Zdravotně sociální fakulta
Faculty of Health and Social Sciences

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

Hybridní hrozby a státní bezpečnostní agenda

DIPLOMOVÁ PRÁCE

Studijní program: OCHRANA OBYVATELSTVA

Autor: Bc. Šárka Doležalová

Vedoucí práce: Mgr. Štěpán Strnad, Ph. D.

České Budějovice 2022

Prohlášení

Prohlašuji, že svoji diplomovou práci s názvem **„Hybridní hrozby a státní bezpečnostní agenda“** jsem vypracovala samostatně pouze s použitím pramenů v seznamu citované literatury.

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

V Českých Budějovicích dne 8.8.2022 ……

Bc. Šárka Doležalová

Poděkování

Tímto bych ráda poděkovala vedoucímu diplomové práce Mgr. Štěpánu Strnadovi, Ph.D. za jeho čas, strávený nad společnou kontrolou této diplomové práce, pomoc při jejím zpracování, za jeho cenné rady a vstřícnost.

Hybridní hrozby a státní bezpečnostní agenda

Abstrakt

Hybridní hrozby a státní bezpečnostní agenda jsou v dnešní době velmi diskutovaným tématem. S neustálým vývojem IT technologií a změnami ve vojenských i nevojenských taktikách se hybridní válka postupně stává dominantním způsobem vedení moderních konfliktů, které probíhají z velké části v kyberprostoru. Státní bezpečnostní agenda úzce souvisí s hybridními hrozbami, jelikož popisuje fungování bezpečnostního systému České republiky, a to i v souvislosti s konvenčními i moderními bezpečnostními hrozbami.

Hlavním cílem této diplomové práce je analýza a aplikace zvolené diskurzivní metody na zprávy o ukrajinském konfliktu. Dílčími postupy práce, zásluhou kterých k cíli docílíme je získání kompletních informací o hrozbách v kyberprostoru (zejména pak, jak můžeme těmto hrozbám čelit), dále analýza vzniku a šíření tzv. fake news (falešných zpráv), které ohrožují lidskou společnost a v neposlední řadě informační válka a kompetence vlády proti jejich šíření.

Teoretická část práce se zabývá základními definicemi z oblasti bezpečnosti státu, státního bezpečnostního systému, hybridní války, kyberprostoru a fake news. Vybraná témata se vztahují k současnému stavu a ke specifikům v České republice. Dále je v teoretické části popsána diskurzivní analýza, jelikož tato metoda byla použita v praktické části práce.

Praktická část se zabývá diskurzivní analýzou fake news z Rusko-ukrajinského konfliktu, kdy základním článkem je souhrn několika fake news a jejich uvedení na pravou míru. Ke každé fake news byla snaha nalézt relevantní článek z českých médií a zjistit, do jaké míry se názory v nich shodují a jak jsou jednotlivé události vnímány v České republice.

Výsledkem analýzy jsou odpovědi na otázky ze zadání, které zní: *„Jaký vliv mají falešné zprávy na bezpečnostní politiku států? Jak lze zastavit šíření falešných zpráv?“* Pomocí těchto otázek se podařilo splnit cíl této diplomové práce.

Klíčová slova

Fake news, Dezinformace, Bezpečnostní politika státu, Hybridní hrozby, Diskurzivní analýza

Hybrid threats and national security agenda

Abstract

Hybrid threats and the state security agenda are currently very much debated topics. With the continuous development of IT technologies and changes in military and non-military tactics, hybrid warfare is gradually becoming the dominant way of conducting modern conflicts, which take place largely in cyberspace. The national security agenda is closely related to hybrid threats, as it describes the functioning of the security system of the Czech Republic, in connection with both conventional and modern security threats.

The objectives of this thesis are three in total, it involves obtaining information about threats in cyberspace, and how to counter these threats, and further analyze the emergence and spread of so-called fake news that threatens human society. Last objective is to describe the so-called information war and the competence of the government against the spread of fake news.

The theoretical part of this thesis first deals with basic definitions from the areas of state security, state security system, hybrid warfare, cyberspace and fake news. The selected topics are related to the current situation and specifics in the Czech Republic. Next part of the theoretical part describes discursive analysis, as it is a method used in the practical part of this thesis.

The practical part focuses on the discursive analysis of fake news from the Russia-Ukraine conflict. The basic article is about summary of several fake news and correcting them. For each fake news, there was an effort to find a relevant article from the Czech media and to find out to what extent the opinions in them coincide and how individual events are perceived in the Czech Republic.

The resulting analyzes answered the question from the assignment "What effect do fake nws have on the state security policy?" How can we stop the spread of fake news?" And thanks to them, all 4 goals were met.

Key words

Fake news, Disinformation, State security policy, Hybrid threats, Discursive analysis

Obsah

Úvod

Svět, ve kterém žijeme, se stává stále více závislým na technologiích a informacích. To samé platí o válčení, kdy v minulosti válka představovala fyzický boj se zbraněmi, zatímco dnes se válčí zejména za pomoci informací.

V současné době čelí Evropa novému druhu válčení, tzv. hybridním hrozbám. Tyto hrozby představují pro společnost riziko, jelikož v sobě spojují různé způsoby válčení. Hybridní hrozby jsou definovány jako soubor nátlakových a podvratných činností konvenčních i nekonvenčních metod (např. diplomatických, vojenských, ekonomických a technologických), které mohou státní i nestátní aktéři koordinovaným způsobem využívat k tomu, aby dosáhli konkrétních cílů, aniž by formálně vyhlásili válku. Předložená diplomová práce je zaměřena na problematiku hybridních hrozeb a státní bezpečnostní agendy. Tato práce je zaměřena zejména na hrozby v kyberprostoru. Kybernetický prostor představuje prostředí, kde se jednotlivé dimenze moci prolínají, a jeho význam pro fungování států a ekonomik je velmi kritický. Kybernetické útoky umožňují zasáhnout a ohrozit fungování veřejné správy, kritické infrastruktury, finančního sektoru a jsou mimo jiné prostředkem špionáže a prostředkem dezinformačních kampaní. Bezpečnostní politika všech států by měla dávat pozor na informační prostor – kdo lidem informace dává. Také musí umět zasáhnout proti falešným zprávám, vyvracet mýty a uvádět je na pravou míru.

Stanoveným cílem je analýza a aplikace zvolené diskurzivní metody na zprávy o ukrajinském konfliktu. A za pomoci dalších dílčích postupů získat informace o hrozbách v kyberprostoru, jak těmto hrozbám čelit, analyzovat vznik a šíření tzv. fake news, které ohrožují lidskou společnost a v neposlední řadě popsat tzv. informační válku a kompetence vlády proti šíření falešných zpráv. Použitou metodou je diskurzivní analýza článků o fake news v rámci invaze na Ukrajinu.

Toto téma jsem si vybrala pro svoji diplomovou práci zejména kvůli tomu, že hybridní hrozby jsou velmi zajímavé, a hlavně aktuální téma. Při zpracování části týkající se státní bezpečnostní agendy jsem si zopakovala téma ke státní závěrečné zkoušce z mého oboru.

1. Současný stav

1.1 Definice hybridní války

Války se vedly od počátku lidské civilizace, kdy spolu začali lidské bytosti nesouhlasit. Válečné konflikty trvají dodnes a jejich konec je v nedohlednu. Vítězi války se stávali od pradávna ti, kteří byli nejlépe informováni a byli schopni na tyto informace co nejdříve zareagovat. V historii válčení byly informace vždy klíčové. Většinou se jednalo o získání vědomostní převahy nad nepřítelem za účelem lepšího rozhodování nebo skryté ovlivňování protivníků, spojenců nebo obecné populace. Konvenční válka je popisována jako ozbrojená konfrontace mezi národy nebo organizacemi, která má za následek smrt a destrukci. [1]

Česká republika je rovněž ohrožena hybridními hrozbami. Hybridní nebezpečí není v současné době v České republice jednoznačně definováno. Připravenost a kapacita bezpečnostních složek ČR adekvátně reagovat na tuto skutečnost nebyla dosud předmětem žádné odborné debaty zúčastněných stran. Všechny bezpečnostní složky, zejména tajné služby, policie a celní správa, budou muset přijmout holistickou strategii, aby na tyto hrozby dlouhodobě účinně reagovaly. [2]

Hybridní válka je ozbrojený konflikt, který kombinuje vojenské a nevojenské taktiky s cílem donutit protivníka k akcím, které by sám neprovedl. Stát je vždy na jedné straně boje. Cílů moderní války je většinou dosaženo nevojenskou taktikou, v podobě psychologické operace, propagandy, ekonomických sankcí, embarg, trestné činnosti, terorismu a další podvratné činy podobného druhu. Vojenské operace jsou prováděny kombinovanými silami, které združují symetrické a asymetrické způsoby vedení bojových operací proti celé společnosti, zejména proti jejím politickým strukturám, orgánům státní správy a samosprávy, státní ekonomice, morálce obyvatelstva a ozbrojeným silám. Moderní boj je čím dál tím méně o použití hrubé síly. [1]

Někteří autoři tvrdí, že myšlenka hybridního válčení je stará jako válka samotná. Tato myšlenka však v poslední době nabyla na významu, zejména v důsledku rozvoje informačních technologií. Termín „hybridní válka“ byl poprvé použit v USA v roce 2005, kdy vyšel článek s názvem „O vzestupu hybridních hrozeb“. Článek byl zaměřený zejména na to, jak moderní válka často kombinuje konvenční a nekonvenční vojenské taktiky a plány, zejména s ohledem na její psychologické a informační komponenty. [1]

Ruská invaze na Krymský poloostrov v roce 2014, která primárně využívala dezinformací a zneužívání nejistého politického klimatu na Ukrajině, byla druhým velkým zlomem v historii slovního spojení „hybridní válka“. [1]

Konvenční válka je obtížnější, dražší a více riskantní než hybridní válka bez fyzického útoku. Otázkou však nadále zůstává, zdali nepřímé „útoky“ a strategie vůbec klasifikovat jako válku. Určitá míra nejednoznačnosti při řešení tohoto druhu konfliktu je dalším kamenem úrazu. Jedná se o cílený výsledek v řadách cíle. Náročné odhalení pachatele určitého útoku je pro útočníky jednou z mnoha výhod těchto způsobů vedení války. Když totiž nevíme „kdo to udělal“, těžko se realizuje odvetná akce. [1]

1.2 Vznik a evoluce hybridní války

Na počátku hybridní válka představovala konflikty mezi státy a nestátními subjekty za použití souběžně vedených konvenčních a speciálních operací. Konflikty mezi vojensky nebo technologicky rozvinutými mocnostmi a jejich málo rozvinutými nepřáteli měly být vyřešeny pomocí hybridní války. Tyto konflikty měly být vedeny nekonvenčními prostředky, jako je například terorismus, partyzánská neboli guerillová válka, informační válka nebo nasazení zbraní hromadného ničení. Termín „hybridní válka“ je připisován autorům T. Mockaitisimu a R. Walkerovi. [6]

Válka mezi Ruskem a Čečenskem z roku 1994 -1996 a následně 1999 - 2009 se stala prvním jakýmsi příkladem hybridní války. Příčinou tohoto konfliktu byl převoz kaspické ropy přes území Čečenska. V tomto konfliktu čečenská strana využívala konvenční a partyzánský způsob boje. Neváhala také využít ke svému prospěchu teroristické akce. [4]

Doktor Francis G. Hoffman vyjádřil svůj názor na hybridní válku ve své studii, která byla zveřejněna v roce 2005. *„Technologický rozvoj a superiorita USA v této oblasti nezastíní dominantní lidskou dimenzi a budoucí protivníci nebudou této superioritě čelit konvenčním způsobem, ale kombinací překvapivého využití technologických prvků a nekonvenčních taktických postupů.“* Dle doktora Hoffmana budou všechny konflikty v budoucnosti hybridní povahy. Dále objasnil rozdíl mezi hybridní válkou a tzv. compoud war. [5]

Thomas Huber definoval compoud war ve svém díle That Fatal Knot. V českém jazyce nemá toto slovo žádný ekvivalent, proto se používá anglický výraz. Jedná se o nejčastější druh válčení, při kterém konvenční a nekonvenční síly spolupracují pod společným vedením na strategické úrovni. Doktor Hoffman označil jako hybridní konflikt např. Búrskou válku (1899–1902), válku v Indočíně (1946–1954), konflikty v Afghánistánu a Libanonu a srbskou invazi do Kosova. Ve svém díle uvádí konflikty, které jsou sporné s aspekty hybridního válčení. A proto je jeho seznam uvedených konfliktů velmi problematický. [6]

Československo – německý konflikt z roku 1938 je dle mnoha autorů ukázkovým příkladem hybridní války v České republice. V tomto konfliktu byly odděleny pohraniční oblasti našeho státu a zanikla Československá republika. Avšak i tento příklad je pokládán za diskutabilní, neboť se odchyluje od původních amerických koncepcí hybridní války. Mnozí autoři odkazovali na Peloponéskou válku nebo válku Římského impéria, jelikož v sobě měli základy hybridní války. [6]

Další významnou osobností zabývající se tématem hybridní války v anglosaském prostředí byl americký velitel T. McCulloh, který rozšířil myšlenku hybridního válčení a rozvinul ucelený rámec svých znalostí. Jeho práce je založena na šesti hlavních myšlenkách:

1) *„složení hybridních sil, jejich schopnosti a účinky jsou unikátní vzhledem ke kontextu sil;*
2) *všechny hybridní síly mají specifickou ideologii, která pro tyto síly vytváří vnitřní příběh organizace;*
3) *hybridní síly vždy čelí existenční hrozbě;*
4) *v hybridní válce je mezi soupeři disproporční rozdíl ve schopnostech;*
5) *hybridní síla obsahuje jak konvenční, tak i nekonvenční komponenty;*
6) *hybridní síly se snaží využívat obranných operací. "* [7]

David Kilcullen byl dalším expertem, který se zabýval myšlenkou hybridní války. Vymyslel definici, která říká, že se jedná o protivníka, který využívá taktiky zahrnující konvenční vojenské operace, povstalecké taktiky a teroristické útoky využívající moderní technologie. Počítal s tím, že v jednadvacátém století bude převládat hybridní válčení. [8]

Myšlenka hybridní války vzbudila zájem u mnoha dalších odborníků. V dnešním moderním světě existuje mnoho různých pohledů na hybridní válku. [6]

1.3 Státní bezpečnostní systém

Každý stát má svou jedinečnou bezpečnostní politiku. Bezpečnostní politika našeho státu se také zabývá myšlenkou hybridního válčení a obrany proti němu. Základní státní zájmy a cíle i strategie k jejich dosažení tvoří bezpečnostní politiku státu. [9]

„Tato společenská činnost směřuje k zabezpečení státní svrchovanosti a územní celistvosti státu a jeho demokratických základů, činnosti demokratických institucí, ekonomického a sociálního rozvoje státu, ochrany zdraví a života občanů, majetku, kulturních statků, životního prostředí a plnění mezinárodních bezpečnostních závazků. "
Bezpečnostní politika státu se skládá z pěti základních prvků:

- *„Obranná politika státu*
- *Hospodářská politika státu v oblasti bezpečnosti*
- *Zahraniční politika státu v oblasti bezpečnosti*
- *Vnitřní bezpečnostní politika státu*
- *Veřejná informační politika státu v oblasti bezpečnosti.“* [9]

Česká republika vydává pravidelně aktualizovaný dokument, který se nazývá bezpečnostní strategie ČR. Tento dokument má funkci efektivního nástroje pro vládu ČR k zajišťování svých klíčových úkolů, kterými jsou zajištění bezpečnosti obyvatel a obrana svrchovanosti a územní celistvosti země. Bezpečnostní strategie České republiky je základní dokument pojednávajícím o bezpečnosti ČR. Na zpracování se podílí parlament, kancelář prezidenta a mnoho dalších specialistů v oboru. Základní legislativou je zejména ústava ČR, zákon č. 110/1998 sb. o bezpečnosti ČR., dále potom mezinárodní závazky s NATO, EU a OSN. K datu zpracování této diplomové práce je nejaktuálnější strategie z roku 2015, která navazuje na svá předchozí znění z roků 2003 a 2011. [10]

S bezpečností strategií ČR přímo souvisí bezpečnostní zájmy ČR, které se bezpečnostní strategie snaží prosazovat. Bezpečnostní zájmy ČR se děli na životní, strategické a další významné. Životní zájmy jsou zajištění suverenity, územní celistvosti a politické nezávislosti státu, základních práv a svobod. Pro jejich zajištění použije ČR všechny dostupné prostředky včetně vojenských. Strategických zájmů má ČR mnohem více než životních, obecně to jsou takové zájmy, které zajištují rozvoj a prosperitu státu a občanů. Prosazují se prostředky přiměřenými situaci. Za další významné zájmy řadíme ty, které přispívají k zajištění životních a strategických zájmů. „*Bezpečnost ČR je založena na principu zajištění bezpečnosti jednotlivce, ochrany jeho života, zdraví, svobody, lidské důstojnosti a majetku.“* [10]

1.4 Kdo je v ČR odpovědný za vnitřní bezpečnost

Česká republika má vybudovaný důkladný hierarchický bezpečnostní systém, který slouží k zachování bezpečnostních zájmů státu. Bezpečnostní systém je složen ze sektoru politického, vojenského, sektoru vnitřní bezpečnosti a civilní ochrany, ekonomického, finančního, legislativního a právního. [31]

Všechny orgány vnitřní bezpečnosti státu nabízejí komplexní ochranu před všemi formami aktuálních i potenciálních vnitřních hrozeb. [11]

Prezident republiky je primárním a nejvýznamnějším subjektem odpovědným za zajišťování bezpečnosti České republiky. Úlohu prezidenta republiky a jeho umístění v rámci bezpečnostního systému České republiky vymezují zejména následující zákony:

- ústavní zákon č. 1/1993 Sb., Ústava ČR;
- ústavní zákon č. 110/1998 Sb., o bezpečnosti ČR;
- zákon č. 218/1995 Sb., o rozsahu branné povinnosti a vojenských správních úřadech;
- zákon č. 219/1999 Sb., o ozbrojených silách ČR;
- zákon č. 220/1999 Sb., o průběhu základní nebo náhradní služby a vojenských cvičení a o některých právních poměrech vojáků v záloze
- zákon č. 221/1999 Sb., o vojácích z povolání;
- zákon č. 222/1999 Sb., o zajišťování obrany ČR;
- zákon č. 153/1994 Sb., o zpravodajských službách ČR (dále jen „zákon o zpravodajských službách“);
- zákon č. 90/1995 Sb., o jednacím řádu Poslanecké sněmovny;
- zákon č. 107/1999 Sb., o jednacím řádu Senátu;
- zákon č. 114/1993 Sb., o Kanceláři prezidenta republiky;

- zákon č. 218/1999 Sb., o rozsahu branné povinnosti a o vojenských správních úřadech (branný zákon), (dále jen „branný zákon“). [12]

Vrchním velitelem ozbrojených sil České republiky je prezident. Prezident má jako vrchní velitel následující pravomoci:

- přijímá základní vojenské zákony,
- jmenuje a odvolává náčelníka Vojenského úřadu,
- uděluje čestné nebo slavné tituly vojenským útvarům a vojenským institucím,
- zapůjčuje bojové prapory vojenským útvarům a vojenským institucím. [13]

Prezident má povoleno účastnit se zasedání vlády a parlamentu. To samé platí i o jeho přítomnosti na zasedáních Bezpečnostní rady státu. Má právo vyžadovat od bezpečnostní rady státu nebo jejích členů zprávy nebo s nimi projednávat důležité otázky týkající se bezpečnosti ČR. [14]

Podle zákona o zpravodajských službách jsou zpravodajské služby povinné předložit prezidentovi zprávu o svém působení. V případech, která nesnesou odkladu jsou povinni ho informovat ihned. Prezident republiky společně s vládou pověřují zpravodajské služby úkoly, které spadají do jejich působnosti. [14]

Zpravodajské služby hrají v bezpečnostním systému ČR zásadní roli při získávání, shromažďování a analýze dat nezbytných pro bezpečnost státu a pro rychlé odhalování bezpečnostních hrozeb a nebezpečí. Zpravodajské služby České republiky jsou rovnocennými účastníky při plnění úkolů a povinností, a to i přesto, že legislativní předpisy upravující postavení jednotlivých služeb se liší, včetně např. postupu při výběru či odvolání jejího ředitele. Zpravodajské služby jsou vždy řízeny, organizovány a vykonávány pod vládní autoritou. [15]

V případě vyhlášení nouzového stavu anebo stavu ohrožení státu má prezident republiky po celou dobu jejich trvání přikazovací právo. Mezi jeho kompetence spadá například vyhlášení mobilizace, demobilizace nebo mimořádné služby. Prezidentovi

republiky se dávají na vědomí všechny kroky při přípravě a zajišťování obrany státu, avšak zodpovědnost za ní má vláda. [16]

Dalším důležitým bezpečnostním orgánem našeho státu je vláda ČR, která představuje nejvyšší instituci výkonné moci v České republice. Funkce a její vymezení definují tyto zákony:

- Ústava ČR;
- ústavní zákon č. 110/1998 Sb., o bezpečnosti ČR;
- zákon č. 218/1999 Sb., o rozsahu branné povinnosti a o vojenských správních úřadech;
- zákon č. 219/1999 Sb., o ozbrojených silách ČR;
- zákon č. 222/1999 Sb., o zajišťování obrany ČR;
- zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon);
- zákon č. 241/2000 Sb., o hospodářských opatřeních pro krizové stavy a o změně některých souvisejících zákonů, (dále jen „zákon o HOPKS“);
- usnesení vlády ze dne 19. března 1998 č. 188, Legislativní pravidla vlády (pravidla přípravy, tvorby, obsahu a formy právních předpisů), v platném znění
- usnesení vlády ze dne 16. září 1998 č. 610, Jednací řád vlády, v platném znění. [12]

Vláda ČR je odpovědná za funkčnost celého bezpečnostního systému České republiky. Rozlišují se její činnosti ve stávajícím stavu a těmi v krizových situacích. Vláda primárně za doby trvání mimořádných stavů:

- přijímá strategickou koncepci obrany státu;
- analyzuje pravděpodobná rizika a nebezpečí v bezpečnostní oblasti ČR a přijímá nezbytná opatření ke zmírnění či odstranění těchto rizik;
- určuje obecné směry budování, přípravy a využití ozbrojených sil ČR;
- řídí proces plánování obrany státu a rozhoduje o hlavních opatřeních přípravy a organizace obrany státu;
- přijímá opatření k zajištění řádného fungování bezpečnostního systému ČR;

- určuje prioritu plnění úkolů spojených s obranou státu;
- určuje prostředky nezbytné k vedení války. [12]

Předsedou BRS (Bezpečnostní rady státu) je předseda vlády. Pokud je funkce prezidenta republiky neobsazena přebírá vláda velení AČR (armáda České republiky). [17]

Bezpečnostní rada státu je státem řízená stálá pracovní organizace, která v mezích vládního mandátu (plánování) řídí a zkoumá bezpečnostní problémy v České republice a rozvíjí náměty na jejich řešení. Primární odpovědností BRS je napomáhat při koordinaci spolehlivého a efektivního bezpečnostního systému České republiky, jakož i při zajišťování bezpečnosti a dohledu nad opatřeními k zajištění bezpečnosti České republiky a plnění mezinárodních povinností. Ve světle současných bezpečnostních nebezpečí a hrozeb v České republice je BRS vnímána jako orgán odpovědný nejen za přípravu bezpečnostních opatření, ale i za řešení krizí. Jejím primárním cílem je zajistit bezpečnost celého systému. [18]

Ministerstvo zahraničních věcí je vládním orgánem, který zodpovídá za zahraniční politiku. Rozvíjí koncepce, plánuje programy mezinárodní pomoci a dohlíží na mezinárodní obchod. Dále pak dohlíží na vztahy mezi Českou republikou a jinými národy, mezinárodními organizacemi a integračními organizacemi, koordinuje aktivity vyplývající z bilaterální a multilaterální spolupráce a řeší otázky částečně spadající do působnosti Ministerstva spravedlnosti. [19]

Ministerstvo obrany je významný státní orgán, který odpovídá za bezpečnost našeho státu. Mezi jeho hlavní funkci patří tvorba návrhů vojenské obranné politiky státu. Ministerstvo obrany například rozvíjí myšlenku operační připravenosti pro státní území, koordinuje činnost ústředních organizací, správních organizací, orgánů samosprávy a právnických osob, dohlíží na vojenské zpravodajství a obranné zpravodajství a zaručuje neprostupnost vzdušného prostoru České republiky a koordinaci vojenského a civilního leteckého provozu. [20]

