybridnímu působení, 2021. *Ministerstvo obrany České republika* [online]. Praha [cit. 2021-4-25]. Dostupné z: https://1url.cz/gKJsx

*NATO: Co je NATO?* [online], ©2020. [cit. 2020-11-17]. Dostupné z: https://1url.cz/tMdR4

O projektu, ©2021. *No More Ransom* [online]. [cit. 2021-01-22]. Dostupné z: https://www.nomoreransom.org/cs/about-the-project.html

*Obranná strategie České republiky: The defence strategy of the Czech Republic*, 2017. Praha: Ministerstvo obrany České republiky - VHÚ Praha. ISBN 978-80-7278-702-9.

OBRÁTIL, Miroslav, 2013. Mediální výchova ve škole. In: *Lipka* [online]. Brno [cit. 2021-03-28]. Dostupné z: https://1url.cz/xKzDN

*Ochrana obyvatelstva a krizové řízení: skripta*, 2015. Praha: Ministerstvo vnitra - generální ředitelství Hasičského záchranného sboru ČR. ISBN 978-80-86466-62-0.

OSINGA, Frans, 2002. *Asymmetric Warfare: Rediscovering the Essence of Strategy*. The Royal Norwegian Air Force Academy.

PAULUS, František et al., 2015. Analýza hrozeb pro Českou republika: Závěrečná zpráva. In: *Databáze strategií* [online]. Praha [cit. 2021-01-03]. Dostupné z: https://1url.cz/Tz9jj

Phishing, ©2021. *ESET* [online]. [cit. 2021-01-21]. Dostupné z: https://www.eset.com/cz/phishing/

RÁCZ, András, 2015. *Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist*. Helsinki: FIIA.

ŘEHKA, Karel, 2017. *Informační válka*. Praha: Academia. XXI. století. ISBN 978-80-200-2770-2.

SDĚLENÍ KOMISE EVROPSKÉMU PARLAMENTU, EVROPSKÉ RADĚ, RADĚ, EVROPSKÉMU HOSPODÁŘSKÉMU A SOCIÁLNÍMU VÝBORU A VÝBORU REGIONŮ o strategii bezpečnostní unie EU, 2020. In: EVROPSKÁ KOMISE. EUR-Lex [online]. Brusel [cit. 2021-02-20]. Dostupné z: https://1url.cz/eKz3y

SMEJKAL, Vladimír a Karel RAIS, c2010. *Řízení rizik ve firmách a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada. Expert (Grada). ISBN 978-80-247-3051-6.

SMEKALOVÁ, Monika, 2021. Mediální gramotnost - jak je na tom česká společnost? In: EPALE - Electronic Platform for Adult Learning in Europe [online]. [cit. 2021-03-28]. Dostupné z: https://1url.cz/QKzdS

SMOLÍK, Josef a Tomáš ŠMÍD, 2010. *Vybrané bezpečnostní hrozby a rizika 21. století*. Brno: Masarykova univerzita, Mezinárodní politologický ústav. ISBN 978-80-210-5288-8.

SOULEIMANOV, Emil, 2006. Terorismus: válka proti státu. Praha: Eurolex Bohemia. ISBN 80-86861-76-7.

STOJAR, Richard, 2018. *Bezpečnostní prostředí 2018: implikace pro obrannou politiku a ozbrojené síly ČR*. Brno: Univerzita obrany. ISBN 978-80-7582-053-2.

Strategie vyzbrojování a podpory rozvoje obranného průmyslu České republiky do roku 2025, 2016. In: *Ministerstvo obrany České republika* [online]. Praha [cit. 2021-02-27]. Dostupné z: https://1url.cz/3zm7T

ŠEFČÍK, Vladimír, 2009. *Analýza rizik*. Zlín: Univerzita Tomáše Bati ve Zlíně. ISBN 978-80-7318-696-8.

ŠESTÁK, Bedřich et al., 2015. *Krizové řízení a bezpečnostní systém České republiky* [online]. Ochrana a bezpečnost o. s., 42 s. [cit. 2020-11-11]. ISSN 1805-5656. Dostupné z: https://1url.cz/1zPfF

THORNTON, Rod, 2007. *Asymmetric Warfare: Threat and Response in the 21st Century*. 256 s. ISBN 978-0-745-63365-7.

Terminologický slovník pojmů z oblasti krizového řízení, ochrany obyvatelstva, environmentální bezpečnosti a plánování obrany státu, 2016. In: *Ministerstvo vnitra České republika* [online]. Praha [cit. 2021-01-03]. Dostupné z: https://1url.cz/Sz9jC

TICHÝ, Milík, 2006. *Ovládání rizika: analýza a management*. V Praze: C.H. Beck. Beckova edice ekonomie. ISBN 80-717-9415-5.

