Dezinformace jako nástroj hybridní války

Bc. David Zbraněk

Diplomová práce
2023

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: 2022/2023

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. David Zbraněk**
Osobní číslo:	**L21259**
Studijní program:	**N1032A020002 Bezpečnost společnosti**
Specializace:	**Ochrana obyvatelstva**
Forma studia:	**Prezenční**
Téma práce:	**Dezinformace jako nástroj hybridní války**

Zásady pro vypracování

1. Zpracujte literární rešerši v dotčené problematice.
2. Analyzujte problematiku hybridních a asymetrických hrozeb a vyhodnoťte současnou bezpečnostní situaci v Evropě.
3. Analyzujte současnou strategii boje proti dezinformacím a navrhněte zlepšení.
4. Navrhněte způsob využití dezinformací jako nástroje pro prosazování cílů České republiky a Severoatlantické aliance.

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

Seznam doporučené literatury:

1. *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.
2. KIRCHER, Stefan. *Asymmetric Warfare. A Challenge for International Humanitarian Law?*. Munich: GRIN Verlag, 2015, 12 s. ISBN 9783668112650.
3. 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.
4. ŘEHKA, Karel, 2017. Informační válka. *Informační válka*. Praha: Academia, s. 5. XXI. století. ISBN 978-80-200 2770-2.

Další odborná literatura dle doporučení vedoucího diplomové práce.

Vedoucí diplomové práce: **Ing. Jakub Rak, Ph.D.**
Ústav ochrany obyvatelstva

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

L.S.

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

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

V Uherském Hradišti dne 2. prosince 2022

PROHLÁŠENÍ AUTORA DIPLOMOVÉ PRÁCE

Beru na vědomí, že:

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

Prohlašuji,

- že jsem 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: 28.4.2023

Jméno a příjmení studenta: Bc. David Zbraněk

.....
podpis studenta

ABSTRAKT

Diplomová práce se zaměřuje na problematiku dezinformací v kontextu vedení hybridní kampaně. Samotná práce je rozdělena na dvě části, teoretickou a praktickou. V části první jsou sepsána veškerá teoretická východiska, která jsou následně využita v části praktické. Praktická část je dále rozdělena na další dvě části, kdy první část obsahuje analytickou část zkoumající obranyschopnost České republiky vůči dezinformacím a následné návrhy na zlepšení současné situace. Druhá část se již zabývá uplatněním hybridních nástrojů pro prosazování zájmů České republiky s příklady na zemích, které do jisté míry dle bezpečnostních dokumentů České republiky představují pro českou bezpečnost riziko.

Klíčová slova: dezinformace, hybridní válka, hybridní hrozby

ABSTRACT

The diploma thesis focuses on the issue of disinformation in the context of conducting a hybrid campaign. The work itself is divided into two parts, theoretical and practical. In the first part, all theoretical starting points are written down, which are subsequently used in the practical part. The practical part is further divided into two, where the first part contains an analytical part examining the defense capability of the Czech Republic against disinformation and subsequent proposals for improving the current situation. The second part deals with the application of hybrid tools for the promotion of the interests of the Czech Republic with examples on countries which, according to the security documents of the Czech Republic, pose a risk to Czech security.

Keywords: disinformation, hybrid warfare, hybrid threats

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

OBSAH

ÚVOD

Hybridní válka a hybridní hrozby jsou v posledních letech často zmiňovaným tématem. Jedním z hlavních důvodů je bezpochyby fakt, že se i samotná Česká republika stala terčem mnoha útoků, které měli charakter vedení hybridní války. Nicméně v současné době je stále chápaní hybridních hrozeb na poměrně špatné úrovni což vede k mnohem větší náchylnosti vůči těmto útokům. Jedním z nejrozšířenějších nástrojů hybridní války jsou právě dezinformace, kterými se bude tato diplomová práce primárně zabývat.

Dezinformace, i přes to, že nemají takový ničivý charakter jako jiné nástroje hybridní války, jsou považovány za jeden z nejškodlivějších elementů pro bezpečnostní prostředí, a to z toho důvodu, že dokáží ovlivnit velké množství obyvatelstva najednou, přitom tvorba takové dezinformace není finančně ani časově náročná.

Téma práce bylo zvolené z důvodu rychle měnící se bezpečnostní situace v Evropě spjaté s používáním nových metod válčení, které nevyžadují přímou, vojenskou konfrontaci. Druhým důvodem pro zvolení tohoto tématu je výsledek šetření Auditu národní bezpečnosti ve vztahu schopnosti bránit se před hybridními hrozbami, kde výsledek jasně hovořil o nepřipravenosti České republiky čelit hrozbám tohoto typu.

Zaměření práce na dezinformace bylo vybráno proto, že se s dezinformacemi setkáváme každý den, ať už to bylo během pandemie onemocnění Covid-19, ruské invazi na Ukrajinu, či během prezidentských voleb. S dezinformacemi se samozřejmě setkáváme mnohem déle, a proto je v této diplomové práci popsán i vývoj tohoto fenoménu od druhé světové války.

Samotná práce je rozdělena na teoretickou a praktickou část, kdy v teoretické části je popsaná zvolená problematika, včetně orgánů a dokumentů, které se tímto tématem zabývají. Praktická část se zabývá analýzou současného systému a jeho připravenosti na obranu před dezinformacemi. Dále se praktická část zabývá tvorbou procesu, jakým by mohla Česká republika prosazovat své zájmy za použití dezinformací či jiných prostředků hybridní války. Věřím, že práce přinese nejen lepší chápání problematiky hybridních hrozeb, ale i výsledky v poli obrany proti dezinformacím a případně i jiným hybridním hrozbám a zároveň vytvoří základ pro používání hybridních nástrojů jakožto prostředků pro prosazování zájmů České republiky a jejích spojenců.

I. TEORETICKÁ ČÁST

1 CÍLE A METODY

Diplomová práce má vytyčené dva hlavní cíle. Prvním je analýza obranyschopnosti současného systému před dezinformacemi, jakožto nástrojem vedení hybridní kampaně. Cílem druhým je návrh strategie pro využití nástrojů hybridní kampaně se důrazem na dezinformace k prosazování zájmů České republiky a spojenců. V teoretické části jsou nejprve vypsány pojmy, legislativa a jednotlivé instituce řešící danou problematiku, takovým způsobem, aby navazovali právě na stanovené cíle v části praktické

V samotné praktické části dochází k dosažení těchto stanovených cílů pomocí dvou hlavních analýz. Nejdříve je pomocí bodové analýzy sestaven seznam jednotlivých nástrojů hybridní kampaně v rámci rizika, které představují pro Českou republiku. Na základě výsledků této analýzy je provedena další analýza, opět bodová, která má však za cíl vyhodnotit riziko jednotlivých informačních nástrojů, konkrétně jednotlivých druhů dezinformací. Následně je provedena analýza SWOT, jejímž cílem je právě vyhodnocení současného stavu bezpečnosti České republiky ve vztahu k informačním nástrojům hybridní kampaně.

Po SWOT analýze již následuje druhý stanovený cíl, kterým je vytvoření návrhu pro využití hybridních nástrojů k prosazování zájmů České republiky. Jelikož se však jedná o poměrně nové téma, které se velmi špatně dokumentuje, jsou tyto návrhy diskutabilní, nicméně vychází z dosavadních poznatků, které z vedení hybridní kampaně existují. Praktická část byla vypracována s pomocí zaměstnance Vojenského zpravodajství.

2 POJMOVÝ APARÁT

Pro plné pochopení dané problematiky, je nutno popsat jednotlivé pojmy, které mají mnohdy podobný název, nicméně popisují naprosto odlišné věci.

Dezinformace je taková informace, která je svou podstatou mylná, jejíž cílem je ovlivnit či manipulovat s osobami, které této informaci byly vystaveny.

Misinformace je taková informace, která je rovněž mylná, nicméně není šířena se záměrem ovlivňování či manipulování osob.

Malinformace je pravdivá informace, která má za cíl poškodit či diskreditovat určitou skupinu či jedince.
Fake news je druh žurnalistiky, který záměrně šíří dezinformace. Příkladem jsou dezinformační weby jako Aeronet. Mezi fake news se nicméně řadí i satirické zprávy, které nemají za cíl škodit.

Hoax je zpráva, která má za cíl předat poplašnou, mystifikující či podvodnou zprávu. Hoax je zpravidla přeposílán pomocí e-mailů a k jeho šíření přispívají samotní uživatelé, kteří tuto zprávu dále šíří mezi sebou.

Propaganda nemá jednotnou definici, jelikož může být použita jak pro dobré, tak i zlé účely, a to za použití jak pravdivých, tak lživých informací. Pro potřeby této práce je propaganda chápána jako proces přesvědčování lidí, k čemuž jsou využívány nástroje jako právě dezinformace.

Hrozba je v kontextu této práce jakýkoliv jev, který má potenciál poškodit zájmy a hodnoty státu.
Konvenční válka je druh ozbrojeného konfliktu, během kterého dochází k použití konvenčních zbraní, tedy všech, kromě zbraní hromadného ničení. Tento druh válčení se zpravidla drží vojenským právem a zúčastněné strany respektují mezinárodní dohody.

Nekonvenční válka narozdíl od konvenčního válčení využívá široké spektrum vojenských, polovojenských a civilních prostředků a personálu. Tyto prostředky slouží k plnění úkolů jako sabotáž, podvratné činnosti, zpravodajské činnosti nebo přímé vedení partyzánské války.

Asymetrická válka je druh konfliktu, kde je jedna strana jednoznačně silnější než druhá. Slabší strana tak zpravidla volí asymetrický způsob boje, který jí umožňuje v jednotlivých

bitvách získat výhodu. Příkladem je například Zimní válka ve Finsku nebo válka v Afghánistánu.

Nepravidelná válka popisuje situaci, kdy se slabší strana naprosto snaží vyhnout konfrontaci s nepřátelskými silami a místo toho útočí na civilní obyvatelstvo, ať už přímo nebo nepřímo. Cílem je demoralizace a vyčerpání protivníka, k čemuž slouží nejen vojenské prostředky, ale i nevojenské v podobě propagandy, dezinformací a dalších psychologických a informačních operací. Příkladem nepravidelné války je mezinárodní terorismus nebo situace mezi Palestinou a Izraelem. Americká doktrína popisuje nepravidelnou válku jako násilný boj mezi státními a nestátními subjekty o legitimitu a vliv nad příslušnou populací.

Hybridní válka je druh konfliktu, který propojuje jednotlivé způsoby válčení, primárně se však jedná o propojení konvenčního a nepravidelného válčení. Nicméně je možné, že k samotnému konvenčnímu střetu sil nikdy nedojde a zapojené strany vedou například takové operace, které mají pouze ekonomicky poškodit druhou stranu, pomocí útoků v kyberprostoru nebo sankcemi. Pokud však ke střetu sil dojde, je pravděpodobné, že mu předcházela velmi dlouhá doba nepravidelného válčení.

Hybridní kampaň je synonymum pro hybridní válku a hybridní válčení, které vychází z dokumentu Severoatlantické aliance *Strategie pro úlohu NATO v boji proti hybridnímu válčení* z roku 2015.

3 PRÁVNÍ NORMY

Česká republika nemá ve své legislativě pevně stanovenou definici dezinformace či propagandy. Stejně tak v trestním právu není vymezená skutková podstata trestného činu šíření propagandy nebo dezinformací. Pokud však dezinformace či propaganda šíří poplašné zprávy, podněcuje k násilí či jiným způsobem poškozuje jiné osoby, je možné autora a šiřitele této informace trestně stíhat na základě trestního zákoníku.

V kontextu hybridní války a obrany před hybridními hrozbami však existuje široký rámec zákonů, které budou popsány v této kapitole.

3.1 Klíčové zákony

Mezi hlavní zákony pokrývající tématiku nejen dezinformací, ale hybridní války obecně patří následující zákony, které berou v potaz například i svobodu projevu, ale zároveň i bezpečnost České republiky.

- Ústavní zákon č. 1/1993 Sb., Ústava České republiky, ve znění pozdějších předpis (ČESKO, 1993a),
- usnesení č. 2/1993 Sb., Usnesení předsednictva České národní rady o vyhlášení LISTINY ZÁKLADNÍCH PRÁV A SVOBOD jako součástí ústavního pořádku České republiky (ČESKO, 1993b),
- ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky (ČESKO, 1998),
- zákon č. 222/1999 Sb., o zajišťování obrany ČR, ve znění pozdějších předpisů (ČESKO, 1999b),
- zákon č. 153/1994 Sb., o zpravodajských službách ČR (ČESKO, 1994a),
- zákon č. 154/1994 Sb., o bezpečnostní informační službě (ČESKO, 1994b),
- zákon č. 289/2005 Sb., o Vojenském zpravodajství (ČESKO, 2005),
- zákon č. 181/2014 Sb., o kybernetické bezpečnosti. (ČESKO, 2014)

3.2 Doplňující zákony

Mezi další zákony jsou zařazeny takové zákony, které vycházejí ze závěrů klíčových zákonů a souvisí s danou problematikou pouze za specifických situací.

- zákon č. 239/2000 Sb., o integrovaném záchranném systému a o změně některých zákonů, ve znění pozdějších předpisů (ČESKO, 2000a),
- zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů (ČESKO, 2000b),
- zákon č. 241/2000 Sb., o hospodářských opatřeních pro krizové stavy a o změně některých souvisejících zákonů, ve znění pozdějších předpisů (ČESKO, 2000c),
- zákon č 219/1999 Sb., o ozbrojených silách České republiky, ve znění pozdějších předpisů (ČESKO, 1999a),
- zákon č. 585/2004 Sb., o branné povinnosti a jejím zajišťování (branný zákon), ve znění pozdějších předpisů (ČESKO, 2004),
- zákon č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů (ČESKO, 2008),
- zákon č. 320/2015 Sb., o Hasičském záchranném sboru České republiky a o změně některých zákonů, ve znění pozdějších předpisů. (ČESKO, 2015)

4 LITERÁRNÍ REŠERŠE

Hybridní válka jako nový fenomén v bezpečnostním prostředí Evropy je první ze čtyř základních vybraných odborných publikací na vybrané téma. Publikace se snaží vytvořit definici hybridní války, což vzhledem k již mnoha existujícím definicím pouze přidává ke zmatení osob, které se o tomto tématu chtějí dozvědět více.

Autoři také uvádí příklady využívání hybridní války, konkrétně v Gruzii a na Ukrajině, kde je však zmíněno pouze období mezi rokem 2014 a 2015, kdy působení hybridních nástrojů bylo jednoznačně na nejvyšší úrovni do začátku ruské invaze na Ukrajinu, nicméně mnoho podstatných událostí je zde tímto rozhodnutím opomenuto. Na druhou stranu je nutné vzít v potaz, že publikace poměrně v krátkém rozsahu dokáže popsat základy hybridního válčení a jako úvodní literatura do tohoto tématu je více než dostačující.

Publikace taktéž přináší řadu návrhů ke zlepšení nejen obranyschopnosti České republiky před hybridními hrozbami, ale také pro využití hybridních nástrojů pro prosazování zájmů České republiky a spojenců, čímž také představuje ideální zdroj pro tuto diplomovou práci.

Druhým vybraným literárním zdrojem je publikace **Asymmetric Warfare. A Challenge for International Humanitarian Law?** V překladu: Asymetrická válka: Výzva pro mezinárodní humanitární právo? Publikace se nezabývá hybridním válčením jako takovým, ale spíše, jak samotný název napovídá, asymetrickou válkou, což je jedna z mnoha forem konvenčního ozbrojeného konfliktu, který může vzniknout právě působením hybridních nástrojů. V publikaci je kladen důraz na popsání situace, která panovala během války v Jugoslávii. Konkrétně je zde zvýrazněna situace, kdy o samotném válčení nerozhodovali zástupci armád, ale spíše politici či jednotlivé ozbrojené skupiny.