Posledním uvedeným orgánem v této práci je Ministerstvo vnitra, které je pověřeno nad dohledem všech vnitřních záležitostí státu. Ministerstvo vnitra odpovídá například za veřejný pořádek, matriky, občanské průkazy, požární ochranu, cestovní doklady, územní členění státu, státní symboly, veřejné sbírky, telekomunikační systém Policie ČR pečlivě dohlíží na kryptografickou službu a v celosvětovém měřítku spolupracuje s Interpolem. [21]

1.5 Kybernetický prostor

Kybernetický prostor je definován jako globální doména v rámci informačního prostředí sestávající ze vzájemně závislé sítě infrastruktur informačních systémů včetně internetu, telekomunikačních sítí a počítačových systémů. [22]

Obecně o něm můžeme hovořit jako o virtuálním světě, který je tvořený spojeními mezi počítači, severy a dalšími komponenty internetové infrastruktury. Na rozdíl od internetu samotného mluvíme o kyberprostoru jako „místě“, které je těmito spojeními tvořeno. [23]

Kyberprostor označuje konkrétněji elektronické médium, které se používá k usnadnění online komunikace. Kyberprostor umožňuje uživatelům kromě mnoha dalších aktivit sdílet informace, komunikovat, vyměňovat si nápady, hrát hry, zapojovat se do diskuzí nebo sociálních fór, podnikat či vytvářet intuitivní média. [24]

1.5.1 Historie kyberprostoru

Termín kyberprostor poprvé zavedl autor William Gibson ve své knize Neuromancer z roku 1984. Gibson tento termín v pozdějších letech kritizoval a nazval ho „evokativním a v podstatě nesmyslným“. Přesto je tento termín stále široce používán k popisu téměř jakéhokoli zařízení nebo funkce, která je propojena s internetem. [24]

1.5.2 Kyberzločiny

Kyberzločin je jakákoli trestná činnost, která se týká počítače, síťového zařízení nebo sítě. Zatímco většina kyberzločinů se provádí za účelem vytvoření zisku pro kyberzločince, některé kybernetické zločiny jsou prováděny proti počítačům nebo zařízením přímo za účelem jejich poškození nebo deaktivace. Jiní používají počítače nebo sítě k šíření malwaru, nelegálních informací, obrázků nebo jiných materiálů. Některé kybernetické zločiny dělají obojí – tedy cílí na počítače, aby je infikovaly počítačovým virem, který se pak šíří do dalších strojů a někdy i do celých sítí. Primární cíl kybernetické kriminality je tedy finanční. [25]

Kyberzločin může zahrnovat mnoho různých typů trestné činnosti zaměřené na zisk, včetně ransomwarových útoků, e-mailových a internetových podvodů a podvodů s identitou, stejně jako pokusy o krádež informací o finančních účtech, kreditních kartách nebo jiných platebních kartách. Kyberzločinci se mohou zaměřit na soukromé informace jednotlivce nebo firemní data za účelem krádeže a dalšího prodeje. [25]

Kyberzločinci – od nepoctivých jednotlivců přes skupiny organizovaného zločinu až po státem sponzorované frakce – používají jako součást svých kybernetických útoků techniky jako phishing, sociální inženýrství a všechny druhy malwaru. Profesionalizace a šíření kybernetické kriminality každoročně zvyšuje nespočet nákladů na škody, což má dopad na jednotlivce, podniky, a dokonce i vlády. Odborníci odhadují, že škody způsobené kyberkriminalitou dosáhnou do roku 2022 6 bilionů dolarů ročně, což z ní činí jeden z nejlukrativnějších zločineckých podniků. [26]

Kyberzločin je zastřešující termín používaný k popisu dvou úzce propojených, ale odlišných oblastí trestné činnosti. Tzv. Cyber-dependant (volně přeloženo jako kyber-závislé trestné činy) jsou trestné činy, které lze spáchat pouze pomocí počítače, počítačových sítí nebo jiných forem informačních komunikačních technologií (ICT).

Zahrnují:

- nedovolené vniknutí a hackování do sítí
- narušení funkčnosti počítače šířením virů nebo jiného malwaru
- distribuované útoky odmítnutí služby (DDoS)

A „Cyber-enabled“ (Kyberneticky-povolené) trestné činy jsou na druhé straně tradiční trestné činy, jejichž rozsah nebo dosah lze zvýšit použitím počítačů, počítačových sítí nebo jiných forem ICT. [27]

Hlavní formy kybernetických zločinů by byly:

- sexuální zneužívání dětí
- podvody
- vydírání. [27]

Nezisková organizace Information Security Forum, která se sama označuje za „přední světovou autoritu v oblasti kybernetické, informační bezpečnosti a řízení rizik“, ve své každoroční studii Threat Horizon varuje před zvýšeným potenciálem pro:

- Narušení – přílišné spoléhání se na křehkou konektivitu vytváří potenciál pro předem promyšlené výpadky internetu, které mohou srazit obchod na kolena a zvýšené riziko, že ransomware bude použit k napadení internetu věcí.
- Zkreslení – záměrné šíření dezinformací, způsobuje ohrožení důvěry v integritu informací.
- Zhoršování stavu – rychlý pokrok v inteligentních technologiích a protichůdné požadavky vyplývající z vyvíjející se národní bezpečnosti a jednotlivých předpisů na ochranu soukromí negativně ovlivňují schopnost organizací kontrolovat své vlastní informace. [28]

1.5.3 Novinky v kyberbezpečnosti v roce 2022

Rozmach sociální inženýrství: oklamat člověka je mnohem snazší než prolomit bezpečnostní systém. 85 % všech úniků dat se týká lidské interakce. V roce 2022 pravděpodobně uvidíme, že útoky sociálního inženýrství, jako je phishing a předstírání identity v e-mailové komunikaci, se budou nadále vyvíjet, aby zahrnovaly nové trendy, technologie a taktiky. Například útoky související s kryptoměnami vzrostly mezi říjnem 2020 a dubnem 2021 téměř o 200 %.[29]

Vystavení třetím stranám: Kyberzločinci mohou obejít bezpečnostní systémy hackováním méně chráněných sítí patřících třetím stranám, které mají privilegovaný přístup k primárnímu cíli hackera. V roce 2022 se narušení třetích stran stanou ještě naléhavější hrozbou, protože společnosti se stále více obracejí na nezávislé dodavatele, aby dokončili práci, kterou zpracovávají zaměstnanci na plný úvazek. [29]

Špatná kybernetická hygiena: „Kybernetická hygiena“ označuje běžné návyky a postupy týkající se používání technologií, jako je vyhýbání se nechráněným Wi-Fi sítím a implementace bezpečnostních opatření, jako je VPN nebo vícefaktorové ověřování. Bohužel výzkumy ukazují, že návyky Američanů v oblasti kybernetické hygieny jsou často žalostné. Díky rozmachu práce na dálku jsou systémy chráněné slabými hesly nyní přístupné z nechráněných domácích sítí a hesla psaná často doslova „na kus papíru“ se dostávají do veřejných kaváren. a pracovníci se přihlašují na osobních zařízeních, u kterých je mnohem vyšší pravděpodobnost ztráty nebo odcizení. [29]

1.5.4. Vybrané zdroje kybernetických hrozeb

Jedním z možných zdrojů kybernetického ohrožení jsou vlády různých států. Jejich útoky mohou být různého typu od propagandy a drobných změn webových stránek až po závažná narušení funkce infrastruktury cíle spojená někdy i se ztrátou na životech (jako příklad uveďme nabourání se do řídícího systému jaderné elektrárny a zapříčinění masivního úniku radiace do okolí). Kupříkladu Spojené státy americké v dnešní době (a v blízké budoucnosti do cca 10let) považují za jediné strůjce kybernetických útoků schopné výrazně a dlouhodobě narušit jejich infrastrukturu právě některými státy

financované skupiny osob. Teroristické organizace i jednotlivci jsou dalším možným zdrojem kybernetických hrozeb. I v současné době se zdá, že jsou teroristé méně rozvinutí ve využití počítačových technologií, a tak fyzické útoky jsou pro ně stále ještě častější. S nástupem mladších generací, u kterých se předpokládá vyšší úroveň technické gramotnosti, do těchto skupin se v budoucnu očekává zvýšení nebezpečí od nich plynoucí. [30]

Dalším zdrojem hrozeb jsou průmyslový špióni a organizovaný zločin. Jsou považováni za středně závažnou hrozbu, a to zejména kvůli zaměření se na získávání citlivých firemních dat anebo na digitální krádeže velkých částek. Obecně se dá říci, že záměr této skupiny je zpravidla finanční obohacení. [30]

Samozřejmě zmíníme samotné hackery. Dají se popsat jako jednotlivci, kteří ilegální nabourávání do systému provozují zpravidla jako své hobby. Jen malý zlomek těchto jednotlivců je vybaven schopnosti a technologiemi, které mají potenciál ohrozit kritickou infrastrukturu, a ještě méně z nich k tomu mají dobrý důvod. Opět je zde výhled do budoucna s predikcí mladších generací, které jsou více sžití s moderními technologiemi a mají tak větší potenciál být hrozbou pro různé cíle. [30]

Samotní hackeři se dají rozdělit do několika skupin. Jednou z nich jsou málopočetné hackerské komunity, dále tvz. script kiddies (zpravidla velmi málo kvalifikovaní hackeři závislí na prostředcích a nástrojích schopnějších hackerů, jejich hlavním cílem je úspěch činnosti), tvůrci počítačových virů (hackeři zaměření na tvorbu malware ale ne na samotné prolamování infikovaných systémů, jejich cílem je většinou popularita), a na tvz. white hat a black hat (White hat, nebo také etničtí hackeři jsou profesionálové najímáni firmami k testování zabezpečení a hledání bezpečnostních děr. Black hat jsou opakem, tedy profesionálové, kteří jsou placeni za nabourávání systémů. Obě skupiny mají za cíl zisk.) [30]

1.5.5 Vybrané typy kybernetických hrozeb

1. Malware

Malware je škodlivý software, jako je spyware, ransomware, virus a červ. Malware se aktivuje, když uživatel klikne na škodlivý odkaz nebo přílohu, což vede k instalaci nebezpečného softwaru. Cisco uvádí, že malware po aktivaci může:

- Blokovat přístup ke klíčovým síťovým komponentám (ransomware)
- Instalovat další škodlivý software
- Skrývat získávání informací přenosem dat z pevného disku (spyware)
- Narušit jednotlivé důležité části systému, čímž se systém stane nefunkčním

2. Emotet

Cybersecurity and Infrastructure Security Agency (CISA) popisuje Emotet jako „pokročilý, modulární bankovní trojan, který primárně funguje jako downloader nebo dropper jiných bankovních trojanů. Emotet patří mezi nejdražší a nejničivější malware."

3. „Odepření služby"

Denial of service (DoS) je typ kybernetického útoku, který zaplaví počítač nebo síť, takže nemůže reagovat na požadavky. Distribuovaný DoS (DDoS) dělá totéž, ale útok pochází z počítačové sítě. Lze použít několik technik a někteří kybernetičtí útočníci využívají dobu, po kterou je síť deaktivována, ke spuštění dalších útoků. Podle Jeffa Melnicka z Netwrix, softwarové společnosti pro zabezpečení informačních technologií, je botnet typem DDoS, ve kterém mohou být miliony systémů infikovány malwarem a řízeny hackerem. Botnety, někdy nazývané zombie systémy, cílí a přetěžují schopnosti zpracování cíle. Botnety jsou v různých geografických lokalitách a je těžké je vysledovat.

4. „Člověk uprostřed"

K útoku typu man-in-the-middle (MITM) dochází, když se hackeři vloží do transakce dvou stran. Po přerušení výměny dat mohou podle Cisco filtrovat a krást data. K útokům MITM často dochází, když návštěvník použije nezabezpečenou veřejnou Wi-Fi síť.

Útočníci se vkládají mezi návštěvníka a síť a poté pomocí malwaru instalují software a škodlivě využívají data oběti.

5. Phishing

Phishingové útoky využívají falešnou komunikaci, jako jsou podvodné e-maily, aby příjemce oklamaly, aby jej otevřel a provedl pokyny uvnitř, jako je např. poskytnutí čísla kreditní karty. „Cílem je ukrást citlivá data, jako jsou kreditní karty a přihlašovací údaje, nebo nainstalovat malware do počítače oběti," uvádí Cisco.

6. SQL Injection

„Injekce" jazyka SQL (Structured Query Language) je typ kybernetického útoku, který je výsledkem vložení škodlivého kódu na server, který používá SQL. Při infikování server uvolní informace. Odeslání škodlivého kódu může být stejně jednoduché jako jeho zadání do vyhledávacího pole zranitelného webu.

7. Útoky heslem

Se správným heslem má kybernetický útočník přístup k velkému množství informací. Sociální inženýrství je typ útoku heslem, který Data Insider definuje jako „strategii, kterou používají kybernetičtí útočníci, která se silně spoléhá na lidskou interakci a často zahrnuje oklamání lidí, aby prolomili standardní bezpečnostní postupy. Mezi další typy útoků na hesla patří přístup k databázi hesel nebo prosté hádání.[31]

1.6 Kybernetická bezpečnost

Kybernetická bezpečnost je definována jako komplexní obrana sítí proti kybernetickým útokům a hrozbám, aby byla všechna data v bezpečí. [32]

Vzhledem k tomu, že kybernetická bezpečnost je stále mladé odvětví, je důležité přizpůsobit se jedinečným hrozbám. Česko a Evropská unie však pracují na hledání nových a účinných odpovědí a díky mezinárodní koordinaci a spolupráci jsme schopni

novou realitu reprezentovat v podobě dobře fungujících politik. Můžeme očekávat nástup zcela nových a inovativních technologií, jako jsou kvantové počítače nebo umělá inteligence, které budou mít velký dopad na využívanou kryptografii a další oblasti, protože se jedná o neustále se měnící odvětví. [33]

Evropská komise v prosinci 2020 představila Novou strategii kybernetické bezpečnosti EU, jejímž cílem je zabezpečit globální a otevřený internet využitím a rozvojem všech prostředků a zdrojů k zajištění bezpečnosti a zachování evropských hodnot a základních práv. [33] Tento plán obsahuje seznam strategických iniciativ a v současné době se připravuje řada zásadních dokumentů. Za povšimnutí bezesporu stojí tzv. novela směrnice NIS2 o bezpečnosti sítí a informačních systémů. Původní směrnice byla vydána v roce 2016, ale již není použitelná protože nereaguje na nová nebezpečí z důvodu rychlého pokroku v oblasti digitalizace. Jedním z jejích cílů je poskytovat standardní stupeň kybernetické bezpečnosti v celé EU. Oblasti, jako je veřejná správa, kosmický výzkum, farmaceutická výroba a správa vodovodních a odpadních sítí, by měly být zahrnuty do nové úpravy. Novela vymezuje životně důležité sektory a zavádí minimální stupeň kybernetické bezpečnosti na jejich ochranu před útoky. [33]

Další oblastí, která zvyšuje a zlepšuje spolupráci expertů v oblasti kybernetické bezpečnosti, je Společná kybernetická jednotka (JCU), kterou doporučila Evropská komise. Cílem jednotky bude maximálně využít zdroje a dovednosti, které mají k dispozici jednotlivé členské státy a EU jako celek. Díky sdílené platformě a know-how bude možné se vyhnout potenciálním kybernetickým událostem a krizím, bojovat s nimi a reagovat na ně. JCU usnadní spolupráci aktérů kybernetické bezpečnosti z mnoha sektorů, včetně občanské společnosti, diplomatických komunit a komerčního sektoru. Tito specialisté obvykle jednají sami, ale JCU jim poskytne virtuální a fyzickou platformu pro spolupráci: příslušné orgány, orgány a agentury EU ve spolupráci s členskými státy budou moci postupně vybudovat evropskou platformu pro solidaritu a pomoc při rozsáhlých kybernetických útocích. [33]

1.6.1. Evropská připravenost v oblasti kybernetických hrozeb

Od roku 2017, kdy Evropou otřásla řada významných kybernetických útoků, byly politiky EU v oblasti kybernetické bezpečnosti v centru pozornosti. Málokdo si však uvědomuje, co je to kybernetická válka, jak bojovat s kyberzločiny a jakou roli v tom všem hraje EU, pokud vůbec nějakou. Politika kybernetické bezpečnosti Evropské unie se zabývá zejména dvěma problémy: kybernetickou kriminalitou, jako jsou třeba online podvody, a kybernetickými útoky, jako je například nabourání se do řídícího systému subjektu kritické infrastruktury. Kyberzločiny jsou ziskový byznys, který neustále roste. Státní i nestátní aktéři mohou pro členské státy EU představovat kybernetické nebezpečí. [32]

Četnost kybernetických útoků proti institucím EU roste exponenciálně. Úroveň přípravy na kybernetickou bezpečnost se v jednotlivých institucích EU liší, ale vzhledem k eskalujícím hrozbám je často nedostatečná. Protože jsou členové EU tak propojeni, narušení bezpečnosti jednoho by mohlo jiného vystavit bezpečnostním rizikům. Vyplývá to ze speciální studie týmu EU z roku 2022, která hodnotí, jak dobře jsou řídící orgány EU připraveny čelit kybernetickým hrozbám. Mezi lety 2018 a 2021 vzrostl výskyt významných kybernetických bezpečnostních incidentů v orgánech EU více než desetinásobně; práce na dálku značně rozšířila počet potenciálních přístupových bodů pro hackery. [34]

Evropská léková agentura se stala terčem jednoho z těchto útoků, při kterém byly upraveny citlivé materiály s cílem poškodit důvěru veřejnosti v očkování proti COVID-19. [34]

Evropská komise v dubnu 2022 navrhla nařízení požadující, aby organizace EU vytvořily rámec pro efektivní řízení rizik kybernetické bezpečnosti. Rozhodnutí přichází vzhledem k přetrvávajícímu nebezpečí kybernetických útoků, které se s největší pravděpodobností zaměří na vlády a subjekty kritické infrastruktury. Jedním z hlavních důvodů pro toto rozhodnutí je invaze Ruska na Ukrajinu a s ní spojená připomínka toho, co můžou kyberútoky napáchat na vládní a kritické infrastruktuře. [35]

Politika kybernetické bezpečnosti Evropské unie, která byla zahájena v roce 2013, má za cíl vytvořit nejbezpečnější internetové prostředí na světě a s cílem podpořit růst

digitální ekonomiky. Návrh plánu byl zveřejněn na začátku roku 2013 ve dvou částech, z nichž první je sdělení Evropské komise pro zahraniční věci a bezpečnostní politiku o strategii kybernetické bezpečnosti EU. Druhou částí je návrh směrnice o bezpečnosti sítí a informací od Evropské komise, která je jednou z nejvýznamnějších strategických směrnic o kybernetické bezpečnosti pro budoucnost EU. [36]

Spolu s konvenčními oblastmi konfliktů vzduchu, země a moře uznalo NATO v roce 2016 kyberprostor jako další možnou oblast vojenských operací. Úsilí NATO v kyberprostoru, stejně jako ve všech ostatních oblastech, je obranné, přiměřené a v souladu s mezinárodním právem. Spojenci věří, že kybernetický prostor, který je předvídatelný, otevřený, svobodný a bezpečný bude prospěšný nám všem. I když je každý spojenec odpovědný za svou vlastní kybernetickou obranu, NATO poskytuje spojencům prostředí, kde se mohou radit o záležitostech kybernetické obrany, sdílet informace o kybernetických hrozbách, diskutovat o osvědčených postupech a koordinovat úsilí. [37]

"V současnosti neexistuje žádná hrozba bez kybernetické složky" - Jens Stoltenberg, generální tajemník NATO. [38]

"Kybernetické hrozby patří mezi největší hrozby nejen pro Evropu, ale pro celý svět" cit. Casper Clynge, viceprezident Microsoftu pro záležitosti evropských vlád. [38]

V roce 2002 na zasedání NATO v Praze se poprvé lídři jednotlivých zemí rozhodli zaměřit se na zesílení obranných schopností aliance proti kybernetickým útokům. Od té doby se kyberbezpečnost stala čím dál více debatovaným tématem na dalších summitech. V roce 2008 ustanovili členové první politiku NATO v otázkách kyberbezpečnosti a v roce 2014 se kyberobrana stala jedním z hlavních částí kolektivní obranné strategie NATO, ustanovilo se tehdy totiž, že kyberútok může vést k invokaci klauzule o společné obraně. [39]

I přes to, že V boji proti škodlivým kybernetickým aktivitám učinilo NATO a jeho spojenci značný strategický, operační a technický pokrok musí Aliance neustále vyhodnocovat, zda se přizpůsobuje a správně reaguje s ohledem na přetrvávající výzvy a dynamickou povahu kybernetických hrozeb. [39]

V poslední době se kybernetická kriminalita projevila jako reálná hrozba s citelnými následky ve fyzickém světě. Například v nedávné minulosti Íránští hackeři napadli Izraelské vodní zařízení kde se jim téměř povedlo zvýšit obsah chloru v pitné vodě na toxickou úroveň. Dalším příkladem je jeden z kyberútoků v souvislosti invaze Ruska na Ukrajinu - Rusko zaútočilo na satelitní sít Viasat se záměrem narušení přenosu a výroby elektřiny v Německu s následným poškozením Ukrajinských komunikačních kanálů. Vzhledem k tomu, že operace v kyberprostoru – jak destruktivní útoky, tak dezinformace – je stále komplexnější a v některých případech dokonce nahrazují konvenční kinetické operace, musí NATO svůj pohled na tuto problematiku změnit. [40]

1.6.2 Národní strategie kybernetické bezpečnosti České republiky

Moderní technologie a internet se stali součástí našeho každodenního života. Probíhající digitalizace české společnosti posiluje naši ekonomiku, konkurenceschopnost a celkový blahobyt. To všechno znamená vyšší nároky na kybernetickou bezpečnost. Díky technologickému pokroku nyní žijeme v době nepředvídatelně nestabilních bezpečnostních podmínek a bouřlivých společenských transformací. [46]

Strategie České republiky v oblasti kybernetické bezpečnosti byla od počátku postavena na úspěšném modelu spolupráce všech aktérů na národní i mezinárodní úrovni, přičemž každá organizace má vymezené odpovědnosti a potřebnou pravomoc. V poslední době kybernetická bezpečnost nabyla na významu a stala se předmětem zahraniční politiky. Národní strategie kybernetické bezpečnosti bude usilovat o dosažení co největšího stupně bezpečnosti v kyberprostoru. Budou vytvořeny podmínky pro bezproblémový chod informační společnosti. Kybernetická bezpečnost bude nadále zásadní pro ochranu nejen nejdůležitějších součástí naší infrastruktury, ale také všech ostatních sítí a systémů, což umožní jednotlivcům rozvíjet své aktivity a vládě dosáhnout ekonomických a sociálních cílů. [46]

Bezpečnostní složky státu a organizace veřejné správy jsou klíčovými skupinami této strategie. Strategie vzdělává a informuje ostatní části české společnosti, aby pochopily opatření přijatá vládou sloužící k řešení kybernetických nebezpečí a hrozeb. Plán je rozdělen do tří hlavních vizí. První se nazývá sebevědomí v kyberprostoru, druhá vize stabilní a spolehlivá partnerství a poslední třetí vize silnější společnost 4.0. Akční plán kybernetické bezpečnosti ČR na odbobí 2021–2025 obsahuje časové plnění z konkrétních aktivit, které jsou v tomto plánu stanoveny. [46]

1.6.2.1 Bezpečnostní prostředí

Bezpečnostní prostředí v České republice je tvořeno řadou faktorů, díky nimž se provádí zahraniční politika. Vzhledem k tomu, že Evropa a euroatlantický region jsou vystaveny velkým bezpečnostním obavám a hrozbám z východu a širšího jihu, bezpečnostní prostředí v současnosti prochází podstatnými změnami. [47]

Tendence mnoha konvenčních bezpečnostních problémů přenášet se zcela nebo alespoň částečně do kyberprostoru je stále přítomná, což vytváří další nebezpečí jedinečná pro toto prostředí. Navíc dochází k intenzivnějšímu prolínání různých nebezpečí a hybridizaci bezpečnostního prostředí, jehož dynamiku zvyšuje právě internet a současné technologie. Kyberprostor je intenzivně využíván pro prosazování státních zájmů v zahraniční politice. České vládní instituce jsou dlouhodobě primárním cílem kybernetické špionáže. Česká republika a její strategické zájmy jsou pak po úniku informací ohroženy při diplomatických jednáních. Cílem státních aktérů jsou zejména orgány veřejné moci, dále pak malé podniky s cennými odbornými znalostmi, univerzity a výzkumné ústavy. Dochází k nárustu průmyslové špionáže, která může mít dopad na naši konkurenceschopnost. V tomto ohledu je pro Českou republiku zásadní soustředit se nejen na problémy týkající se kybernetické bezpečnosti, ale adaptovat se na nové prostředí, které se neustále vyvíjí. K tomu, aby dokázala čelit nově vznikajícím kybernetickým hrozbám musí hledat nové způsoby a mít potřebné schopnosti. [46]