VALA, Marek, 2020. #VimeCoMame - Ministerstvo obrany podporuje český obranný průmysl. In: *Ministerstvo obrany České republika* [online]. [cit. 2021-02-26]. Dostupné z: https://1url.cz/OzmYD

VEJVODOVÁ, Petra, 2012. Politický extremismus a jeho základní charakteristiky: Extremisté na české politické scéně. In: *Vysoká škola CEVRO Institut* [online]. [cit. 2021-01-12]. Dostupné z: https://1url.cz/izct7

Veto List, ©2020. In: *Dag Hammarskjöld Library* [online]. [cit. 2020-11-17]. Dostupné z: https://1url.cz/XzPfa

VOLNER, Štefan, 2007. Asymetrické války. *Vojenské rozhledy*. (3), 15 - 26.

*Vojenská strategie*, c2008. Praha: Ministerstvo obrany ČR - Prezentační a informační centrum MO. ISBN 978-80-7278-475-2.

*Vše o OSN: historie, struktura, financování*, c2014. V Praze: Informační centrum OSN, 16 s. ISBN 978-80-86348-18-6.

Výroční zpráva Bezpečnostní informační služby za rok 2019, 2020. In: *Bezpečnostní informační služba* [online]. [cit. 2020-11-15]. Dostupné z: https://1url.cz/xzPf3

Výroční zpráva Vojenského zpravodajství za rok 2019, 2020. In: *Vojenské zpravodajství* [online]. [cit. 2020-11-15]. Dostupné z: https://1url.cz/VzPfV

Vzdělávací akce, ©2021. In: *Vzdělávání E-Bezpečí* [online]. [cit. 2021-04-03]. Dostupné z: http://vzdelavani.e-bezpeci.cz/?akce=edukace

Zpráva o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území České republiky v roce 2019, 2020. In: *Ministerstvo vnitra České republika* [online]. Praha: Ministerstvo vnitra ČR, odbor prevence kriminality [cit. 2021-01-17]. Dostupné z: https://1url.cz/2zcbC

#VIMECOMAME, ©2021. *Ministerstvo obrany České republika* [online]. [cit. 2021-02-26]. Dostupné z: https://1url.cz/gzmxl

# SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

| | |
|---|---|
| BIS | Bezpečnostní informační služba |
| ČR | Česká republika |
| DSSS | Dělnická strana sociální spravedlnosti |
| ESCTF | East StratCom Task Force |
| EU | Evropská unie |
| GPI | Global Peace Index |
| GTI | Global Terrorism Index |
| HDP | Hrubý domácí produkt |
| HZS | Hasičský záchranný sbor |
| IEP | Institute for Economics and Peace |
| NAKIT | Národní agentura pro komunikační a informační technologie |
| NATO | Severoatlantická aliance |
| OBSE | Organizace pro bezpečnost a spolupráci v Evropě |
| OSN | Organizace spojených národů |
| PNH | Pravděpodobnost ohrožení (P), následků (N) a názor hodnotitelů (H) |
| POKOS | Příprava občanů k obraně státu |
| Sb. | Sbírka zákonů |
| SBOP | Společná bezpečnostní a obranná politika |
| SPD | Svoboda a přímá demokracie |
| TDKIV | Česká terminologická databáze knihovnictví a informační vědy |
| USA | United States of America |
| UTB | Univerzita Tomáše Bati |
| ÚZSI | Úřad pro zahraniční styky a informace |
| VZ | Vojenské zpravodajství |
| ZZS | Zdravotnická záchranná služba |

# SEZNAM OBRÁZKŮ

Obrázek 1: Procentuální vyjádření vítězství asymetrických konfliktů podle typu aktéra ve čtyřech padesátiletých obdobích (Arreguín-Toft, 2001, s. 97; vlastní zpracování). ..... 15

Obrázek 2: Hybridní válka v kontextu s jinými formami války (Houvinen, 2011, s. 9; vlastní zpracování)..... 21

Obrázek 3: Hlavní složky hybridní války (Munich Security Report 2015, 2015, s. 35; vlastní zpracování)..... 22

Obrázek 4: Typy útoků podle regionu od roku 2000 do roku 2019 (Global Terrorism Index 2020, 2020, s. 44)..... 48

