Hybridní hrozby

Bc. Filip Tuček

Diplomová práce
2022

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

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

Akademický rok: 2021/2022

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Filip Tuček**
Osobní číslo:	**L20469**
Studijní program:	**N1032A020002 Bezpečnost společnosti**
Specializace:	**Ochrana obyvatelstva**
Forma studia:	**Prezenční**
Téma práce:	**Hybridní hrozby**

Zásady pro vypracování

1. Zpracujte literární rešerši v oblasti hybridních hrozeb.
2. Popište problematiku dezinformačního působení na sociální a bezpečnostní prostředí České republiky.
3. Proveďte dotazníkové šetření s cílem postihnout vnímání dané problematiky populací.
4. Dotazníkové šetření vyhodnoťte a navrhněte opatření k zlepšení stávajícího stavu.

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

Seznam doporučené literatury:

1. *Hybridní válka jako nový fenomén v bezpečnostním prostředí Evropy.* Aktualizované a rozšířené druhé vydání. Praha: pro informační centrum o NATO vydalo Jagello 2000, 2016. ISBN 978-80-904850-4-4.
2. TÁBORSKÝ, Jiří. *V síti (dez)informací: proč věříme alternativním faktům.* Praha: Grada Publishing, 2020. ISBN 978-80-271-2014-7.
3. *Social Media and Democracy: The State of the Field, Prospects for Reform.* Cambridge: Cambridge University Press, 2020. ISBN 9781108890960.

Další odborná literatura podle doporučení vedoucího diplomové práce.

Vedoucí diplomové práce: **doc. RSDr. Václav Lošek, CSc.**
Ústav ochrany obyvatelstva

Datum zadání diplomové práce: **1. prosince 2021**
Termín odevzdání diplomové práce: **6. května 2022**

L.S.

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

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

V Uherském Hradišti dne 1. prosince 2021

PROHLÁŠENÍ AUTORA
DIPLOMOVÉ PRÁCE

Beru na vědomí, že:

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

Prohlašuji,

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

V Uherském Hradišti, dne: 5.8.2022

Jméno a příjmení studenta: Bc. Filip Tuček

.....
podpis studenta

ABSTRAKT

Diplomová práce je zaměřena na problematiku hybridních hrozeb. Teoretická část práce se zabývá upřesněním pojmů hybridní hrozby, hybridní válka, dezinformace a bezpečnostní prostředí. Praktická část práce pojednává o vnímání dezinformací veřejností, kdy je toto vnímání posouzeno pomocí dotazníkového šetření, které je následně vyhodnoceno, a jsou navržena opatření ke zlepšení stávajícího stavu. Následně je v praktické části použita metoda kontrolního seznamu (Checklistu), která ukazuje postup ověření informací. Také je pomocí diagramu znázorněn postup šíření dezinformací k veřejnosti. Závěrem praktické části je uveden výběr internetových stránek zabývajících se bojem proti šíření dezinformací.

Klíčová slova: dezinformace, hybridní hrozby, hybridní válka, misinformace.

ABSTRACT

The diploma thesis is focused on the issue of hybrid threats. The theoretical part of the work deals with specifying the concepts of hybrid threats, hybrid warfare, disinformation and security environment. The practical part of the thesis deals with the perception of disinformation by the public, when this perception is assessed by using the questionnaire survey, which is evaluated afterwards and measures to improve the current situation are proposed. Subsequently, in the practical part, the Checklist method is used to show how to verify the information. Also, with the help of the diagram, there is shown the process of spreading disinformation. The practical part concludes with a selection of websites fighting against the spread of disinformation.

Keywords: disinformation, hybrid threats, hybrid warfare, misinformation.

Touto cestou bych rád poděkoval mému vedoucímu práce panu doc. RSDr. Václavu Loškovi, CSc., za jeho vedení a odborné rady při sepisování mé diplomové práce. Dále bych rád poděkoval své rodině za neutuchající a bezmeznou podporu v průběhu studia a při zpracování diplomové práce.