1.6.2.2 Zajišťování kybernetické bezpečnosti v ČR

Za řízení, provoz a údržbu celého bezpečnostního systému v České republice odpovídá vláda České republiky, která je nejvyšším výkonným orgánem. Národní úřad pro kybernetickou a informační bezpečnost je odpovědný za řízení kybernetické bezpečnosti a slouží jako vedoucí správní orgán. [46]

Dohlíží také na kryptografickou ochranu a zabezpečení citlivých dat ve vztahu k informačním a komunikačním sítím. Jeho dosah se řídí zákony o kybernetické bezpečnosti, ochraně utajovaných informací a bezpečnostní způsobilosti. Úřad má také na starost satelitní systém Galileo. Dále se pak na systému zajišťování kybernetické bezpečnosti podílí například ministerstvo zahraničních věcí, zpravodajské služby, ministerstvo průmyslu a obchodu, Český telekomunikační úřad, Ministerstvo vnitra, Ministerstvo školství, mládeže a tělovýchovy a mnoho dalších institucí. [46]

V souladu se zákonem č. 181/2014 Sb. o kybernetické bezpečnosti a jeho prováděcími předpisy hrají vládní týmy typu CERT (GovCERT.CZ) a CSIRT zásadní roli při ochraně informační infrastruktury a významných informačních systémů. Každý národ, jehož klíčové systémy jsou připojeny k internetu, musí být schopni řešit bezpečnostní problémy, reagovat na události, plánovat akce k jejich řešení a předcházet nehodám. Mezi povinnosti těchto týmů patří zejména sloužit jako hlavní zdroj bezpečnostních informací ve prospěch lidí, organizací a vládních úřadů. Oba významně přispívají ke zvyšování povědomí o otázkách bezpečnosti internetu. [48]

Úlohou armády bylo vždy primárně vedení války. Po pádu východního bloku došlo k podstatnému snížení pravděpodobnosti rozsáhlých konvenčních bojů a k prudkému nárůstu tendencí, které využívají vojenské síly k jiným činnostem, než jsou ty, které měly čistě vojenský charakter. A tento trend stále pokračuje. Přístup v České republice, který je zakotvený ve Vojenské strategii ČR a Doktríně Armády ČR říká, že armáda může vést vojenské operace po celém světě a proti jakékoliv bezpečnostní hrobě, avšak za předpokladu, že k tomu bude vyzvána v rámci NATO. V zákoně č. 219/1999 Sb., o ozbrojených silách České republiky najdeme zmíňku o převzetí povinností od Policie ČR,

pokud síly a prostředky ČR budou nedostatečné k udržení pořádku a bezpečnosti. Armáda má tedy přístup k řadě aktivit, na nichž se může podílet, včetně těch v kyberprostoru. [49]

Armáda České republiky byla nucena se na tuto realitu připravit poté, co byl digitální svět uznán jako bojiště. Bitevní pole se stále více digitalizuje a robotizuje, a tak se více začala využívat virtuální realita a umělá inteligence. [51]

Armáda České republiky se musela začít soustředit především na využití výpočetní techniky, a to nejen jako nástroje pro zpracování dokumentů, ale také na využití kapacit informačních systémů pro podporu některých pracovních procesů, jako je proces plánování a rozhodování. [50] V kyberprostoru neboli v informační doméně mají zpravodajské služby velmi významnou roli. V kyberprostoru nelze vždy jasně rozlišit mezi vnějším a vnitřním útokem, také je velmi obtížné určit o jaký typ útoku se jedná, zdali jde například o teroristický, kriminální nebo špionážní čin. Zpravodajské služby jsou určeny k tomu, aby se podílely na ochraně státu před všemi druhy hrozeb. Jedinou zpravodajskou službou, která působí v našem státě i v cizině je Vojenské zdravotnictví. Vojenské zpravodajství a ozbrojené síly jsou součástí resortu Ministerstva obrany. V novele zákona č. 289/2005 Sb., o Vojenském zpravodajství se říká, že Vojenské zpravodajství se podílí na kybernetické obraně státu. [51]

Dne 1. srpna 2016 se Útvar pro odhalování organizovaného zločinu SKPV a Útvar odhalování korupce a finanční kriminality SKPV sloučily a staly se Národní centrálou proti organizovanému zločinu Služby kriminální policie a vyšetřování (NCOZ SKPV). NCOZ SKPV slouží jako ředitelství pro kriminalistické a policejní útvary na území ČR, zaměřuje se především na identifikaci závažné hospodářské kriminality, kybernetické kriminality, terorismu nebo extremismu. Je to podstatné národní kontaktní místo pro kybernetickou kriminalitu. [52]

1.7 Informační válka

Informační válkou je nazývána akce používaná k přelstění protivníka a získáním informačních výhod. Kontrola vlastního informačního prostoru, zabezpečení přístupu k vlastním informacím, shromažďování a využívání informací protivníka, deaktivace jeho informačních systémů a zasahování do toku informací, to vše jsou součástí této strategie. [41]

Informační válka není novým fenoménem, i když se vyznačuje špičkovými technologickými pokroky, které způsobují rychlejší šíření informací. Informační bitva v souvislosti s rusko-ukrajinským konfliktem a ruskou anexi Krymu v roce 2014 vzbudila v poslední době velkou pozornost. [41]

Informační válka je stále více chápána jako prvotní útok předtím, než dojde k fyzickému útoku. Armády po celém světě zaměstnávají čím dál více specialistů na informační technologie. [42]

V minulosti se používala pouze jako způsob podpory; například během první světové války byly nepřátelským silám rozesílány letáky povzbuzující k odporu. Taktika tvrdého boje se v posledních letech jednoznačně změnila ve prospěch rychlého růstu různých typů informační války. Slovní spojení „informační válka“ se často používá zaměnitelně se slovním spojením „kybernetická válka“, které se na druhou stranu označuje pouze konflikty vedené pomocí výpočetní techniky a počítačových sítí. [43]

Informační válka je podle Severoatlantické aliance využívání a manipulace s informacemi, aby jedna strana konfliktu získala převahu nad druhou. V informačním válčení dochází ke shromažďování taktických informací, zajišťování přesnosti vlastních informací, šíření propagandy a nepravdivých informací s cílem demoralizovat nepřítele a obecnou populaci, snižovat kvalitu informací protivníka a bránit mu v jejich sběru. [44]

1.7.1 Operační a informační prostředí

Válčení je vždy zásadně ovlivněno prostředím, ve kterém se bojuje. Válčení vždy záviselo na informacích. Informace jsou pro vojenské operace a vedení války obecně stále důležitější, stejně jako pro všechny aspekty lidské civilizace. Státy a ozbrojené síly musí být schopny porozumět, orientovat se v informačním prostředí a úspěšně v něm pracovat, aby mohly provádět současné bojové a vojenské operace. [44]

Definujme zde pojem „operační prostředí“. Je to prostředí, ve kterém se vojenské operace odehrávají, a zahrnuje nejen region, kde operace probíhá, ale také všechny aspekty, které mohou mít potenciálně vliv na průběh operace. Operační prostředí je kompletní soubor geografického prostoru a ostatních faktorů a je součástí širšího bezpečnostního prostředí, které navíc zahrnuje prostor i ostatní faktory mající vliv na celkovou bezpečnost daného státu. Největší vliv na zvýšení významu informačních aktivit ve vedení války mají změny v operačním prostředí. Očekává se, že rostoucí počet asymetrických a nepravidelných válek, kde alespoň jedna z válčících stran není státem, nahradí tradiční ozbrojené konflikty mezi státy, tvrdí řada vojenských teoretiků, kteří tento trend v posledních letech předpovídají. To však, ale neznamená, že můžeme v budoucnu vyloučit možnost konvenčního střetu.[44]

Pojem „informační prostředí“ označuje oblast, kde dochází k manipulaci s informacemi, a kde komunikace probíhá výhradně elektronickými kanály. Informační chování můžeme charakterizovat jako „složený systém interakcí, hmoty, energie a informací v čase, kde probíhají informační procesy, zejména při využívání informací“. Armáda definuje vojenský informační prostor jako součást globálního informačního prostoru tvořeného vlastními, spojeneckými a nepřátelskými informačními systémy, vojenskými i civilními, které podporují vojenské operace nebo mají vliv na probíhající operaci. [45]

Oficiální vojenská politika Severoatlantické aliance pro informační operace, která byla schválena Vojenským výborem NATO, popisuje současný stav informačního prostředí a jeho dopad na způsob vedení vojenských operací a bitev. Definice Severoatlantické aliance zní: *„Informační prostředí zahrnuje samotné informace,*

jednotlivce, organizace a systémy, které přijímají, zpracovávají a přenášejí informace; a kognitivní, virtuální a fyzický prostor, ve kterém se vše odehrává.“

Informační prostředí zahrnuje i kybernetický prostor. *„Jedná se o imaginární prostředí, ve kterém jsou digitalizované informace přenášeny počítačovými sítěmi.“* [44]

1.7.2 Typy informační války

Velení a řízení, zpravodajství, elektronická válka, psychologická válka, ekonomická informační válka, diplomatická válka, hackerská válka a konečně kybernetická válka jsou některé z mnoha druhů, které se v informační válce kombinují a doplňují.[43]

1) Válka „Vedení a řízení“ je druhem informační války, která se opírá o myšlenku, že jsou dvě možnosti, jak odříznout tok informací od velení k vojenským jednotkám. První možnost je útok na „hlavu“, neboli „dekapitace“. Jedná se o snahu elektronického útoku přímo na velení na velící informační zázemí. Druhou možností je útok na tzv. „dveře“, tedy komunikační kanály mezi velením a jednotkami.
2) Válka ve zpravodajství, anglicky inteligence warfare, je zaměřená na hledání cílů, hodnocení válečných cílů, na prevenci překvapení a další. [3]
3) Elektronická válka je druh konfliktu, kde se strany snaží za použití různých způsobů ovlivnit nepřátelská elektronická zařízení a systémy, včetně těch vojenských. Do elektronické války patří i využití elektromagnetických energií k přímému narušení funkce elektronických systémů nepřítele. [3]
4) Termín psychologická válka se dá stručně vysvětlit jako využití informací proti lidské mysli. Psychologická válka je velmi důležitým druhem, a to si uvědomují státní i nestátní aktéři. Například USA psychologickou válku považuje za součást každého ozbrojeného konfliktu. [3]
5) Hackerské válčení je další formou informační války. Nejčastěji se jí účastní jednotlivci. Udává se, že nejčastěji je hackerským cílem blokace nebo změna obsahu konkrétní webové stránky. Dopady hackerského útoku se odvíjejí od počtu zapojených hackerů a od koordinovanosti útoků. [3]

1.8 Dezinformace (fake news) a konspirační teorie

Termín fake news a dezinformace je úzce spjat s vývojem v médiích za posledních 30 let. Dříve každý vydavatel novin nebo časopisů odpovídal za pravost informací dle etických standartů zpravodajství a žurnalistiky. Naprostá většina lidí v populaci byli pouze příjemci těchto informací. Na zveřejňování informací (noviny, časopisy) byli potřeba finance. Všechna omezení zmizela se vznikem informační společnosti. Dostupnost internetu a stránek sociálních sítí umožnili všem uživatelům vytvářet obsah kdekoli a kdykoli bez potřeby finančních zdrojů nebo ověřování informací. Čtenář se stal tvůrcem obsahu (blogy, kanály YouTube, alternativní webové stránky). Každý čtenář by měl být schopen rozeznat, které informace jsou pravdivé, a které nikoliv. Značná část populace však postrádá dovednosti potřebné k vyhodnocování informací a nechá se snadno ovlivnit dezinformacemi, hoaxy nebo fake news. Nepravdivé informace se začaly šířit mnohem rychleji a více než kdykoli v minulosti se zavedením nových médií, zejména sociálních sítí. [53]

Propaganda, lži, hoaxy, manipulace a dezinformace, to všechno jsou historické fenomény. Propaganda v mnoha podobách a šíření nepravdivých a zkreslených informací hrálo roli v téměř každé světové válce, stejně jako v předvolebních a povolebních konfliktech v řadě politických systémů (např. KLDR, Kuba, Čína) . Informace byly šířeny tiskem, rozhlasem a televizí, ke kterým měla přístup pouze malá skupina spotřebitelů, a proto se infomace šířily pomaleji než nyní. V 90 letech minulého stolení nastal zlom, kdy se k šíření hoaxů začal využívat e-mail. [55]

Hoax je popisován jako výstražná zpráva, která varuje například před fiktivní hrozbou, počítačovým virem, žádá o pomoc nebo má za účel pouze pobavit. Velmi často se jedná o zprávu, která je přeposílaná jako řetězová zpráva. Hoax je nejčastěji identifikován právě pomocí žádosti o přeposlání. Anglický výraz, z něhož je slovo „hoax“ odvozeno, v překladu znamená „falešné zprávy“, „mystifikace“, „novinářská kachna“, „poplachová zpráva“, „výmysl“ a „kanadský vtip“. Cílem hoaxu je podněcování teroru, šíření nepravdivých informací, ovlivňování veřejného mínění, poškozování společnosti, značky nebo produktu. [54]

Je známo mnoho případů, kdy se podvodníkům díky hoaxu podařilo vylákat finanční hotovost. V těchto případech nezbývá nic jiného, než se obrátit na policii a případ nahlásit. Je třeba vzít v úvahu skutečnost, že metody podvodníků jsou velmi sofistikované a že peníze jsou obvykle přesouvány do zemí, kde i přes maximální úsilí úřadů nelze peníze právně vymáhat. V těch lepších případech si člověk může šířením hoaxu poškodit svou pověst v očích svých přátel a ostatních uživatelů, kteří si ověří pravdivost zprávy, než ji znovu rozešlou. Hoaxy bychom měli smazat nebo označit jako spam, nepřeposílat dále a neotevírat přílohy. [54]

Dalším významným pojmem je misinformation neboli mylná informace. Tento pojem je velmi často chápán jako dezinformace. Avšak mezi těmito dvěma pojmy je jeden zásadní rozdíl. Dezinformace jsou šířeny záměrně s úmyslem ublížit, zatímco misinformation jsou šířeny omylem bez zlého záměru. Velmi známým příkladem je fotomontáž zobrazující delfíny v Benátkách během první koronavirové krize. Problém nastává ve chvíli, kdy obrázek někdo nečestně využije a dále interpretuje. Může se pak dostat do široké veřejné distribuce, a z nepravdivé informace se rázem stává dezinformace. [63]

Deepfake neboli software pro umělou inteligenci je navržen tak, aby uměl vytvářet falešné fotografie či filmy, která působí skutečně. Deepfake je velmi často využíván k propagaci dezinformací, jelikož je obtížně rozpoznatelný od reality. [86] Deepfakes jsou nejčastěji obrázky nebo videa, která jsou upravena tak, aby zobrazovala tvář jiné osoby. Fungují jako vylepšená verze záměny obličejů. Navzdory skutečnosti, že se jedná o falešná videa, většina z nich působí reálným dojmem. Deepfakes byli zpočátku nejčastěji využívány ve falešné pornografii. Postupem času se začali rozšiřovat do politiky, hudebního, ale i komerčního prostředí. [87]

Nejznámějším příkladem byla pornografická videa, kde byl obličej herce nahrazen obličejem známé osobnosti. Nebo videa politiků, kteří na videu říkají věci, které nikdy neřekli. Videa či obrázky značně pomáhali k šíření hoaxů, nepravdivých informací a dalších forem podvodů. Většina dnešních deepfakes je při troše pozornosti relativně lehce odhalitelná. [57]

Fake news je nový pojem pro dezinformace. Jedná se o nepravdivé nebo zavádějící informace, které jsou zveřejňovány v médiích nebo na platformách sociálních médií. V důsledku toho jsou některé informace, které tato sdělení poskytují, nepřesné nebo klamavé. Autoři těchto informací chtějí ovlivnit nebo zmanipulovat příjemce. Dezinformace mají za cíl na rozdíl od hoaxů manipulovat lidmi. Tvůrci dezinformací mohou být i vlády některých států, kteří chtějí oklamat své protivníky nebo ovládnout vlastní obyvatelstvo. [57]

Tvůrci dezinformací používají média, aby ovlivnili politiku nebo názory jednotlivců. Cílem autora dezinformace je, aby se příjemce zaměřil na jiné téma, většinou takové jaké sám určil autor samotné dezinformace. Zprávy mají zmást a přesvědčit příjemce sdělení, aby změnil svůj názor. V dnešní době dezinformační kampaň obvykle začíná informací v nepopulárních médií. Sdělení by proto mělo být dostatečně důležité a přesvědčivé, aby se dostalo do mainstreamových médií. Pokud se tomu tak stane, je dezinformační kampaň považována za úspěšnou. Téměř každý den se v médiích objevují dezinformace (fake news), kdy k jejich šíření výrazně napomohl internet a sociální sítě. Vše, co člověka vytrhne z každodenní práce, včetně skandálů, senzací a zločinů, je často medializováno. [57]

Autoři těchto článků se neomezují standardy etických přístupů k žurnalistice a vrtají se do soukromých životů známých osobností, překrucují pravdu nebo si vymýšlejí. Dezinformace, se kterými se setkáváme, mohou být nebezpečné a mají mnohem větší dopad na naše myšlení, než si možná uvědomujeme. Tyto informace říší nepravdivá obvinění, nenávist, strach a mohou podporovat extremistické tendence. [57]

Dalším velmi podobným dezinformačním fenoménem jsou konspirační teorie. Konspirační teorie jsou příběhy o spiknutí. Hlavní myšlenkou těchto příběhů je, že náš život má na starosti jiný člověk nebo, že nám někdo zkresluje určité události. Lidé mají tendence pochopit dění na naší planetě a proto věří v konspirační teorie. Velmi často, když člověk něčemu nerozumí a současně k tématu nemá dostatek informací má tendence se uchýlit k přiřazování mystických vlastností, vymýšlení si nebo popisování věcí po svém.

Konspirační teorie všech typů budou do budoucna sofistikovanější a nepochybně jich bude přibývat. možná budou i složitější. Zejména političtí aktéři je budou využívat, jelikož se jedná o jednoduchou a nenákladnou techniku, jak narušit důvěru veřejnosti v zavedenou autoritu a podnítit konflikty mezi občany nebo alespoň znejistit obyvatelstvo. [57]

Konspirační teorie se teprve nedávno začali používají v moderní verzi propagandy. Událost sestřelení letadla MH17 na východní Ukrajině v roce 2014 byla úplným začátem. V podstatě ihned se čtenář mohl setkat s několika verzemi o vzniku události. Rusko, Ukrajinská republika a proruští separatisté začali házet vinu jeden na druhého. Začali se objevovat také spekulace, že události se zůčastnili NATO a USA. Hlavní myšlenkou konspiračních teorií o sestřelení letounu bylo ospravedlnění vojenské akce na Ukrajině. Zároveň se začali také objevovat fámy o tom, že letadlo se v regionu vůbec nevyskytovalo a trosky byly falešné. [57]

1.8.1 Od propagandy k fake news

„Cílem moderní propagandy není jen dezinformovat nebo vám vnutit cizí názory. Jde o to vyčerpat kritické myšlení a zcela vymazat pravdu.“ [57]

Pojem „propaganda“ pochází z latinského Sacra Congregatio de Propaganda Fide, což byl dozorčí výbor zřízený Vatikánem v roce 1662 pro propagaci římskokatolické víry. Termín rychle ztratil svou neutralitu v kontextu protireformace a získal hanlivý nádech, který přetrvává dodnes. Propaganda je obecně definována jako systematické šíření informací a myšlenek, především neobjektivním nebo zavádějícím způsobem, za účelem

prosazování nebo podpory politické kauzy nebo názoru. V aktuálním kontextu mezinárodního vývoje je pojem propaganda nejčastěji spojován s politickým přesvědčováním a psychologickou válkou – ta je definována jako použití propagandy proti protivníkovi s cílem zlomit jeho vůli bojovat nebo se bránit, případně jej naklonit vlastní pozici. Metody propagandy se neustále mění. Použití propagandy mohou vyžadovat aktéři z různých důvodů a okolností. [56]

Sílu propagandy pochopilo mnoho států a začalo ji velmi využívat, a to nejen Rusko, ale i státy západní Evropy. V roce 1939 Velká Británie založila ministerstvo informací, které mělo na starost cenzuru a propagandu. Na veřejnost se díky cenzuře dostaly pouze zprávy, které prospívaly strategickým cílům Británie a nesnižovaly bojového ducha obyvatel. Podobně propracované projevy používali přední politici. Německé vyhlášení války premiéra Nevilla Chamberlaina bylo pro svou morální přitažlivost a zobrazení boje proti zlu nakonec velmi silnou propagandou. Winston Churchill se svými projevy na toto navázal. Říkalo se o něm, že zmobilizoval Angličtinu a poslal ji do bitvy. [62]

Propaganda se dělí na tři kategorie, které se liší stupněm důvěryhodnosti a agresivity. Bílá propadanda je nejméně problematickým typem, jelikož informace a finanční prostředky jsou zřejmé. Příkladem bílé propagandy mohou být orgnizace, které vyzdvihují veganskou stravu. Druhým typem je tzv. černá propaganda, která využívá klamavé a nepřesné informace k ovlivnění cílových skupin. Posledním typem je pak šedá propaganda, která se nachází na pomezí bílé a černé. Dezinformace a propaganda spolu úzce souvisí. Zejména v černé propagandě mají dezinformace jasnou roli. Dopad propagandy může být mnohem silnější než dříve, a to díky pokroku současných technologií a používání dezinformačních nástrojů (např. fake news apod.). [63]

1.8.2 Dezinformace a jejich význam

Za ovlivňování našeho chování je především zodpovědný reklamní byznys, který k tomu využívá stovky různých strategií. Cílem dezinformací je přesvědčit nás pomocí lží. Organizace šířící dezinformace používají klam, aby ovlivnily naše názory a činy. Záměrně se vyhýbají používání konvenčních rozhodovacích procesům ve snaze dosáhnout určitého cíle. Následujících pět příkladů ukazuje, jak lze využít dezinformace

k mnoha účelům. Slouží také jako příklad toho, jak lze cíle a taktiky kombinovat různými způsoby. Namísto očekávání komplexního a systematického souboru technik, které lze využít v boji proti dezinformacím kvůli jejich proměnlivé povaze, je zásadní nejprve pochopit jejich cíl a základní komunikační komponenty. [72]

1. Ekonomický

Kampaně na šíření dezinformací mají finanční cíle. Například tzv. clickbait se pokouší zvýšit počet „kliknutí“. Používají titulek nebo jiná multimédia, které klamavě předvědčují čtenáře, aby navštívili konkrétní web. Mnoho webových stránek může být infikováno malwarem nebo jinými formami sledovacího softwaru. [72]

2. Protože mohu

Cílem dezinformační aktivity je riskantní nebo obtížný úkol. Podobné jednání vychází z „hackerské“ nebo „hráčské“ mentality. Nejdůležitější je rozsah úkolu, vlastní výhoda a získání obdivu ostatních. Mezi sekundární následky pak může patřit nabourání se do kritických systémů, únik důvěrných materiálů, zneužití algoritmů či jiných digitálních systémů a také neetické používání uživatelských dat k lepšímu zacílení dezinformací, například u reklam viditelných pouze vybraným uživatelům. [72]

3. Diskreditace

Dezinformační kampaně mají poškodit důvěryhodnost, spolehlivost a pověst. Šiřitelé dezinformací se pomocí nepravd snaží ublížit určitému jednotlivci nebo skupině. Někdy také dochází k diskreditaci konkrétní organizace, na jejíž službách je závislá určitá skupina příjemců. Jedním z nejčastějších cílů dezinformačních aktivit je právě diskreditace. [72]

4. Polarizace:

Dezinformační kampaně mají za cíl prohloubit již existující rozdíly jejich rozšířením. Šiřitelé dezinformací využívají probíhající konverzace a vkládají do ní falešný obsah s cílem vyvolat reakci na obou stranách a zmenšit tak prostor pro rozumný kompromis. Cíle jsou obvykle politické nebo sociální. Mezi možné důsledky patří poškození pověsti

nebo důvěryhodnosti, časté hádky spíše než konstruktivní rozhovory zahájené například online trolly, ostřejší polarizace politického diskurzu způsobená například vytahováním citlivých témat. [72]

5. Operace zahrnující informační vliv:

Účelem dezinformačních aktivit je ohrozit národní bezpečnost a prosperitu. Dezinformace jsou typicky šířeny nepřátelskými státy nebo nestátními aktéry. Dezinformace mají často negativní dopad na to, jak různé sociální skupiny vnímají vládní instituce. Důsledky by mohly zahrnovat ovlivnění úsudku politiků, narušení důvěry veřejnosti ve vládu, snížení sociální soudržnosti a převrat v mezinárodních aliancích. [72]

1.8.2.1 Kdo dezinformace šíří

Dezinformátoři v České republice se soustředí na současná znepokojující témata. Bezpečnostní centrum pro evropské hodnoty uvádí, že se v České republice vyskytuje více než 40 webů, které šíří falešné informace. Dezinformace se v dnešní době stále častěji objevují na webových stránkách a platformách sociálních médií. Dalším zdrojem nepravdivých informací mohou být reportéři, celé vlády, zákonodárci, zpěváci a umělci, ale i běžní lidé. [88]

Lidé šíří dezinformace jen výjimečně. Nejčastěji pokud byli po přečtení článku nebo titulku zděšeni, a chtěli tak upoutat pozornost svých přátel. Zatímco jiní lidé šíří dezinformace často. Vědci tvrdí, že tuto druhou skupinu tvoří zejména vyznavači konspirací všeho druhu. „*Podle výzkumníků dezinformace šíří asi jen 1 procento lidí z celé populace, takže z deseti milionů obyvatel Česka asi 100 tisíc lidí dezinformace vymýšlí a sepisuje. Asi 5 procent lidí tyto dezinformace aktivně šíří a asi deset procent populace, tedy 1 milion lidí, je aktivně vyhledává.*" [89]

Vzhledem k tomu, že pojem „dezinformace" a „propaganda" nejsou v České republice uznávanými právními pojmy, není žádný z těchto pojmů používán k označení trestného činu podle českého trestního práva. Tyto činnosti jsou nezákonné pouze tehdy, pokud při nich dochází k porušení následujících paragrafů, a to zejména § 181

Poškozování práv druhých, § 184 Pomluva, § 345 Nepravdivá obvinění, § 355 Hanobení rasy, národa nebo jiné skupiny lidí, § 356 Podněcování nesnášenlivost vůči skupině osob nebo omezování jejich práv a svobod, § 357 Šíření poplašných zpráv, § 365 Schvalování trestného činu nebo § 404 vyjadřování podpory hnutí směřujícímu k omezování lidských práv a svobod podle trestního zákoníku (zákon č. 40/2009 Sb.) [66]

1.8.2.2 Jak odhalit dezinformace

Rozpoznat dezinformační text, který se snaží ovlivnit náš názor je velmi obtížné. Konečná formulace může být někdy zcela změněna pouze změnou významu několika frází v jednom článku. Tak funguje mnoho klamavých webových stránek, například když redaktor položí otázky způsobem, který ponechává prostor pro více než jeden možný výklad.