Obrázek 5: Grafické znázornění záhlaví dotazníkového šetření v Google Forms (Formuláře, ©2021; vlastní zpracování)..... 56

Obrázek 6: Věkové složení respondentů (Březina, 2021; vlastní zpracování). ..... 57

Obrázek 7: Cítíte se v ČR bezpečně? (Březina, 2021; vlastní zpracování). ..... 58

Obrázek 8: Jaký stát/organizace je pro Českou republiku největší hrozbou? (Březina, 2021; vlastní zpracování). ..... 59

Obrázek 9: Jaká bezpečnostní hrozba Vás nejvíce zneklidňuje? (Březina, 2021; vlastní zpracování)..... 60

Obrázek 10: Myslíte si, že je Česká republika obětí hybridní války? Pokud ano, kdo je agresor? (Březina, 2021; vlastní zpracování)..... 61

Obrázek 11: Z jakých zdrojů nejčastěji čerpáte informace? (Březina, 2021; vlastní zpracování)..... 62

Obrázek 12: Souhlasíte s působením České republiky v Severoatlantické alianci (NATO)? (Březina, 2021; vlastní zpracování). ..... 64

Obrázek 13: Byli byste pro znovuzavedení povinné vojenské služby? (Březina, 2021; vlastní zpracování)..... 66

Obrázek 14: Kterým z níže uvedených nejvíce důvěřujete? (Březina, 2021; vlastní zpracování)..... 67

# SEZNAM TABULEK

Tabulka 1: Očekávané účinky strategické interakce na výsledky konfliktů (očekávaní výherci v buňkách) (Arreguín-Toft, 2001, s. 108; vlastní zpracování). ..... 17

Tabulka 2: Postavení bezpečnostní legislativy v právním řádu ČR (Balabán a Stejskal, 2010, s. 71; vlastní zpracování). ..... 27

Tabulka 3: Pravděpodobnost vzniku a existence nebezpečí (Koudelka a Vrána, 2006, s. 10; vlastní zpracování). ..... 40

Tabulka 4: Možné následky ohrožení (Koudelka a Vrána, 2006, s. 10; vlastní zpracování). ..... 40

Tabulka 5: Názor hodnotitelů (Koudelka a Vrána, 2006, s. 10; vlastní zpracování). ..... 40

Tabulka 6: Míra rizika vyjádřena bodovou metodou PNH (Koudelka a Vrána, 2006, s. 10; vlastní zpracování). ..... 41

Tabulka 7: Bezpečnostní rizika vyhodnocená metodou „PNH“ (Koudelka a Vrána, 2006, s. 13-16; vlastní zpracování). ..... 43

Tabulka 8: Identifikace prioritních rizik (vlastní zpracování). ..... 46

Tabulka 9: Doporučené způsoby minimalizace rizika (Božek, 2015, s. 111; vlastní zpracování). ..... 47

# SEZNAM PŘÍLOH

Příloha P I: Dotazník

Příloha P II: Finanční prostředky na obranu České republiky od roku 1993 do roku 2024

## PŘÍLOHA P I: DOTAZNÍK

# Jak vnímáte bezpečnostní situaci v České republice?

Dobrý den, jmenuji se Jakub Březina a jsem studentem UTB ve Zlíně, Fakulty logistiky a krizového řízení a oslovuji Vás s prosbou o vyplnění mého krátkého dotazníku. Dotazník je zcela anonymní a jeho vyplnění Vám nezabere více jak 5 minut - skládá se pouze z uzavřených otázek. Dotazníkové šetření bude sloužit ke zpracování diplomové práce. Dotazník budete moci vyplnit a odeslat nejpozději do 26. 12. 2020. Předem děkuji za Váš čas.