Samotná publikace nehovoří o konceptu hybridní války, ale byla vybrána z důvodu, že se tento přelom ve vedení války se může považovat za jeden z mnoha bodů, kdy došlo k přelomu ve válčení a do popředí se od té doby dostává právě válčení hybridní. Samozřejmě těchto bodů lze v historii najít několik a přesnou událost zodpovědnou za vývoj ve válčení není možné určit.

Samotná problematika humanitárního práva pak dále navazuje na fakt, že je v případě vedení asymetrické války a kampaně podobného typu není jednoduché monitorovat dodržování pravidel války a také je složité najít zodpovědnou osobu v případě porušování těchto pravidel.

Třetí publikace nese název **Informační válka,** kterou napsal současný náčelník generálního štábu, generálmajor Karel Řehka. Kniha pojednává o tom, jak rozvoj informačních

technologií pomohl změnit vedení vojenské kampaně. Autor vychází z historických událostí a generací válčení, které jsou taktéž vysvětleny v této diplomové práci, autor zároveň nastiňuje možnou podobu válčení budoucnosti.

V knize je vyzdvihnuta problematika, že s rostoucím množstvím informačních nástrojů společně s pokroky v tomto poli sice roste naše schopnost využívat tyto prostředky efektivněji, ale zároveň se jedná o dvojsečný meč a více takových prostředků zároveň představuje více možností pro potencionálního protivníka, který může tyto nástroje využít k útoku na Českou republiky a spojence.

4.1 Poznatky

Vybraná literatura přinesla důležité poznatky pro zvolené téma diplomové práce. Hlavním poznatkem je samotný původ hybridní války, jejímž cílem je subverze protivníka. Jedná se o marxisticko-leninistický koncept, který byl hojně využíván Sovětským svazem, který vykonával útoky na různé politické aktéry, vyvolával nepokoje, šířil propagandu a dezinformace, či pomáhal vytvářet separatistické útvary. Tato strategie stále hraje v doktríně současné Ruské federace významnou roli.

Samotná subverze má dle výše zmíněných a dalších zdrojů několik etap, těmito etapami jsou:

1. demoralizace cílové společnosti,
2. destabilizace cílové společnosti,
3. vyvolání krize v cílové společnosti,
4. převzetí kontroly nad cílovou společností vnitřními silami napojenými na útočníka.

Vybraná literatura taktéž určuje situace, ve kterých se daný stát může stát terčem hybridního útoku, primárně se jedná o špatně spravovaný stát s rozštěpenou společností nebo vybraný stát není schopný efektivně bránit své hranice a nemá žádné spojence či není členem žádného společenství.

5 STRATEGICKÉ BEZPEČNOSTNÍ DOKUMENTY

Základ bezpečnostní legislativy České republiky tvoří bezpečnostní a strategické dokumenty, které se zpravidla obnovují v určitém časovém úseku. Hlavní bezpečnostní a strategické dokumenty jsou:

- Bezpečnostní strategie České republiky (2015)
- Obranná strategie České republiky (2017)
- Audit národní bezpečnosti (2016)
- Národní strategie kybernetické bezpečnosti České republiky na období let 2021–2025 (2020)
- Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2021 až 2025 (2021)
- Bílá kniha o obraně (2011)
- Koncepce výstavby Armády České republiky 2030 (2019)
- Koncepce přípravy občanů k obraně státu 2019-2024 (2019)
- Koncepce ochrany obyvatelstva do roku 2020 s výhledem do roku 2030 (2013)

5.1 Bezpečnostní strategie České republiky

Bezpečnostní strategie České republiky je hlavním dokumentem, který formuje bezpečnostní politiku České republiky. V současné době je nejaktuálnějším vydáním verze z roku 2015. Jedná se o vládní dokument, na jehož tvorbě se podílela Kancelář prezidenta republiky společně s Parlamentem České republiky a představitelé bezpečnostní komunity ze státní a soukromé sféry.

Dokument navazuje na zhoršenou bezpečnostní situaci způsobenou událostmi roku 2014 a hovoří o asymetrických hrozbách ze strany Daesh a hybridního válčení ze strany Ruské Federace, nicméně jmenovitě tito aktéři nejsou v dokumentu zmíněni.

Bezpečnostní strategie je dále rozdělena na čtyři hlavní části, které popisují východiska bezpečnostní politky České republiky, bezpečnostní zájmy České republiky, bezpečnostní prostředí a strategii prosazování bezpečnostních zájmů České republiky. (Ministerstvo zahraniční, 2015)

5.2 Obranná strategie České republiky

Obranná strategie České republiky z roku 2017 je dokumentem navazujícím na předešlé vydání z roku 2012. Dokument se opírá nejen o Bezpečnostní strategii České republiky, ale vychází i ze spojeneckých smluv a dohod v rámci Severoatlantické aliance a Evropské unie. Dokument vytváří strategii obrany České republiky založenou na třech pilířích:

- Stát.
- Ozbrojené síly.
- Občan.

První pilíř hovoří o zodpovědném přístupu České republiky k obraně a k mezinárodním dohodám a partnerům. Druhý pilíř popisuje důležitost bojeschopných ozbrojených sil a poslední, třetí pilíř si zakládá na občanské povinnosti k obraně České republiky.
Narozdíl od Bezpečnostní strategie, Obranná strategie přímo jmenuje viníky zhoršené bezpečnostní situace ve světě a v Evropě. Těmito viníky je Ruská federace, která prosazuje své mocenské zájmy nejen vojenskou silou, ale právě i hybridním válčením a nebojí se tak porušovat mezinárodní právo a jako dalšího viníka dokument jmenuje Daesh, který je schopen vést asymetrickou válku. Zvláště je zde vyzdvižena propaganda a dezinformace, které mají za cíl buď demoralizovat, získat podporu mezi obyvatelstvem nebo v případě Daesh, radikalizovat a přímo rekrutovat z civilního obyvatelstva daných zemí. (Ministerstvo obrany, 2017)

5.3 Audit národní bezpečnosti

Audit národní bezpečnosti je dokument schválený usnesením vlády v roce 2016. Na vypracování tohoto dokumentu se podílelo několik desítek odborníků s cílem vyhodnocení nejzávažnějších hrozeb pro vnitřní bezpečnost České republiky.
Výsledkem výzkumu bylo zjištěno, že Česká republika je schopna účinně odolávat tradičním hrozbám, jako je migrace nebo kriminalita, na druhou stranu stát není schopen se efektivně bránit před hrozbami hybridními. Důležitým faktem je, že i přesto, že Česká republika není schopna se bránit rozsáhlému hybridnímu útoku, tak je velmi nepravděpodobné, že by takový útok byl proti České republice podniknut a pokud k takové situaci dojde je více pravděpodobné, že bude zasaženo několik států, konkrétně spojenců České republiky v rámci Severoatlantické aliance nebo Evropské unie. V případě zasažení několika států by mělo dojít k rozmělnění následků hybridního útoku mezi několik států.

I přes nízkou pravděpodobnost takového útoku existuje několik opatření, které je možné podniknout, aby takový útok buď nebylo možné provést nebo aby následky hybridního útoku byli minimální. Mezi tyto opatření patří soudržná společnost, fungující ekonomika, bezpečnost a obrana. Tyto opatření budou dále rozebrány v praktické části. (Ministerstvo vnitra, 2016)

6 INSTITUCE ŘEŠÍCÍ DANOU PROBLEMATIKU

Hybridní kampaň představuje široké spektrum hrozeb, před kterými je nutno se chránit, a proto lze říci, že každá instituce se může podílet na řešení této problematiky, nicméně je pověřeno devět hlavních orgánů, mezi jejichž hlavní úkoly patří právě bojování proti hybridním hrozbám.

Prvním krokem je samozřejmě zjištění, že byl, je nebo bude proti České republice či proti spojencům České republiky podniknut útok, v tomto případě hybridního charakteru. Aby k takovému zjištění mohlo dojít, je nutné učinit sběr informací, které je následně nutno vyhodnotit. Za tento krok jsou zodpovědné zpravodajské služby, mezi které se řadí:

- Bezpečnostní informační služba (BIS),
- Vojenské zpravodajství (VZ),
- Úřad pro zahraniční styky a informace (ÚZIS).

Prvotní, nevojenské hrozby, vycházející z hybridní kampaně mají podobu útoků v kyberprostoru. Mezi hlavní orgány bránící zájmy České republiky v kyberprostoru patří:

- Národní centrum kybernetických operací (NCKO),
- Národní bezpečnostní úřad (NBÚ),
- Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB)
- Computer Emergency Response Team (CERT).

Poslední skupinou jsou instituce, které mají výkonnou pravomoc a nástroje k jejímu prosazování, tyto instituce jsou:

- Ministerstvo vnitra (MV),
    - Centrum proti terorismu a hybridním hrozbám,
- ozbrojené síly České republiky,
- orgány vnitřní bezpečnosti,
- orgány ochrany obyvatelstva. (Ministerstvo vnitra, 2016)

6.1 Zpravodajské služby

Činnost zpravodajských služeb je zakotvena v zákonech č. 153/1994 Sb., o zpravodajských službách ČR, zákonem č. 289/2005 Sb., o Vojenském zpravodajství a zákonem č. 154/1994

Sb., o bezpečnostní informační službě. Z obecného hlediska je činnost těchto orgánů zaměřena na neustálé získávání a vyhodnocování informací s cílem najít takové informace, které ohrožují bezpečnost České republiky, občanů a zájmů.

Zpravodajské služby se nezaměřují pouze na informace vojenského charakteru, ale zabývají se také informacemi, které mohou poškodit demokratické základy, ekonomiku, průmysl či bezpečnost jako takovou. Činnost zpravodajských služeb taktéž zahrnuje spolupráci s obdobnými službami v zahraničí, samozřejmě v souladu se zákonem 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. Zpravodajské služby se nezapojují do opatření zajišťování bezpečnosti státu.

6.1.1 Výroční zpráva Vojenského zpravodajství za rok 2021

Výroční zpráva popisuje zhoršenou bezpečnostní situaci, ke které za rok 2021 přispěla i pandemie onemocnění Covid-19, která zapříčinila nestabilitu v mnoha zemích světa. Zpráva dále hovoří o tom, že státy místo dialogu řeší problémy iracionálně a vyvíjí nátlak či hrozí otevřenou konfrontací svým protějškům.

Zpráva taktéž popisuje vývoj nových zbraňových systémů, konkrétně autonomních zbraňových systémů, které eliminují potřebu personálu k provozu takového systému. Jako další zpráva vyzdvihuje výzkum v poli hypersonických prostředků, kde je zdůrazněno, že Ruská federace má v tomto ohledu náskok před ostatními zeměmi, a to díky svým raketám Kinžál a Cirkon. Současné dění na Ukrajině, kde Ruská federace, alespoň tedy podle ruských zdrojů, nasadila právě hypersonické prostředky typu Kinžál naplňuje výsledky plynoucí z poslední výroční zprávy. (VZ, 2021)

6.1.2 Výroční zpráva Bezpečnostní informační služby za rok 2021

Bezpečnostní informační služba ve své výroční zprávě hovoří o zhoršených vztazích s Ruskou federací. Za tuto skutečnost dle BIS velkým dílem přispěla kauza Vrbětice, kdy roku 2021 vyšetřování došlo k závěru, že za vybuchlý muniční sklad nese odpovědnost ruská vojenská rozvědka GRU. Mimo Ruskou federaci je taktéž jako hrozba vnímána Čína, která se pomocí dezinformací a propagandy snaží podkopat suverenitu Tchaj-wanu. Jakožto třetího aktéra, který představuje bezpečnostní hrozbu pro bezpečnost České republiky je v této zprávě zmíněn Írán, který však není schopen vést hybridní kampaň proti České republice a jejím spojencům, ale může však ze západních zemí čerpat finance na prosazování svých zájmů na Blízkém východě.

Bezpečnostní informační služba ve své výroční zprávě klade mnohem větší důraz na téma dezinformací než zpráva Vojenského zpravodajství. Konkrétně je zde zmíněna situace, kdy se dezinformační weby snažili ovlivnit volby. Největší hrozbu zde představovali weby, které přidávali dezinformační a jinak manipulativní obsah mezi pravdivé informace a čtenář těchto webů tak nedokázal škodlivou informaci rozeznat. Z pohledu hybridní kampaně se podařilo odhalit i takové weby a organizace, které se prezentovali jako nezávislé, nicméně se jednalo o dezinformační a propagandistické platformy s vazbou na Ruskou federaci. (BIS, 2021)

6.2 Kybernetická bezpečnost

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti určuje Národní bezpečností úřad jako hlavního aktéra kybernetické bezpečnosti. Cíle NBÚ ve vztahu k hybridní kampani jsou zajišťování kybernetické bezpečnosti, zvyšování odolnosti informační infrastruktury a bránění kybernetickým útokům. K prosazování těchto cílů využívá NBÚ své pracoviště CERT.

Na základě akčního plánu o kybernetické bezpečnosti z roku 2015, který předcházel současný plán z roku 2021, buduje Vojenské zpravodajství Národní centrum kybernetických operací, které roku 2018 představilo svou první strategii pro zajišťování obrany v kyberprostoru. NCKO považuje za největší hrozbu fakt, že mocenský vliv se v dnešní době neprosazuje vojensky, ale do popředí se dostávají informační prostředky. Zároveň zdůrazňuje, že šíření dezinformací, špionáž a další jednání s negativním dopadem na bezpečnost České republiky je činnost, kterou vykonávají jedinci či skupiny pracující ve prospěch daných států, čímž tyto konkrétní státy nenesou odpovědnost za případné odhalení takového jednání. NCKO dále varuje, stejně jako mnoho dalších institucí zabývajících se kyberbezpečností, že velkým rizikem je stále rostoucí počet zařízení s nedostatečným zabezpečením, které jsou připojeny k internetu společně s nízkou digitální gramotností.

6.3 Ozbrojené síly České republiky

Hlavními úkoly ozbrojených sil České republiky je odstrašení protivníka od útoku proti státu a jeho občanům či odvrácení nebo eliminace již hrozícího útoku. Tyto úkoly jsou plněny na základě kolektivní obrany ve spolupráci s ostatními členskými státy Severoatlantické aliance. Jelikož Česká republika není hraničním státem NATO, je velmi nepravděpodobné, že se možný ozbrojený konflikt přenesl na státní území, nicméně za takových podmínek by bylo využito veškerých kapacit ozbrojených sil, včetně nástrojů mobilizace. Pro plnění kolektivní obrany je však minimálním příspěvkem poskytnutí alespoň jednoho brigádního

úkolového uskupení, které je schopné samostatné činnosti. Ozbrojené síly mohou být taktéž použity k posílení složek Policie České republiky, jako tomu bylo například během zhoršené bezpečností situace ve světe v návaznosti na činnost Daesh nebo při ochraně hranic České republiky proti migraci.

V případě hybridní kampaně je činnost ozbrojených sil mnohem důležitější, než se může zdát. Jelikož je hlavním úkolem odstrašení je nutné dát najevo možnému protivníkovi, že Česká republika je schopna použít vojenské prostředky k obraně a prosazování svých zájmů a zároveň dodržet spojenecké závazky a odradit tak protivníka od útoku i na spojenecké země.

K demonstraci toho, že je Česká republika připravena bránit sebe a své spojence je možné použít právě prostředky hybridní kampaně jako propagandu či dezinformace obdobným způsobem, jakým k tomu přistupovala například armáda Ruské federace, která několikanásobně zveličovala schopnosti a velikost své armády, včetně technologií. Tento přístup Ruské federace jednoznačně pomohl k tomu, aby odstrašil členské státy NATO od poskytnutí vojenské podpory v prvních dnech války proti Ukrajině a dodnes je tento přístup jeden z hlavních důvodů, proč západní země váhají se zasíláním modernějších vojenských systémů.