Pozorný čtenář si však všimne následujících nesrovnalostí:

- Nadpisy článků jsou napsány velkými písmeny, aby na sebe upoutaly, co největší pozornost.
- Snažte se sledovat více než jen titulky. Podstata článku se vůbec nemusí shodovat s obsahem titulního názvu.
- Podívejte se, kdo je autorem textu, a zdali je členem nějaké redakce. Především u zahraničních zdrojů je nutné zkontrolovat, zdali se nejedná o fake news nebo špatně přeložený (překroucený) text.
- Ověřte si datum zprávy. Je běžné, že se šíří staré zprávy pod rouškou, že se jedná o nové zprávy obsahující aktuální dění.
- Projděte si pozorně obrázky v článku. Pomocí možnosti „najít podobnou fotografii“ můžete rychle určit, zda se fotografie hodí k tématu článku nebo zda byla pořízena na jiném místě v jinou dobu.
- Sledujte emocionální vývoj článku. Některé články nás doslova rozčílí, ať už svým názvem nebo obsahem bez ohledu, zdali se jedná o pravdivou nebo nepravdivou zprávu.

- Zkontrolujte obsah zprávy. Pokud máte nějaké pochybnosti, pokuste se zkontrolovat vše, co se vám na informaci nezdá přesné, ať už s pomocí vyhledávače nebo webových stránek, které se zaměřují na zpochybňování těchto informací. [67]

Na začátku roku 2022 se správce české domény organizace CZ.NIC rozhodla dle vlády ČR k neobvyklé akci a zakázala řadu dezinformačních webů, které ohrožovala bezpečnost našeho státu. Mezi nejznámější weby, které šíří nepravdivé informace patří např. Aeronet.cz, Protiproud.cz, Ceskobezcenzury.cz, Voxpopuliblog.cz, Prvnizpravy.cz, Czechfreepress.cz, Exanpro.cz apod. Východisko CZ.NIC je možné obejít, protože se dotýká pouze domény, a ne samotného webu, ale pro drtivou většinu lidí to bude nepřekonatelná bariéra. [68] V polovině května však CZ. NIC vydalo varování, že pokud nedostane pokyn od soudu, policie nebo jiného příslušného úřadu, weby zpřístupní. Následující týden po prohlášení všechny weby byly zpřístupněny krom jednoho, který postrádal přesné údaje z registru. [69]

Na jaře roku 2022 připravilo Ministerstvo vnitra návrh zákonu, který by umožnil zablokování konkrétních informačních zdrojů. Proběhla dlouhá odborná politická diskuse na toto téma. Návrh ministerstva vnitra by podle mnohých mohl zabránit šíření nepravdivých informací a nedocházelo by k politickému ovlivňování. Avšak zákon stále v tuto chvíli nebyl uzákoněn. [70]

Dle slov vládního zmocněnce pro oblast médií a dezinformací Michala Klímy je nebezpečný nadále jakýkoliv web šířící dezinformace. Zastával se akce se zablokováním dezinformačních webů. Tvrdil, že akce měla smysl, jakmile ruské síly napadly Ukrajinu, protože posloužily ke snížení dopadu ruské propagandy na české obyvatelstvo. Klíma tvrdí, že toto období bylo klíčové, protože se ukázalo, že dopad dezinformací se na několik týdnů snížil. [71]

1.8.2.3 Moc sociálních sítí a jejich vliv na šíření dezinformací

Sociální sítě jsou velkým pomocníkem přenosu informací, a to skutečných či nepravdivých. Nikdy nebyla komunikace snadnější. V této době můžeme sledovat

doslova celý svět a celý svět může sledovat nás. Bohužel i další aspekt zlepšování komunikace má své nevýhody, jako je například zneužívání osobních informací nebo tendence vstupovat do sociálních bublin. Interakce na sociálních sítích může potenciálně vést ke kyberšikaně, což je vážný problém. Pod mnoha články na zpravodajských serverech se objevují různá diskuzní fóra, kde se objevují různá obvinění. Totéž se děje i na sociálních sítích. Někteří komentátoři cítí potřebu psát nepravdivé informace, které jsou mnohdy plné vulgarit. [57]

Facebook je nejznámější sociální síť, kde nejčastěji dochází k ovlivňování jednotlivců nebo skupin lidí. Britští vědci přišli se zjištěním, že téměř 27 zemí podporuje trollování zejména u novinářů a politických oponentů. Například v Číně, Venezuele nebo Vietnamu je zaměstnáno několik týmů pracovníků, jejichž cílem je ovlivnit veřejné mínění. [78]

Troll neboli člen konverzace, který záměrně poskytuje pobuřující, urážlivý nebo irelevantní obsah o citlivých tématech, zejména pokud je v rozporu s konsensuálním postojem. Troll se snaží se vyvolat emocionální reakci ostatních uživatelů nebo jinak bránit smysluplnému diskutování. Praxe trollingu není nic nového, v dnešní době se pouze přesunul na jiný komunikační prostředek. Již staří Řekové ho dříve používali, když se snažili změnit téma na jiné. Ve starověkém Řecku probíhal z moderní perspektivy offline, jelikož se všichni navzájem viděli a slyšeli. To ho odlišovalo od dnešního trollingu, ve kterém většina trollů používá fiktivní identity, aby nikdo nemohl rozpoznat o koho se jedná. [79]

Termín „trolling“ původně popisoval druh rybolovu, kdy lovci tahali sítě a návnady do oblastí, kde předpokládali největší koncentraci zvěře. Podobně jako offline trollingu se daří i online trollingu, a to zejména v situacích, kdy je vysoká šance, že se někdo nachytá. Záměrem je vyvolat emocionální reakci a přerušit smysluplnou konverzaci. Z počátku sloužil pouze jako druh zábavy, která znamenala, že ne vše, co bylo vysloveno je myšleno vážně. Trolling je nyní častěji chápán jako provokace s cílem vyvolat reakci a je často doprovázen nepříjemným nadávkami a fyzickým násilím. [80]

Běžně v praxi dochází k vytváření unikátních facebookových stránek s provokativním materiálem. Většina z těchto uvedených stránek byla mezitím zrušena, jednalo se příklad o stránky „Matky s kočárky nepatří do MHD“, „Pohrdám vozíčkáři“, „Den šikany tlustých dívek“ a „Baví nás ubližovat domácím mazlíčkům a zvířatům." Všechny zmíněné stránky se měli zaměřovat na zranitelné cíle a vyvolat emocionální reakci. Znepokojivým trendem je použití trollingu jako propagandistické zbraně v online rozhovorech. Nejznámějším případem je šířící se prokremelská propaganda na sociálních sítích z Petrohradského centra pro internetový výzkum, které se stalo rodištěm tisíců falešných účtů. V centru je zaměstnána spousta lidí, kteří pracují nepřetržitě. Jejich úkolem je účastnit se online diskuzí, kde spolupracují v týmech a s definovanými odpovědnostmi. Alespoň jeden zaměstnanec působí jako provokatér a kritik ruského systému, zatímco ostatní mu odporují. [80]

1.8.3 Fackchecking

Snaha potvrdit nebo vyvrátit tvrzení se jmenuje Fact-checking, neboli ověřování faktů. Jakékoliv odvětví, ve kterém se tvoří prohlášení fact-checking vyžaduje, například média, internet či politika. [58]

Jedná se o důležitý nástroj především v moderní žurnalistice. Dá se říci, že pro správnou žurnalistiku je fast-checking základem, tedy že novinář by měl vždy provést fast-check před publiací informací. V minulosti se používal zejména pro politické výroky ale s rozmachem dezinformací hlavně na sociálních sítích se fast-checking stal důležitou částí snad všech médií po celém světě. [59]

Fast-checking se dělí na dva druhy, tzv. ante hoc fast-checking a post hoc fast-checking. První zmiňovaný se také nazývá editační fast checking, který se využívá před publikací článku, aby si autor byl jistý správností. Post hoc fast-checking je proces po formulaci článku či informace a používá se v boji s fake news a dezinformacemi. [60]

I běžným uživatelům se doporučuje vlastní fast-checking. Jedná se zejména o důvěru v ověřené zdroje informací a o určitou míru skepse ke zdrojům, které se zdají být subjektivně podezřelé. Existuje také množství doporučení pro koncové uživatele právě k

provádění vlasního fact-checkingu, patří sem například kontrola bezpečnostního certifikátu webových stránek.[61]

Agence France-Presse (AFP) je přední mezinárodní zpravodajská organizace, která nabízí rychlé, důkladné a ověřitelné pokrytí událostí a problémů, které ovlivňují náš svět. S pomocí Evropské komise bude AFP spolupracovat s pěti dalšími evropskými fact-checking organizacemi na vývoji Kodexu profesionální integrity pro nezávislé fact-checkery. V rámci projektu European Fact-checking Standards Project bude AFP spolupracovat s organizacemi jako jsou například Correctiv, Demagog, Pagella Politica , EU DisinfoLab a Fundación Maldita.es. [64]

V České republice působí zejména iniciativa Demagog.cz, která ověřuje správnost tvrzení českých politiků a informací hojně sdílených na sociálních sítích. Hlavní činností Demagogu je odhalování lživých a manipulativních tvrzení, která deformují veřejný prostor. Projekt pomocí analýz zkoumá a hodnotí výroky a prohlášení českých politiků. Vše probíhá tak, že dochází k nalezení původních zdrojů všech informací. Demagog se především snaží poukázat na to, kdy čeští politici prezentují pravdu, nebo naopak veřejnosti lžou. [65]

1.9 Diskurzivní analýza

Pojem diskurzivní analýza se týká různých myšlenek a metodologických technik. Primárními jsou diskurzivní psychologie, foucaultovská diskurzivní analýza, kritická diskurzivní analýza. Kritická diskurzivní psychologie (critical discursive psychology, CDP) je jednou z nejpopulárnějších technik v České republice. Jejím jádrem je hledání interpretačních repertoárů, diskurzů a předmětových pozic. V dalším textu se budu zabývat zejména kritickou diskurzivní analýzou. [73]

Hlavními body kritické diskurzivní analýzy jsou:

1) Interpretační repertoáry

Tento termín se vztahuje k souborovým popisům a rétorickým obratům, které jsou velmi často organizovaných kolem metafor nebo živých obrazů. V řeči jsou pak používány k vytvoření různých interpretací činů, sebe sama a sociální kultury. Ve způsobu vzájemné komunikace jsou zakořeněny sdílené významy. Tím, jak věci, lidi a sociální jevy popisujeme, jim dáváme i určitý význam. [73]

2) Diskurz

Nepřímo podstata komunikace ovlivňuje diskurz. Odkazují na to, jak se věci dělají v naší kultuře a jak je vnímáme. Diskurzy se nepřímo vztahují k určitým společensky přijímaným přesvědčením. Do těchto očekávání je také zahrnuto, co se má a nemá dělat. Diskurz také formuje pozice aktérů. Ty často upřednostňují jednu stranu a posilují ji, zatímco druhou stranu znevýhodňují a oslabují. [73]

1.9.1 Kritická diskurzivní analýza

Fráze „kritická diskurzivní analýza“ (CDA) se v poslední době stala uznávanou akademickou disciplínou. Na jeho koncepci se podílela skupina vědců, včetně Normana Faircloughа, Ruth Wodakové a Teuna van Dijka. Vědci z počátku 90. let vytvořili síť kolegů, kteří se vzájemně ovlivňují, sdílejí společné předpoklady a metody a spolupracují na výzkumných projektech. Je důležité nezaměňovat výsledky kritické diskurzivní analýzy s výsledky jiných metodologií. [74]

Lingvistický přístup k diskurzu (systematické zkoumání jazykových jevů) jej propojuje se sociálně-psychologickou diskurzivní analýzou. V tomto ohledu byla kritická diskurzivní analýza primárně ovlivněna systémovou funkční lingvistikou Michaela Hallidaye. Druhým zdrojem vlivu je Foucaultův poststrukturalismus, který na diskurz nahlíží jako na soubor omezení a pravidel pro tvorbu výpovědí. Jeho práce je oceňována jako vynikající sociální teorie diskurzu, která mimo jiné vysvětluje, vztahy mezi diskurzem a diskurzivní konstrukci subjektu. Současně je dílo také kritizováno za

přílišnou abstraktnost a za ignorování lingvistických složek konverzace. Přídavné jméno „kritický“ se může ukázat jako ovlivněné postmarxistickým myšlením. [74]

Kritická diskurzivní analýza tvrdí, že jazyk nelze redukovat na jiné aspekty společnosti (jako jsou materialistické), také varuje před extrémem, který tvrdí, že vše (veškerá společenská aktivita) je diskursem. Kritická diskurzivní analýza nevidí diskurz jako nezávislý fakt, na rozdíl od Foucaulta. Je založen na myšlence, že jazyk je dialekticky příbuzná a neredukovatelná složka společenské aktivity. Kritická diskurzivní analýza rozlišuje mezi diskurzivními a nediskurzivními prvky a rysy společenského života. [74]

Diskurz je proces, jehož prostřednictvím se vytváří význam. Vazba a interakce mezi diskursem a dalšími složkami sociální aktivity, respektive sociálními dopady textů, lze díky tomuto rozlišení zkoumat analyticky. Podobně jako sociálněpsychologická analýza diskurzu využívá kritická analýza diskurzu důkladné zkoumání textu (někdy nazývána jako textově orientovaná analýza diskurzu). Zároveň přidává další dva analytické aspekty. K lingvistické a rétorické analýze textu je přidáno zkoumání diskurzivního (významotvorného) chování v jeho širším sociálním a historickém kontextu. [74]

1.9.1.1. Techniky a postupy kritické diskurzivní analýzy

Autor Fairclough rozděluje diskurzivní analýzu na tři odlišné, ale vzájemně propojené části diskurzu.

1) Deskripce

Deskripce zkoumá formální stránku jazyka. Jedná se o konvenční lingvistickou studii, která se zabývá prvky jazyka, jako je mimo jiné slovní zásoba, syntax, tón a směrovost řeči. Fairclough rozděluje tři tematické stavební prvky této analýzy na slovní zásobu, gramatiku a strukturu textu. Zaměřuje se na četná témata v každém z nich, včetně:

a) prožitkových, vztahových, expresivních a metaforických kvalit slov;

b) zážitkové, vztahové a vyjadřovací hodnoty gramatiky;

c) interakční normy a textovou strukturu. [75]

2) Interpretace

Podle Faircloughа je intertextová analýza zásadním doplňkem lingvistické analýzy, protože v rámci textové analýzy spolupracují jako komplementární dvojice. Jazykové rysy textu zhmotňují intertextové aspekty textu. Interpretace se zaměřuje na to, jak se tvoří a interpretují texty, tedy co a jak je prostřednictvím textů tvořeno déle pak co a jak se v textech nachází. Zde zkoumáme diskurzivní praxi jako takovou. Jedná se o rozpoznání a analýzu mnoha diskurzivních druhů (diskurzů a žánrů) spojených s různými okolnostmi a také na tom, jak ovlivňují myšlenky (reprezentace), předměty a mezilidské vztahy. Zaměřuje se především na:

a) „co se děje“ („what´s going on“)
b) zúčastněné strany („who´s involved“)
c) vztahy mezi subjekty („relationships between subjets“) a souvislosti („role language in what´s going on“). [75]

3) Explanace

Podle Faircloughа se třetí segment označuje jako „explanace“. Tento segment pojednává o sociálních vlivech procesu produkce a interpretace, a také o jejich společenských dopadech. Druhé vysvětlení explanace je, že se jedná o způsob, jak lze na jazyk nahlížet v rámci procesu mocenských sociálních bitev. Jedná se o objevení:

a) Sociálních faktorů, které ovlivňují diskurz na situační, institucionální a společenské úrovni;
b) Ideologických složek interpretací;
c) účinků, zda diskurz podporuje nebo upravuje mocenské vztahy. [75]
d) Fairclough tvrdí, že analytik a další aktéři interpretují stejným způsobem, ale že pro (kritického) analytika je klíčové, aby tyto „přirozené“ a „zdravé“ předpoklady rozebral. [75]

1.9.1.2 Pravidla kritické diskurzivní analýzy

Při provádění analýzy je třeba dodržovat několik jednoduchých pokynů. Prvním je princip spolehlivosti, který zdůrazňuje, že analýza by měla být založena na několika textových (lingvistických) znaků, nikoli pouze na jednom. Navíc je to pokus o kompletnost analýzy neboli o spolehlivé spojení mezi lingvistickými a intertextuálními znaky. V neposlední řadě to souvisí s transparentností zjištění, což ve skutečnosti znamená, že by výsledky měly být podpořeny více citacemi a pasážemi z textu, které odkazují na výsledky. Zároveň bychom se měli vyvarovat všech nedostatků v diskurzivní analýze, které si toto označení nepravdivě nárokují, konkrétně:

a) analýza prostřednictvím shrnutí textu;
b) analýza prostřednictvím vyjádření názoru;
c) analýza prostřednictvím neukotvených citací;
d) analýza založená pouze na identifikaci diskurzů a odlišných mentálních konstruktů;
e) analýza provedená za použití špatného výzkumu;
f) analýza omezená na lingvistické detaily. [75]

1.9.2 Obsahová analýza

Konkrétnější názvy kvantitativní obsahová analýza nebo formální obsahová analýza jsou někdy zaměňovány s obecnějším pojmem obsahová analýza. V některých knihách se výraz „obsahová analýza“ používá v obecnějším smyslu a odkazuje na kvantitativní i kvalitativní přístupy analýzy dat. [77]

Obsahová analýza (content analysis) lze obecně charakterizovat jako rozbor zkoumání informací obsažených v záznamu konkrétní komunikace. Tento přístup je někdy konkrétněji popsán jako zkoumání textu nebo skupiny textů. V této situaci lze také použít termín „textová analýza“. Tento přístup, vycházející z pozitivistických metodologických tradic, si klade za cíl nalézt určitá slova a pojmy ve zkoumané komunikaci a zjistit jejich četnost výskytu, význam, vzájemné vztahy apod. Nejčastěji se tato technika používá při analýze mediálního sdělení. [76]

1.9.3 Termín narativ a narativní analýza

V posledních 25 letech se aplikace narativní analýzy, tedy analýza vyprávěného příběhu začala velmi hojně používat. Využití narativních principů je velmi rozsáhlé, a to zejména v psychologii a sociologii. Dále je využívám ve výuce, historii, etnologii a antropologii. [81]

Cílem narativní analýzy je nalézt společné rysy nebo hlavní principy toho, jak lidé vyprávějí své životní zkušenosti. V příbězích se zaměřujeme především na to, co mají příběhy společné, a dále pak na archetypy, které v těchto příbězích převládají. Příběh vždy zahrnuje posluchače nebo výzkumníka, jehož dotazování a nastouchání formují příběh. Vyprávěný příběh by neměl být přesnou replikou předchozí zkušenosti. Myslíme si, že jednotlivci zapomínají na konkrétní detaily, nevyjadřují vše a nepopisují vše přesně. Místo toho, aby byl přesným popisem událostí, je vyprávění výtvorem založeným na nich. [81]

Výzkumníkova interpretace dříve převyprávěných informací vypravěčem tvoří podstatu narativní analýzy. Analýza se nejčastěji využívá při pochopení konkrétních životních zlomů, vývojových posunů a přechodných krizí. [82] Indukce je základem narativní analýzy a umožňuje nám vyvodit závěry z velikosti vzorku zkoumaných příběhů. Je velmi nepravděpodobné nashromáždit tolik rozhovorů, abychom splnili maximální počet dat pro zakotvenou teorii, tj. že by již nebylo možné získat více poznatků ze zkušeností jiných respondentů. Informace o jevech, které již byly prozkoumány méně rozsáhlými technikami a produkovaly pouze povrchní informace o pravděpodobně obsahově bohatých jevech, lze nicméně na základě četných rozhovorů rozšířit, prohloubit, doplnit či upřesnit. Způsob sběru dat Často má formu narativního rozhovoru, ale může mít také podobu analýzy literárního díla nebo osobní korespondence, blogu, časopisu, samostatného psaní atd. [81]

Často se používá životopisný příběh. Během narativního rozhovoru by měl výzkumník, co nejméně zasahovat do průběhu rozhovoru. Je na respondentovi, jak si svůj příběh uspořádá. [81]

Pro narativní analýzu existují tři různé metodologie. Je to interakcionistický, strukturalistický a hermeneutický přístup. [85]

a) Interakcionistický přístup představuje prostředí scénáře, ve kterém aktéři interagují. Scénář nediktuje podstatu příběhu, ale vyprávění se spíše vyvíjí a mění. V rámci studie jsou zkoumány interakce mezi dotazovaným a tazatelem a prioritou je předchozí komunikace. [85]
b) Strukturalistická metoda se často snaží identifikovat opakující se vzorec postav a událostí. Jedná se o techniky, které jsou integrovány do příběhu a mění se na základě typu vyprávění. Díky tomu je pro čtenáře obzvláště jednoduché předvídat, jak se příběh bude vyvíjet, jaký bude průběh a závěr. [85]
c) Základem hermeneutické metody, na rozdíl od výše naznačeného strukturalistického přístupu, je tzv. předporozumění neboli znalost pozadí textu, se kterým čtenář do textu vstupuje. Nalezení významu, který vypravěč příběhu přiřadil, slouží jako základ hermeneutické metody. [85]

Grafické zobrazení průběhu pozorovaných událostí se velmi často používá jako nástroj při sběru narativních dat. Na list papíru s vodorovnou osou před sebou jsou zaznamenány roky od začátku události do současnosti. Tato osa označuje významné orientační body a klíčové momenty. [82]

Grafické znázornění významných momentů pomáhá strukturovat vyprávění a nedojde snadno k vynechání důležitých dat. V narativním výzkumu mohou být rozhovory s vypravěči vedeny opakovaně. Při opakovaném setkání se účastníci výzkumu vzájemně setkávají a více se otevírají. K oživení vzpomínky na sledované události napomáhá i předchozí vyprávění. Opakované rozhovory se využívají např. v biografických výzkumech. [83]

V následujícím textu si představíme vybrané modely narativní analýzy.