**Jaké je Vaše pohlaví?**

☐ Muž

☐ Žena

**Do jaké věkové kategorie patříte?**

☐ do 18 let

☐ 19 až 30 let

☐ 31 až 40 let

☐ 41 až 50 let

☐ 50 let a více

**Jaké je Vaše nejvyšší dosažené vzdělání?**

☐ Základní

☐ Střední bez maturity

☐ Střední s maturitou

☐ Vyšší odborné

☐ Vysokoškolské

**Cítíte se v České republice bezpečně?**

☐ Rozhodně ano

☐ Spíše ano

☐ Spíše ne

☐ Rozhodně ne

**Myslíte si, že se bezpečnostní situace v posledních pěti letech zhoršila?**

☐ Rozhodně ano

☐ Spíše ano

☐ Spíše ne

☐ Rozhodně ne

**Jaký stát/organizace je pro Českou republiku největší hrozbou?**

☐ Ruská federace

☐ Čínská lidová republika

☐ Islámský stát

☐ Spojené státy americké

☐ Žádný/žádná

☐ Jiná…

**Jaký bezpečnostní hrozba Vás nejvíce zneklidňuje? (vyberte maximálně 3)**

☐ Terorismus

☐ Nelegální migrace

☐ Organizovaný zločin

☐ Politický extremismus

☐ Kybernetické útoky

☐ Šíření zbraní hromadného ničení a jejich nosičů

☐ Dezinformace a propaganda

☐ Ozbrojený konflikt

☐ Přerušení dodávek strategických surovin nebo elektrické energie

☐ Žádný/žádná

☐ Jiná…

**Myslíte si, že je Česká republika obětí hybridní války? Pokud ano, kdo je agresor?**

Pozn.: Hybridní válka je druh ozbrojeného konfliktu vedeného útočníkem za kombinace konvenčních a nekonvenčních prostředků, mezi které patří např.: psychologické operace a propaganda, kybernetické útoky, kriminální a teroristické aktivity, ekonomické sankce apod.

☐ Ruská federace

☐ Čínská lidová republika

☐ Islámský stát

☐ Spojené státy americké

☐ Ne

☐ Jiná…

**Z jakých zdrojů nejčastěji čerpáte informace?**

☐ Televize

☐ Rádio

☐ Tištěné noviny

☐ Sociální sítě

☐ České zpravodajské weby (idnes.cz, aktualne.cz, lidovky.cz aj.)

☐ Zahraniční zpravodajské weby

☐ Jiná…

**Byli jste někdy v minulosti obětí kybernetického útoku?**

☐ Ano

☐ Ne

☐ Nevím

**Víte, jakým způsobem čelit kybernetickým útokům?**

☐ Ano

☐ Ne

**Setkali jste se někdy v minulosti s dezinformacemi (fake news) či propagandou?**
Pozn.: Fake news (doslovně „falešné zprávy“) jsou úmyslně šířící dezinformace či hoaxy za účelem ovlivnit a zmanipulovat příjemce.

☐ Ano

☐ Ne

☐ Nevím

**Víte, jakým způsobem čelit dezinformacím (fake news) a propagandě?**

☐ Ano

☐ Ne

**Souhlasíte s působením České republiky v Severoatlantické alianci (NATO)?**

☐ Rozhodně ano

☐ Spíše ano

☐ Spíše ne

☐ Rozhodně ne

**Myslíte si, že je prezident České republiky politicky orientovaný spíše na:**

☐ Východ (Rusko, Čína aj.)

☐ Západ (USA, Francie, Německo aj.)