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

OBSAH

ÚVOD

Již od samého vzniku je lidstvo spojeno s válkou. Přípravou na válku, vedením války či obranou v případě napadení. Jak lidstvo samotné, tak i vedení války se mění. Agresivní boje a krveprolití se postupně změnily ve hry na pozadí, které ovládají celý svět. V současnosti jsme zahlceni informacemi. Každý okamžik se odehrají desítky či stovky událostí, o kterých jsme díky propojení celého světa informováni v řádu vteřin. Avšak toto globální propojení skýtá i hrozbu hybridních útoků, především formou dezinformací. Denně jsou zveřejňovány tisíce zpráv, ať už v tištěné nebo elektronické formě. Ovšem zdali jsou pravdivé, to je věc, kterou musí čtenáři posoudit sami. Ovlivnění člověka zprávami, je v podstatě jednoduchá věc a v dnešní době je tato činnost často zneužívána. Využívají ji jednotlivci nebo organizované skupiny za účelem zisku, uspokojení svých zájmů nebo z pouhého přesvědčení. Pravda v dnešní době ztratila svůj smysl a atraktivitu a informace a zprávy jsou stále zabarvenější a obsahují pouze zrnko pravdivého základu. Zjistit pravdivost zpráv a ověřit si informace je pro mnohé osoby zdlouhavý a únavný proces. Mnozí lidé podléhají manipulativním a nepravdivým zprávám z důvodu přesvědčivosti informací, nezájmu o problematiku nebo nepotřebnosti si zprávy ověřovat. Lidé věří, čemu chtějí, ale často se může stát, že se jim víra v předkládané informace vymstí. Různé podvody, klamavé reklamy a manipulativní zprávy ve snaze přinést útočníkům a šiřitelům bohatství, zahlcují internetový a mediální prostor. Stejně tak vysoce postavené osobnosti a jejich organizace, ve snaze ovlivnit co nejvíce lidí a přesvědčit je ke sdílení jejich názorů, zneužívají dezinformace ve velké míře. Při přehlcení lživými informacemi si veřejnost ve své zmatenosti není jistá koho následovat a občané jsou často jeden druhým kritizováni za jejich víru a přesvědčení. Mnoho názorů a myšlenek osobností a národů v boji proti sobě ovlivňuje občany, kteří ve víře, že zrovna oni jsou v právu a mají pravdu, uráží druhé a v nejhorších případech se uchylují k agresi. Konflikty takto vznikají nejen mezi státy, politickými stranami a osobnostmi, ale také mezi občany samotnými, jejich rodinami a kolegy. Informace jsou silná zbraň, která se dá jednoduše zneužít, a vzniklé negativní následky se těžko uvádí na pravou míru.

CÍLE PRÁCE A POUŽITÉ METODY

Cílem diplomové práce je popsat působení dezinformací, jako jedné z forem hybridních hrozeb na bezpečnostní prostředí České republiky.

Za účelem naplnění cíle byly stanoveny následující dílčí cíle diplomové práce:

- popsat hybridní hrozby a jejich formy,
- popsat hlavní cíle při šíření dezinformací,
- popsat působení dezinformací na obyvatelstvo.

Ke zpracování diplomové práce byly použity následující metody. Při sepisování teoretické části byla použita obsahová analýza. Informace byly čerpány z odborné literatury, internetových zdrojů a zahraničních publikací. V praktické části práce bylo využito shromažďování informací pomocí dotazníkového šetření, které bylo následně vyhodnoceno analýzou údajů. Dále byl zpracován kontrolní seznam (Checklist) sloužící jako možný návod k ověření relevance informací.

Výzkumné otázky

1. Lze zabránit vzniku a šíření dezinformací?
2. Lze spolu se zapojením médií omezit šíření dezinformací?
3. Jakými způsoby si může veřejnost ověřit informace?