McLeodova metoda (2001/2005)

Autor tvrdí, že když jsou příběhy analyzovány pomocí fenomenologické metody nebo s cíli zakotvené teorie, je kladen důraz na jednotlivé motivy, střípky významu a

kategorie. Výše uvedené postupy mohou vést k potlačení celkového pohledu, což je klíčové pro uchopení smyslu příběhu. [84]

V analýze se proto buď můžeme pokusit porozumět procesu vyprávění pomocí analýzy přepisů vyprávění dílčích událostí nebo se soustředit na životní narativ jako celek. Při hodnocení životních příběhů jsou hlavními výzkumnými rysy koherence a kontinuita, zatímco při zkoumání sekvencí je to struktura a konfigurace. [84]

Mishlerova metoda (1986)

Podle Mishlerových pozorování v textech vyplývajících z rozhovorů poskytuje souhra a kontrast mezi odlišnými částmi v příběhu určitý stupeň významnosti, který by nebyl sdělen bez ohledu na narativní perspektivu. Domníval se proto, že je důležité zaměřit se především na to, jak jsou příběhy strukturovány. Dle něj je aplikování nazativní analýzy přínosné. Typologii pro kategorizaci narativní studie v souladu s její výzkumnou dominancí později navrhuje Mishler, který čerpá inspiraci z Halidayova přístupu k jazyku (odkaz, struktura a funkce): 1. odkaz a časový řád, který odkazuje na vztah mezi tím, jak jsou události uspořádány v reálném čase a jak jsou uspořádány v narativní jednotce; 2. textová koherence a struktura, kterou lze určit pohledem na jazykové a narativní techniky použité při tvorbě příběhu; a 3. narativní funkce, která odkazuje na funkci příběhu ve společnosti a kultuře jako celku. [84]

Omerova metoda (1994)

Autor Omer využívá holisticko-formální přístup pro hodnocení východisek ve své narativní psychoterapii. Tvrdí, že v psychoterapii se vytváří místo pro klientova a terapeutova tvorbu životních příběhů. Klient obvykle představuje příběh, jehož koherence je narušena nebo ohrožena. Snaží se rozpoznat, zdali se v klientova příběhu nachází mezera či opomenutí nebo je příběh zaplátovanou narativitou nebo pokus o koherenci. Zabývá se také tím, zda je životní příběh otevřený ke změně nebo uzavřený do sebe a chronologickým pořadím životních událostí. [84]

Každá z výše uvedených modalit se vztahuje k určitému druhu výzkumné problematiky, k různým textům a je vhodná pro různé vzorky. Rozdíly však nejsou vždy zřejmé; například rozdíl mezi formou a obsahem není vždy zřejmý. [84]

2. Cíl práce a výzkumné otázky

Výzkumné otázky diplomové práce jsou již definovány v zadání. První otázka zní: *„Jaký vliv mají falešné zprávy na bezpečnostní politiku státu?“* A druhá otázka zní: *„Jak lze zastavit šíření falešných zpráv?“* Odpovědi na tyto otázky budou rozebrány v diskuzi. Pod výsledky se budou nacházet odpovědi, které získáme pomocí poznatků z teoretické i praktické části práce.

Hlavním cílem této diplomové práce je analýza a aplikace zvolené diskurzivní metody na zprávy o ukrajinském konfliktu. Dílčími postupy práce, zásluhou kterých k cíli docílíme je získání kompletních informací o hrozbách v kyberprostoru (zejména pak, jak můžeme těmto hrozbám čelit), dále analýza vzniku a šíření tzv. fake news (falešných zpráv), které ohrožují lidskou společnost a v neposlední řadě informační válka a kompetence vlády proti jejich šíření.

3. Použitá metodika

V praktické části je použit souhrnný článek od důvěryhodné zpravodajské stanice Deutche Welle (dále jako „DW“), jelikož se tento celý článek zaměřuje na problematiku Rusko-Ukrajinského konfliktu. Celá praktická část této diplomové práce je zaměřena na Rusko-ukrajinský konflikt.

Původně měla být použita některá z klasických metod diskurzivní analýzy, ale po nalezení výše zmíněného článku byl zvolen hybridní přístup. Výsledkem je kvantitativně - kvalitativní výzkum, jelikož zvoleným hlavním zdrojem je souhrnný článek od DW. Tento článek obsahuje jednotlivé fake news z Rusko-ukrajinského konfliktu. Každá z těchto fake news je následována fack checkem přímo od specialistů z DW. K těmto fake news jsou ve většině případech nalezeny články z českých zpravodajských portálů. České články jsou následně porovnány a analyzovány s hlavním článkem od DW.

V případě některých zpráv se bohužel nepodařilo nalézt české ekvivalenty. Naopak u dalších zpráv existuje nepřeberné množství českých článků na stejné téma. V této práci jsou vždy upřednostněny známější zpravodajské portály. Naopak zde byla snaha vyhýbat se bulvárním portálům.

Výsledných analýz je celkem třicet. Každá z těchto analýz se vztahuje, až na některé výjimky k jedné fake news od DW a zároveň k českému článku se stejným nebo nejvíce podobným obsahem.

Analýzy použité v této práci tedy nezapadají ani do jednoho z modelů diskurzivní analýzy. Analýz je celkem třicet, a tím se dostáváme spíše k výzkumu kvantitativnímu. Texty se nicméně nejvíce přiklánějí ke strukturálním a z části také k hermeneutickým metodám narativní analýzy, které jsou popsané v teoretické části práce.

4. Výsledky

Článek pojednává, jak je z názvu zřejmé, o fast-checkingu fake news, které souvisí s Rusko-ukrajinským konfliktem. V úvodu článku je nastíněno, jak a kdy ke konfliktu došlo. Dále pak jak společně s ozbrojeným konfliktem v reálném prostoru začala současně i online informační válka. Tým z DW se údajně zaměřil na několik falešných tvrzení ze strany Ruska i Ukrajiny a udává, jaký je reálný stav oproti tvrzení. V době psaní tohoto textu bylo ve článku uvedeno, že jeho poslední aktualizace proběhla 12. května 2022. Poslední věta článku říká, že byl přeložen z originálu v němčině Michaelem Trobridgem.

DW zpráva č. 1: První z uvedených faktů tvrdí, že při příležitosti každoroční vojenské přehlídky v Moskvě ruský prezident Vladimír Putin učinil několik prohlášení o Ukrajině a akcí západních zemí. Některá z těchto prohlášení byla speciality z DW prošetřena. První prověřenou zprávou jsou Putinova slova o „možném nabytí jaderných zbraní Ukrajinou a aktivním vojenském posilování sousedních území Ruska“. Tato slova DW označila za lež, neboť jejich fact check prokázal, že se po mezinárodní dohodě v roce 1994 Ukrajina vzdala svých jaderných zbraní, které jim pozůstali po SSSR. A to za záruku nezávislosti a zachování ukrajinských hranic. Prezident Putin narážel na to, že zejména kvůli zabrání Krymu Ruskem v roce 2014 se narušila samostatnost Ukrajiny. Prezident Zelenský prohlásil, že se od smlouvy distancuje. DW však udává, že nejsou žádná data či důkazy o tom, že by Ukrajina chtěla znovu nabýt jaderný arzenál.

1. E15.cz článek nazvali „Putin: Rozhodnout o invazi bylo těžké. Přesvědčily ho snahy Kyjeva získat jaderný status“. Článek je z 5. března 2022. Ve článku mimo jiné upřesňují Putinova slova. Údajně totiž tvrdil, že rozhodnutí o invazi na Ukrajinu bylo těžké a snaha Kyjeva získat jaderný arzenál ho k tomu přivedla. Důkazem údajné snahy se pro Putina mělo stát vystoupení Zelenského na bezpečnostní konferenci v Mnichově. Článek je zajímavý tím, že výroky prezidenta Putina v článku cituje ruská odnož BBC, která následně uvádí na pravou míru realitu Zelenského vystoupení. Skutečné výroky ukrajinského prezidenta směřovali pouze k vypovězení dohody, ve které se Ukrajina zavázala vzdát se jaderných zbraní zárukou za bezpečnost. E15 na konci článku shrnuje Putinova výroky o invazi, respektive „speciální vojenské operaci“, o ochraně rusky mluvících obyvatel a o demilitarizaci a denacifikaci Ukrajiny. Články s podobnými názvy a téměř shodným obsahem se dají nalézt i na serverech iDnes.cz či Novinky.cz.

Analýza 1

Z tohoto tvrzení je zřejmé, že jednou z mnoha snah Ruska je probudit zejména u svých občanů sympatie k invazi na Ukrajinu, případně její ospravedlnění. Jedná se nejspíš o čistě propagandistický krok. Kdyby bylo toto prohlášení cíleno na okolní svět, nejspíše by se zcela minulo účinkem, zejména kvůli obecné absenci cenzury a většinové globální sympatii k Ukrajině. Důvod prvního místa na seznamu článků od DW je jasný – hrozba jaderné války ze strany Ruska byla snad nejvíce medializovaným tématem, a to zejména na začátku rusko-ukrajinského konfliktu. Je tedy zcela přirozené, že i zmínka (a sice z druhé strany, tedy možná hrozba naopak Ukrajinou) o jaderných zbraních bude na prvním místě hledaných událostí.

Článek z portálu E15 se dle očekávání ve většině shoduje s článkem od DW. Doplňující informaci typu „Rozhodnout o invazi bylo těžké.“ ještě více potvrzuje odstavec výše. Ruskojazyčné CNN jako jeden ze zdrojů portálu E15 může navodit dojem, že se jedná o ruský propagandistický kanál. Avšak dokazuje, že tomu tak není, jelikož dle E15 zdravodajská služba CNN ihned uvedla na pravou míru slova ruského prezidenta. Počet variací tohoto článku na mnoha jiných českých zpravodajských platformách potvrzují mediální sílu zmínky o jaderných zbraních.

DW zpráva č. 2: Dalším prověřovaným tvrzením jsou opět slova Ruského prezidenta Putina ospravedlňující ruskou invazi. Dle jeho slov se jedná pouze o preventivní opatření, která jsou nutná, a to z důvodu „příprav na operace v Donbasu“ a údajné plánované invaze na historicky ruská území, včetně Krymu a Donbasu.

Fact-checking DW opět ukázal, že se jednalo o lež. DW uvádí, že ukrajinská vláda několikrát zdůrazňovala, že se snaží o diplomatické řešení konfliktu na Donbasu, a to přímo prezidentem Zelenským na bezpečnostní konferenci krátce před invazí. V článku DW se píše o tom, že na začátku invaze nebyli vidět žádné známky údajné chystané ukrajinské ofenzívy. Navíc zmínka, o „historicky ruských území“ je mylná, neboť Donbas a Krym jsou ukrajinská území. Připojení Krymu k Rusku není globálně akceptováno.

2. CeskeNoviny.cz vydali 9. května článek s názvem „Putin v projevu označil útok na Ukrajinu za správné rozhodnutí“. Článek pojednává o Putinově projevu, a to konkrétně na Moskevské přehlídce. Prohlásil prý mimo jiné, že obrana vlasti je nejposvátnější povinností, a že právě „za vlast“ bojují ruská vojska v Donbasu. Invazi označil za „jediné správné rozhodnutí v reakci na chování Kyjeva a Západu. V další části textu se dočteme o chystané „další kárné operaci Kyjeva proti proruským „seperatistům“ a nezávislosti republik na východě Ukrajiny, které Rusko uznalo těsně před začátkem invaze. V tomto českém článku také najdeme zmíňku o „Historicky ruských území včetně Krymu“. České noviny dále popisují ostatní výroky Putina, na které se zaměříme v následujícím textu.

Analýza 2

Z dalšího Putinova výroku vyplývá zoufalá snaha ospravedlnit invazi a očernit Ukrajinu, a to zejména před ruskými občany. Ti mají nabýt dojmu, že Rusko se „pouze brání“. Po celou dobu jsou v právu a pouze se snaží chránit své území a občany.

Český článek se opět téměř shoduje se závěry z německého webu, zejména pak výroky o „historických území Ruska“. Zajímavý je dodatek o „další kárné operaci Kyjeva“. Z toho lze snadno vyvodit závěr, že se nejedná o první krok Kyjevský krok proti Rusku. Propaganda a cílení zpravidla na ruské občany je i zde cela zřejmá.

DW zpráva č. 3: Další Putinova výrok směřoval k Ukrajině a jejímu spojení s neonacismem. Dle DW tvrdil, že neonacisté řídí Ukrajinu, a že střet s nimi je nevyhnutelný. Zdůraznil, že civilisté v Donbasu „zemřeli na následky útoků neonacistů". I toto tvrzení po fact-checkingu vyšlo jako lež. DW uvádí, že Ukrajince za neonacisty označuje nejen Putin a ruská vláda ale i ruská média. Toto označení se nezakládá na pravdě. Mezi nacistickým Německem a demokratickou Ukrajinou není dle článku žádná spojitost.

3. Ohledně ruských slov o denacifikaci Ukrajiny existuje mnoho článků. V této práci je uveden článek z Novinky.cz, který se nazývá „Lavrov vysvětlil, co si Rusko představuje pod pojmem denacifikace Ukrajiny". V článku se uvádí, že Sergej Lavrov (ruský ministr zahraničí) prohlásil v televizní stanici Russia Today (RT), že denacifikace pro Rusko znamená zrušení všech zákonů, které diskriminují místní ruskojazyčné obyvatelstvo. Dále pro Rusy denacifikace znamená zrušení zákonů, které podporují nacistickou ideologii a praktiky. Lavrov se ve článku odkazuje mimo jiné na prezidenta Zelenského, který apeloval na obyvatele Donbasu, kteří se cítí být Rusi, aby Donbas opustili. Realita ohledně výroku je však taková, že prezident Zelenský mluvil pouze o problémech rozvoje Donbasu a jeho obyvatelích. Dodal, že pokud se někteří obyvatelé Donbasu cítí být Rusy, tak by měli zvážit, zdali by je v Rusku nečekala lepší budoucnost.

Analýza 3

Toto tvrzení se nesmyslně snaží „očernit" Ukrajinu. Dle DW není žádný důkaz, o tom že by neonacismus na Ukrajině hrál jakoukoliv roli. A tak je zřejmé, že toto označení Putin použil zcela účelově. Slovo nacismus je napříč generacemi vnímáno silně negativně, a to je zřejmě důvod jeho použití v ruské propagandě.

V českém článku není zmíňka o vyvrácení ruských výroků, ale z citace projevu prezidenta Zelenského je jasné překrucování faktů. Fact-check DW prokázal, že žádné nacistické ideologie nejsou na Ukrajině zakořeněné, a už vůbec ne v její legislativě. Denacifikaci a údajnou diskriminaci Rusů považuje Lavrov za synonymum.

DW zpráva č. 4: DW následně popisuje slova Ruského prezidenta, která cílí na „bezpečnostní smlouvy“ z prosince roku 2021. Prezident Putin hovoří o ruských zájmech jako otevřených, diplomatických a snažících se o kompromisy. Členy NATO vykresluje jako ignorantské a „mající zcela jiné plány.“ Z fact-checku vyplývá, že toto tvrzení není lživé (pouze zavádějící) narozdíl od všech předchozích. Zpravodajský kanál vysvětluje, že Putin hovořil o soupisu požadavků, které Rusko předložilo NATO v prosinci 2021, tedy těsně před začátkem invaze. Soupis obsahoval údajně osm požadavků, na kterých se NATO s Ruskem mělo shodnout, aby se předešlo konfliktu. NATO a jeho členové reagovali zamítnutím některých požadavků soupisu.

4. Článek na portálu Denik.cz se nazývá „Putin trvá na ruských požadavcích. Chce hledat diplomatické řešení krize“. Byl publikován dne 15.2.2022. V úvodu článku je popsána snaha Ruska o diplomatickém řešení „krize ve vztazích se Západem kvůli Ukrajině“. Putin dle článku několikrát zopakoval požadavky o rozmístění zbraní u hranic Ruska. Dále se dožadoval zaručení, že NATO nikdy nepřijme Ukrajinu za jednoho ze svých členských států. V článku je uvedeno Putinovo další prohlášení *„Válku v Evropě nechci, ale situace v separatistických regionech je genocidou.“*

Analýza 4

Putinův dokument s navrhnutými dohodami o bezpečnosti jsou ve skutečnosti nepřátelské a zcela jednostranné požadavky. Jejich odmítnutí je pro země Západu zcela logické, neboť jejich odsouhlasení by významně zvýšilo vliv Ruska a reálně mohlo ohrozit členské státy NATO. Putinova propaganda představuje Rusko jako benevolentní, mírumilovný a diplomatický stát, neboť realita opresivního, militaristického agresora je méně mediálně přijatelná.

Článek z Denik.cz více prohlubuje a potvrzuje zjištění DW. V článku se objevuje zajímavý fakt, o snaze Ruska zabránit válce. Avšak toto se dělo pouze několik dní před začátkem invaze, kterou Putin musel plánovat mnohem déle dopředu. Zpětně tedy všechny jeho výroky v tomto směru absolutně ztrácí váhu. To, že se Rusové nebojí používat slova, která ihned upoutají pozornost jako neonacismus, či genocida je dnes už pro jejich výstupy typické.

DW zpráva č. 5: V následujícím odstavci článku DW se píše o šířícím se obrázku (zejména na sociálních sítích) mladé plakající ženy. Pod obrázkem se objevuje popisek, že se jedná o sedmnáctiletou dceru prezidenta Zelenského. Žena na obrázku údajně tvrdí, že nesnáší svého otce, kterého nazývá nacistou a vrahem ukrajinského lidu. Stejnou fotografii sdílely i ruské webové stránky.

Fact-check portálu DW opět potvrzuje, že se ve skutečnosti jedná o lež. Po jednoduchém a zpětném vyhledání fotografie se spojila s videem, které pochází z roku 2017. V tomto roce bylo pravé dceři Zelenského 13 let. Žena na fotografii je však mnohem starší.

5. Český článek z webové stránky Forum24.cz. je pojmenovaný *„Lidé na internetu šíří lživé video. Neznámou dívku vydávají za dceru Zelenského“*. Článek byl publikován dne 25.4. 2022. Internetový portál Forum24 příběh rozšiřuje tím, že píše o videu, které se mělo objevit na Facebooku. Na videu měla být mladší tmavovlasá žena, která údajně na videu pláče. V ruštině prosí svého přítele, aby jí koupil iPhone. Hlavní problém pak podle českého webu nastal tehdy, když se fotografie vystřižená ze zmíněného videa začala šířit prostřednictvím dezinformačních účtů i v Čechách, s popisem „Oleksandra Zelenská, Zelenského dcera nenávidí svého otce, nazývá ho nacistou a vrahem ukrajinského lidu.“ Sama dle popisu navíc uprchla do Polska. Článek dále uvádí, že žena není pravá Oleksandra Zelenská a odkazuje na britský server Evening Standart, který měl publikovat reálnou aktuální fotografii dcery Ukrajinského prezidenta. Navíc dodává, že není jediný důkaz o tom, že by se dívka nacházela v Polsku a měla s otcem jakékoliv neshody.

Analýza 5

Tento článek názorně ukazuje, jak může zapůsobit jedna fotografie na sociální mínění. Vyhledání fotografie mohl provést naprosto kdokoliv, a to během pár sekund například přes vyhledávač Google. Je zřejmé, že se tak v mnoha případech nestalo. Naopak se objevilo hromadné sdílení dezinformace, čehož Ruská média snadno využila ve svůj prospěch. Dá se předpokládat bez velkých spekulací, že údajná slova o nacismu a „vrahovi Ukrajinského lidu“ byla od začátku výplodem ruské propagandy.

Český článek s německým článkem souhlasí, zajímavé je však zjištění, že zdrojové video nemá s válkou vůbec nic společného, což ve článku od DW není zřejmé.

DW zpráva č. 6: V dalším odstavci DW popisuje falešné video, které mělo naopak cílit proti Rusku. Dle DW se na sociálních sítích objevilo virální video, které zobrazuje vykolejený vlak s vojenskou technikou. Tento vlak měl mířit z Ruska na Ukrajinu. Autoři příspěvku se tímto způsobem vysmívali Ruské armádě. Někteří z účastníků diskuzí tvrdili, že se jedná o činnost ukrajinských partyzánů. DW fact-check vyhodnotil tento příspěvek za falešný. Zpětné hledání screenshotů z videa údajně odhalilo, že je video mnohem staršího data a odehrává se tisíce kilometrů od současného konfliktu.

Analýza 6

Zdůvodněním těchto falešných příspěvků se jeví snaha podpořit nenávist k Rusku a to (téměř) za každou cenu. Je zřejmé, že vymyšlené zprávy nepomáhají nikomu, ba naopak po tom, co pravda vyjde na povrch se prohloubí nedůvěra v podobné zprávy. K tomuto příběhu nebyl nalezen ekvivalentní příspěvek na českých zpravodajských webech.

DW zpráva č. 7: V dalším odstavci tohoto článku se objevuje na krátké Twitterové video s údajnými vojenskými úspěchy ukrajinské armády proti armádě Ruska. Jedná se o falešnou stránku, která má statisíce fanoušků, a tím tedy velký dosah. Fact-check odhalil zavádějící realitu tohoto příspěvku. DW tvrdí, že šest incidentů ve videu jsou natočeny před konfliktem, tudíž s aktuální situací nemají nic společného. Například jeden ze záběrů záběr pochází od ruských vojsk v Sýrii. Zbylých deset videí může být dle DW legitimních.

7. Ani u tohoto příběhu nebyl nalezen žádný článek v českém jazyce. Zpráva je zmiňována na sociálních sítích. Objevil se český twitterový příspěvek, který upozorňuje na tweet oficiálního twitterového účtu ukrajinské vlády. Ten oznamuje, že se objevil „nový fake účet“ ozbrojených sil Ukrajiny. Následně je upřesněno, že byl Twitterem zanedlouho po nahlášení smazán.

Analýza 7

Přehnaná snaha vyzdvihnout stranu, která je v právu a napadená (v tomto případě Ukrajina) není vždy k dobru, ba právě naopak. Stejně jako u předešlého tvrzení se dá usuzovat, že po verifikaci pravosti záběrů může tvůrce tohoto videa Ukrajinské straně naopak uškodit, a to i přes to, že původní úmysl autora byl dobře myšlený. Na kredibilitě falešnému účtu přidává velká fanouškovská základna. Někteří lidé, kteří stránku neznají by si mohli myslet, že se jedná o oficiální účet Ukrajinské armády (název „Armed forces Ukr.").

České příspěvky na sociálních sítích ke tvrzení přidávají informaci o tom, že se nejedná o první falešný účet ukrajinské armády. Je tedy zřejmé, že se jedná o osvědčenou dezinformační metodu.

DW zpráva č. 8: V další části článku DW popisuje video od reportéra z portálu CNN. Na videu se objevuje reportér v živém vysílání při požáru rezerv pohonných hmot u města Lvova, které měli začít hořet po ruském ostřelování. Jeden ze zasahujících hasičů na videu má na zádech nápis „Edmonton". Z toho někteří sledující usoudili, že se jedná o falešné video, které se ani neodehrává na Ukrajině. DW proto provedlo fact-check, který potvrdil autenticitu videa. V roce 2017 Edmontský hasičský sbor věnoval 600 zásahových obleků a další vybavení Ukrajině, a proto má hasič na videu uniformu kanadských hasičů. DW si toto tvrzení potvrdila přímo v interview s vedoucím hasičské pomoci Ukrajině, Kevinem Roylem.

8. Na webu Fakticke.info (fact-checkový český zpravodajský kanál) se dočteme o článku *„CNN nezfalšovala snímky požáru ve Lvově. Šlo o darovanou výstroj"*. Již název článku potvrzuje shodu s článkem od DW. Český článek se zabývá zejména dezinformačním tweetem s českým textem. V něm se dočteme o tom, že „u požáru na Ukrajině byli první hasiči z Kanady". Fakticke.info v článku samo hodnotí zprávu jako nepravdivou a odkazuje se na neziskovou organizaci Firefighter Aid for Ukraine (Hasičská pomoc pro Ukrajinu), která mimo jiné shromažďuje nepotřebné hasičské vybavení. Dále také na vedoucího Edmontských hasičů Joe Zatylny, který potvrdil darovaní vybavení.

Analýza 8

S proruskými sympatizanty budou v tomto případě souhlasit také příznivci konspiračních teorií. Někomu k pochybnostem stačí právě zmíněný nápis na hasičských uniformách. Někdo by mohl dokonce tvrdit, že CNN celé video vytvořila pro podporu Ukrajiny.