**Souhlasíte se zahraničními misemi Armády České republiky?**

☐ Rozhodně ano

☐ Spíše ano

☐ Spíše ne

☐ Rozhodně ne

**Byli byste pro znovuzavedení povinné vojenské služby?**

☐ Rozhodně ano

☐ Spíše ano

☐ Spíše ne

☐ Rozhodně ne

**Měly by se ve školách vyučovat předměty o bezpečnosti České republiky?**

☐ Rozhodně ano

☐ Spíše ano

☐ Spíše ne

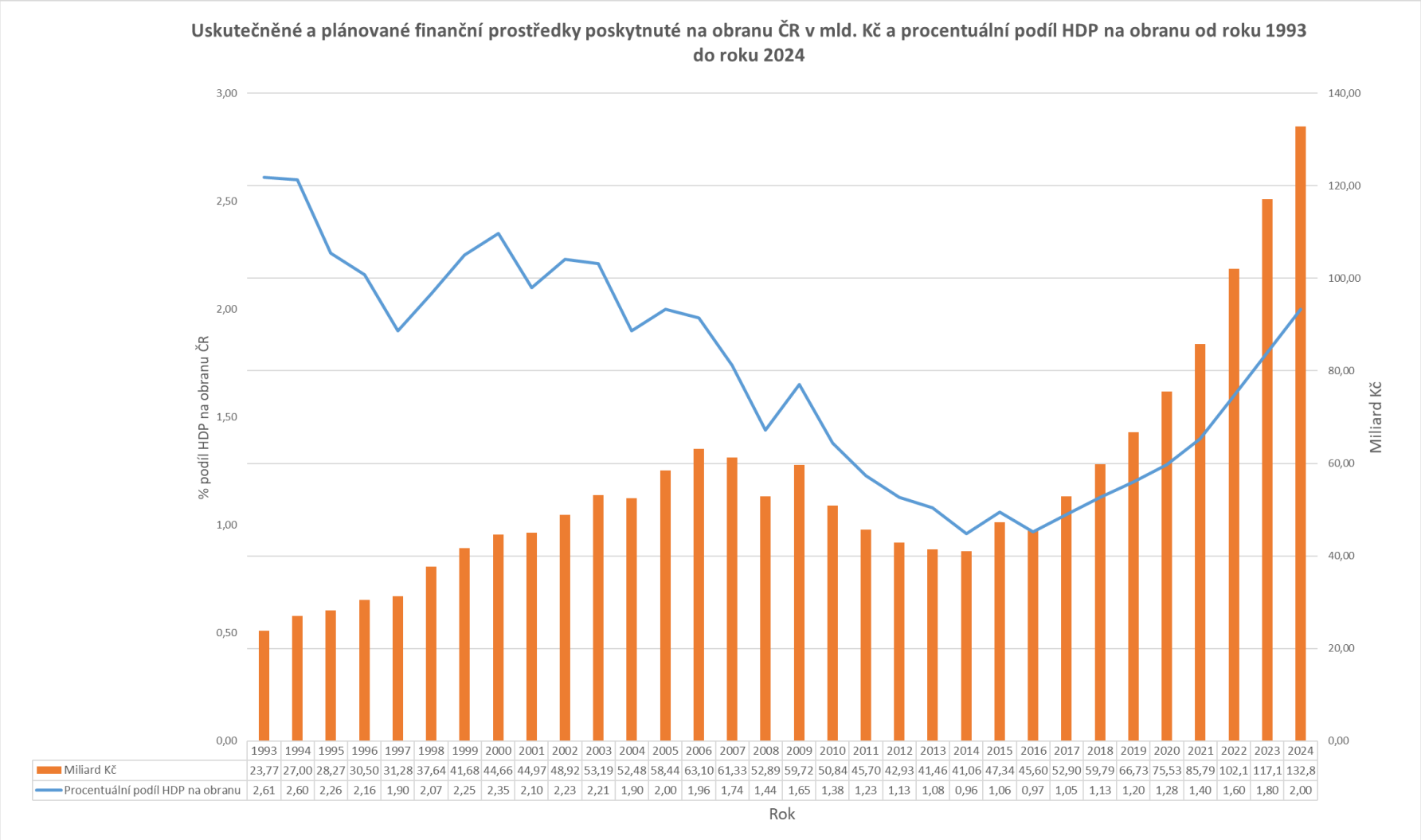
☐ Rozhodně ne

**Kterým z níže uvedených nejvíce důvěřujete?**
Pozn.: Pokud danému subjektu důvěřujete, zaškrtněte políčko. Můžete zaškrtnout všechny políčka nebo taky žádné.

☐ Prezident

☐ Vláda
☐ Poslanecká sněmovna
☐ Senát
☐ Armáda
☐ Police
☐ Hasičský záchranný sbor
☐ Zdravotnická záchranná služba
☐ Zpravodajské služby (Bezpečnostní informační služba aj.)

# PŘÍLOHA P II: FINANČNÍ PROSTŘEDKY NA OBRANU ČESKÉ REPUBLIKY OD ROKU 1993 DO ROKU 2024




| | 1993 | 1994 | 1995 | 1996 | 1997 | 1998 | 1999 | 2000 | 2001 | 2002 | 2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 | 2022 | 2023 | 2024 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Miliard Kč | 23,77 | 27,00 | 28,27 | 30,50 | 31,28 | 37,64 | 41,68 | 44,66 | 44,97 | 48,92 | 53,19 | 52,48 | 58,44 | 63,10 | 61,33 | 52,89 | 59,72 | 50,84 | 45,70 | 42,93 | 41,46 | 41,06 | 47,34 | 45,60 | 52,90 | 59,79 | 66,73 | 75,53 | 85,79 | 102,1 | 117,1 | 132,8 |
| Procentuální podíl HDP na obranu | 2,61 | 2,60 | 2,26 | 2,16 | 1,90 | 2,07 | 2,25 | 2,35 | 2,10 | 2,23 | 2,21 | 1,90 | 2,00 | 1,96 | 1,74 | 1,44 | 1,65 | 1,38 | 1,23 | 1,13 | 1,08 | 0,96 | 1,06 | 0,97 | 1,05 | 1,13 | 1,20 | 1,28 | 1,40 | 1,60 | 1,80 | 2,00 |

(Resortní rozpočet, 2019 a Koncepce výstavby Armády České republiky 2030, 2019, s. 38; vlastní zpracování)