I. TEORETICKÁ ČÁST

1 HYBRIDNÍ HROZBY

Pojem „*hybridní hrozba*“ se v současném smyslu používá zhruba od roku 2014. Tedy od Ruské anexe Krymu, potažmo války na východní Ukrajině. Podle podporovatelů konceptu hybridních hrozeb, současní aktéři vytvářejí nový typ válčení pomocí technologií 21. století, komunikačních sítí a nových kombinací konvenčních a nekonvenčních prostředků lišících se od tradičního vedení boje. (Jasper, 2014)

1.1 Definice

Definovat pojem *hybridní hrozby* je velmi obtížné. V podstatě každý stát, organizace či jednotlivec si tento pojem vykládá podle svých zkušeností a přesvědčení. Avšak podstatu hybridních hrozeb můžeme spatřovat v použití kombinace civilních a vojenských prostředků k dosažení cíle a ukotvení útočících subjektů a destabilizaci subjektu jiného. Jádrem hybridní hrozby je promyšlená forma vedení řady menších (vzájemně nespojitelných) útoků na mezinárodní či vnitrostátní úrovni. (Kartusová, 2021)

Nutné je podotknout, že tyto útoky prováděné v rámci hybridního válčení mohou být postaveny na základech konvenčních či nekonvenčních sil nebo mohou být útoky vedeny v rámci politických či ekonomických tahů konaných na nejvyšší úrovni. (Kartusová, 2021)

1.2 Druhy hybridních hrozeb

Hybridní válčení může zahrnovat působení cizí moci; narušení surovinové, energetické a průmyslové bezpečnosti; hrozby v kyberprostoru; zneužití aspektů migrace; terorismus či extremismus. Všechny tyto prvky se vhodně kombinují a podporují působením dezinformací na domácí obyvatelstvo. Všechno za účelem změny veřejného mínění a poměrů v dané zemi. (Ministerstvo vnitra České republiky, c2022b)

Jednotlivé prvky mohou na první pohled působit neškodně a nemusí představovat hrozbu. Avšak velké nebezpečí vedení hybridní války spočívá ve vhodném kombinování jednotlivých prvků, které se ve svých účincích podporují a vzájemně zesilují. Také se mohou tyto prvky užívat v různém časovém odstupu, kdy si na ně obyvatelstvo jistým způsobem přivykne a již jim nevěnuje pozornost a poté buď přidá další prvky, nebo ty stávající zesílí. (Ministerstvo vnitra České republiky, c2022b)

Hybridní hrozby zahrnují následující nástroje:

1) Politický nátlak na oficiální delegace států.
2) Manipulace s veřejným míněním prostřednictvím komunikačních kanálů, sociálních médií apod.
3) Různé formy otevřeného či skrytého využití ozbrojených složek.
4) Ekonomický nátlak na ekonomiku státu prostřednictvím uvalení cel, embarg, narušení dodávek surovin či znemožnění vývozu surovin dané země.
5) Nátlak na finanční sektor prostřednictvím destabilizace měny, narušení akciových trhů, bankovního sektoru či obchodováním se státními dluhopisy.
6) Provádění špionážních operací, získávání tajných spolupracovníků či informátorů.
7) Provádění aktivit za účelem rozvratu hodnotového, právního či společenského uspořádání. (Ministerstvo vnitra České republiky, c2022b)

Z výše uvedeného shrnutí nástrojů vyplývá, že více než na vojenskou sílu se v případě hybridního válčení spoléhá na diplomatické, ekonomické a jiné než válečné síly a provádění podvratných aktivit. Za tímto účelem se protivník snaží využít vnitřní napětí a nepořádek cílové země ke svému prospěchu. Tím, že prostřednictvím médií upozorňuje na vnitřní problémy a znevažuje kroky místní vlády.

1.3 Hybridní kampaň

Hybridní kampaň je důmyslné a promyšlené použití jednotlivých prvků.