Případy působení hybridních hrozeb na vojáky z povolání, případy extrémismu a dalšího jednání které podlamuje činnost ozbrojených sil České republiky či ohrožuje bezpečnost České republiky primárně řeší Vojenská policie. Působnost Vojenské policie vychází ze zákona č. 300/2013 Sb., o Vojenské policii a o změně některých zákonů (zákon o Vojenské policii).

Činnost ozbrojených sil České republiky vychází z následujících zákonů a dokumentů:

- ústavní zákon č. 110/1998 Sb., o bezpečnosti ČR,
- zákon č. 222/1999 Sb., o zajišťování obrany ČR,
- zákon č. 219/1999 Sb., o ozbrojených silách ČR,
- zákon č. 585/2004 Sb., o branné povinnosti a jejím zajišťování (branný zákon),
- Bezpečnostní strategie České republiky,
- Obranná strategie České republiky.

7 HYBRIDNÍ VÁLKA

Pojem hybridní válka byl poprvé definován Frankem Hoffmanem, který tento druh vedení konfliktu popsal jako vojenskou strategii, která využívá nejen konvenčních prostředků, ale i prostředků iregulární války, války v kyberprostoru a nevojenských nástrojů. K těmto způsobům vedení války se dají zařadit dnes často zmiňované prostředky, jež si kladou za cíl demoralizovat civilní obyvatelstvo, podkopat důvěru státního zřízení daného státu či vytvořit mezi civilním obyvatelstvem buňky, které budou spolupracovat s nepřátelskými vojsky. Právě kvůli těmto prostředkům zaměřujícím se na nevojenské cíle, s využíváním nevojenských nástrojů je hybridní válka specifická.

Mezi tyto prostředky můžeme zařadit například fake news, propagandu, dezinformace či ovlivňování voleb. Podstatným faktem je, že k používání těchto způsobů vedení hybridního konfliktu nemusí být jednotlivé státy mezi sebou ve válce. Pravidlem je, že dezinformace a propaganda jsou hojně využívané v tzv. šedé zóně mezinárodních vztahů, což je období mezi mírem a válkou mezi státy, které jsou buď ekonomickými, politickými či vojenskými soupeři.

V takovém případě dochází za použití vybraných prostředků hybridní války k oslabení daného státního útvaru nebo k nalezení slabin v jeho obranném mechanismu v případě, že by v budoucnu mohla situace eskalovat v ozbrojený konflikt. K takovému oslabení by ideálně mělo dojít takovým způsobem, aby nevyvolalo nevyžádanou reakci cíleného státního útvaru jako například vyhlášení války. Z tohoto důvodu za hybridními útoky stojí většinou jedinci, organizované skupiny nebo jako tomu bylo například během anexe Krymu, neoznačení vojáci. Tímto způsobem stát, který stojí za podobnými útoky, není přímo odpovědný. (Vojenské rozhledy, 2008)

7.1 Generace válčení

Cílem dělení válčení na několik generací je snaha o popsání měnících se způsobu vedení války. Tato teorie byla poprvé popsána v roce 1989 historiky a vojenskými důstojníky v článku Marine Corps Gazzete. V současné době žijeme na přelomu čtvrté a páté generace, která teprve nabírá svůj specifický tvar a hybridní válka je jeden z hlavních faktorů, který pomáhá tuto novou teorii formovat.

Právě kvůli řádné chybějící analýze a historické dokumentaci někteří odborníci zatím existenci páté generace popírají, nicméně současné vedení války na Ukrajině se jasně odlišuje od způsobu vedení války generace čtvrté. (Balík, 2015)

7.1.1 První generace války

Za první generaci války se označuje období od Vestfálského míru do druhé poloviny 19. století. Tato generace je specifická svou formálností a bojích ve čtvercových formacích, které se snažili maximalizovat palebnou sílu. V tomto období docházelo také docházelo k hlubší profesionalizaci armád, rozšíření hodností, jednotek či standardizace uniforem. (Lind, 2001)

7.1.2 Druhá generace války

Za přelom mezi první a druhou generací války se dá označit začátek industriální revoluce, která postupem času umožnila mnohem jednodušší zásobování armád a výrobu nových, efektivnějších zbraní. Mezi tyto efektivnější zbraně patří především opakovací pušky a dělostřelectvo, které zaznamenalo během této generace významný pokrok. Válčení bylo lineární a statické, existovali dlouhé frontové linie, tvořené převážně zákopy a pevnostmi, o které se vedli boje. Čtvercové formace byly nahrazeny dělostřelectvem, které poskytovalo dostatečnou palebnou sílu, aby pěchota mohla zaútočit na pozice protivníka. (Lind, 2001)

7.1.3 Třetí generace války

Třetí generace vedení války naprosto změnilo způsoby válčení, které doposud existoval. Za průkopníka této generace se jednoznačně považuje Heinz Guderian, který světu představil doktrínu bleskové války. Oproti předchozím generacím je tato válka nelineární a je kladen velký důraz na mobilitu, dochází zde ke snaze proražení obrany nepřítele a jeho následné obklíčení, což je naprostý opak toho, co dosud bylo v bojích zaznamenáno. Mimo jiné je také kladen důraz na samostatnost jednotek, které přebírali iniciativu a neřídili se pouze rozkazy od velení. To umožnilo rychlejší a efektivnější reakci na měnící se frontovou situaci. Třetí generace se považuje za začátek moderního válčení. (Lind, 2001)

7.1.4 Čtvrtá generace války

Tato generace přímo vychází z generace třetí. Doktrína mobility a rychlých, efektivních úderů tvoří základ strategie téměř každé armády světa. Nicméně v rámci měnící se geopolitické situace se i pojetí války muselo změnit, což dalo za vznik právě nové generaci

válčení. Čtvrtá generace, ve které se právě nacházíme my, se vyznačuje především bojem proti nestátním aktérům, jako povstaleckým skupinám či terorismu. Tyto nestátní aktéři často využívají prvky partyzánské a asymetrické války, kde cílem není vyhrávat na bojišti, ale postupem času opotřebovávat nepřátelskou armádu a tím také oslabovat důvěru obyvatel vůči vládě. Příkladem je válka v Afghánistánu nebo občanská válka v Libyi. (Lind, 2001)

7.1.5 Pátá generace války

Jak je zmíněno v úvodu této kapitoly, tak pátá generace války je teorie, která se teprve formuje, nicméně se objevuje mnoho názorů, které označují koncept hybridní války jako základní stavební kámen této generace, stejně jako tomu byla doktrína bleskové války během generace třetí. Pátá generace se vyznačuje především využíváním nevojenských nástrojů, primárně politických, ekonomických a technologických. Hlavním cílem válčení páté generace je tedy oslabení protivníka takovým způsobem, aby byla snížena jeho konkurenceschopnost či schopnost obrany v případě ozbrojeného konfliktu, a to takovým způsobem, aby to cílený stát nezaznamenal, nebo aby nemohl obvinit jiný stát z vedení takové kampaně vůči němu. (Lind, 2001)

7.2 Nástroje hybridní války

V současné době chybí jednotný názor na rozdělení nástrojů hybridní kampaně. Důvodem je poměrně malé množství zaznamenaných útoků tohoto charakteru, během kterých bylo využito rozdílných nástrojů. Pro potřeby této práce je použito poměrně jednoduché dělení těchto nástrojů, které sice nebere v potaz specifické situace, ale pro pochopení dané problematiky je více než dostačující.

V prvé řadě je třeba rozdělit tyto nástroje na vojenské a nevojenské, kdy nástroje nevojenského charakteru převyšují počet nástrojů vojenských, což opět vychází ze specifik vedení hybridní kampaně. Na druhou stranu vojenské prostředky jsou mnohem lépe dokumentovatelné, a i Česká republika se stala terčem takového útoků. (Hybrid CoE, 2023)

7.2.1 Nevojenské nástroje

Jak bylo zmíněno, hybridní kampaň využívá veškerých dostupných zdrojů a prostředků k dosažení stanovených cílů. Samotný ozbrojený konflikt či vojenská intervence je v naprosté většině případů nežádoucím řešením, které je mnohem náročnější na lidské zdroje, finance a materiál. Z tohoto důvodu hybridní kampaň klade důraz právě na nevojenské nástroje, které představují téměř nulové negativní dopady na stát či jiný subjekt,

který tyto nástroje využívá. Nevojenské nástroje se dále dělí na nástroje politické, ekonomické, informační a kybernetické.

Politické nástroje jsou čistě v gesci státních útvarů a aliancí. Jedná se o poměrně široký pojem, který popisuje vše od pouhých jednání mezi státy, skupinami osob a jinými zřízeními až po organizování protivládních protestů, státních převratů, politických vražd, infiltraci politiky a státních zřízení. Dle jiných způsobů dělení hybridních nástrojů se místo vojenských a nevojenských nástrojů tyto prostředky dělí na politické a vojenské, jelikož politické nástroje, skrz svou rozsáhlost, mohou z obecného hlediska zastřešovat veškeré nevojenské nástroje zmíněné v této kapitole.

Ekonomické nástroje, podobně jako nástroje politické, i ekonomické jsou až na výjimky čistě v rukou státních zřízení. Tyto výjimky se týkají jednotlivých podniků, které na vlastní rozhodnutí ukončí nebo jiným způsobem změní své působení v dané zemi.

Do ekonomických nástrojů se řadí sankce, embargo, obchodní omezení a další. Samotné sankce se mohou projevovat různými způsoby, jako zmražením majetku osob, či zákazu vstupu těchto osob na území dané země, nicméně nejznámějším a nejpoužívanějším způsobem zavádění sankcí jsou sankce hospodářské, které se projevují například kvótami a tarify na zboží. Embargo se týká kompletního zákazu importu či exportu zboží.

Informační nástroje jsou narozdíl od předchozích nástrojů velmi zřídka přímo napojené na stát, to ovšem neznamená, že stát, který je těmito nástroji reprezentován o jejich existenci neví, v některých případech jsou dokonce jedinci či skupiny osob za takovouto činnost státem finančně odměněni, jako je tomu v případě čínských „trollích farem“. Mezi informační nástroje se řadí právě dezinformace, psychologické operace a propaganda a jednoznačně se řadí mezi nejpoužívanější nástroje hybridní kampaně, kde primárním cílem je civilní obyvatelstvo.

Kybernetické nástroje, jak název napovídá, jsou nástroje, které jsou užívány v kyberprostoru. Rozsah zapojení států do vedení války v kyberprostoru se dá poměrně špatně určit, nicméně mnoho armád a států má složky, které slouží k takovému účelu, na druhou stranu pro jednotlivce či skupiny osob je mnohem těžší zapojit se do tohoto způsobu vedení hybridní války.

Cílem kyberútoků je narušení funkčnosti státních zřízení během míru, ale i narušení vojenských operací během války. Příkladem může být nabourání bankovnictví, zdravotnictví či energetické infrastruktury a omezit tak její provozuschopnost. Během vedení válečných operací je možné například odposlouchávat nepřátelskou komunikaci či sbírat data ze státních zdrojů, které mohou odhalit slabiny protivníka. (Řehka, 2017)

Obtížnost a nejednotnost dělení jednotlivých nástrojů vychází právě z informačních a kybernetických prostředků, které se mohou v některých případech překrývat. Takovým případem může být kyberútok na státní televizi či rádio, kde se následně přehráván záznam s dezinformací či propagandou. Dalším důvodem je také to, že mnoho lidí považuje slovo „informační“ za termín, který je spojený s informačními technologiemi a počítači, a proto mezi informačními a kybernetickými nástroji nedělají rozdíl.

7.2.2 Vojenské nástroje

I přesto, že použití vojenské síly během hybridní kampaně není žádoucí, dochází k jejímu využívání dvěma způsoby; konvenčními a nekonvenčními. Tyto nástroje popisují konvenční a nekonvenční vedení ozbrojeného konfliktu.

Konvenční nástroje zastupují klasické, konvenční válčení. Tedy takové, kdy se válčí na zemi, ve vzduchu a na vodě za použití všech konvenčních prostředků. Jak bylo zmíněno, jedná se zpravidla o poslední krok vedení hybridní kampaně, která dostatečně oslabila protivníka takovým způsobem, že jeho schopnost obrany před ozbrojeným konfliktem byla narušena.

Nekonvenční nástroje se mohou projevovat i bez ozbrojeného konfliktu. Příkladem může být terorismus, ať už v podání organizované skupiny či útoků jednotlivce. V dřívějších dobách by se dalo hovořit o partyzánské válce, jakožto nástroje hybridní války, nicméně tento fenomén se v dnešní době vyvinul do problematiky separatismu, jako tomu je na východní Ukrajině. Dále se mezi nekonvenční nástroje může řadit také sabotáž, kdy může dojít k poškození infrastruktury, komunikací a dalších zařízení, které jsou důležité pro fungování států. Samotná Česká republika se stala terčem nekonvenčních nástrojů hybridní války, kdy v roce 2014 došlo k útoku na muniční sklady ve Vrběticích. Následné vyšetřování označilo za viníka ruskou zpravodajskou službu GRU a tento akt je často označován jako státní terorismus proti České republice. Za nekonvenční vedení hybridní kampaně je považováno také používání zbraní hromadného ničení a dalších nekonvenčních zbraní a vybavení, které nespadá do konvenčního vedení ozbrojeného konfliktu.

7.3 Příklady hybridní války

Příkladů používání hybridních nástrojů pro prosazování vlastních zájmů je celá řada. Pokud však hovoříme o vedení samotné hybridní kampaně a páté generaci válčení, nelze zacházet tak hluboko do minulosti. Dva nejvýznamnější příklady vedení hybridní kampaně jsou jednoznačně válka v Iráku a válka na Ukrajině.

7.3.1 Válka v Iráku

Během války v Iráku se podařilo přesvědčit širokou veřejnost o tom, že Irák vlastní funkční zbraně hromadného ničení a zároveň podporuje teroristickou organizaci al-Qaeda. Vláda Spojených států již před začátkem invaze věděla, že tyto informace nejsou pravdivé, nicméně jimi odůvodnila svůj vpád do Iráku a svržení režimu Saddáma Husajna. Důvodů k invazi samozřejmě bylo více, nicméně dodnes je tato válka i mezi veterány kontroverzním tématem.

Zatímco se válka v Iráku dá v tomto kontextu považovat za přelom ve válčení, válka na Ukrajině je mnohem lepším příkladem, jelikož je mnohem lépe zdokumentovaná, a právě tento konflikt tvoří základy vedení hybridní kampaně. V následující kapitole budou popsány hlavní události, jakými proti Ukrajině a dalším státům byla vedena právě hybridní kampaň. (Kircher, 2015)

7.3.2 Hybridní válka na Ukrajině

Nejlepším příkladem vedení hybridní války je ruská agrese vůči Ukrajině, kde byly nástroje hybridní války užívané ještě před invazí 24. února 2022. První známky hybridní války se začaly objevovat již v roce 2003, kdy došlo ke konfrontaci mezi Ukrajinou a Ruskem na ostrově Tuzla v Kerčském průplavu, což vedlo ke značnému poškození reputace tehdejšího ukrajinského prezidenta Leonida Kučmy.

Následující rok se konali prezidentské volby, kde se do druhého kola těchto voleb dostal Viktor Juščenko a Viktor Janukovyč. Výsledek druhého kola voleb byl jasně ovlivněný ve prospěch proruského kandidáta Janukovyče a tudíž se za pomoci zahraničních pozorovatelů muselo konat třetí kolo, které již vyhrál Juščenko. Výsledkem tohoto ovlivňování voleb byla Oranžová revoluce a také další rozštěpení společnosti a narušení již tak křehké stability.

Štěpení společnosti následně pomocí propagandy, dezinformací a fake news trvalo až do roku 2014, kdy došlo za vlády Viktora Janukovyče k protestům zvaným Euromajdan, které vyústili v anexi Krymu neoznačenými vojáky Ruské federace a otevřenými nepřátelskými akcemi mezi provládními složkami a proruskými separatisty.