Český článek na stejné téma se pochopitelně zabývá zejména obdobou této falešné zprávy na českých sociálních sítích. Kromě toho se v něm dočteme o konkrétní organizaci zodpovědné za darované hasičského vybavení. A o vedoucím Edmontonských hasičů.

DW zpráva č. 9: Dále se v článku od DW objevil výrok ruské propagandy, že mrtvoly na ulicích v Buči byly nafingované. Rusko tvrdí, že po odchodu jejich vojsk z Buče, a to 30. března 2022se na ulicích nenacházela žádná těla. Videa a fotografie, která byla umístěna na sociálních sítí jsou dle nich falešná. Fact-check stanice DW prokázal, že se jedná o pravá videa a fotografie. Potvrzují je rovněž satelitní snímky a očití svědci.

9. Seznamzpravy.cz zveřejnil podobný článek - *„Česko je na Facebooku jednou z kolébek lží o Buči, ukázala analýza“*. V článku z 21.dubna 2022 se dozvíme, že mezi desítku nejsdílenějších příspěvků na českém Facebooku o událostech v Buči se dostalo hned pět zavádějících. Nejčastější dezinformace pak byly ty v souladu s Ruskou propagandou. Jednalo se o informace typu, že masakr v Buči je podvrh, a na zemi leží herci. Dle těchto informací za fotografiemi a videi stojí Západ. Jako zdroj pro tato tvrzení udává server Seznamzpravy.cz výsledky z analýzy londýnského institutu pro strategický dialog.

Analýza 9

Snaha zahladit stopu Ruské armády je v tomto případě naprosto jasná. Od začátku bylo zcela zřejmé, že je pouze otázkou času, kdy pravda vyjde na povrch. I samotné obyvatele Ruska musí záběry z Buči vyděsit. Jistě se vzhledem k tomu zvýší procento těch, kteří nesouhlasí s Putinovým režimem, jelikož většinu civilistů důkazy o masakru nevinných lidí šokuje.

Dezinformace na toto stejné téma se hromadně šířila i českým internetem, zejména pak na sociální síti Facebook. Ruská propaganda a „ruští trollové", jak je diskutující nazývají, jsou častým tématem v diskuzích pod články na téma Ruská invaze. V českém článku najdeme přesnější informace o údajném zapojení západních zemí do „podvrhu" a „herců". Článek sice mluví o dezinformacích a nepravdivých informacích, ale na rozdíl od DW nepředkládá žádné důkazy, které tyto dezinformace vyvracejí.

DW zpráva č. 10: S předešlou fake news souvisí další výrok Ruské vlády, která tvrdila, že mediální záznamy mrtvých těl jsou falešné. Dokonce se na sociálních sítích objevilo video, které se snažilo diváka přesvědčit, že jedna z „mrtvol" hýbe rukou. DW tvrdí, že po prověření údajného pohybu ruky se dá s jistotou říct, že se jednalo o pouhou optickou iluzi. Dodávají, že mediální analýzy od jiných zdrojů dospěli ke stejnému názoru.

10. Český článek na toto téma se nazývá *„Hýbání mrtvolami z Buče? Slovenská policie odhalila triky dezinformátorů."* Tento článek byl zveřejněný dne 9.4.2022 na zpravodajském portálu Novinky.cz. Autorem článku je bratislavský zpravodaj Ivan Vilček. Článek pojednává o tricích, které pomáhají proruským dezinformátorům navodit dojem, že se mrtvoly na záběrech v Buči hýbou. Slovenská policie uvádí, že podvodníci záměrně šíří video ve velmi špatné kvalitě, aby se iluze dala hůře odhalit. Ve skutečnosti nejde o pohyb ruky mrtvoly, ale o kapku na čelním skle auta, která tuto iluzi vytvořila. Druhá iluze v článku se týkala údajného posunutí těla mrtvoly. Policie vysvětlila, že efekt posunu těla byl dán tím, že zrcátko na autě, ze kterého pocházel záznam bylo pokřivené.

Analýza 10

Zmíněná mediální analýza provedená západními médii nebude mít pro většinu příznivců ruské invaze žádnou váhu. Optická iluze je obecně těžko obhajitelná. Průměrný divák navíc může snadno nabít dojmu, že se jedná o opravdové pohyby.

Článek z Novinky.cz se opírá o konkrétní zjištění Slovenské policie. Společným znakem videí je hlavně nízká kvalita obrazu, která vzniku optických iluzí nahrává. Závěr je nicméně opět shodný s tvrzením DW.

DW zpráva č. 11: DW dále popisuje výrok ruské mluvčí ministerstva zahraničí, která uvedla na svém oficiálním facebookovém profilu, že videa a fotky, která ukazují bombardování měst na Ukrajině jsou podvrhem a nastrčené členskými státy NATO. DW po ověření tvrdí, že tento ruský výrok je další lží, jelikož útoky na civilní objekty a civilisty na Ukrajině jsou velmi dobře zdokumentované. Existují hned dva věrohodné zdroje, které zaznamenávají civilní oběti invaze. Jsou to Bellingcat a vrchní komisař Spojených národů pro lidská práva.

11. Dne 18.3.2022 vydal webový portál irozhlas.cz článek s názvem *„Domy se hroutí, lidi sedí ve sklepích a záchrana nikde, popisuje situaci v Mariupolu uprchlice Anna.“* Autorem článku je reportér Martin Dorazín, který se v danou dobu nacházel v Záporoží. V článku ihned na úvod zazní výrok mluvčí ruského ministerstva zahraničí Marii Zacharovové, že Rusko na Ukrajině žádná města nebombarduje. Všechna videa a fotografie jsou fiktivní a nastražená NATO. V článku se dále objevuje výpověď paní Anny a pana Vladimíra z Ukrajiny, kteří popisují situaci v Mariupolu.

Analýza 11

Ještě před zveřejněním mrtvých těl v Buči na internetu se dalo říci, že videa a fotografie zobrazující bombardování ukrajinských měst byla nejvíce šokujícími zprávami z Ukrajiny. Na jejich základě i původní skeptici v mnoha případech uvěřili, že invaze opravdu začala, a že Ruská vláda lže o tom, o co se snaží (jedno z prvních prohlášení Ruska, které se objevovalo na českých zpravodajských webech bylo, že Rusové útočí pouze na vojenské objekty).

Český článek se zaměřuje na osobní výpovědi dvou údajných svědků. I irozhlas.cz popisuje výroky ruské vlády proti těmto výpovědím, fotografiím a videím. Výpovědi očitých svědků jsou jednoznačně méně věrohodné než komisař spojených národů, nicméně na tom, že bombardování civilních objektů jsou pravdivá se oba zpravodajské články shodly.

DW zpráva č. 12: Další zpráva se týká Tik Tokového videa. Na tomto videu neznámá žena prohlašuje, že teprve šestnáctiletý uprchlík narozený v Rusku byl napaden ukrajinskými uprchlíky na německém vlakovém nádraží. Dodala, že tento mladík na následky svých zranění zemřel. DW opět fact-checkem vyvrací tento příběh. Místní policejní oddělení potvrdilo, že žádný podobný zločin se nikdy nestal. Následně požádali, aby bylo video odstraněno z platformy. Žena se později omluvila a v jiném videu uvedla, že jednalo o informaci od známého, který jí lhal. K tomuto videu bohužel nebyl nalezen žádný zdroj v češtině.

Analýza 12

Dá se předpokládat, že se i v tomto případě se nejspíše jednalo o ruskou sympatizantku. Popis videa a slova v něm byla velmi konkrétní (věk údajné oběti, přesné místo atd.), proto působilo věrohodně. Jednalo o velmi zdařilý koncept na virální video, které mělo vyvolat nenávist k Ukrajině a zároveň lítost nad Rusy. Následné druhé „omluvné" video je chabý pokus o obnovu pověsti autorky po vyvrácení lží místní policií.

DW zpráva č.13: Na Twitteru a jiných sociální platformách se objevila videa Zelenského, který ohlašoval kapitulaci Ukrajiny. Vladimír Putin zase údajně ohlašoval vyhlášení míru s Ukrajinou. Po video analýze DW odhalilo, že se v obou případech jednalo o deepfakes.

14. Portál idnes.cz vydal dne 23.3.2022 článek s názvem *„Falešná kapitulace Zelenského je start, deepfakes změní svět, říká odborník.“* Autorem článku je Karolína Novotná, která ve svém článku píše o falešné výzvě bojujícím Ukrajincům od prezidenta Volodymyra Zelenského, který vyzývá ke kapitulaci. I zde idnes.cz uvádí, že ve skutečnosti prezident Zelenský ke kapitulaci nevyzval, a že se jednalo pouze o video vytvořené za pomocí technologie deepfake.

Analýza 13

Využití technologie deepfake v tomto kontextu ukazuje její mocný potenciál. Videa vidělo obrovské množství lidí, kteří mu okamžitě mohli uvěřit. Dnešní deepfakes jsou při bližším zkoumání velmi dobře rozeznatelné. Od reálných videí budou v blízké budoucnosti k nerozeznání. To může mít za následek například vytvoření chaosu a vyprovokování k útokům.

Český příspěvek se zaměřuje pouze na deepfake Zelenského prohlašující „kapitulaci“. Poskytuje také rozhovor s odborníkem na toto téma. Odborník v článku v podstatě potvrzuje text výše. Ani v tomto případě se názory domácích a zahraničních médií neliší.

DW zpráva č. 14: Zejména na začátku konfliktu se často objevovali zprávy o tom, že prezident Zelenský utekl před válkou z hlavního města Ukrajiny. DW tvrdí, že vzhledem k verifikovatelným video důkazům je zcela jasné, že Zelenský zůstal v Kyjevě.

14. Český článek na toto stejné téma je opět z portálu Novinky.cz. Název článku zní: *„Zelenskyj se vysmál Rusům, že utekl ze země. Prezident je tu!“*. Článek vyšel dne 25.2.2022. Autorem je redaktor Jaroslav Šindelář. Na začátku článku se dočteme o večerním videu natočeného z kyjevských ulic prezidentem Zelenským, a to spolu s hlavními členy tamní vlády, kterým má ukrajinské obyvatele vyzývat k tomu, aby bojovali proti ruské propagandě. Vyvrátil tím fake news o tom, že uprchnul z Kyjeva. Video mělo publikovat ukrajinské ministerstvo obrany na Twitteru. Prezident Ukrajiny měl ještě údajně dodat, že ze země neodejde „za žádnou cenu“.

Analýza 14

Skutečnost, že by prezident napadeného státu uprchl z hlavního města krátce po invazi by velice nahrála Ruské propagandě. Zároveň by dozajista úspěšně velmi demoralizovala Ukrajinské síly. Zelenský zveřejňuje videa na sociálních sítích, přímo z Kyjeva, což dokazuje, že se v Kyjevě stále nachází. Místní obránce bezpochyby motivuje a zároveň nutí více lidí z celého světa Ukrajině fandit. Videa, která mají dokazovat přítomnost Zelenského v hlavním městě by se dala celkem snadno zfalšovat, například pomocí technologie deepfake z předchozího článku.

Článek nalezený na českém portálu má tendenci být velmi pozitivní. Z diskuze pod článkem je zřejmé, že podpora Ukrajině byla v této době ze strany Čechů asi největší. Využití krátkého videa, které současně zachytilo, jak další členy ukrajinské vlády, tak Kyjev v pozadí je jistě velmi chytrý a časově nenáročný nástroj, který jistě splnil svou úlohu.

DW zpráva č. 15: DW v dalším odstavci zmiňuje video, které zobrazuje velkou explozi (opět z platformy Tik Tok). Uživatelka, která toto video nahrála v popisu tvrdí, že se jedná o výbuch v Ukrajinském městě Charkově. Stejné video je následně nahrané na sociální síti Facebook, kde je pro změnu napsáno, že se jedná o ostřelování „ukrajinského velení“. DW provedlo video analýzu a zjistilo, že se ve skutečnosti jedná o záběry z Bejrútu pocházející z roku 2020.

15. Bohužel nebyl nalezen český článek, který by se týkal konkrétně tohoto videa. Příspěvek na webové stránce iRozhlas.cz, který se nazývá *„Falešná nebo stará videa údajně z války na Ukrajině. BBC přinesla návod, jak se nedat oklamat“* ho alespoň zmiňuje. Byl publikován dne 14.3. 2022. Autorkou je Helena Berková. Jak je již z názvu článku zřejmé, pojednává o obecných návodech, jak odhalit falešná videa z ukrajinského konfliktu. Návody mají být původně od BBC. Výbuch, o kterém pojednávám v předešlém odstavci je zmíněný v úvodu článku jako *„dávný výbuch v libanonském Bejrútu“* a je s několika dalšími videi označen jako příklad falešných videí, která jsou na internetu považovaná za reálné záběry z Ruské invaze. Portál iRozhlas.cz dále upřesňuje, že návody od BBC jsou konkrétně od jejich redaktorky Marianny Spring, která se údajně specializuje na dezinformace. Mimo jiné k ověření autenticity videí redaktorka BBC radí všímat si počasí na videích a ověřovat si polohu pomocí Google maps nebo používat funkce zpětného hledání obrázku od Google.

Analýza 15

S trochou nadsázky lze říct, že téměř jakýkoliv videozáznam výbuchu by se dal označit za záběr z ruské invaze. Ač bychom mohli říct, že se jedná o příliš snadný pokus oklamat diváka, tak právě jednoduchost je v tomto případě klíčem k úspěchu. Laik si takové video jen těžko sám ověří a snadno se tak stane obětí dezinformace. I expert na tuto problematiku se může celkem snadno ztratit v záplavě záběrů, které jsou kombinací reálných a falešných zpráv objevujících se na internetu.

Tipy pro rozpoznání falešných videí z českého článku, respektive od redaktorky BBC jsou sice šikovné, ale pro průměrného čtenáře příliš složité. Shoda se zdrojem z DW je i zde zřejmá. Nepřekvapila by, ani kdyby článek nečerpal z britské BBC.

DW zpráva č. 16: Následující odstavec opět ukazuje, že fake news nejsou výsadou jen ruské strany. Na začátku konfliktu se začala na sociálních sítích velmi rychle šířit fotografie starosty Kyjeva Vataliho Kličkova ve vojenské uniformě spolu s kulometem. Popisek fotky tvrdil, že jde o fotku starosty, který bojuje za svou vlast na předních liniích. DW toto tvrzení vyvrátilo. Tvrdí, že „jednoduché zpětné hledání“ potvrdilo, že se jedná o fotografii z vojenského cvičení, které se konalo v roce 2011.

16. Jedinou zmínkou na českých platformách, kde se objevuje zpráva o falešné fotografii Vataliho Kličkova pochází z bulvárního portálu Extra.cz. Jedná se o vcelku zavádějící článek s názvem *„Tři hrdinové, kteří nahánějí Rusům strach. Starosta Kličko, prezident Zelenskyj a Fantom Kyjeva“*. Autorem článku je Štěpán Karlesz. Byl publikován dne 26.2.2022. Dle názvu je zřejmé, že se článek kromě Klička zabývá ještě prezidentem Zelenským, konkrétně vyvrací jeho útěk z Kyjeva. Dále článek pojednává o tzv. duchovy z Kyjeva. I tento fakt nebude skutečný (viz níže). Ve spojitosti s Kličkem portál udává, že i když je fotka staršího data, tak burcuje veřejnost k podpoře Ukrajiny.

Analýza 16

Lze říct, že falešný příspěvek po odhalení téměř vždy způsobí opak toho, o co se autor snažil. I kdyby šíření Kličkova fotografie s kulometem odstartoval podporovatel Ukrajinské obrany, po odhalení podvodného popisu videa by mohlo dojít ke zhoršení důvěry ve zprávy, které mají být nápomocné ke globálnímu vnímání Ukrajinských snah. Je také možné, že příspěvek vytvořil proruský sympatizant, který záměrně uvedl lživý popisek k fotografii. Čekal na jeho odhalení, aby tím Ukrajině uškodil. To jsou ale pouze spekulace.

Český bulvární plátek se musí brát s rezervou, stejně tak jako všechny bulvární noviny. Zavádějící a neúplné informace zde vznikají ve velkém a v době informační války mezi Ruskem a Ukrajinou mohou takto strukturované příspěvky zhoršit povědomí Čechů o Ukrajině. I přes obecnou pověst bulvárů mají jejich texty velkou váhu, protože se obecně těší velkému množství čtenářů.

DW zpráva č. 17: Další odstavec článku popisuje virální video ruského ministerstva zahraničí, kde vzpěračka Maryana Naumova tvrdí, že Ukrajinci jsou nuceni žít v těžkých podmínkách kvůli neonacistům a že Rusko nenapadá civilisty. Jedná se o video směřované k Arnoldu Schwarzeneggrovi. DW dále upřesňuje, že se mělo jednat o odpověď na otevřenou žádost zmíněného kulturisty a herce. Ten žádal Rusko, a především obyvatele Ruska, aby zastavili války. DW tvrdí, že celé video je zcela shodné s ruskou propagandou a v žádném případě se nezakládá na pravdě.

17. Titulek *„Ruská vzpěračka Schwarzeneggera obdivovala, teď ji vytočil: Přijďte na frontu, vzkazuje“* se objevil na webovém portálu isport.blesk.cz dne 23. března 2022. Jedná se o sportovní rubriku bulvárního časopisu Blesk.cz. Autor tohoto článku není uveden. Ruská vzpěračka a údajně milovnice tamní komunistické strany Maryana Naumovová měla prý kulturistu Arnolda Schwarzeneggera za svého velkého idola. Až do doby, než Schwarzenegger napsal o tom, že informace, které ruská vláda předkládá tamním obyvatelům, se nezakládají na pravdě. Maryana ve videu, které je mířeno hercovi a známému kulturistovi obhajuje speciální vojenskou operaci v duchu Putinovy propagandy a tvrdí, že ukrajinci jsou nacisti a od počátku nepokojů na Donbasu zahynulo více než čtrnáct tisíc lidí. Těm podle vzpěračky vůbec nepomohlo to, že Zelenský je Žid, na což Arnold poukázal v souvislosti s ruskou snahou zemi „denacifikovat“.

Analýza 17

Zde se jasně jedná o pokus Ruska zapůsobit zejména na mladší generaci využitím mladé sportovkyně. Téměř sedmiminutové video mělo vzbudit dojem, že je adresované výhradně světově známé celebritě. Je ale zcela jasné, že se jedná pro vzkaz mířený západnímu světu,a to jak ospravedlnit Ruské kroky a hrát si na oběť („naši občané jsou terorizováni Ukrajinci“) a zároveň na osvoboditele Ruského lidu na Ukrajině.

Český bulvární plátek zcela souhlasí s výroky DW. Portál vcelku hrubě kategorizuje sportovkyni za „milovnici tamní komunistické strany“, a to i přes to, že je zcela zřejmé, že s ní úzce spolupracuje. Dobrovolnost jejího počínání je ale čistě spekulativní. I český článek se odkazuje na ruskou propagandu a přidává konkrétní číslo údajných ruskojazyčných lidí při nepokojích na Donbase.

DW zpráva č. 18: Dle DW se na sociálních sítích, a také v reportážích několika médií objevily zprávy, že Rusko na Ukrajině používá tzv. motýlí miny. Jedná se o typ zakázaných nástražných výbušnin, které vypadají jako dětské hračky. DW tyto zprávy nedokázalo potvrdit ani vyvrátit. Věc uzavřelo tím, že se jim nepovedlo najít žádný věrohodný důkaz o použití těchto zbraní na Ukrajině.

19. Český článek „Motýlí“ miny (PFM-1) protipěchotní miny pouze zmiňuje, a to v příspěvku z roku 2015. Jedná se o server zprávy.aktualne.cz a článek má název *„Zabíjení neskončí. Miny mění Ukrajinu v "ďáblovu zahradu"*. Jedná se o článek, který pojednává o konfliktu na východní Ukrajině v roce 2015, a to mezi Ukrajinou a proruskými separatisty. Podrobnější článek o těchto minách použitých v současném konfliktu se v českém jazyce nepovedlo dohledat.

Analýza 18

Dle závěru DW se dá těžko říct, zda se tato tvrzení zakládají na pravdě či nikoliv. Už ale jen z důvodu, že se tyto zprávy objevili současně na tolika místech a komunikačních kanálech se dá říct, že se alespoň z části jedná o pravdu. Bez ohledu na to, jak je to ve skutečnosti, každá zpráva týkající se ohrožení dětí se společností silně manipuluje. Konkrétně tato zpráva velmi ovlivnila sociální pohled na invazi. Český článek je zde uveden pouze pro doplnění, nemá žádnou přidanou hodnotu.

DW zpráva č. 19: Další virální video na sociálních sítích zobrazovalo loučení ukrajinských vojáků s jejich rodinami před odchodem na frontu. DW následně potvrdilo, že se ve skutečnosti jedná o scény z filmu. Poukazuje na to, že se tento typ videí objevuje velmi často a má tendenci se šířit i dlouhou dobu po tom, co se vyvrátí jeho pravost. K tomuto konkrétnímu videu nebyl nalezen žádný český článek. Česká média však obsahují spousty jiných fotografií a videí zobrazující loučící ukrajinšté vojáky.

Analýza 19

Na portálu DW si může pozorný divák všimnout nápadně nacvičených scén i výrazů vojáků na videu. Dezinformační videa a fotografie zakládají na nepozornosti publika. Předpokládá se, že budou shlédnuté v rychlosti, často na mobilních telefonech, jejichž poměrně malé displeje k rozeznání falešných médií (viz. deepfakes výše) zrovna nepomáhají.

DW zpráva č. 20: Další fake news je velmi úsměvná. DW popisuje snímek z ukrajinských televizních zpráv zobrazující velice zvláštní vrak a bílé pozadí, které vypadá jako sníh. I bez fact-checku DW je mnohým jasné, že se jedná o snímek ze sci-fi

filmu „Star Wars“. Fack-check to samozřejmě potvrzuje. Ani k tomuto příběhu nebyl nalézen český ekvivalent.

Analýza 20

Jak bylo uvedeno výše, tato fake news je spíše úsměvná. Je téměř jisté, že zejména starší generace (nebo jen neznalci zdrojového materiálu) mohou při dostatečně krátkém klipu uvěřit, že jim televizní stanice ukazuje reálné záběry z Ukrajiny.

DW zpráva č. 21: Následující odstavec v článku DW popisuje tvrzení ruské mluvčí Marie Zakharové. Ta údajně čtyři dny po začátku invaze pronesla, že Ukrajina začala válku, ne Rusko. Podle ní je současná ruská invaze na Ukrajinu součástí širšího konfliktu na Donbasu, za který je podle odpovědná Ukrajina. Dodala k tomu, že Donbaská populace čelí ze strany Ukrajiny systematické exterminaci. DW udává, že toto tvrzení je lživé. A ve svém fact-checku více rozvádějí, proč to, co mluvčí tvrdí není pravda. Dále v textu DW uvádí, kdy došlo k anexaci Krymu Ruskem a kdy a odkud začala letošní ruská invaze.

21. Na českém portálu deník.cz byl dne 4.března 2022 zveřejněn článek nazvaný *„Moskva ukončuje válku, kterou Ukrajina začala? Ruská mluvčí zkresluje fakta“*. Článek pojednává o vyjádření ruské mluvčí ministerstva zahraničí Marie Zacharovové na jejím facebookovém profilu. Dle jejích slov „Moskva jedná tak, aby „ukončila systematické vyhlazování obyvatel Donbasu“, zjednodušeně Rusko válku nezačalo, ale ukončuje ji. Tvrdí, že pokračující ruská invaze na Ukrajinu je součástí rozsáhlejšího konfliktu na Donbasu, který trvá už roky.

Analýza 21

Svést celou vinu na Ukrajinu se zdá být, zejména na začátku konfliktu rozumným krokem ze strany Ruska. Dá se ale říct, že se jednalo jen o jakési „ujištění“ pro část ruské populace, že ruské počínaní je naprosto v pořádku, a že oni jsou „ti hodní“.

Deník.cz se snaží ujasnit některá fakta. Například, že výrok se měl objevit na facebookové stránce mluvčí. Český deník také udává, že Ruská strana tvrdí, že válku nezačala (jako kdyby říkala „jsme pouze obránci našeho lidu“), ale také následně, že ji

ukončuje („jsme vojenská velmoc a Ukrajina nemá šanci"). Je zajímavé, jak lze v jedné větě vykreslit Rusko pouze v pozitivním světle.