- Využití slabin protivníka,
- znemožnění jasného vysvětlení událostí a zamezení spojení vzájemných souvislostí,
- komplikování či znemožnění identifikace původce událostí,
- komplikovat či destabilizovat rozhodovací procesy v dané zemi. (Ministerstvo vnitra České republiky, c2022b)

Cílem hybridní kampaně je poškodit životní, strategické či bezpečnostní zájmy dané země takovým způsobem, kdy je velmi obtížné až nemožné odhalit původního útočníka. Přímé vojenské nasazení není primárně vyžadováno, avšak nelze nepředpokládat přímé vojenské akce v rozvinuté fázi hybridní kampaně. (Ministerstvo vnitra České republiky, c2022b)

DÍLČÍ ZÁVĚR

Kapitola první hovořila o hybridních hrozbách. O definici hybridních hrozeb, druzích hybridních hrozeb a vedení hybridní kampaně. Hybridní hrozby jako realita geopolitických konfrontací 21. století představují vážné nebezpečí směřující k oslabení hodnot našeho civilizačního okruhu.

2 HYBRIDNÍ VÁLKA

V současné době však existuje problém s jednoznačnou, jasnou a odbornou veřejností přijímanou definicí tohoto pojmu. O stanovení jasné definice se pokusil docent Kříž se svým kolektivem při tvorbě publikace *Hybridní válka jako nový fenomén v bezpečnostním prostředí Evropy.* Hybridní válku definuje jako:

„Ozbrojený konflikt vedený kombinací nevojenských a vojenských prostředků s cílem jejich synergickým efektem přinutit protivníka k učinění takových kroků, které by sám o sobě neučinil. Alespoň jednou stranou konfliktu je stát.“ (Kříž a kol., 2015, s. 8)

V případě nevojenských prostředků se jedná o:

- Psychologické prostředky:
  - propaganda,
  - dezinformace.
- Ekonomické prostředky:
  - sankce,
  - embarga.
- Násilné prostředky:
  - teroristické operace,
  - kriminalita. (Kříž a kol., 2015, s. 8)

„Vojenské operace útočníka jsou vedeny na zapřenou nepravidelnými silami kombinujícími symetrické a asymetrické způsoby vedení bojové činnosti proti celé společnosti a zejména proti jejím politickým strukturám, orgánům státní správy a samosprávy, ekonomice státu, morálce obyvatelstva a ozbrojeným silám.“ (Kříž a kol., 2015, s. 8)

2.1 Hybridní války v minulosti

Koncept hybridní války a hybridních hrozeb obecně není záležitostí posledních několika let. Objevuje se ve větší či menší míře v různých historických konfliktech. Stále se také mění vnímání samotné hybridní války. V minulosti se užívání principů hybridního válčení vnímalo jako slabost útočníka, neboť neměl k dispozici dostatek konvenčních vojenských sil a musel se proto spoléhat i na nejrůznější doprovodné a podvratné činnosti.

Principy vedení hybridní války sepsal již v 6. století čínský generál a filosof Sun-c' ve svém díle „*Umění války"*. Techniku čínského generála později převzali a zdokonalili japonští shinobi[1], kteří se pomocí nekonvenčních metod, špionáže a atentátů snažili udržet nezávislost se sousedícími samuraji. O století později byla forma hybridní války využita i americkými patrioty ve Válce za nezávislost, kteří díky efektivnímu sběru informací o nepříteli dokázali zneužít jejich slabin a obrátit průběh války ve svůj prospěch. Jistou historickou zkušenost s vedením hybridní války má i náš národ, kdy prostřednictvím účinného šíření dezinformací došlo k ovlivnění a radikalizaci německé menšiny v československém pohraničí. Hybridních válek bylo v minulosti vedeno nespočet, od šíření dezinformací, atentáty až po tajné operace. Způsob vedení této války však zdokonalil generál Ruské federace Valerij Gerasimov a pozvedl ji na Válku nové generace. (Bartošík, 2022)

S postupným rozvojem technologií a nově získaných poznatků se zcela jistě mění i užívané principy válčení.