Po roce 2014 se působení nástrojů hybridní války Ruské federace rozšířilo po celém světě za účelem vytvořit, převážně v západních zemích, základnu lidí, kteří by podporovali nově vzniklé separatistické státní útvary a ruskou mezinárodní politiku v opozici k Evropské unii a Severoatlantické alianci. S ohledem na současnou situaci se dá říct, že Ruská federace si těmito podvratnými elementy snažila odůvodnit svou agresi vůči Ukrajinu a vytvořit si

ideální podmínky pro invazi, která mimo jiné začala rozsáhlými kyberútoky na ukrajinskou infrastrukturu v předvečer začátku války.

V rámci České republiky se dá říct, že snahy Ruské federace byly do jisté míry úspěšné. Primárním nástrojem užívaným vůči českému obyvatelstvu byli dezinformace a fake news, zprostředkované pomocí dezinformačních webů, které nabízeli nemainstreamový pohled na dění ve světě, což přilákalo značné množství lidí. Těmto dezinformačním webům také pomohla pandemie onemocnění Covid-19, kdy poměrně malá informovanost obyvatelstva ohledně tohoto tématu vedla spíše k negativnímu vnímání jednotlivých opatření, čehož právě tyto weby využili a i osoby, které nemuseli nutně souhlasit s politickou agendou těchto webů byli postupně vystavovány dezinformacím různého typu.

Následky působení daných nástrojů hybridní války vůči České republice byly patrné již před samotnou invazí Ruské federace na Ukrajinu, kdy došlo například k nezákonnému vytvoření konzulátu Doněcké lidové republiky či zapojení se několika občanů České republiky do bojů na straně proruských separatistů.

Po začátku války jsou však následky působení Ruské federace mnohem zřetelnější. Je možné pozorovat osoby používající rétoriku dezinformačních webů pro ospravedlnění násilí na ukrajinském obyvatelstvu, objevili se názory proti posílání jakékoliv pomoci Ukrajině či dokonce názory typu o vystoupení ze Severoatlantické aliance či Evropské unie a prohloubení vztahů s Ruskou federací. Zde je nutné si položit otázku, zda v takových případech zaručovat svobodu slova i přes fakt, že tyto názor představují hrozbu pro samotný systém, který jim tuto svobodu nabízí. (Kříž, 2016)

8 DEZINFORMACE

Dezinformace, jak je zmíněno v pojmovém aparátu, hovoří o záměrném šíření nepravdivých informací. Dezinformace si kladou za cíl ovlivnit názory lidí, kteří přijdou do kontaktu s takovou informací.

V prvé řadě je nutné si uvědomit, že dezinformace nemají pouze charakter nástroje hybridní války či jiného podvratného aktu mezi státními a nestátními protějšky, ale s dezinformacemi se můžeme setkat i v civilním životě, ve vnitřní politice, ale i na osobní úrovni. (Ministerstvo vnitra, 2023)

8.1 Druhy dezinformací

Dezinformace se dají rozdělit na několik druhů, dle jejich povahy, původu a cíle, kterého se snaží dosáhnout. Žádné oficiální dělení dezinformací nicméně neexistuje, vzhledem k tomu, o jak široký pojem se jedná. Tudíž pro potřeby této práce bylo vybráno sedm druhů, se kterými je nejběžnější se setkat. Mnoho zdrojů řadí také editorskou chybu či propagandu do dezinformací, ale fakticky se jedná o úplné jiné věci a editorské chyby by se spíše měli řadit do kategorie misinformací.

- Vymyšlený obsah
- Manipulovaný obsah
- Podvodný obsah
- Zavádějící obsah
- Chybný kontext
- Satira a parodie
- Sponzorovaný obsah
- Syntetický nebo umělý obsah (UNHCR, 2023)

Mimo těchto sedm hlavních kategorií, je možné dezinformace dále dělit na aktivní a pasivní. Kdy dezinformací aktivní se rozumí takové informace, které záměrně vytvářeny nebo pozměňovány tak, aby měli škodlivý efekt. Na druhou stranu dezinformace pasivní popisuje proces, kdy se se samotnou informací, ať už pravdivou či ne, nakládá takovým způsobem, že se nemusí dostat k cílové skupině lidí nebo se k této skupině může dostat později, jedná

se tedy o různé zatajování, likvidaci či záměrně opožďování předání této informace, což může opět vést k ohrožení bezpečnosti České republiky.

8.1.1 Vymyšlený obsah

Vymyšlený obsah jednoduše popisuje takovou zprávu či informaci, která je kompletně vymyšlená, nezakládá si na žádné reálně skutečnosti či faktu. V dnešní době se s takovou formou dezinformace setkáváme stále méně a méně. Důvodem je volný přístup k informacím a většina osob je schopna rozeznat takovou informaci od ostatních, pravdivých informací.

8.1.2 Manipulovaný obsah

Manipulovaný obsah je nejčastější formou dezinformace, se kterou je možné se setkat. Jedná se informaci, která vychází z jiné pravdivé informace, ale byla do určité míry upravena tak, aby si zachovala určitou míru věrohodnosti. Může se jednat o upravený text, fotky, či dokonce videa. Příkladem může být video nově zvoleného prezidenta Petra Pavla, ve kterém autor videa zaměnil zvukovou stopu a prezident Petr Pavel tak místo vyjádření podpory Ukrajině otevřeně vyzýval k zapojení České republiky do války.

8.1.3 Podvodný obsah

Podvodný obsah hovoří v kontextu dezinformací o takové informaci, který předává lživý obsah, ale vydává se důvěryhodnou organizaci, službu či jiné zřízení a tím si získává věrohodnost. Tento druh dezinformací je často využíván internetovými podvodníky, kteří se mohou například vydávat za mobilní operátory a ke zprávě, která hrozí čtenáři zvýšením cen mobilního tarifu, přiloží také phishingový odkaz.

8.1.4 Zavádějící obsah

Zavádějící obsah je druh dezinformace, který prezentuje neověřené zdroje nebo zdroje vytržené z kontextu jako fakt. Tyto zdroje pochází převážně z dezinformačních webů a dají se lehce vyvrátit.

8.1.5 Chybný kontext

Chybný kontext popisuje stav, kdy nadpis článku přímo nereflektuje obsah článku. Často se jedná o články s populistickým nebo clickbaitovým nadpisem. Samotný nadpis však nemusí nutně přenášet škodlivou informaci, která se však nachází v obsahu samotném.

8.1.6 Satira a parodie

Vymyšlené či manipulované informace, které mají za cíl pobavit, nikoliv škodit. Někdy je tato snaha pobavit čtenáře jasná, příkladem je satirické zpravodajství webu AZ247. V některých případech však pro čtenáře může být složitější rozeznat satiru či parodickou povahu článku a může ho tak považovat za pravdivý.

8.1.7 Sponzorovaný obsah

Sponzorovaný obsah obecně opět nemusí být nutně dezinformace, takový obsah může předkládat i pravdivé informace. Nicméně je zde nutné zmínit, že takový obsah nejspíše nebude sdílet nezávislý obsah a často sdílí malinformace. V kontextu dezinformací a hybridní kampaně je vhodné zmínit dezinformační weby, které jsou buď sponzorovány čtenáři nebo jsou přímo či nepřímo napojeny na státní či nestátní aktéry, kteří představují hrozbu pro bezpečnost.

8.1.8 Syntetický či umělý obsah

Jedná se o obsah, který je čistě tvořen umělou inteligencí, která díky strojovému učení v současné době dokáže vyprodukovat takový obsah, který je téměř nerozeznatelný od reality. Takový obsah může znázorňovat specifické osoby při různých aktivitách, včetně rozhovorů s nimi, kde umělá inteligence dokáže napodobit i jejich hlas. Jedná se tedy o vymyšlený či manipulovaný obsah, který však za poměrně krátkou dobu dokázala vytvořit umělá inteligence. V budoucnosti se počítá s tím, že takový obsah bude představovat největší hrozbu.

8.2 Historie dezinformací

Pojem *dezinformace* byl poprvé zaznamenán v roce 1949 a pravděpodobně vychází z ruského slova дезинформация [dezinformacija]. I přesto, že pojem dezinformace je relativně nový, samotný akt dezinformování a šíření nepravdivých informací je starý jako lidstvo samo. Už od starověku či středověku je zdokumentováno mnoho aktů intrik, ovlivňování politiků a obyvatel daných území, atentátů a dalších činů, které by dle dnešního chápaní alespoň částečně spadali pod označení hybridních nástrojů. (Ministerstvo vnitra, 2023)

Za největší rozvoj vedení dezinformačního a propagandistického boje se dá označit období druhé světové války. Důležitost a působení propagandy v tomto období jistě není třeba představovat, jelikož jí použili všechny strany jak na válečné, tak i na domácí frontě, ať už

shazováním letáků, které vyzývali druhou stranu ke kapitulaci nebo k motivování vlastního obyvatelstva k práci v továrnách, obraně a dalších oblastech.

Nejúspěšnější dezinformační kampaň druhé světové války je bezpochyby vylodění v Normandii, respektive tedy to, co vylodění předcházelo a pomocí čeho se podařilo, aby se vojska nacistického Německa zaměřovali na obranu oblasti Pas-de-Calais ve Francii a nesoustředili tak své síly v Normandii. Operace Fortitude, jak spojenecká vojska označovali tuto klamnou operaci, používala mnoho prostředků, které zmátli německá vojska, včetně známých nafukovacích vozidel, která měla zmást snahy o leteckou špionáž, až po prozrazování falešných plánů invaze skrz nechráněnou rádiovou komunikaci, po úmyslné přeřeky politiků a generálů při rozhovorech a využívání dvojitých agentů.

Používání dezinformací k prosazování vlastních zájmů se však nestahovalo pouze na válečné období, ale trvalo i po něm, vlastně se dá říci, že je to stále trvající jev. Na území tehdejší Československé socialistické republiky proběhla roku 1964 poměrně velká dezinformační kampaň s názvem Operace Neptun. Kdy na dně Černého jezera na Šumavě Státní bezpečnost ukryla bedny s údajnými nacistickými dokumenty. Tyto dokumenty měli zdiskreditovat a poškodit mnoho politiků, zvláště v Západním Německu a Rakousku, jelikož z nich vyplývalo, že tyto osoby spolupracovali se složkami Třetí říše. Operace působila velmi věrohodně a vedla k rezignaci několika politiků, ale také i k několika sebevraždám.

S pokrokem informačního věku se působení dezinformací začalo stupňovat. Dezinformace už nejsou záležitostí pouze státních aktérů, kteří mezi sebou soupeří, ale za šíření a tvorbu dezinformací jsou v dnešní době odpovědní nestátní aktéři, organizace, organizované skupiny či jedinci. Právě fakt, že došlo k tak velké decentralizaci v poli dezinformací je největším problémem pro vedení úspěšného boje proti těmto informacím.

Mezi nové hrozby vzhledem k šíření dezinformací tak patří volnost vytváření vlastních webových stránek, kde mnoho domén nabízí i možnost vytvoření vlastních blogů bez jakýchkoliv poplatků a možnost tvorby falešných profilů na sociálních sítích. Toto umožňuje osobám téměř neomezené šíření dezinformací bez jakéhokoliv postihu.

Co se týče nových hrozeb ohledně tvorby dezinformací, do popředí se na přelomu roku 2022 a 2023 dostala umělá inteligence, která dokáže perfektně napodobit hlas osob. Toto, v kombinaci s technologií, která je schopna tvořit tzv. deep fake, což umožňuje tvorbu videí s lidmi pouze na základě jejich fotky, představuje velké riziko, jelikož může dojít k tvorbě takového materiálu, který je naprosto nerozeznatelný od reality.

Umělá inteligence obecně zaznamenává v posledních letech významné pokroky, například dokáže generovat obrázky čistě na základě klíčových slov, tvoří rozsáhlé texty a také dokáže

vést plnohodnotnou konverzaci s lidmi. Veškeré tyto prostředky je možné využít ke tvorbě či šíření dezinformací, je také možné, že umělá inteligence dokáže dezinformace generovat a sdílet sama. (Řehka, 2017)

8.3 Dezinformační weby

Dezinformační weby získali na popularitě během pandemie Covid-19 a získali si také velké množství podporovatelů během invaze Ruské federace na Ukrajinu. Jedná se o online médium, které šíří lživé, neúplné nebo zavádějící informace. Jelikož dezinformační weby plní subversivní činnost, bylo na popud Vojenského zpravodajství nemalé množství těchto webů v České republice zablokováno.

V současné době je většina těchto webů dostupných nebo ukončilo svou aktivitu po jejich zákazu. Za dostupnost těchto webů, které otevřeně šíří dezinformace, které mají za cíl poškodit stabilitu a bezpečnost České republiky může do jisté míry legislativa, která nijak nedefinuje aktivitu těchto webů. I přes to však existuje několik seznamů všech dezinformačních webů, jeden takový vytvořilo i ministerstvo vnitra, nicméně tento seznam není dostupný pro veřejnost, a proto je nutno ověřovat, zda se čtenář nachází na dezinformačním webu na sekundárních zdrojích.

8.4 Vliv dezinformací

Vliv dezinformací na civilní obyvatelstvo je téměř nemožné dokázat. Jedinou studií, která se tímto tématem zabývala s měřitelnými výsledky je studie o amerických prezidentských volbách v roce 2016, kdy se mezi sebou utkali Donald Trump a Hillary Clintonová. Tato studie přinesla tyto výsledky:

- Celkem 14 % všech občanů Spojených států amerických používá sociální sítě jako hlavní zdroj informací.
- Až na ojedinělé případy, každý, kdo měl přístup k internetu přišel do kontaktu alespoň s jednou lživou či zavádějící informací.
- Více než polovina osob, které s takovou informací přišli do kontaktu, této informaci věřila.
- Lidé spíše přijímají takovou dezinformaci, která je v souladu s jejich názory.

Studie také přinesla mnoho dalších poznatků, jako, že dezinformace ve prospěch Donalda Trumpa převyšovali dezinformace ve prospěch Hillary Clintonové tři ku jedné, nicméně tyto informace nejsou pro tuto diplomovou práci podstatné.

Tato studie poukazuje na fakt, že dezinformace jsou v dnešní době velmi rozšířené, jelikož každá osoba s takovou informací přišla do styku. Tuto skutečnost ještě více zhoršuje fakt, že poměrně velké množství osob čerpá informace ze sociálních sítí, bohužel počet osob, které čerpají obsah z dezinformačních webů a dalších médií není známý.

Poznatek, že lidé spíše přijímají takovou informaci, která podporuje jejich názory vysvětluje, proč mnoho osob konzumuje dezinformační média. Naprostá většina dezinformací v České republice se zaměřuje právě na Euroskepticismus či samotný odchod z Evropské unie a také samozřejmě vystoupení ze Severoatlantické aliance. Tyto názory jdou v naprosté většině případu ruku v ruce a osoby s těmito názory se tak jednoduše dostanou právě na tyto dezinformační média, což samo o sobě není problém. Problém nastává, když tyto osoby začnou obsah těchto médií konzumovat, protože sdílí s autory těchto dezinformací podobné názory, tudíž je mnohem jednodušší tyto osoby přesvědčit o pravdivosti těchto lživých a zavádějících informací.

V roce 2019 byl proveden výzkum ohledně dezinformací i v českém prostředí, kterého se však zúčastnilo velmi malé množství osob a z celkem 1015 respondentů, kteří se tohoto výzkumu účastnili se ukázalo, že téměř 20 % dotázaných osob považuje bulvární média za dezinformační a víceméně jediné, co tento výzkum přinesl je, že česká společnost nemá o této problematice přehled i přes to, že se s ní setkává každý den. Zároveň, 61% dotázaných mělo problém rozeznat, zda se nachází na dezinformačním webu.