DW zpráva č. 22: Následující odstavec popisuje twitterový účet, který se vydával za oficiální účet mediální stanice CNN. Z tohoto účtu byl zveřejněn tweet o smrti Američana na Ukrajině. DW dodává, že tento tweet se stal virálním zejména z toho důvodu, že stejná osoba měla být již zabita v Afganistánu. DW se údajně obrátilo přímo na CNN. Mluvčí CNN jim sdělil, že fotografie, tweet i celý twitterový účet jsou falešné. DW v článku nezmiňuje reálný osud osoby z tweetu.

22. Článek na toto stejné téma se objevil na publicistickém webu Manipulátoři.cz. Byl publikován dne 18.3.2022 autorem Janem Cemperem. Jedná se sice pouze o převzatý článek právě od DW, ale zajímavostí je, že autor ke článku přikládá snímky z českých facebookových účtů, kteří se na šíření této fake news podíleli. Web udává, že se má jednat o Bernieho Gorese, který je na jednom z falešných účtů (CNN Afganistán) popisován jako novinář. Na druhém falešném účtu (CNN Ukrajina) je znovu vydávaný za mrtvého, tentokrát je však označen za aktivistu. Článek navíc upozorňuje, že se ve skutečnosti jedná o osobnost z platformy YouTube, jménem Jordie McCrathy Jordan.

Analýza 22

Článek DW se v tomto případě opírá o tvrzení mluvčího CNN, na kterém v podstatě stojí celý fact-check. V tomto případě se jednalo o velmi promyšlenou fake news. Bylo zapotřebí vytvořit dva falešné, ale důvěryhodné twitterové účty mezinárodní zpravodajské stanice, dále nashromáždit signifikantní množství fanoušků těchto stránek (nejspíš za pomoci falešných účtů) a potom vydat dva zmíněné příspěvky. Jediným viditelným přešlapem je použití tváře známé osobnosti, která by se dala zpětně snadno dohledat. Využití neznámého obličeje by fake news určitě vylepšilo.

Český (převzatý) článek opět doplňuje informace, zejména pak reálnou identitou „oběti". Zajímavé je vidět reálné české příspěvky se zmanipulovanými osobami. Snahou bylo podkopat důvěru v západní média.

DW zprávy č. 23: Dále se v článku dočteme o tvrzení ukrajinského letectva, které dle DW udávalo, že v budoucnu by mohlo začít vzlétat v rámci bojových misí z polských letišť. V tomto odstavci není uvedeno, kde měli údajné prohlášení ukrajinské letecké síly pronést. Novináři zprávu podrobili fact-checku. DW tvrdí, že tvrzení je lživé a udávají, že „jeden analytik, se kterým hovořili" řekl, že kdyby se tak stalo, bylo by to pro NATO stejné, jako se přímo vložit do probíhajícího konfliktu. Bohužel, ani k tomuto článku neexistuje ekvivalent z české stránky.

Analýza 23

Tento příběh je zvláštně napsaný. Zaprvé zde DW udává verdikt zprávy za zavádějící, následně ho označí přímo za lživý. DW ani neuvádí platformu, na které se mělo tvrzení objevit a vysvětlení konkrétního fact-checku „Jeden analytik, se kterým hovořili" nezní moc přesvědčivě. Pokud se ale skutečně jednalo o falešný příspěvek z (falešného) účtu ukrajinského letectva tak se nabízí vysvětlení, že záměrem autora byla navodit pocit, že Ukrajina si přímo přeje angažovanost NATO v konfliktu.

DW zpráva č. 24: Následující zpráva se jmenuje „Hon na Ducha z Kyjeva". Tvrzení se zabývá údajným ukrajinským pilotem, o kterém se říká, že sestřelil šest ruských letounů, a že se vychvaluje jako válečný hrdina na sociálních sítích. K tvrzením jsou prý i přiloženy fotografie, které ho mají zobrazovat. DW toto tvrzení vyvrací a v dalším textu zmiňuje, že většina videí a fotografií, které jsou na internetu spojeny s tzv. „Duchem z Kyjeva" jsou falešné. DW ještě dodává, že ukrajinské ministerstvo obrany na jejich dotazy ohledně identity pilota nereagovalo.

24. Český článek pochází z portálu cnn.iprima.cz a je nazván: *„Kdo je „Duch z Kyjeva"? Legenda o pilotovi dodává Ukrajincům naději v boji s Ruskem"*. Článek byl publikován dne 25.2.2022. Autorkou článku je Monika Kabourková. Příspěvek začíná větou *„Nikdo neví, jestli je skutečný, mnozí v to však doufají"*. Pilot by měl dle článku obsluhovat stíhací letoun typu MiG-29. Prima také dodává, že úplně nezáleží na tom, jestli je tvrzení pravda či nikoliv, přesto prý lidem dodává naději. Dále se také dočteme, že lidé na sociálních sítích jsou skeptičtí už kvůli tomu, že sestřelení šesti letounů během jednoho dne je až nadlidský úkol.

Analýza 24

V této analýze se poprvé setkáváme s rozdílným názorem na věc mezi pohledy DW a českými médii. DW udává, že po jejich fact-checku bylo zjištěno, že většina obsahu, která má údajného pilota zobrazovat se ukázala být falešná. Jedna z posledních vět v německém článku, však ale úplně nevyvracela celý koncept „Ducha z Kyjeva". Tvrdí totiž, že se Ukrajinské úřady k dotazům ohledně pilota nevyjadřují. Naopak český článek v tomto případě nedělá žádné závěry, několikrát se však opírá o skutečnost, že nezáleží, zda se jedná o pravdivou zprávu či fake news, efekt na Ukrajince je podle nich totožný v obou případech. V tomto případě se nedá zjistit, zdali v době psaní českého článku nebyly důkazy o falešných fotografiích a videích k dispozici, nebo zdali tyto fakta Prima v článku nepoužila záměrně.

DW zprávy č. 25: Další odstavec se týká Tik Tokového videa, které zobrazuje velkou explozi, která má dle popisku znázorňovat útok na Ukrajinu. A to den před oficiální invazí Ruska na Ukrajinu. I toto video novináři označují za falešné. DW píše o tom, že video zobrazuje vzplanutí čerpací stanice v ruském městě Novosibirsk.

25. Český článek zmiňující toto falešné video nebylo nalezeno. Podařilo se však dohledat zprávu z portálu TN.cz od autora Petra Zeleného z roku 2021. Zpráva popisuje reálný výbuch čerpací stanice, který se dle článku měl odehrát v Rusku dne 14.6.2021.

Analýza 25

Tato zpráva má nejspíš, stejně jako mnoho předešlých zpráv, za cíl popsat Rusko, v co nejhorším světle. Jak již ale bylo řečeno v předešlých analýzách, přehnaná snaha se může po odhalení fake news minout účinkem. Český článek zde opět pouze doplňuje a upřesňuje některé informace.

DW zpráva č. 26: Dále se v článku dočteme o reportérovi, který v televizním kanálu německých novin „Bild“ hovořil o videu, které ukazuje stovky ruských vojáků, kteří seskakují s padáky nad Charkovem. DW označuje tvrzení za lživé. Jejich fact-check prokázal, že toto video bylo publikováno již v roce 2016 na různých platformách a mělo zobrazovat ruské parašutisty při tréninku na ruském území.

26. Jediným českým článek, který tento příspěvek alespoň obsahoval je po přečtení pouze překlad z britské stanice BBC. Není žádným překvapením, že i zde se tvrzení shodují s článkem od DW.

Analýza 26

Je určitě s podivem, že se v tomto případě stal zdrojem dezinformace také německý zpravodajský kanál. I když se v některých zdrojích můžeme setkat s označením deníku Bilb jako bulvárního plátku, čtenář by u německého zdroje mohl automaticky čekat určitou váhu, a tedy i pravdivost zpráv. Dle fact checku se tedy zdá, že jedinou pravdivou částí zprávy bylo to, že parašutisté byli Rusové.

DW zpráva č. 27: Následující část se zabývá tweetem, který obsahoval video, které mělo popisek „přímý přenos války na Ukrajině“. Video zobrazovalo formaci bojových letounů letícími velmi blízko osídlené oblasti. Dle fact-checku se jedná o lež, video se údajně vyskytuje na internetu již od roku 2020 a zobrazuje leteckou show nedaleko Moskvy.

27. Stejné video se objevuje v českém článku z portálu idnes.cz s názvem *„Dezinformace kolem Ukrajiny: šíří se falešná videa i proruské narativy“*. Vydán byl dne 24.2.2022. Video zachycující formaci ruských stíhacích letounů je jen jedním z mnoha lživých videí, které se v článku nacházejí. Portál iDnes stíhací letouny označuje za „bombardéry“. V článku je mimo jiné uvedeno, že policie ČR vyzvala Čechy k obezřetnosti.

Analýza 27

I v tomto případě autoři dezinformace uvedli pouze jedinou pravdivou informaci – skutečně se jedná o ruské stíhací letouny. Zobrazená letová formace svou souhrou, a

hlavně okolním městským prostředím jistě dokáže u diváka vytvořit pocit strachu z ruských vojenských sil.

DW zpráva č. 28: Další v pořadí je odstavec hovořící o videu zveřejněném na sociálních sítích, které se mělo údajně objevit na začátku konfliktu. Dle popisku zobrazuje bitvu země-vzduch mezi Ruskem a Ukrajinou. DW udává, že se ve skutečnosti jedná o záběry z počítačové hry „Arma 3" pocházející z roku 2013. DW dodává, že se nejedná o první instanci, kde se snímky z videoher vydávají za boje v reálném světě.

28. Český žurnalistický web hlidacipes.org ve svém příspěvku zmiňuje videa ze hry Arma 3 vydávající se za reálné záběry z ukrajinského konfliktu. Dodává také, že se údajně tohoto typu dezinformace měl dopustit i oficiální twitterový účet ukrajinského ministerstva obrany. Ten použil úseky z leteckého simulátoru „Digital combat simulator world". V článku bohužel chybí zdroj tohoto tvrzení.

Analýza 28

V dnešní době se dají některá videa z videoher, zejména v krátkých záběrech vydávat za skutečná. Avšak využití titulu z roku 2013 nedává úplně smysl. Nízká kvalita záběrů ubírá videu na uvěřitelnosti.

Pokud je tvrzení z českého webu pravdivé, znamená to ostudu pro ukrajinské ozbrojené síly.

DW zpráva č. 29: V článku se pojednává o virálním videu, které se údajně šířilo na sociálních sítích. Na videu se údajně nachází tancující ruští vojáci, kteří mají slavit začátek války. Dle DW se ve skutečnosti jedná o video z roku 2018, kdy uzbecká vojenská kapela hrála v uzbeckém hlavním městě. I v tomto případě nebylo možné dohledat článek na stejné téma v češtině.

Analýza 29

Snahou autora je poškodit ruské vojáky tím, že chce navodit dojem, že mají vojáci z invaze radost. Toto video není spravedlivé, vzhledem k mladým ruským vojákům, kteří dle některých zpráv netušili, že jdou do války.

DW zpráva č. 30: Často udávaná „denacifikace“ Ukrajiny je častým tématem tohoto konfliktu. V článku se dočteme o ospravedlnění invaze ruským prezidentem. Rusko se dle jeho slov pouze „musí bránit“, zastavit genocidu a denacifikovat Ukrajinu. DW označuje výrok za „zavádějící/lživý“. V následující části textu tvrdí, že se jedná o falešné tvrzení, kdy Rusko jednoznačně začalo agresivní útok.

Analýza 30

Zpráva č. 30 nebyla analyzována. Je to zejména kvůli tomu, že zpráva č. 30 se významově téměř shoduje se zprávou č. 3, a tak by analýza byla téměř identická. Z toho důvodu nebyli dohledány další české články.

DW zpráva č. 31: Poslední zprávou v článku je Putinovo tvrzení o tom, že moderní Ukrajina byla vytvořena Ruskem, nikdy neměla žádné pořádné tradice nebo opravdový status státu. Toto prohlásil v televizním vysílání. Fact-check zprávu označil za zavádějící či falešnou. DW dodalo, že tyto skutečnosti konzultovalo s experty v oboru. Ukázalo se, že ukrajinská lidová republika existovala od roku 1918, a obsazena Rudou armádou byla až o dva roky později. Samostatnost získala zejména za pomoci hnutí za nezávislost proti vládě ruského cara. Území, která tvoří Ukrajinu, byla z velké části součástí ruské říše, do jejího rozpadu v roce 1917.

31. Český článek se nazývá *„Putinův mylný výklad historie. Ukrajinské dějiny se vyvíjely nezávisle na Rusku“* a byl publikován dne 24.2.2022 na portále idnes.cz. Autor článku není uveden. Český článek pojednává o Putinově prohlášení, že Ukrajina nemá vlastní tradice, a že je umělým konstruktem, který si nárokuje ruská území. Dle slov Putina byla Ukrajina vytvořena Leninem. Putin také prohlásil, že Rusové a Ukrajinci jsou „jeden lid“, a že Kyjev je „matka všech ruských měst“. Dodal, že za konflikt mezi nimi můžou západní státy.

Analýza 31

Český článek zejména upravuje některá tvrzení od DW. Je pravda, že některé konkrétní výrazy mohli být pozměněny při překladu (mnou i portálem iDnes). Zejména u tvrzení, že moderní Ukrajina byla vytvořena Ruskem, přičemž český článek tvrdí, že Putin

pronesl, že Ukrajina je umělý konstrukt nárokujíce si ruská území. Český článek přidává informaci o tvrzení, že Ukrajinu měl vytvořit Lenin, a také že Putin přímo tvrdil, že Rusové a Ukrajinci jsou jeden lid, za konflikt dle jeho slov může Západ. Nárokování „historicky ruských území" se ale v obou příspěvcích shoduje.

V praktické části bylo celkem analyzováno třicet zpráv (respektive 31, nepočítaje jednu téměř duplicitní) z německého článku od DW. Celkem šest ekvivalentních zpráv z tohoto článku se nepodařilo nalézt na českých zpravodajských webech. K dalším několika zprávám z německého článku byly nalezeny pouze zmínky v jinak zaměřených českých článcích nebo pouze zmínky na sociálních sítích. I přesto, že snahou bylo vyhnout se bulvárním portálům, jsou v některých případech v této práci použity. A to z důvodu, že dané téma se nedalo nalézt na věrohodných zpravodajských portálech.

Zdroje k výsledným článkům:

DW zpráva č. 1 – 31:

Fact check: Fake news thrives amid Russia-Ukraine war. Deutsche Welle – DW. Europe – News. 28.04.2022. [online]. [cit. 30.06.2022]. Dostupné z: https://www.dw.com/en/fact-check-fake-news-thrives-amid-russia-ukraine-war/a-61477502

České zdroje:

1. *Putin: Rozhodnout o invazi na Ukrajinu bylo těžké. Přesvědčily ho snahy Kyjeva získat jaderný status.* E15.cz. [online]. [cit. 02.07.2022]. Dostupné z: https://www.e15.cz/valka-na-ukrajine/putin-rozhodnout-o-invazi-bylo-tezke-presvedcily-ho-snahy-kyjeva-ziskat-jaderny-status-1388221
2. *Putin v projevu označil útok na Ukrajinu za správné rozhodnutí.* České noviny | ČeskéNoviny.cz [online]. [cit. 03.07.2022]. Dostupné z: https://www.ceskenoviny.cz/zpravy/putin-v-projevu-oznacil-utok-na-ukrajinu-za-spravne-rozhodnuti/2203386
3. *Lavrov vysvětlil, co si Rusko představuje pod pojmem denacifikace Ukrajiny.* Novinky.cz. [online]. [cit. 05.07.2022]. Dostupné z: https://www.novinky.cz/valka-na-ukrajine/clanek/lavrov-vysvetlil-co-si-rusko-predstavuje-pod-pojmem-denacifikace-ukrajiny-40390943
4. *Putin trvá na ruských požadavcích. Chce hledat diplomatické řešení krize.* Deník.cz. [online]. [cit. 07.07.2022]. Dostupné z: https://www.denik.cz/staty-mimo-eu/putin-rusko-scholz-ukrajina-krize-20220215.html
5. *Lidé na internetu šíří lživé video. Neznámou dívku vydávají za dceru Zelenského.* Forum24. [online]. [cit. 07.07.2022]. Dostupné z: https://www.forum24.cz/lide-na-internetu-siri-lzive-video-neznamou-divku-vydavaji-za-dceru-zelenskeho/
6. *Oficiální účet Ozbrojených sil Ukrajiny před chvílí upozornil na nový fake účet. Twitter by měl zareagovat velmi rychle.* Uživatel „Roman M“, Twitter. [online]. [cit. 08.07.2022]. Dostupné z: https://twitter.com/Fbeyeee/status/1495350575998844932?ref_src=twsrc%5Etfw

7. *Český článek nebyl nalezen.*

8. *CNN nezfalšovala snímky požáru ve Lvově. Šlo o darovanou výstroj.* Faktické.Info. [online]. [cit. 08.07.2022]. Dostupné z: https://www.faktícke.info/cnn-nezfalsovala-snimky-pozaru-ve-lvove-slo-o-darovanou-vystroj/

9. *Česko je na Facebooku jednou z kolébek lží o Buči, ukázala analýza.* Seznam Zprávy. [online]. [cit. 08.07.2022]. Dostupné z: https://www.seznamzpravy.cz/clanek/zahranicni-cesko-je-na-facebooku-jednou-z-kolebek-lzi-o-buci-ukazala-analyza-199105

10. *Hýbání mrtvolami z Buče? Slovenská policie odhalila triky dezinformátorů.* Novinky.cz. [online]. [cit. 10.07.2022]. Dostupné z: https://www.novinky.cz/zahranicni/evropa/clanek/hybani-mrtvolami-z-buci-slovenska-policie-odhalila-triky-dezinformatoru-40392849

11. *Domy se hroutí, lidi sedí ve sklepích a záchrana nikde, popisuje situaci v Mariupolu uprchlice Anna.* iRozhlas. [online]. [cit. 10.07.2022]. Dostupné z: https://www.irozhlas.cz/zpravy-svet/uprchlici-z-ukrajiny-svedectvi-pribehy-mariupol_2203170836_ern

12. Český článek nebyl nalezen.

13. Falešná kapitulace Zelenského je start, deepfakes změní svět, říká odborník. iDNES. [online]. [cit. 10.07.2022]. Dostupné z: https://www.idnes.cz/zpravy/domaci/deepfakes-dezinformace-kyberbezpecnost.A220322_093249_domaci_knn

14. *Zelenskyj se vysmál Rusům, že utekl ze země. Prezident je tu!* Novinky.cz. [online]. [cit. 10.07.2022]. Dostupné z: https://www.novinky.cz/zahranicni/clanek/zelenskyj-se-vysmal-rusum-ze-utekl-ze-zeme-prezident-je-tu-40388428

15. *Falešná nebo stará videa údajně z války na Ukrajině. BBC přinesla návod, jak se nedat oklamat.* iRozhlas. [online]. [cit. 11.07.2022]. Dostupné z: https://www.irozhlas.cz/zpravy-svet/falesna-videa-dezinformace-bbc-navod-poznavani_2203141735_pik

16. *Tři hrdinové, kteří nahánějí Rusům strach. Starosta Kličko, prezident Zelenskyj a Fantom Kyjeva.* Expres.cz. [online]. [cit. 11.07.2022]. Dostupné z:

https://www.expres.cz/zpravy/ukrajina-rusko-valka-kyjev-volodymyr-zelenskyj-vitalij-klicko.A220226_091504_dx-zpravy_stes

17. *Ruská vzpěračka Schwarzeneggera obdivovala, teď ji vytočil: Přijďte na frontu, vzkazuje.* iSport.cz. [online]. [cit. 12.07.2022]. Dostupné z: https://isport.blesk.cz/clanek/blesk-sport/411192/ruska-vzperacka-schwarzeneggera-obdivovala-ted-ji-vytocil-prijdte-na-frontu-vzkazuje.html

18. *Zabíjení neskončí. Miny mění Ukrajinu v "ďáblovu zahradu".* Aktuálně.cz. Zprávy - Aktuálně.cz [online]. [cit. 12.07.2022]. Dostupné z: https://zpravy.aktualne.cz/zahranici/miny-meni-ukrajinu-v-dablovu-zahradu/r~d0c2b3c6cc7611e4a66e0025900fea04/

19. Český článek nebyl nalezen.

20. Český článek nebyl nalezen.

21. Moskva ukončuje válku, kterou Ukrajina začala? Ruská mluvčí zkresluje fakta. Deník.cz. [online]. [cit. 13.07.2022]. Dostupné z: https://www.denik.cz/ze_sveta/ministerstvo-zahranicnich-veci-ruske-federace-ukrajina-valka.html

22. Americký aktivista nebyl zabit zároveň na Ukrajině a v Afghánistánu. Manipulátoři.cz. [online]. [cit. 13.07.2022]. Dostupné z: https://manipulatori.cz/americky-aktivista-nebyl-zabit-zaroven-na-ukrajine-a-v-afghanistanu/

23. Český článek nebyl nalezen.

24. *Duch z Kyjeva: Příběh pilota, který dává Ukrajincům naději.* CNN Prima NEWS. [online]. [cit. 13.07.2022]. Dostupné z: https://cnn.iprima.cz/kdo-je-duch-kyjeva-legenda-o-pilotnim-esu-dodava-ukrajincum-nadeji-v-boji-s-ruskem-82000

25. *VIDEO: Ohnivá zkáza. Obří výbuch benzínky v Rusku zranil desítky lidí!* TN.cz. [online]. [cit. 13.08.2022]. Dostupné z: https://tn.nova.cz/zpravodajstvi/clanek/437905-video-ohniva-zkaza-obri-vybuch-benzinky-v-rusku-zranil-desitky-lidi

26. *FAKENEWS: Údajné záběry z Ukrajiny pocházejí často odjinud, varuje BBC.* Deník.cz. [online]. [cit. 14.07.2022]. Dostupné z: https://www.denik.cz/ze_sveta/bbc-ukrajina-valka-

27. Dezinformace kolem Ukrajiny: šíří se falešná videa i proruské narativy. iDNES.cz. [online]. [cit. 14.07.2022]. Dostupné z: https://www.idnes.cz/zpravy/domaci/dezinformace-rusko-ukrajina-invaze.A220224_091401_domaci_knn¨

28. *Válka v přímém přenosu. Některá "autentická" videa z Ukrajiny jsou z počítačových her*. HlídacíPes.org. [online]. [cit. 14.07.2022]. Dostupné z: https://hlidacipes.org/valka-v-primem-prenosu-nektera-autenticka-videa-z-ukrajiny-jsou-ale-z-pocitacovych-her/

29. Opakující se článek.

30. Putinův mylný výklad historie. Ukrajinské dějiny se vyvíjely nezávisle na Rusku. iDNES.cz. [online]. [cit. 15.07.2022]. Dostupné z: https://www.idnes.cz/zpravy/zahranicni/ukrajina-rusko-putin-historie-kyjevska-rus.A220223_123427_zahranicni_jhr

5. Diskuze

Z výsledků analýzy v praktické části práce je zřejmé, že v drtivé většině případů česká média podávají stejné informace jako ty západní, v našem případě reprezentované německým článkem od DW. Toto zjištění není vůbec překvapivé, protože česká média ve většině případů čerpají informace k tvorbě článků právě ze západních zdrojů. V některých českých článcích se objevili určité nepřesnosti nebo nesrovnalosti se zprávami od DW, těžko ale říci, jaký byl jejich důvod. Mohl to být například špatný překlad či neúplné informace.

Článek z DW také nelze považovat za „absolutně pravdivý". Je zřejmé, že stejně jako jiná média (západní nebo východní) jsou více či méně ovlivněna propagandou z obou stran. V této práci je praktická část založena na německém článku, a proto by pro některé čtenáře nemusela být zcela objektivní. Já jako autorka této práce jsem bezpochyby ovlivněna západním výkladem skutečností rusko-ukrajinského konfliktu. A proto se nemohu, stejně tak jako kdokoliv jiný, označit za zcela nestrannou.

Mnoho Čechů podporuje ruské narativy, což je zřejmé zejména ze zmíněných příspěvků na sociálních sítí nebo z diskusí pod použitými články. Avšak většina lidí v České republice má jednoznačně spíše prozápadní smýšlení, a tak mají mnohem větší tendence souhlasit se zprávami ze Západu. Určitý vliv na tom má nenávist spousty lidí ke komunismu a Rusku všeobecně, která je zde zakořeněná ještě z dob ČSSR.