9 DÍLČÍ ZÁVĚR

V teoretické části došlo kromě vypsání pojmů spjatých s tématem a současné legislativy k popsání institucí a strategických dokumentů, které se danou problematikou zabývají. V kapitole o institucích řešící problematiku hybridní války jsou taktéž zmíněny některé dokumenty a výroční zprávy, které vyzdvihují současné působení hybridních nástrojů vůči České republice, konkrétně se jedná o dezinformační kampaně během voleb či fungování dezinformačních webů, které se snaží o rozštěpení společnosti a své argumenty si zakládají na pandemii onemocnění Covid-19 a válce na Ukrajině.

V další částí byla popsán samotný koncept hybridní války, jejíž definice je poměrně komplikovaná, jelikož se jedná o poměrně nový koncept, jak je vysvětleno v kapitole generací válčení, a proto existuje mnoho definic, které však nepopisují plnou podstatu samotné hybridní kampaně. Na tuto kapitolu pak dále navazuje kapitola o dezinformacích samotných, kde je tento fenomén podrobně rozebrán, jednotlivé druhy dezinformací jsou zde rozděleny do několika kategorií, které jsou následně popsané.

Zároveň je zde vysvětlena problematika dezinformačních webů a také jsou zde uvedeny dva výzkumy, které byly ohledně dezinformací provedeny, jeden ve Spojených státech amerických a druhý v České republice, kdy výsledek českého výzkumu přinesl znepokojivé závěry, které hovoří o tom, že 61 % dotázaných osob nerozezná dezinformační weby a 20 % osob považuje bulvární média za dezinformace.

II. PRAKTICKÁ ČÁST

10 ROZDĚLENÍ PRAKTICKÉ ČÁSTI

Praktická část se zabývá dvěma tématy. Jedním z nich je obrana před nástroji hybridní kampaně se zaměřením na dezinformace a druhá část se zabývá využitím těchto nástrojů k prosazování zájmů České republiky a Severoatlantické aliance.

Pro výzkum obrany před nástroji hybridní kampaně bude použitá bodová analýza pro ohodnocení nebezpečnosti jednotlivých nástrojů a zároveň zde bude použita analýza SWOT, jejímž cílem bude zanalyzovat současný stav schopnosti bránit se před těmito hrozbami.

Ve druhé části, zabývající se prosazováním zájmů, nebude provedena analýza žádná, z důvodu rozsáhlosti tohoto tématu. Nicméně zde dojde k sepsání všech dostupných prostředků, které by mohli sloužit k danému účelu. Následně zde dojde k vypsání hlavních konkurentů České republiky a Severoatlantické aliance a zvolen vhodný způsob užití nástrojů hybridní kampaně k odstrašení, oslabení nebo přímému útoku na tyto aktéry globální politiky.

11 BODOVÁ ANALÝZA

Bodová analýza je poměrně jednoduchou metodou, díky které dojde k odhalení největšího rizika pomocí vzorce mR = P x N x H. Vzorec tak bere v úvahu pravděpodobnost vzniku daného rizika (P), závažnosti jeho následků (N) a také bere v potaz názor hodnotitelů na dané riziko (H). Hodnotitelem je v tomto případě zaměstnanec Vojenského zpravodajství, který si nepřál, aby bylo zveřejněno jeho jméno.

Celkově budou v této části provedeny dvě bodové analýzy. První bodová analýza se týká jednotlivých druhů hybridních nástrojů, kde dojde k určení takového nástroje, který představuje největší riziko pro bezpečnost České republiky a druhá bodová analýza bude hodnotit jednotlivé druhy dezinformací, které pro naši bezpečnost taktéž představují riziko.

11.1 Bodová analýza hybridních nástrojů

V této části budou vyhodnoceny jednotlivé nástroje vedení hybridní kampaně, které vychází z teoretické části této diplomové práce. Je důležité zmínit, že při hodnocení se v potaz bralo členství v Evropské unii, Severoatlantické alianci, Visegrádské skupině a dalších společenství, do kterých Česká republika patří, a proto některé nástroje, jako například ekonomické, představují mnohem menší riziko pro naši bezpečnost než pro státy, které nejsou členy žádného podobného společenství. Z toho důvodu se také analýza týká pouze situace v České republice a výsledky není možné aplikovat na jiné státy.

11.1.1 Politické nástroje

Vzhledem ke stabilitě demokratického zřízení v České republice je pravděpodobnost využívání politických nástrojů k oslabení či poškození bezpečnosti České republiky velmi malé, jelikož by takový útok neměl žádaný efekt. Důležité je zmínit, že v případě úspěšné vedení hybridní kampaně je možné, že dojde k narušení stability a bezpečnosti České republiky a v takovém případě by bylo využití politických nástrojů mnohem efektivnější.

mR = 2 x 1 x 2 = 4

11.1.2 Ekonomické nástroje

Jak je zmíněno v úvodu této kapitoly, vzhledem ke členství v několika společenstvích, není Česká republika významným způsobem náchylná vůči ekonomickým nástrojům hybridní kampaně. Nicméně i přesto, že primární riziko je velmi malé, dopady sekundárního rizika

plynoucího z ekonomických nástrojů je možné v dnešní době zaznamenat například v podobě zdražování energií v souvislosti s válkou na Ukrajině.

mR = 2 x 2 x 2 = 8

11.1.3 Informační nástroje

Informační nástroje jednoznačně představují největší riziko pro bezpečnost České republiky. Hlavním důvodem je, jak bylo zmíněno v teoretické části, že využívat informačních nástrojů k prosazování zájmů státu či skupiny může každý, kdo má přístup k prostředkům sloužícím k šíření těchto nástrojů. Z tohoto důvodu byla zvolena nejvyšší možná pravděpodobnost. Závažnost následků byla stanovena na hodnotu tři, jelikož informační nástroje působí na značný počet osob najednou, nicméně většina těchto osob není těmito nástroji ovlivněna do takové míry, aby tím byla ohrožena bezpečnost České republiky.

mR = 5 x 3 x 4 = 60

11.1.4 Kybernetické nástroje

Kybernetické nástroje se společně s informačními nástroji drží v popředí nástrojů, které představují největší hrozbu pro bezpečnost České republiky. Oproti informačním nástrojům zde byla zvolena pravděpodobnost tři, jelikož k používání kybernetických prostředků k vedení hybridní kampaně již vyžaduje určitou specializaci a zároveň existují alespoň základní prvky obrany proti útokům v kyberprostoru, které takový útok mohou pasivně zastavit.

Na druhou stranu jsou možné následky pro bezpečnost České republiky mnohem vyšší, příkladem takového útoku může být narušení energetické infrastruktury na Ukrajině pár hodin před vpádem ruské armády. Takový útok, který dokáže efektivně vyřadit elektřinu na několik hodin v dnešní době představuje velké riziko. V České republice jsou však známější útoky na zdravotnické zařízení či bankovní služby.

mR = 3 x 4 x 4 = 48

11.1.5 Konvenční nástroje

Vznik ozbrojeného konfliktu a vedení konvenční války je, jak bylo několikrát zmíněno, nežádoucí a zároveň velmi nepravděpodobné i vzhledem k současnému dění v Evropě. Kvůli situaci na Ukrajině byla vedena diskuse, jak velká má pravděpodobnost vzniku takového konfliktu být. V rámci Severoatlantické aliance by hodnota pravděpodobnosti byla dva, nicméně v rámci České republiky samotné, byla zvolena hodnota jedna. Hlavním důvodem byl i fakt, že v případě, že by došlo k ozbrojenému konfliktu, do kterého by byla

Severoatlantická aliance zapojena, je velmi nepravděpodobné, že by se válčilo na území České republiky a došlo by k významnému narušení bezpečností České republiky pomocí konvenčních prostředků. Následky vedení konvenčního ozbrojeného konfliktu by však měli velmi velké následky, a to i v případě, že by nedošlo k bojům na samotném území České republiky.

mR = 1 x 5 x 2 = 10

11.1.6 Nekonvenční nástroje

Nekonvenční nástroje jsou v kontextu vedení hybridní kampani poměrně častým jevem, nicméně samotná Česká republika v současné době není atraktivním cílem pro takové útoky, ale i přesto se taková situace nedá plně vyloučit, čemuž nasvědčují události ve Vrběticích, takový útok však nebyl veden za účelem přímo poškodit Českou republiku. Hodnota pravděpodobnosti tak byla stanovena na dva, jelikož, jak bylo zmíněno, Česká republika není významným cílem, ale je stále členskou zemí několika světových společenství, což v tomto kontextu zvyšuje riziko útoku. Předpokládané následky použití nekonvenčních nástrojů by neměli být tak závažné, jako následky použití konvenčních nástrojů. Toto hodnocení nebere v potaz použití zbraní hromadného ničení.

mR = 2 x 3 x 2 = 12

11.2 Bodová analýza dezinformací

První analýza potvrdila, že informační nástroje představují největší hrozbu pro bezpečnost České republiky. V rámci informačních nástrojů jsou dezinformace hlavním prostředkem, který je používán k vedení tohoto způsobu hybridní kampaně. V této podkapitole jsou stejným způsobem vyhodnoceny jednotlivé druhy dezinformací na základě rizika, které představují pro bezpečnost České republiky. V této časti nebudou zahrnuty dezinformace satirického typu, jelikož, i přesto, že se jedná o dezinformaci, nemají za cíl poškodit bezpečnost a nejsou využívány pro vedení hybridní kampaně.

11.2.1 Vymyšlený obsah

Vymyšlený obsah je jednoznačně druh dezinformací, který je ve vedení hybridní kampaně nejpoužívanější, z tohoto důvodu je hodnota pravděpodobnosti pět. V dřívějších dobách měl tento typ dezinformací mnohem závažnější následky, nicméně v současné době tomu tak není. Hlavním důvodem je mnohem jednodušší přístup, k mnohem většímu počtu informací. Zároveň takový obsah je velmi často napsán neprofesionálně, což je důsledkem toho, že

dezinformace může opravdu může tvořit úplně každý, z tohoto důvodu byly následky ohodnoceny váhou dva. I přes to, že však nebezpečnost je velmi malá, pro instituce, které se touto problematikou zabývají se stále jedná o závažnou problematiku, protože množství těchto dezinformací se od začátku pandemie onemocnění Covid-19 několikanásobně zvětšilo, a proto je názor hodnotitelů na úrovni čtyři.

mR = 5 x 2 x 4 = 40

11.2.2 Manipulovaný obsah

Dezinformace tohoto typu jsou oproti vymyšlenému obsahu mnohem nebezpečnější. Důvodem je, jak je zmíněno v teoretické části této diplomové práce fakt, že si částečně zakládají na pravdě, a proto je pro mnoho lidí špatné tento obsah označit za dezinformaci, pokud o dané problematice nemají přehled. Takový obsah není používaný tak často jako vymyšlený obsah, ale stále se jedná o jeden z nejčastěji používaných forem dezinformací, a proto byla pravděpodobnost opět ohodnocena nejvyšší hodnotou. Následky jsou, oproti vymyšlenému obsahu, mnohem větší, právě z toho důvodu, že dokážou ovlivnit mnohem více lidí, proto byla zvolena hodnota čtyři.

mR = 5 x 4 x 4 = 80

11.2.3 Podvodný obsah

Podvodný obsah se velmi zřídka používá k vedení hybridní kampaně. Taková forma dezinformace se primárně snaží o získání informací či přístup k účtům různých institucí, které se podílí na obraně a zajišťování bezpečnosti České republiky. Stejně jako u vymyšleného obsahu, i u podvodného obsahu byly následky v minulosti mnohem vyšší, protože takové útoky byly mnohem efektivnější. V dnešní době je tento obsah používán spíše jedinci proti civilnímu obyvatelstvu. Jelikož se tento způsob dezinformací k vedení hybridní kampaně již tolik nepoužívá, byla zvolena hodnota pravděpodobnosti dva, nicméně následky takového útoku mohou být stále vysoké, a proto hodnota následků byla stanovena hodnotou tři.

mR = 2 x 3 x 2 = 12

11.2.4 Zavádějící obsah

I přes to, že se zavádějící obsah dá lehce vyvrátit, stále představují velké riziko. Důvodem je, že mnoho lidí nekontroluje zdroje, ze kterých tento obsah čerpá. Těmito zdroji jsou často dezinformační weby, které už od začátku pandemie Covid-19 získali velkou podporu jakožto forma alternativních médií. Tento obsah je méně častý, protože provoz webové stránky

vyžaduje finance a alespoň základní znalosti práce s takovou webovou stránkou, nicméně existují i domény, které poskytují založení webových stránek zdarma, či je možné vytvořit takovou stránku na sociálních sítích, z toho důvodu byla zvolena hodnota pravděpodobnosti tři. Dezinformační weby a sítě sice byly se začátkem války na Ukrajině zakázány, ale v dnešní době je tento zákaz poměrně lehké obejít pomocí služeb VPN, kterou dnes má zabudovanou i mnoho internetových prohlížečů a uživatelé jí tak mohou jedním stisknutím používat zdarma a opět získat k těmto webům přístup, proto je hodnota názoru hodnotitelů čtyři.

mR = 3 x 4 x 4 = 48

11.2.5 Chybný kontext

Chybný kontext v naprosté většině případů není používán k vedení hybridní kampaně, z tohoto důvodu se vyskytuje velmi málo a hodnota pravděpodobnosti tak byla zvolena dva. Riziko plynoucí z tohoto typu dezinformací je taktéž malé, pokud si čtenář tohoto obsahu přečte jak nadpis, tak samotný obsah dané zprávy a zjistí, že spolu nesouvisí. Mnohem škodlivější je chybný kontext, kde nadpis je pravdivý, ale obsah lživý než naopak, protože pravdivostí nadpisu článek nabírá mnohem větší důvěryhodnost.

mR = 2 x 1 x 1 = 2

11.2.6 Sponzorovaný obsah

Hodnocení sponzorovaného obsahu bylo poměrně komplikovanější, jelikož je možné vznést argument, že každý obsah je v dnešní době sponzorovaný. V takovém případě by bylo hodnocení pravděpodobnosti pět. Nakonec bylo rozhodnuto, že za sponzorovaný obsah v kontextu vedení hybridní války bude brán pouze takový obsah, který je sponzorován státy, jež představují nebo mohou představovat riziko pro bezpečnost České republiky. Zároveň byli při hodnocení bráni v potaz i jedinci či skupiny osob a organizace, které ohrožují nebo by mohli ohrožovat bezpečnostní zájmy České republiky. Tyto činitelé jsou definováni ve strategických dokumentech České republiky. Po tomto kroku se pravděpodobnost zmenšila na hodnotu dva.

Kvůli jisté transparentnosti, která však není nijak vyžadována, existence sponzorovaného obsahu nenese tak velké následky, jelikož spojitost s těmito negativními činiteli vůči bezpečnosti České republiky je každému čtenáři tohoto obsahu jasná. Z tohoto důvodu se těmto formám dezinformací vystavují lidé z větší části dobrovolně, protože s těmito činiteli sympatizují. Riziko následků spočívá v tom, že právě tito jedinci jsou dále radikalizování,

nicméně se jedná dle hodnotitelů o opravdu malé množství osob, a proto byla zvolena výše následků a hodnotitelů dva.

mR = 2 x 2 x 2 = 8

11.2.7 Syntetický nebo umělý obsah

Tento typ dezinformací bylo taktéž složité hodnotit, protože je zde nutné zmínit fakt, že se jedná o poměrně nový druh obsahu. Uměle tvořený obsah je bezpochyby na vzestupu a umělá inteligence již dnes dokáže psát i odborné texty, za zmínku stojí případ studenta, který dokázal obhájit práci, která byla z velké části napsaná právě umělou inteligencí. Použití tohoto obsahu v rámci vedení hybridní kampaně zatím nebylo prokázáno, ale je předpokládáno, že v rámci několika let dojde k velkému rozsahu tohoto obsahu. Hodnocení pravděpodobnosti bylo ohodnoceno číslem tři, nicméně tato hodnoto nereflektuje současnou dobu, ale postupný nárůst dezinformací tohoto typu v budoucnosti. Dle hodnotitelů je jasné, že tato forma obsahu předběhne počet dezinformací jiných typů a za několik let se tak hodnocení pravděpodobnosti vyšplhá na hodnotu pět.

Následky této formy dezinformací jsou taktéž jedny z nejvážnějších, a to kvůli svému počtu, ale i kvůli tomu, že umělá inteligence dokáže tvořit dezinformace jiných typů a cílit tak na všechny skupiny lidí. Z tohoto důvodu jsou možné následky a zároveň názor hodnotitelů na hodnotě pět.

mR = 3 x 5 x 5 = 75

11.3 Výsledky bodové analýzy

Bodová analýza hybridních nástrojů ukázala, že největší hrozbou pro bezpečnost České republiky jsou informační nástroje hybridní kampaně. Na druhém místě s podobným hodnocením jsou kybernetické nástroje. Ostatní prostředky hybridní války nemají oproti těmto prostředkům významné hodnoty. Pořadí dle rizika pro bezpečnost České republiky je následující:

1. Informační nástroje.
2. Kybernetické nástroje.
3. Nekonvenční nástroje.
4. Konvenční nástroje.
5. Ekonomické nástroje.
6. Politické nástroje.

Bodová analýza dezinformací vyhodnotila mezi sebou jednotlivé formy dezinformací. Součástí analýzy nejsou dezinformace, které neslouží k vedení hybridní kampaně, jedná se o satiru, parodii, editorské chyby a další. Analýza odhalila, že v současné době představuje největší hrozbu manipulovaný obsah. Na druhém místě je o pouhých pět bodů syntetický nebo umělý obsah, jehož hodnocení je velmi problematické, protože k vedení hybridní kampaně v současné době neslouží a hodnocení tak vychází z předpokládaného vývoje v poměrně krátké budoucnosti. Dle názoru zaměstnance Vojenského zpravodajství je jisté, že do pěti let bude syntetický a umělý obsah na prvním místě a ostatní druhy dezinformací oproti tomuto obsahu upadnou. Celkové pořadí výsledků analýzy je následující:

1. Manipulovaný obsah.
2. Syntetický nebo umělý obsah.
3. Zavádějící obsah.
4. Vymyšlený obsah.
5. Podvodný obsah.
6. Sponzorovaný obsah.
7. Chybný obsah.

12 ANALÝZA SWOT

Analýza SWOT je druhou analýzou této diplomové práce. Analýza si klade za cíl odhalit schopnost současného systému bránit se před dezinformacemi jakožto nástrojem vedení hybridní kampaně. Jelikož tato analýza navazuje na výsledky Auditu národní bezpečnosti, kde výsledky označili náš systém za neschopný čelit hybridním hrozbám, obdobný výsledek se očekává i v této analýze. Stejně jako u bodové analýzy, i zde byl výběr a hodnocení jednotlivých bodů uskutečněn za pomoci zaměstnance Vojenského zpravodajství.

Audit národní bezpečnosti se však, alespoň ve své publikované formě, nezabýval přímým řešením problémů a nedostatků, které byly během analýzy odhaleny. Výsledky této analýzy SWOT tak budou využity pro návrh opatření pro ochranu před dezinformacemi v kontextu vedení hybridní kampaně.

Analýza SWOT je základní analýzou pro vyhodnocení vybraného systému. Název SWOT je odvozen od anglických slov *strengths – weaknesses – opportunities – threats*, v češtině tedy *silné stránky – slabé stránky – příležitosti – hrozby*. Analýza mezi sebou srovnává tyto čtyři kategorie a výsledkem je jedna ze čtyř kombinací, dle které se zvolí další postup. SWOT analýza má za cíl odhalit, zda vybraný systém je schopný odolávat rizikům či je nutné navrhnout opatření pro zlepšení daného systému.

12.1 Silné stránky

Do silných stránek bylo zařazeno pět bodů, o které se v zajišťování bezpečnosti v kontextu hybridní kampaně Česká republika opírá. Prvním bodem je stabilita, který je bezpochyby nejdůležitějším faktorem v obraně proti útokům, který mají podvratný charakter.

Druhým a třetím bodem silných stránek je členství v Evropské unii a Severoatlantické alianci. Samozřejmě v současné bezpečnostní situaci v Evropě může být vznešen argument, že se může jednat spíše o hrozbu než silnou stránku, nicméně pozitivní stránky našeho členství v Evropské unii a Severoatlantické alianci jednoznačně převyšují veškeré negativní dopady, které by naše členství mohlo přinést v kontextu hybridního válčení. Zároveň je zde nutné zdůraznit, že jak Evropská unie, tak Severoatlantická aliance přispívá k prohlubování stability a bezpečnosti v České republice.

Čtvrtým, významným bodem, je volný přístup k informacím, což se v kontextu dezinformací může opět jevit jako dvojsečný meč, nicméně množství webů a zdrojů, které nesdílí dezinformační obsah převažuje nad obsahem dezinformačním. Zároveň je důležité zmínit, že dezinformační obsah je ve vyhledávácích internetových nástrojích často odsunut do

pozadí ve prospěch pravdivého a ověřeného obsahu. Posledním bodem silných stránek je samotný fakt, že Česká republika nepředstavuje důležitý cíl pro provedení jakéhokoliv hybridního útoku, tato skutečnost však byla ohodnocena poměrně malou hodnotou, jelikož se bezpečnost České republiky nemůže spoléhat na to, že zrovna napadena nebude.

12.2 Slabé stránky

Prvním bodem slabých stránek je legislativa. Důvodem je, že české zákony nemají pevně stanovou definici dezinformací a osoby, které tak záměrně narušují bezpečnost a stabilitu České republiky často nejsou adekvátně potrestáni, pokud k trestnímu stíhání vůbec dojde. Druhým bodem, který byl vybrán je vzdělání. Vzděláním není myšleno školství, ale vzdělávání a školení obyvatelstva ohledně rozpoznávání dezinformací.

Dalším bodem slabých stránek je realizace opatření. Zde analýza naráží na fakt, že jediné opatření, které bylo v rámci dezinformací podniknuto, bylo zablokování některých dezinformačních webů, nicméně ani toto zablokování nebylo účinné a tyto weby byly stále dostupné, popřípadě jejich majitelé používali jiných sítí pro šíření těchto dezinformací, jako například Telegram, Twitter či obyčejné skupiny a stránky na síti Facebook. Realizace opatření je tak v tomto ohledu pouze na povrchové úrovni, ale samotnou problematiku žádným zásadním způsobem neřeší, ovšem některé kroky, které by tuto problematiku dokázali efektivně řešit by potřebovali právě úpravu legislativy.

Čtvrtým bodem je samotná strategie vedení hybridní války, to jak obranné, tak útočné povahy. V současné době neexistuje ucelená strategie, jak čelit hybridním hrozbám. Poslední bod pak dále hovoří o skutečnosti, že je stále více a více zařízení s připojením k internetu, a tudíž je mnohem větší část obyvatelstva náchylná vůči hybridním nástrojům

12.3 Příležitosti

Prvním bodem příležitostí byly vybrány Kybernetické a informační síly Armády České republiky. Jedná se o poměrně mladý útvar ozbrojených sil České republiky, který má však v poli hybridního válčení velký potenciál, a to jak v zajišťování bezpečnosti, tak v prosazování zájmů České republiky.

Na prosazování zájmů České republiky se váže bod druhý, kterým je iniciativa, jakou nám tento útvar dává. Stejně jako v konvenčním válčení, i během hybridní kampaně je iniciativa podstatným faktorem k vítězství v takové kampani. Kybernetické a informační síly Armády České republiky dávají další možnost a prostředky, jak hybridní kampaň přenést na

potencionálně nepřátelské země a země, které ohrožují bezpečnost České republiky, čímž doplňují již existující instituce s takovými možnostmi.

Jako další bod bylo vybráno zapojení civilního obyvatelstva. Využívání civilního obyvatelstva k záměrnému prosazování zájmů České republiky není korektní a samozřejmě možné není, nicméně civilní obyvatelstvo se může podílet na obraně před dezinformacemi. Už v dnešní době existuje několik organizací a mnoho dobrovolníků, kteří vyvrací dezinformace a pomáhají z identifikací dezinformačních webů. Používání civilního obyvatelstva k prosazování vlastních zájmů je, jak bylo zmíněno nejen nekorektním řešením, ale zároveň i nepotřebným, protože zájmy České republiky jsou spíše defenzivního než ofenzivního charakteru, a proto by se tato stránka hybridní kampaně měla nechat spíš na osobním uvážení jednotlivých osob, které budou jednat nezávisle.

Posledními dvěma body je rozšíření řad Severoatlantické aliance, kde se očekává vstup Finské republiky a Švédského království a navýšení rozpočtu ministerstva obrany, který by se měl vyšplhat na 2 % hrubého domácího produktu.

12.4 Hrozby

Mezi hrozby lze jednoznačně zařadit současnou bezpečnostní situaci v Evropě, kdy v současné době existují naprosto dokonalé podmínky pro vedení hybridní války a oslabování bezpečnosti a stability České republiky, což je lehce pozorovatelný akt. Za původce této snahy o poškození České republiky se bezpochyby dají označit dezinformační weby, které jsou dalším bodem v kategorii hrozeb.

Jako další hrozba byla vybrána inflace. Pokud pomineme bezpečnostní situaci v Evropě, tak inflace a její dopady jsou teď hlavním problémem, kterému Česká republika čelí. Právě kvůli negativním dopadům inflace dochází, i skrze dezinformační weby a další prostředky k poškozování stability České republiky. Mnoho dezinformačních webů a šiřitelů tohoto obsahu také často užívá argument o tom, že by se veškerá pomoc Ukrajině měla utnout a napravit politické a obchodní vztahy s Ruskou federací a tím bojovat proti zdražování.

Za další hrozbu byla zvolena umělá inteligence, která je podrobně popsaná v předchozích kapitolách této diplomové práce. Poslední hrozbou jsou útoky jedinců a skupin. Těmto útokům nelze zabránit, pouze se na ně preventivně připravit. Na druhou stranu takové útoky jsou buď jednorázové a často nejsou dobře koordinované, a tudíž málokdy nabudou svého

plného potencionálu nebo se jedná o stálé působení těchto osob, avšak za použití mnohem méně radikálnějších metod, jako jsou právě dezinformační weby.

12.5 Analýza

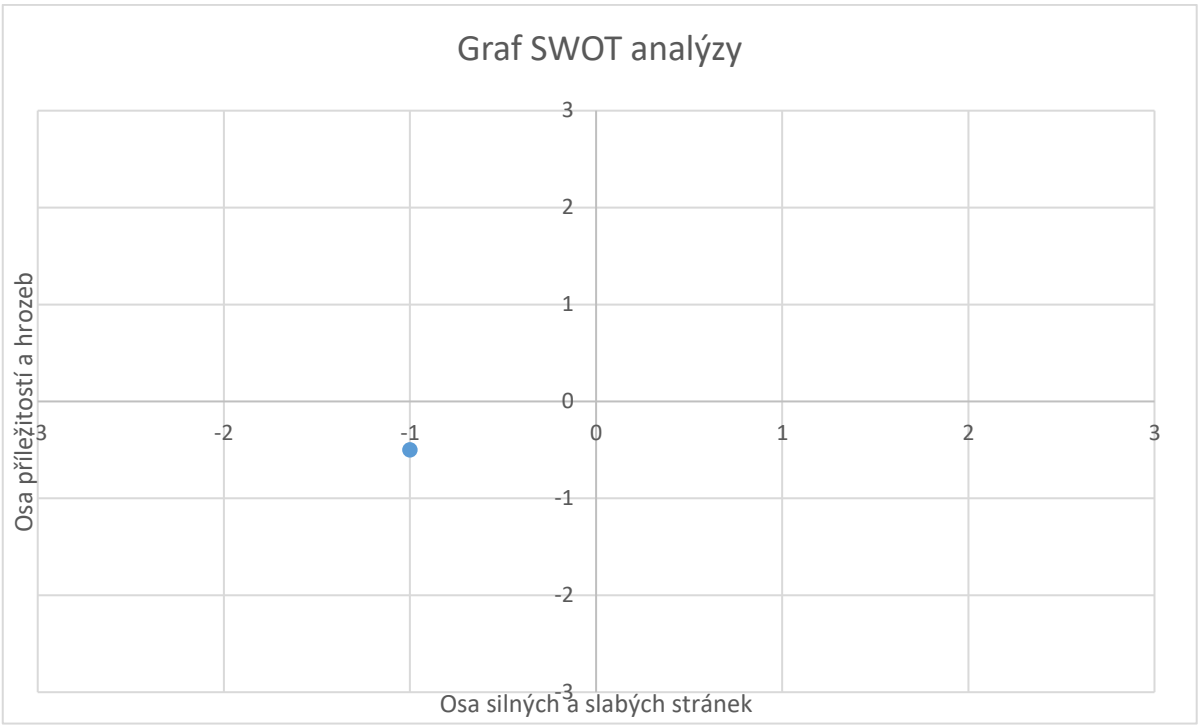
V tabulce č. 1 je vypsáno pět bodů z každé kategorie analýzy SWOT. Tabulka č. 2 obsahuje již vyhodnocené body z tabulky č. 1, které jsou byly následně zaneseny do graf č. 1, který následuje hned za tabulkou č. 2.

Tabulka 1 List SWOT

Silné stránky	**Slabé stránky**
Stabilita	Právní normy
Členství v Evropské unii	Obecné vzdělání
Členství v Severoatlantické alianci	Realizace navržených opatření
Volný přístup k informacím	Absence jednotné strategie
Česká republika není atraktivním cílem	Rostoucí počet zařízení s připojením k internetu
Příležitosti	**Hrozby**
Kybernetické a informační síly AČR	Bezpečnostní situace v Evropě
Iniciativa při vedení hybridní kampaně	Dezinformační weby
Zapojení civilního obyvatelstva, BIS, NUKIB, NBÚ a dalších	Inflace
Rozšíření řad Severoatlantické aliance	Umělá inteligence
Navýšení rozpočtu ministerstva obrany	Útoky jedinců a skupin

Tabulka 2 Body SWOT analýzy

Silné stránky			Slabé stránky		
Body	Váha	Výsledek	Body	Váha	Výsledek
5	0,3	1,5	-5	0,3	-1,5
2	0,2	0,4	-4	0,3	-1,2
2	0,2	0,4	-3	0,1	-0,3
2	0,2	0,4	-3	0,2	-0,6
1	0,1	0,1	-2	0,1	-0,2
<1;5>	Σ1	2,8	<-1;-5>	Σ1	-3,8
Příležitosti			Hrozby		
Body	Váha	Výsledek	Body	Váha	Výsledek
3	0,2	0,6	-4	0,3	-1,2
3	0,2	0,6	-3	0,3	-0,9
3	0,2	0,6	-2	0,2	-0,4
1	0,2	0,2	-1	0,2	-0,2
2	0,2	0,4	-1	0,2	-0,2
<1;5>	Σ1	2,4	<-1;-5>	Σ1	-2,9



Graf 1 SWOT analýza

Graf 1 znázorňuje výsledky SWOT analýzy, který ukázala, že převažují slabé stránky a hrozby. Tento výsledek není překvapivý, jelikož navazuje na výsledky analýzy Auditu národní bezpečnosti, kde výsledek připravenosti před obecnými hybridními hrozbami byl taktéž v neprospěch České republiky.

13 NÁVRH OPATŘENÍ

V této kapitole bude navrhnuta řada opatření, které budou vycházet z negativního výsledků předchozí analýzy SWOT. Opatření budou rozdělena na preventivní a aktivní, přičemž aktivní se budou zabývat dezinformacemi, které se již nějakým způsobem projevují.