První výzkumná otázka zněla: *„Jaký vliv mají falešné zprávy na bezpečnostní politiku státu?"*

Odpověď na tuto otázku je na první pohled velice jednoduchá. Falešné zprávy mají na bezpečnostní politiku státu nezanedbatelný vliv. Fake news se dostávají do popředí stále více, jelikož se jedná o jednu z nejznámějších hrozeb kyberprostoru a vzhledem k současné situaci na Ukrajině se tento pojem dostává do podvědomí široké veřejnosti. Jak již bylo řečeno v teoretické části práce – fake news mají potenciál např. rozpoutávat vojenské konflikty, narušit důvěru ve vládu státu a ve vlastní média. Dále také mohou být

příčinou vzniku nepokojů, demonstrací a dalších velmi závažných bezpečnostních rizik. Vláda české republiky (stejně tak, jako vlády jiných zemí) je připravena na řešení všech zmíněných důsledků fake news. Důležitým faktorem je nejistota, jelikož se předem nedá odhadnout, kdy a v jaké formě se falešná zpráva objeví.

S tím souvisí druhá výzkumná otázka, která zní: *„Jak lze zastavit šíření falešných zpráv?“* Opět se nabízí dvouslovná odpověď – velmi těžko. Jeden z důvodů je výše zmíněná nejistota. Pokud nevíme, kdy a v jaké formě se falešná zpráva objeví, tak na ní nemůžeme dopředu naplánovat účinnou odezvu. Určitým preventivním postupem je edukace obyvatelstva o této problematice, zejména širokou veřejnost laicky učit, jak rozeznat falešnou zprávu. V případě, že se již konkrétní fake news objeví, jediným účinným řešením je co nejdříve falešnou zprávu vyvrátit. Důležité je také uvést informace na pravou míru. Informace o falešné zprávě a současně i pravdivé informace by se měli dostat k co možná nejvíce lidem. V ideálním případě i k těm, kteří o zprávě ještě neslyšeli.

V tomto případě by byla obtížná realizace – takto upravená zpráva by se musela rozšířit prakticky do všech médií, zejména pak na internet, sociální sítě, televizní vysílání, rádio či obyčejné papírové noviny. Jenom tak by bylo možné zajistit, že by se kýžená zpráva dostala k co největšímu počtu osob napříč věkovým a socioekonomickým spektrem.

6. Závěr

Tato diplomová práce se zabývá hybridními hrozbami a státní bezpečnostní agendou. Větší část této práce je zaměřena na hrozby v kyberprostoru, zejména na fenomén „fake news“.

V teoretické části této práce jsou přehledně definovány důležité pojmy jako je např. hybridní válka, státní bezpečnostní systém, kybernetický prostor, kybernetická bezpečnost, informační válka, fake news a diskurzivní analýza.

Praktická část práce je zaměřena na analýzu falešných zpráv z Rusko-ukrajinského konfliktu. V této části je porovnáván shrnující článek z německého portálu Deutche Welle, a dále pak jednotlivé články z českých médií.

V této části je porovnáván shrnující článek z německého portálu Deutche Welle a jednotlivé články z českých médií.

Cílem této práce byla analýza a aplikace zvolené metody diskurzivní analýzy na zprávy o ukrajinském konfliktu. Výsledné analýzy se kvůli povaze dat neprováděli pomocí žádné z konvenčních metod analýzy diskurzu, ale jednalo se o kvantitativně-kvalitativní porovnání s dominantními prvky hermeneutické metody narativní analýzy.

Dalšími dílčími postupy bylo získání informací o hrozbách v kyberprostoru, a jak těmto hrozbám můžeme čelit. V této kapitole byly definované základní pojmy týkající se problematiky kyberprostoru a hrozeb, které z něho plynou. Obecnější informace o obraně proti těmto hrozbám jsou předmětem teoretické části.

Dále se práce zabývala popisem informační války a kompetencí vlády proti šíření falešných zpráv. Tato část je téměř rovnoměrně zpracována v teoretické i v praktické části práce. Představené narativy z války mezi Ruskem a Ukrajinou jsou modelovým příkladem, jak může moderní informační válka vypadat. Kompetence vlády obecně a hlavně ty, které mohou pomoci proti šíření falešných zpráv jsou uvedené v teoretické části diplomové práce.

Práce může být v budoucnu rozšířena dalším bádáním, zejména po shrnutí fake news po ukončení Rusko-ukrajinského konfliktu a vyhodnocení jejich pravosti či nepravosti. Jedná se také o ucelený dokument, který může být dále použit ke studiu této problematiky anebo k přednáškám na dané téma.

7. Zdroje

1. JONES, Andy. Global information warfare: how businesses, governments, and others achieve objectives and attain competitive advantages. 2002. ISBN 0-8493-1114-4.

2. NATO. Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote. NATO – Homepage [online]. [cit. 01.04.2022] Dostupné z: https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.htmlDevelopment_and_Change_of_the_Concept_of_Hybrid_Wa.pdf

3. DAMJANOVIČ, Dragan. Types of information warfare and examples of malicious programs of information warfare. [online]. Srbská republika: Military technical courier, 2017. Dostupné z: https://scindeks-clanci.ceon.rs/data/pdf/0042-8469/2017/0042-84691704044d.pdf

4. SOULEIMANOV, Emil. Konflikt v Čečensku: minulost, současnost, perspektivy. Praha: Sociologické nakladatelství (SLON), 2011. Sociologické aktuality. ISBN 978-80-7419-066-7.

5. HOFFMAN, G., F. Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington: Potomac Institute for Policy Studies 2007, s. 28. Dostupné z: https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf

6. *Vývoj a proměna konceptu hybridní války.* Vojenské rozhledy. [online]. [cit. 10.04.2022] Dostupné z: https://www.vojenskerozhledy.cz/kategorie-clanku/ozbrojene-konflikty/vyvoj-a-promena-konceptu-hybridni-valky

7. McCULLOH,T. *The Inadequacy of Definition and the Utility of a Theory of Hybrid Conflict: Is the Hybrid Threat New?* Joint Special Operations University 2012. Dostupné z : https://apps.dtic.mil/sti/pdfs/ADA611608.pdf

8. KILCULLEN, D. The Accidental Guerilla. Fighting Small Wars in the Midst of a Big One. Oxford-New York: Oxford University Press 2009. ISBN: 978-0-19-536834-5

9. *Bezpečnostní politika státu.* Ministerstvo vnitra České republiky. [online]. [cit. 15.04.2022] Dostupné z: https://www.mvcr.cz/clanek/bezpecnostni-politika-statu.aspx

10. *Bezpečnostní strategie ČR.* Vláda České republiky. 2015. [online]. [cit. 01.05.2022] Dostupné také z: https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf

11. *Ochrana vnitřní bezpečnosti státu.* Ministerstvo vnitra České republiky. [online]. [cit. 01.06.2022] Dostupné z: https://www.mvcr.cz/clanek/ochrana-vnitrni-bezpecnosti-statu.aspx

12. *Kdo je kdo – orgány odpovědné v ČR za vnitřní bezpečnosti*. Ministerstvo vnitra České republiky [online]. [cit. 03.06.2022] Dostupné z: https://www.mvcr.cz/clanek/kdo-je-kdo-organy-odpovedne-v-cr-za-vnitrni-bezpecnosti.aspx

13. Zákon č. 219/1999 Sb. o ozbrojených silách ČR. Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění [online]. [cit. 06.06.2022] Dostupné z: https://www.zakonyprolidi.cz/cs/1999-219

14. Zákon č. 153/1994 Sb. o zpravodajských službách České republiky. Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění [online]. Copyright © AION CS, s.r.o. 2010 [cit. 06.06.2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/1994-153

15. *Bezpečnostní systém ČR.* BIS. Bezpečnostní informační služba České republiky. [online]. Dostupné z: https://www.bis.cz/bezpecnostni-system/

16. Zákon č. 218/1999 Sb. Branný zákon. Zákony pro lidi - Sbírka zákonů České republiky v aktuálním konsolidovaném znění [online]. [cit. 10.06.2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/1999-218

17. *Postavení vlády*. Vláda České republiky. Úvodní stránka [online]. [cit. 10.06.2022] Dostupné z: https://www.vlada.cz/cz/clenove-vlady/postaveni-vlady/postaveni-vlady---ustava-15263/

18. *Bezpečnostní rada státu.* Ministerstvo vnitra České republiky. Úvodní strana - Ministerstvo vnitra České republiky [online]. [cit. 12.06.2022]. Dostupné z: https://www.mvcr.cz/clanek/bezpecnostni-rada-statu-234869.aspx

19. *Vznik a působnost Ministerstva zahraničních věcí.* Ministerstvo zahraničních věcí České republiky. [online]. [cit. 12.06.2022] Dostupné z: https://www.mzv.cz/jnp/cz/o_ministerstvu/vznik_a_pusobnost_ministerstva.html

20. *Působnost a činnosti*. Ministerstvo obrany České republiky. [online]. [cit. 15.06.2022]. Dostupné z: https://mocr.army.cz/ministr-a-ministerstvo/pusobnost/pusobnost-a-cinnosti-5131/

21. *Působnost ministerstva.* Ministerstvo vnitra České republiky. Úvodní strana - Ministerstvo vnitra České republiky [online]. [cit. 17.06.2022]. Dostupné z: https://www.mvcr.cz/clanek/ministerstvo-pusobnost-ministerstva.aspx

22. *Cyberspace.* CSRC Glossary. [online]. [cit. 18.06.2022] Dostupné z: https://csrc.nist.gov/glossary/term/cyberspacecyberspace

23. *Cyberspace.* Encyclopedia Britannica – communications. [online]. [cit. 20.06.2022]. Dostupné z: https://www.britannica.com/topic/cyberspace

24. *What is Cyberspace?* Techopedia. [online]. [cit. 22.06.2022]. Dostupné z: https://www.techopedia.com/definition/2493/cyberspace

25. *What is cybercrime?* Techtarget - SearchSecurity. [online]. [cit. 22.06.2022]. Dostupné z: https://www.techtarget.com/searchsecurity/definition/cybercrime

26. *What Is Cybercrime?* Avast. [online]. [cit. 22.06.2022]. Dostupné z: https://www.avast.com/c-cybercrime

27. *Cybercrime*. Norfolk Constabulary. Homepage [online]. [cit. 25.06.2022]. Dostupné z: https://www.norfolk.police.uk/advice/cybercrime

28. *The Top Cyber Security Blogs and Websites of 2020.* University of San Diego. Online degrees. [online]. [cit. 25.06.2022]. Dostupné z: https://onlinedegrees.sandiego.edu/top-cyber-security-blogs-websites/

29. *Top 10 Cybersecurity Threats in 2022*. Embroker. [online] [cit. 01.07.2022]. Dostupné z: https://www.embroker.com/blog/top-10-cybersecurity-threats-2022/

30. *Cyber Threat Source Descriptions*. CISA. Homepage. [online]. [cit. 01.07.2022]. Dostupné z: https://www.cisa.gov/uscert/ics/content/cyber-threat-source-descriptions

31. *7 Types of Cyber Security Threats.* University of North Dakota. Online degrees. [online]. [cit. 01.07.2022]. Dostupné z: https://onlinedegrees.und.edu/blog/types-of-cyber-security-threats/

32. *Kybernetická bezpečnost*. Vláda České republiky. Informační centrum vlády (ICV) [online].]. [cit. 01.07.2022]. Dostupné z: https://icv.vlada.cz/cz/evropske-zalezitosti/umela-inteligence/kyberneticka_bezpecnost/kyberneticka-bezpecnost-192766/

33. *Kybernetická bezpečnost: jak EU řeší kybernetické hrozby.* Consilium. Rada Evropské unie. [online]. [cit. 03.07.2022]. Dostupné z: https://www.consilium.europa.eu/cs/policies/cybersecurity/

34. *Sharp Increase in Cyberattacks in EU -. Latest breaking news and videos of European and World.* Eupolitical report. [online]. [cit. 07.07.2022]. Dostupné z: https://www.eupoliticalreport.eu/sharp-increase-in-cyberattacks-in-eu/

35. *EU Proposes Stronger Cyber Security Rules Amid Growing Breach Threat.* IT governance. [online]. [cit. 07.06.2022]. Dostupné z: https://www.itgovernance.eu/blog/en/eu-proposes-stronger-cyber-security-rules-as-the-threat-of-breaches-escalates

36. KOVÁCS, László. Cyber security policy and strategy in the European union and NATO. Military Art and Science [online]. Budapešť: National University of Public Service, 2018 [cit. 18.07.2022]. Dostupné z: https://www.armyacademy.ro/reviste/rev1_2018/KOVACS.pdf

37. *NATO Cyber Defence.* NATO. [online]. 2021. [cit. 18.07.2022]. Dostupné z: https://www.nato.int/nato_static_fl2014/assets/pdf/2021/4/pdf/2104-factsheet-cyber-defence-en.pdf

38. *Transatlantic relations and cybersecurity: How NATO tackles cyberthreats?* EURACTIV.pl [online]. [cit. 20.07.2022]. Dostupné z: https://www.euractiv.pl/section/bezpieczenstwo-i-obrona/news/cybersec-transatlantic-relations-cybersecurity-nato-cyberthreats-usa-europe/

39. *NATO's role in cyberspace.* NATO. [online]. [cit. 20.07.2022]. Dostupné z: https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html

40. *Statement by the Euro-Atlantic Security Leadership Group. European Leadership Network.* [online]. [cit. 20.07.2022]. Dostupné z: https://www.europeanleadershipnetwork.org/group-statement/statement-by-the-euro-atlantic-security-leadership-group-addressing-cyber-threats/

41. *Media-(Dis)Information-Security.* NATO – Oficiální webové stránky. [online]. [cit. 22.07.2022]. Dostupné z: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf

42. *Definition of information warfare*. PCMag. [online]. [cit. 22.07.2022]. Dostupné z: https://www.pcmag.com/encyclopedia/term/information-warfare

43. *Vojenské klamání v informačním věku.* Vojenské rozhledy - Aktuality [online]. [cit. 23.07.2022]. Dostupné z: https://www.vojenskerozhledy.cz/kategorie-clanku/teorie-a-doktriny/vojenske-klamani-v-informacnim-veku

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

45. ŠTUDENT, Michal. Informační válka a rusko-ukrajinský konflikt. Blogy Respektu. [online]. Dostupné z: https://student.blog.respekt.cz/informacni-valka-a-rusko-ukrajinsky-konflikt/#_Toc36919953

46. *Národní strategie kybernetické bezpečnosti České republiky*. Národní úřad pro kybernetickou a informační bezpečnost. [online]. [cit. 24.07.2022]. Dostupné z: https://www.dataplan.info/img_upload/7bdb1584e3b8a53d337518d988763f8d/narodni_strategie_kb_2020-2025_-cr.pdf

47. *Bezpečnostní prostředí*. Ministerstvo zahraničních věcí České republiky. [online]. [cit. 24.07.2022]. Dostupné z: https://www.mzv.cz/jnp/cz/zahranicni_vztahy/bezpecnostni_politika/bezpecnostni_prostredi.html

48. *GOVCERT.* Národní centrum kybernetické bezpečnosti. [online]. [cit. 24.07.2022]. Dostupné z: https://www.govcert.cz/cs/vladni-cert/govcert-cz/

49. *Kyberprostor jako „pátá doména"?* Vojenské rozhledy – Aktuality. [online]. [cit. 24.07.2022]. Dostupné z: https://vojenskerozhledy.cz/kategorie-clanku/bezpecnostni-prostredi/kyberprostor-jako-pata-domena

50. DECKEROVÁ, Jana. Bojištěm 21. století se stává kyberprostor. CZ Defence: Czech army and defence magazine [online]. [cit. 25.07.2022]. 2021. Dostupné z: https://www.czdefence.cz/clanek/bojistem-21-stoleti-se-stava-kyberprostor

51. *Kybernetická obrana.* Vojenské zpravodajství České republiky. [online]. [cit. 26.07.2022]. Dostupné z: https://www.vzcr.cz/kyberneticka-obrana-46

52. *Národní centrála proti organizovanému zločinu SKPV* – Policie České republiky. Úvodní strana. [online]. [cit. 26.07.2022]. Dostupné z: https://www.policie.cz/clanek/narodni-centrala-proti-organizovanemu-zlocinu-skpv.aspx

53. SZOTKOWSKI, René a Kamil KOPECKÝ. Dezinformace a fake news: průvodce studiem [online]. [cit. 26.07.2022]. Univerzita Palackého v Olomouci, 2019. Dostupné z: https://www.pdf.upol.cz/fileadmin/userdata/PdF/VaV/2019/odborne_seminare/Kopecky_Dezinformace_a_Fake_News.pdf

54. *Hoax.* Internetem bezpečně. [online]. [cit. 26.07.2022]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/dobre-vedet/hoax/

55. *Fake news.* Internext. [online]. [cit. 26.07.2022]. Dostupné z: https://www.internext.cz/fake-news-co-to-je/

56. *Definice dezinformací a propagandy*. Úvodní strana – Ministerstvo vnitra České republiky [online]. [cit. 27.07.2022]. Dostupné z: https://www.mvcr.cz/cthh/clanek/definice-dezinformaci-a-propagandy.aspx

57. GREGOR, Miloš; VEJVODOVÁ, Petra. Fake News – Nejlepší kniha o dezinformacích a manipulacích! první. vyd. Brno: CPress, 2018. 144 s. ISBN 978-80-264-1805-4.

58. *What is fact checking?* TechTarget. [online]. [cit. 27.07.2022]. Dostupné z: https://www.techtarget.com/whatis/definition/fact-checking

59. *What is fact-checking?* Journalist insight. [online]. [cit. 27.07.2022]. Dostupné z: https://conseilsdejournalistes.com/en/fact-checking/01-le-fact-checking-quest-ce-que-cest/

60. *What is fact-checking?* Arab fact-checkers network. Homepage. [online]. [cit. 27.07.2022]. Dostupné z: https://arabfcn.net/en/home/

61. *Fake News, Misinformation, & Fact-Checking*. Ohio University – Online Master's Degree Programs. [online]. [cit. 27.07.2022]. Dostupné z: https://onlinemasters.ohio.edu/masters-public-administration/guide-to-misinformation-and-fact-checking/

62. TÁBORSKÝ, Jiří. V síti (dez)informací: proč věříme alternativním faktům. Praha: Grada Publishing, 2020. ISBN 978-80-271-2014-7.

63. GREGOROVÁ, Markéta. Dezinformace, hoaxy, propaganda: zpátky k základům. [online]. [cit. 27.07.2022]. Dostupné z: https://gregorova.eu/dezinformace-hoaxy-propaganda-zpatky-k-zakladum/

64. *AFP joins project to create code of conduct for European fact-checkers.* AFP – Agence France-Presse. [online]. [cit. 27.07.2022]. Dostupné z: https://www.afp.com/en/agency/press-releases-newsletter/afp-joins-project-create-code-conduct-european-fact-checkers

65. *O nás.* Demagog.cz [online]. [cit. 27.07.2022]. Dostupné z: https://demagog.cz/stranka/o-nas

66. *Trestněprávní úprava*. Ministerstvo vnitra České republiky. Dezinformační kampaně. [online]. [cit. 27.07.2022]. Dostupné z: https://www.mvcr.cz/chh/clanek/dezinformacni-kampane-trestnepravni-uprava-trestnepravni-uprava.aspx

67. *Hlavní stránka*. Nelež. [online]. [cit. 27.07.2022]. Dostupné z: https://www.nelez.cz/

68. *Aeronet i Protiproud už neexistují, CZ.NIC zablokovalo weby šířící dezinformace.* InSmart.cz. [online]. [cit. 28.07.2022]. Dostupné z: https://insmart.cz/cznic-aeronet-dezinformace/

69. *Vnitro chce omezit dezinformace. Připravilo návrh zákona.* Česká televize – ČT24. [online]. [cit. 28.07.2022]. Dostupné z: https://ct24.ceskatelevize.cz/domaci/3499030-vnitro-chce-omezit-dezinformace-pripravilo-navrh-zakona

70. *Vnitro už připravilo zákon k blokování škodlivých webů.*Novinky.cz – Domácí. [online]. [cit. 28.07.2022]. Dostupné z: https://www.novinky.cz/domaci/clanek/vnitro-uz-pripravilo-zakon-k-blokovani-skodlivych-webu-40399442

71. *Blokace dezinformačních webů byla důležitá, nyní už nemá smysl, říká vládní zmocněnec Klíma.* Česká televize – ČT 24. [online]. [cit. 28.07.2022]. Dostupné z: https://ct24.ceskatelevize.cz/domaci/3494072-blokace-dezinformacnich-webu-byla-dulezita-nyni-uz-nema-smysl-rika-vladni-zmocnenec

72. *Resist: Příručka pro boj s desinformacemi.* Centrum proti terorismu a hybridním hrozbám – MVČR. [online]. [cit. 28.07.2022]. Dostupné z: https://www.mvcr.cz/chh/soubor/resist-cz-pdf.aspx

73. ŘIHÁČEK, Tomáš, Ivo ČERMÁK a Roman HYTYCH. Kvalitativní analýza textů: čtyři přístupy. Brno: Masarykova univerzita, 2013. ISBN 978-80-210-6382-2.

74. BENEŠ, Vít a Petr DRULÁK, ed. Metodologie výzkumu politiky. Praha: Sociologické nakladatelství (SLON), 2019. Studijní texty (Sociologické nakladatelství). ISBN 978-80-7419-283-8.

75. VAŠÁT, Petr. Kritická diskurzivní analýza: sociální konstruktivismus v praxi. Centrum aplikované antropologie a terénního výzkumu. [online]. 2009. Dostupné z: http://www.antropologie.org/sites/default/files/publikace/downloads/317_vasat_kriticka_diskurzivni_analyza_socialni_konstruktivismus_v_praxi.pdf

76. *Obsahová analýza.* Katedra antropologie FF ZČU. [online]. [cit. 29.07.2022]. Dostupné z: http://www.antropologie.org/cs/metodologie/obsahova-analyza

77. DVOŘÁKOVÁ, Ilona. Obsahová analýza / formální obsahová analýza / kvantitativní obsahová analýza. Centrum aplikované antropologie a terénního výzkumu FF ZČU v Plzni. [online]. [cit. 29.07.2022]. Dostupné z: http://www.antropoweb.cz/media/webzin/webzin_2_2010/Dvorakova__I-2-2010.pdf

78. *Sociální sítě jsou k propagandě a dezinformacím využívány stále více, upozorňují analytici z Oxfordu.* iRozhlas. [online]. [cit. 29.07.2022]. Dostupné z: https://www.irozhlas.cz/zpravy-svet/dezinformace-socialni-site-fake-news-trolling-oxford-vyzkum_1909262006_jgr

79. *Trolling a jeho nástrahy ve světě internetu.* Fakescape. [online]. [cit. 30.07.2022]. Dostupné z: https://www.fakescape.cz/blog/trolling

80. *Trollím, tedy jsem. Vzdělávací program* JSNS. [online]. [cit. 30.07.2022]. Dostupné z: https://www.jsns.cz/projekty/medialni-vzdelavani/materialy/vyukove-plakaty/opravdu/opravdu7

81. GULOVÁ, Lenka a Radim ŠÍP, ed. Výzkumné metody v pedagogické praxi. Praha: Grada, 2013. Pedagogika (Grada). ISBN 978-80-247-4368-4.

82. ŘIHÁČEK, Tomáš, Ivo ČERMÁK a Roman HYTYCH. Kvalitativní analýza textů: čtyři přístupy. Brno: Masarykova univerzita, 2013. ISBN 978-80-210-6382-2.

83. ŠVAŘÍČEK, Roman a Klára ŠEĎOVÁ. Kvalitativní výzkum v pedagogických vědách. Vyd. 2. Praha: Portál, 2014. ISBN 978-80-262-0644-6.

84. BLATNÝ, Marek, ed. Metodologie psychologického výzkumu: konsilience v rozmanitosti. Praha: Academia, 2006. ISBN 80-200-1450-0.

85. HÁJEK, Martin. Čtenář a stroj: vybrané metody sociálněvědní analýzy textů. Praha: Sociologické nakladatelství (SLON), 2014. Studie (Sociologické nakladatelství). ISBN 9788074191619.

86. *Co je to Deepfake?* IT Slovník. [online]. [cit. 30.07.2022]. Dostupné z: https://it-slovnik.cz/pojem/deepfake

87. *What Is A Deepfake? Everything You Need To Know*. DeepFake.com [online]. [cit. 30.07.2022]. Dostupné z: https://deepfake.com/knowledge-center/what-is-a-deepfake/

88. *Politici a známé osobnosti. Kdo patří mezi nejvýznamnější české dezinformátory?* Fakescape. [online]. [cit. 30.07.2022]. https://www.fakescape.cz/blog/dezinformatori-ukrajina-koronavirus

89. *Důchodci a všeználci. Kdo šíří „dezinformace"? Nový průzkum.* Parlamentní listy. [online]. [cit. 01.08.2022] Dostupné z: https://www.parlamentnilisty.cz/arena/monitor/Duchodci-a-vseznalci-Kdo-siri-dezinformace-Novy-pruzkum-628510