13.1 Preventivní opatření

Cílem preventivních opatření je omezit počet nově vznikajících dezinformací a také zmírnit jejich následky. Důležité je zmínit fakt, že nelze kompletně zabránit vzniku dezinformací, jak se o to snaží mnoho zemí, včetně České republiky, která svým krokem o zákazu dezinformačních webů spíše k těmto webům přilákala ještě větší pozornost. Strategie boje proti dezinformacím by se tak měla spíše zaměřit na největší propagátory dezinformací, kteří mají velký dosah a zároveň zkušenosti s tvořením důvěryhodných dezinformací.

13.1.1 Právní normy

Problém zakotvení dezinformací v právních normách České republiky byl zmíněn v teoretické části. Jako odpověď na blokování některých webů se začátkem ozbrojeného konfliktu na Ukrajině přijali české soudy řadu žalob, které, i přesto, že byly odmítnuty, poukázali právě na nedostatky českých zákonů v kontextu dezinformací. Jako odpověď na tuto situaci vláda České republiky oznámila, že se pokusí připravit zákon, který by se dezinformacemi a blokováním dezinformačních webů zabýval, nicméně k takovému kroku ještě nedošlo.

Zákon, či zákony, které se touto problematikou budou zabývat, by se měli zaobírat primárně vymezením pojmů a definicí dezinformací, na čemž je pak možné další zákony stavět. Šíření a tvoření dezinformací by mělo být definováno takovým způsobem, aby bylo jasné, že se jedná o proces, který narušuje stabilitu či jinak poškozuje bezpečnost České republiky. V potaz by také měli být stránky, které šíří dezinformace satirického a podobného obsahu, který si neklade za cíl poškodit stabilitu či bezpečnost.

Takový zákon by se měl také spíše zaměřovat, jak je zmíněno v úvodu kapitoly, spíše na větší dezinformátory, kterými jsou v případě České republiky právě dezinformační weby. Na druhou stranu je nutné vzít v potaz jedince, kteří tyto dezinformace šíří dále, zde je třeba vzít v potaz svobodu projevu a také fakt, že tyto osoby pouze opakují agendu webů a dalších médií, které nebyly v čas blokované. Výjimkou jsou ovšem případy, kdy taková osoba svými

dezinformacemi vědomě podporuje extremismus, terorismus, násilí a jiné skutečnosti, které jsou již definované v českém zákoníku.

13.1.2 Obecné vzdělání

V kapitole o vlivu dezinformací v teoretické části byl zmíněn výzkum provedený v České republice, který však čerpal pouze z malého vzorku osob. I přesto však výzkum přinesl dva podstatné výsledky. Prvním výsledkem je, že okolo 20 % osob zaměňuje bulvární a obdobný obsah s dezinformacemi a druhým výsledkem je, že 61 % osob nepozná, že se právě nachází na dezinformačním webu či jiném takovém médiu. Tato skutečnost je jedním z hlavních důvodů, proč je Česká republika jednou z mála zemí, kde mají dezinformační weby takový vliv, zatímco sousední země se spíše potýkají s problematikou sponzorovaného obsahu. Vzdělávání občanů by mělo probíhat takovým způsobem, aby byl co nejméně omezen jejich každodenní život. Jako nejvhodnější metody tak byly zvoleny:

- Reklamní spoty.
- Letáky a příručky.
- Noviny.

Připravit jednotlivce na to, aby dokázal rozpoznat dezinformace je poměrně jednoduchá záležitost, tudíž tyto tři zvolené metody by měly být dostačující. Každopádně předání takových znalostí, které toto umožní by mělo být taktéž provedeno co nejefektivněji. Proto, pokud by došlo k použití těchto prostředků, k šíření povědomí o dezinformacích, je vhodné, aby byly předány pouze podstatné informace k pochopení této problematiky. Mezi tyto informace by mělo patřit:

- Základní definice dezinformací.
- Příklad dezinformační zprávy.
- Seznam hlavních dezinformačních webů.
- Seznam hlavních organizací, které se zabývají dezinformacemi.

Samotné zveřejnění seznamu dezinformačních webů by určitě přispělo ke snížení počtu osob, které nepoznají, že se na dezinformačním webu nachází. Ministerstvo vnitra sice takový seznam má, nicméně pro veřejnost není dostupný. Obdobný seznam například vytvořil časopis Respekt, investigativní web Neovlivní nebo také spolek NELEŽ. Seznam dezinformačních webů samozřejmě vytvořilo mnoho organizací, spolků a dalších, ale

pravdou však zůstává, že nemají takový dosah, jako ministerstvo vnitra, které by uvolněním svého seznamu značně pomohlo při řešení této problematiky. V současné době ministerstvo vnitra poskytuje pouze přeloženou příručku pro boj s dezinformacemi s názvem RESIST.

V úvahu by také mělo být bráno vzdělávání civilního obyvatelstva ohledně Evropské unie a Severoatlantické aliance, jelikož právě na osoby, které mají o těchto tématech poměrně omezené znalosti, cílí dezinformační weby.

13.1.3 Zapojení civilního obyvatelstva

Zapojení civilního obyvatelstva je záležitost, která by jednoznačně měla být na bázi dobrovolnosti. K tomu, aby se však občané mohli zapojit do boje proti dezinformacím je nutné jejich řádné vzdělání v tomto směru, k čemuž by měli posloužit kroky zmíněné v předchozí podkapitole. Pro osoby, které by měli zájem se podílet na boji proti dezinformacím, by měl být vytvořen portál nebo jim předat tyto informace jiným, jednoduchým způsobem, kde by byl výčet organizací a společností, které tuto problematiku řeší.

Tento seznam organizací a společností by mohl být vytvořen na webu ministerstva vnitra, které by tak nemuselo dále zveřejňovat seznam dezinformačních webů, jelikož by zveřejnili seznam všech dalších webů, které buď tento seznam mají veřejný nebo danou problematiku řeší. V současné době je na stránkách ministerstva vnitra uvedeno devět institucí, které se touto problematikou zabývají, ale velké množství podobných institucí, společností a organizací v tomto seznamu stále chybí, zatímco některé z uvedených sítí se bojem s dezinformacemi vůbec nezabývají, jako například projekt HATE FREE.

Pro civilní obyvatelstvo se nabízí celá řada možností, jak se do této problematiky zapojit, může jít o pouhé sledování, zapisování a nahlašování těchto webů a nových témat na které dezinformace zrovna naráží, dále se může jednat například o investigativní novinářství nebo, v extrémních případech je možné zajít i do takzvané morálně šedé oblasti a zapojit se tak do boje proti dezinformačním webů pomocí útoků na tyto weby, čímž je omezena jejich dostupnost. Takový krok už je však opravdu extrémním řešením na hraně zákona, ke kterému by však nemuselo být přistoupeno za předpokladu, že dojde k vytvoření zákonů o blokaci dezinformačních webů. Na druhou stranu je právě takový případ perfektním příkladem používání hybridních nástrojů, kdy stát může využít někoho jiného k provedení takového útoku a tím se zbavit odpovědnosti.

Rozsah zapojení civilního obyvatelstva je opravdu široký a zapojit se tak může téměř každý nehledě na jeho specializaci a vzhledem k výsledkům hledání na webu Google, zájem o tuto problematiku v České republice narůstá.

13.2 Aktivní opatření

Opatření aktivního druhu se týkají takových opatření, které již řeší vzniklou situaci v dané problematice dezinformací. Jelikož v České republice převládají dezinformační weby, jakožto hlavní dezinformační médium, aktivní opatření se tak budou zaměřovat pouze na tyto weby. Z pozorování bylo zjištěno, že aktivita dezinformačních webů se zvyšuje během důležitých událostí, které často rozštěpují společnost. Takovými událostmi byla právě již několikrát zmíněna pandemie onemocnění Covid-19, začátek války na Ukrajině, ale například i tuzemské volby. Této skutečnosti by se také měla přizpůsobit strategie boje s dezinformacemi.

13.3 Strategie

Ucelená strategie pro boj proti dezinformacím v České republice zatím neexistuje. Každá instituce má své vlastní prostředky, postupy a metody, kterými tuto problematiku řeší, na základě toho, co jim dovoluje legislativa. Zde se opět ukazuje, že česká legislativa není připravena na řešení hybridních hrozeb, jak bylo zmíněno v předešlých kapitolách. Samotný návrh strategie pro boj s dezinformacemi se tak bude zabývat současnou situací, za předpokladu, že blokování dezinformačních webů není možné.

Úvod této kapitoly vysvětluje, že k velkému nárůstu dezinformací dochází právě ve chvíli, kdy dochází k důležité světové, či tuzemské události, samozřejmě tento jev není jednorázový, jak můžeme vidět například ve válce na Ukrajině, kde dochází k nárůstu počtu dezinformací nárazově, například v případě nových ofenzív, návštěv zahraničních politiků či v rámci nových materiálních balíčku směřujících na Ukrajinu.

Prvním krokem nové strategie by tak měla být identifikace takových událostí, již zmíněné volby a podobné události, jejichž datum je předem známé, je lehké identifikovat jako události se zvýšenou dezinformační aktivitou, samozřejmě i dezinformační weby využívají tento předem známý termín těchto událostí ve svůj prospěch. Pro takové události by měl být správně vytvořen seznam informací, které by měli být schopné vyvrátit jakékoliv dezinformace, které by mohli během těchto událostí ohrozit stabilitu či bezpečnost státu. Stejně tak i jedinci, kteří se těchto událostí účastní, by měli být upozornění na podniknutí

podobného kroku, který by měl alespoň částečně napomoci tomu, aby nebyla jejich osoba významným způsobem poškozena lživými informacemi.

Druhou situací jsou události, které nelze předvídat, jako právě pandemie či války. Na tyto mimořádné události se samozřejmě nedá důkladně připravit a problematika dezinformací se během těchto událostí tedy řeší až po jejich vzniku. Zde má stát, jeho instituce a soukromé instituce výhodu oproti dezinformačním webům, jelikož mají mnohem rozsáhlejší možnosti, které mohou během začátku takové události využit.

Při vzniku těchto nepředvídatelných událostí totiž existuje krátké, časové okno, které nemá pevně stanovenou délku trvání. Během tohoto okna je aktivita dezinformačních webů ohledně nově vzniklé události takřka nulová, jelikož tyto weby čekají na reakci orgánů České republiky, aby mohli zvolit postoj, který této reakci alespoň částečně odporuje. Toto poměrně krátké časové rozmezí by tak mělo být využito tak, aby jakýkoliv názor, který orgány České republiky zvolí, byl zároveň podpořen veškerými dostupnými informacemi a zdroji, které tento názor podporují a vysvětlují.

Úvod kapitoly o preventivních opatřeních této diplomové práce hovoří o tom, že by se při boji proti dezinformacím mělo zaměřit čistě na největší dezinformační média, kterými v České republice jsou, jak bylo zmíněno, právě dezinformační weby. Jakékoliv potlačování šíření dezinformací na úrovni jednotlivých osob je až na ojedinělé případy, kdy dochází k porušování i dalších zákonů, nerealizovatelné.

Nová strategie se nemůže zabývat právě jednotlivými případy šíření dezinformací už jen z toho důvodu, že výše zmíněný výzkum ukázal, že 61 % osob nepozná, že se nachází na dezinformačním webu, a tudíž obdobné množství lidí může potencionálně šířit dezinformace, aniž by o tom věděli a vyšetřování každé osoby a každé zprávy zvlášť je jednoduše neproveditelné.

Z tohoto důvodu je mnohem jednodušším a účinnějším krokem soustředit se čistě na tyto dezinformační weby, čímž se logicky zredukuje i počet osob, které dále šíří dezinformace, na které narazili právě na těchto webech. Samozřejmě nejlepším a nejrychlejším řešením by byla blokace těchto webů, ale jelikož tento návrh strategie vychází z toho, co současný legislativní systém České republiky dovoluje, je počet nástrojů vhodných pro řešení této problematiky poměrně omezený. Mezi hlavní nástroje a kroky, které by dle této strategie bylo vhodné podniknout patří následující:

- Včasná identifikace událostí, které mohou přinést zvýšenou aktivitu dezinformačních webů a dalších dezinformačních médií.

- Včasné vytvoření informačních zdrojů, které při plánovaných událostech poskytnou dostatečnou ochranu pro bezpečnost a stabilitu České republiky.
- Využití časové okna nečinnosti dezinformačních webů při vzniku nepředvídatelné mimořádné události.
- Důkladné uvedení zdrojů a důvodů u informací, které by potencionálně mohli dezinformátoři využít.
- Zviditelnění a rozšíření institucí, které bojují s dezinformacemi, tak, aby došlo k většímu zapojení civilního obyvatelstva.
- Vytvoření oficiálního seznamu dezinformačních webů vládou České republiky a jeho následné zpřístupnění veřejnosti.
- Prohlubování spolupráce jednotlivých státních institucí.
- Mazání či označování informací jako nepravdivé pomocí umělé inteligence.

14 VYUŽITÍ HYBRIDNÍCH NÁSTROJŮ

Česká republika by neměla být schopna se pouze bránit, ale také by měla efektivně využít nástroje hybridní kampaně k prosazování vlastních bezpečnostních zájmů a zájmů spojenců, ať už v rámci Severoatlantické aliance či Evropské unie. Bezpečnostní zájmy České republiky jsou definovány v Bezpečnostní strategii České republiky, která je rozděluje do tří kategorií; životní, strategické a další významné zájmy.

Do životních zájmů České republiky se řadí územní celistvost a suverenita, udržení demokratických základů, ochrana lidských práv a svobod občanů. Zájmy strategické jsou mnohem rozsáhlejší a specifičtější a zabývají se jak bezpečnostní samotnou, tak posilováním spolupráce mezi jednotlivými aktéry globální politiky, které se účastní i Česká republika. Pro potřeby této práce je vybráno pouze malé množství strategických zájmů, které lze hybridními nástroji přímo prosazovat, těmito zájmy jsou:

- Zajišťování bezpečnosti a stability,
- prevence vzniku konfliktů a jejich zvládání v regionální politice,
- zvládání bezpečnostních hrozeb ohrožující bezpečnost České republiky a spojenců,
- zvládání konfliktů v regionální politice,
- zmírňování následků konfliktů v regionální politice,
- zajišťování vnitřní a vnější bezpečnosti,
- zajišťování hospodářské bezpečnosti a konkurenceschopnosti české ekonomiky,
- zajišťování strategických surovin a rezerv, potravinové, surovinové a energetické bezpečnosti
- posilování obrany v kyberprostoru.

Mezi další významné zájmy, které lze prosazovat hybridními nástroji se řadí boj proti kriminalitě, organizovanému zločinu, extrémismu, boj s korupcí, ale například i ochrana životního prostředí. Zájmy České republiky jsou jasně defenzivního charakteru a tuto skutečnost reflektují i zájmy Severoatlantické aliance.

I přes defenzivní podstatu zájmů České republiky, je stále nutné tyto zájmy bránit i takovým způsobem, který si vyžaduje více agresivní přístup. K takovému kroku by se mělo přistoupit v případě, že se od vybraného státu, režimu, organizace či jiného politického aktéra očekává podobný útok nebo se jedná o režim, který svými zájmy přímo ohrožuje bezpečnost České

republiky a spojenců. Na základě bezpečnostních dokumentů mezi tyto hlavní aktéry politické sféry patří Ruská federace, Čínská lidová republika a Íránská islámská republika. Pokud by měl být takový útok podniknut, je nutné vzít v potaz určité okolnosti, které by mohli zvýšit šanci úspěchu, protože stabilní režim je velmi složité destabilizovat hybridními nástroji. Mezi tyto okolnosti je nutné zařadit:

- Rozštěpení společnosti v dané zemi.
- Jak dobře je stát spravovaný a zda plní své základní funkce.
- Alespoň část obyvatelstva sympatizuje se zájmy a hodnotami státu, který podnikl takový útok proti jejich zemi.
- Daná země nedisponuje bezpečnostním systémem, který je schopný bránit se jak proti nevojenským, tak vojenským útokům.
- Daná země není členem žádného významného mezinárodního společenství a nemá žádné významné spojence.

Pro správné využití nástrojů hybridní kampaně však tyto body nejsou plně dostačující a je k nim také nutná znalost politického dění a vnitřních záležitostí daného státu. Zde by se doktrína využití hybridních nástrojů měla zásadně lišit od doktríny Ruské federace, která zde byla zmíněna. Zatímco Ruská Federace klade důraz na dlouhodobé působení hybridních nástrojů a destabilizace i ve stabilních oblastech za pomoci obrovského množství dezinformací a dalších nástrojů hybridní kampaně, mnohem účinnější je využití menšího množství těchto nástrojů ve správný moment.

Příkladem může být situace na Ukrajině, kde se Ruská federace snažila několik let vytvořit nové, separatistické útvary v poměrně stabilním regionu i přes fakt, že v této oblasti žilo velké množství rusky mluvícího obyvatelstva. K vytvoření těchto pseudostátů sice došlo, nicméně značná část obyvatelstva oblast Donbasu opustila, před začátkem války v únoru roku 2022 bylo registrováno 1,6 milionu osob, které byly nuceny tuto oblast opustit, naprostá většina z nich však zůstala na území Ukrajiny. Do dnešní doby, ani po začátku invaze a otevřeného zapojení armády Ruské federace nezískali tyto separatistické státní útvary kontrolu nad celým svým územím a jedním z hlavních důvodů je, že Ruská federace využívala hybridní nástroje takovým způsobem, že nemaskovala své přímé zapojení či své cíle a od roku 2014 bylo představeno několik desítek scénářů nejen ukrajinských ale i vytvořených Severoatlantickou aliancí, které s konvenční válkou mezi Ruskou federací a Ukrajinou počítali.

Takové dlouhodobé působení hybridních nástrojů jde proti samotnému principu vedení hybridní kampaně, a proto by Česká republika a Severoatlantická aliance měla, pokud to situace vyžaduje, zvolit naprosto odlišný přístup. Jako příklad může posloužit současná situace v Íránu. Za posledních několik let se Írán stává více než regionální mocí, zároveň se snaží o výrobu vlastních zbraní hromadného ničení a také se jedná o významného spojence Ruské federace, které dodává bojové bezpilotní letouny. Tyto skutečnosti z Íránu dělají potencionálního nepřítele Severoatlantické aliance a České republiky.

K oslabení Íránu by tak podle některých vojenských představitelů Severoatlantické aliance mělo dojít v co nejbližší době a vedení hybridní kampaně proti tomuto státu se jeví jako nejlepší způsob, otázkou však zůstává, jaký správný postup zvolit. Působení dlouhodobé hybridní kampaně, která si nezakládá na žádném z pěti výše zmíněných bodů se na příkladu Ruské federace ukázalo jako neúčinným řešením, a proto je nutné vzít v potaz, zda Írán samotný splňuje jednu z pěti vybraných podmínek.

Rozštěpení společnosti a sympatie obyvatelstva s více liberálními a západními hodnotami je v současné době v Íránu poměrně velkým tématem, které začalo velkými protesty v září 2022 a které stále trvají. Tyto protesty si vyžádaly přes 450 obětí, téměř 900 zranění a až 18 tisíc zatčených osob. Jelikož protesty do jisté míry stále trvají, je možné je pomocí správných hybridních nástrojů eskalovat. Mezi vhodné nástroje, které by mohli splnit tento cíl patří informační a ekonomické, které se zaměřují na civilní obyvatelstvo v mnohem větší míře než nástroje jiné.

Cílem informačních nástrojů by mělo být šíření takových informací a dezinformací, které dále dehonestují současný režim a zároveň vyjadřují podporu protestujícím, samozřejmě zde záleží, jestli cílem pouhé oslabení současného režimu či jeho přeorientování na západ a tyto informační nástroje by se dle toho měli přizpůsobit. Využití ekonomických nástrojů je mnohem přímočařejší, pokud by došlo k jejich užití a následného zhoršení ekonomické situace v Íránu, je více než pravděpodobné, že se k již probíhajícím protestům přidají další osoby, jelikož dojde k další destabilizaci současného režimu. Zde se ovšem rýsuje další otázka ohledně vztahů protestujících vůči západním zemím, které za tyto ekonomické problémy budou nést určitou zodpovědnost, jelikož tyto země se nebudou moct schovat za útoky jedinců či skupin. Nicméně tohle ovšem není otázka pro tuto diplomovou práci, kde se nerozhoduje o budoucnosti Íránu, ale pouze o možnosti využití hybridních nástrojů k prosazování zájmů České republiky a Severoatlantické aliance, přičemž Írán slouží pouze jako názorný příklad.

Obdobný přístup je tak možné zvolit i při konfrontaci s dalšími zmíněnými státy. V rámci Ruské federace by za současné situace byl vyvinut tlak na poškození vojenského úsilí ruské armády vůči Ukrajině. Na druhou stranu jakákoliv snaha o destabilizaci ruské populace, která by vedla například k protestům se v současné době jeví jako zbytečná, jelikož ruská populace je buď poměrně rychle a násilně potlačena nebo se takových akcí, na kterých by vyjádřili svůj nesouhlas s kroky ruské vlády s pochopitelných důvodů vyhýbají. Vyvinout tlak tímto směrem by se tak spíše vyplatilo vůči Bělorusku, jehož nejen civilní, ale i vojenské obyvatelstvo mařilo úsilí armády Ruské federace například poškozováním logistických uzlů.

Ohledně Čínské lidové republiky se v současné době nerýsuje žádné citlivé téma, na které by se šlo zaměřit. Během diskuse se zaměstnancem Vojenského zpravodajství se téma vedlo směrem k nulové toleranci vůči Covidu-19, což je ve zkratce série poměrně radikálních kroků, kterými Čína bojuje proti šíření onemocnění Covid-19, nicméně s ohledem na škody na lidských životech a faktu, že tím může být ohrožena i bezpečnost České republiky jsme se tímto tématem dále nezabývali. Místo tohoto tématu však přišla řada na dění ohledně Taiwanu a Hong Kongu, kde poměrně před nedávnou dobou proběhli rozsáhle protesty. Zde je však jakákoliv podpora těchto dvou aktérů složitým tématem, jelikož se jedná o významné spojence Spojených států amerických, a tudíž Severoatlantické aliance a zde je nutné si položit otázku, zda je vhodné využít spojence Severoatlantické aliance k prosazování našich zájmů.

V této kapitole bylo mimo základních podmínek, které by měl cílený stát splňovat před tím, než na něj je proveden útok za pomocí hybridních prostředků také uvedeno několik příkladů na třech hlavních potencionálně nepřátelských států pro Českou republiky. Tyto příklady pokryly širokou řadu faktorů, které je dobré brát v úvahu. Tyto faktory jsou:

- Analýza současného dění v regionální a vnitřní politice daného státu.
- Vybrání nejvhodnějších hybridních nástrojů na základě problémů, kterým vybraný čas v daný okamžik čelí.
- Brát v potaz i útok na spojence daného státu, za předpokladu, že bude mít větší šanci k úspěchu a očekávají se od něj lepší výsledky.
- Analyzovat možná rizika, která by mohla vzniknout pro bezpečnost České republiky či našich spojenců po provedení takového útoku.
- Zvážit, zda takový útok dokáže odůvodnit možné ztráty na životech a majetku.

Diskuse byla také převedena na možnost využívání hybridních nástrojů pro prosazování vnitřních zájmů České republiky, jako bojování proti organizovanému zločinu, extrémismu či korupci. Odpověď je, že se samozřejmě dá využít těchto nástrojů k potlačování těchto vnitřních elementů, které ohrožují bezpečnost České republiky, nicméně v současné době bezpečnostní složky disponují mnohem lepšími způsoby, jak proti těmto elementům bojovat a samotné hybridní nástroje je nezastaví, mohou je pouze do značné míry potlačit.

Ve scénáři, kdy by došlo k použití hybridních nástrojů k takovému účelu by došlo k užití pouze informačních prostředků a nejspíše by došlo k vytváření dezinformací o navýšení aktivity bezpečnostních složek či rozvití několika organizovaných buněk, čímž by mělo dojít k potlačení činnosti buněk reálných.

V poslední řadě se diskuse zabývala teroristickými organizacemi, jako Daesh či al-Qaeda. Závěr této diskuse však byl jednostranně uzavřen tak, že využití hybridních nástrojů proti těmto organizacím a skupinám je téměř nemožné, jelikož se jedná o silně nábožensky či jinak motivované osoby. Tyto skupiny taktéž nemají žádnou informační infrastrukturu, na kterou by bylo možné cílit, a proto se nevojenské prostředky vedení hybridní kampaně považují za velmi neúčinné pro boj s těmito skupinami.

ZÁVĚR

Prvním stanoveným cílem, dle první kapitoly této diplomové práce bylo vytvoření analýzy stavu obranyschopnosti vůči dezinformacím. Tento cíl práce byl naplněn a SWOT analýza odhalila, že současný systém není schopný čelit hybridním hrozbám tohoto typu. Výsledek nebyl nijak překvapivý, protože navazuje na analýzu Auditu národní bezpečnosti, kde analýza proti hybridním hrozbám z obecného hlediska taktéž odhalila nedostatky v současném stavu. Z této analýzy následně vychází řada opatření a okolností, které je nutné vzít v úvahu, aby tak došlo ke zlepšení současné situace.

Druhým stanoveným cílem bylo navržení způsobu, jakým by mohla Česká republika za použití dezinformací a dalších nástrojů hybridní kampaně prosazovat zájmy své a zájmy svých spojenců. V této části bylo navrženo několik scénářů, během kterých je nutné vzít v potaz mnoho různorodých okolností. Tento cíl je poměrně rozsáhlý, a proto byla vybrán pouze obecný popis jednotlivých situací, které však plně postačí jako případný návod, tudíž tento cíl byl také splněn.

Samotná diplomová práce také přinesla rozsáhle poznatky v této problematice. Práce se také snažila o spojení různých názorů na tuto tématiku, dělení hybridních nástrojů a dalších oblastí, kde neexistuje ucelený názor. Pevně věřím, že takový krok poskytne jednodušší pochopení dané problematiky, ze které pak bude možné dále vycházet při jejím dalším zkoumání.

Největším problémem při zpracování této práce byla jednoznačně rozsáhlost tématu hybridní války, což je téma, o kterém se dá diskutovat celé týdny a z tohoto důvodu je jasné, že v práci určitě chybí řada detailů a faktů, které se na toto téma vážou, nicméně veškeré potřebné informace pro pochopení tématu ve vztahu k dezinformacím jsou v diplomové práci zahrnuty.

SEZNAM POUŽITÉ LITERATURY

- ČESKO, 1993a. Ústavní zákon č 1/1993 Sb., Ústava České republiky.
- ČESKO, 1993b. Usnesení č. 2/1993 Sb., Usnesení předsednictva České národní rady o vyhlášení LISTINY ZÁKLADNÍCH PRÁV A SVOBOD jako součástí ústavního pořádku České republiky.
- ČESKO, 1994a. Zákon č. 153/1994 Sb., o zpravodajských službách České republiky.
- ČESKO, 1994b. Zákon č. 154/1994 Sb., o bezpečnostní informační službě.
- ČESKO, 1998. Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky.
- ČESKO, 1999a. Zákon č. 219/1999 Sb., o ozbrojených silách České republiky.
- ČESKO, 1999b. Zákon č. 222/1999 Sb., o zajišťování obrany České republiky.
- ČESKO, 2000a. Zákon č. 239/2000 Sb., o integrovaném záchranném systému
- ČESKO, 2000b. Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon).
- ČESKO, 2000c. Zákon č. 241/2000 Sb., o hospodářských opatřeních pro krizové stavy.
- ČESKO, 2004. Zákon č. 585/2004 Sb., o branné povinnosti a jejím zajišťování (branný zákon).
- ČESKO, 2005. Zákon č. 289/2005 Sb., o Vojenském zpravodajství.
- ČESKO, 2008. Zákon č. 273/2008 Sb., o Policii České republiky.
- ČESKO, 2014. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti.
- ČESKO, 2015. Zákon č. 320/2015 Sb., o Hasičském záchranném sboru České republiky.
- ŘEHKA, Karel, 2017. Informační válka. Informační válka. Praha: Academia, s. 5. XXI. století. ISBN 978-80-200 2770-2.
- KIRCHER, Stefan. Asymmetric Warfare. A Challenge for International Humanitarian Law?. Munich: GRIN Verlag, 2015, 12 s. ISBN 9783668112650.
- 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.

- *Audit národní bezpečnosti*. Praha: Ministerstvo vnitra ČR, odbor bezpečnostní politiky a prevence kriminality, 2016.
- Výroční zpráva Bezpečnostní informační služby za rok 2021. Bezpečnostní informační služba [online]. 2022 [cit. 2023-04-17]. Dostupné z: https://www.bis.cz/vyrocni-zpravy/vyrocni-zprava-bezpecnostni-informacni-sluzby-za-rok-2021-e1718a7b.html.
- Výroční zpráva o činnosti Vojenského zpravodajství za rok 2021. Bezpečnostní informační služba [online]. 2022 [cit. 2023-04-17]. Dostupné z: https://www.vzcr.cz/uploads/41-Vyrocni-zprava-2021.pdf.
- United Nations High Commissioner for Refugees, 2023. Types of Misinformation and Disinformation. [online] Ženeva: UNHCR, 2023 [cit. 2023-04-11]. Dostupné z: https://www.unhcr.org/innovation/wp-content/uploads/2022/02/Factsheet-4.pdf
- Ministerstvo vnitra, 2023. Centrum proti hybridním hrozbám – Dezinformační kampaně [online]. Praha: Ministerstvo vnitra, 2023 [cit. 2023-4-11]. Dostupné z: https://www.mvcr.cz/chh/dezinformacni-kampane.aspx
- Válka čtvrté generace se rozvíjí, válka páté generace vzniká [online]. Praha, 2008 [cit. 2023-04-17]. Dostupné z: https://vojenskerozhledy.cz/kategorie/valka-ctvrte-generace-se-rozviji-valka-pate-generace-vznika.
- CLAUSEWITZ, Carl von. O válce. Praha: Academia, 2008. Europa (Academia). ISBN 978-80-200-1598-3.
- William S. Lind, Keith Nightengale, John Schmitt and Gary I. Wilson, "The Changing Face of War: Into the Fourth Generation," Marine Corps Gazette, November, 2001.
- BALÍK, Stanislav. ČTYŘI GENERACE VÁLEČNICTVÍ. Kulturní noviny [online]. 2015 [cit. 2023-04-17]. Dostupné z: https://www.kulturni-noviny.cz/nezavisle-vydavatelske-a-medialni-druzstvo/archiv/online/2015/42-2015/56249840a6850.
- The European Centre of Excellence for Countering Hybrid Threats. *The European Centre of Excellence for Countering Hybrid Threats* [online]. 2023 [cit. 2023-04-17]. Dostupné z: https://www.hybridcoe.fi/what-is-hybridcoe/.

- Bezpečnostní strategie České republiky 2015. Vláda.cz [online]. Praha: Ministerstvo zahraničních věcí České republiky, 2015 [cit. 2023-04-17]. Dostupné z: https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf.
- Obranná strategie České republiky 2017. Vláda.cz [online]. Praha: Ministerstvo obrany České republiky, 2017 [cit. 2023-04-17]. Dostupné z: https://www.vlada.cz/assets/ppov/brs/dokumenty/obranna-strategie-2017.pdf

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

EU	Evropská unie
NATO	Severoatlantická aliance
BIS	Bezpečnostní informační služba
VZ	Vojenské zpravodajství
ÚZIS	Úřad pro zahraniční styky a informace
NCKO	Národní centrum kybernetických operací
NBÚ	Národní bezpečnostní úřad
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
CERT	Computer Emergency Response Team
MV	Ministerstvo vnitra
MO	Ministerstvo obrany

SEZNAM TABULEK

SEZNAM GRAFŮ