Pro pochopení samotného konceptu hybridního válčení je nutné si uvědomit, že podstatou není boj na fyzickém bitevním poli, ale prostor pro tento boj je prakticky neomezený. „Bojové" operace mohou probíhat v mediálním či kybernetickém prostoru, fyzickém prostoru, ale také ve vesmíru nebo na poli kulturních identit. Právě rozvoj moderních technologií, komunikační techniky apod. je jeden ze základních předpokladů rozvoje hybridního válčení.

Ve vesmíru jsou desítky satelitů umožňujících mezinárodní komunikaci, sledování či navigaci. Poměrně velký problém je mezinárodní terorismus, nukleární hrozby či nebezpečí použití zbraní hromadného ničení. V posledním období se do povědomí populace také dostává pojem kyberzločin či kyberterorismus. Všechny tyto vyjmenované pojmy mohou být součástí hybridní války. Ať již v podobě přímého použití či hrozby jejího použití.

2.2 Koncept hybridní války

Neexistuje způsob jednoznačného odlišení konvenční a hybridní války. Pokud se i přes to pokusíme tyto dva způsoby vedení boje odlišit, je potřeba se zaměřit na použité prostředky vedení boje. V případě *konvenční války* je stěžejním prostředkem vedení boje armáda, či jiná podobná ozbrojená organizace. A tedy vojenské síly převládají nad těmi

[1] Japonští ninjové

nevojenskými. Avšak v případě vedení *hybridní války* je tomu právě naopak, a tedy nevojenské síly jsou stěžejní k dosažení výsledku. Nejlépe pokud nevojenské prostředky není nutné podpořit nasazením ozbrojených složek. (Kříž a kol., 2015, s. 8)

Cílem hybridního válčení je do určité míry ovládnutí myšlení vedení organizace, či státu, potažmo celého obyvatelstva. K tomuto je možno použít masivní šíření dezinformací, provádění klamných operací a v neposlední řadě i teror k ovládnutí mas obyvatelstva. (Kříž a kol., 2015, s. 8)

Samotné vedení hybridní války lze rozdělit do několika etap.

Etapy hybridní války:

1. Demoralizace cílové společnosti.
2. Destabilizace cílové společnosti.
3. Vyvolání krize v cílové společnosti.
4. Převzetí kontroly nad cílovou společností vnitřními silami napojenými na útočníka. (Kříž a kol., 2015, s. 11)

2.3 Fáze hybridního útoku

Jednotlivé fáze útoku nejsou jasně stanoveny. Mnoho médií tyto fáze rozděluje odlišně. Avšak dokument *Background Report* přinesl stručný popis těchto fází. Dle dokumentu se hybridní útok dělí do:

- Přípravné fáze.
- Útočné fáze.
- Stabilizační fáze. (Hybrid Threats, 2015, s. 8)

Přípravná fáze je zpravidla nejdůležitější. Spočívá v jednotlivých rozhodnutích, která je nutno přijmout či upravit před samotným útokem. Zahrnuje přípravu v ekonomické či vojenské oblasti. Také získání určité politické moci (financování politických stran a sdružení), uskutečnění politických her apod. Nezbytné je však prostřednictvím určitých kroků přesvědčit domácí obyvatelstvo a získat jeho podporu k provedení útoku. Za tímto účelem bývá prováděna značná mediální kampaň. Právě úspěšnost této fáze většinou rozhoduje o úspěchu následujícího útoku. (Hybrid Threats, 2015, s. 8-9)

Přehledně schematicky se přípravná fáze rozděluje následovně na jednotlivé dílčí kroky.

- Strategická příprava:
    - zkoumání zranitelných míst cílové země,
    - vytváření sítě nevládních organizací a mediálních kanálů,
    - vytváření silných diplomatických pozic s cílem ovlivňovat publikum.
- Politická příprava:
    - podpora nespokojeností s vládními orgány cílové země,
    - posílení místních separatistických hnutí,
    - posilování etnického, sociálního či náboženského napětí v zemi,
    - uplácení politiků a dalších státních úředníků,
    - navazování kontaktů se skupinami organizovaného zločinu.
- Provozní příprava:
    - zahájení koordinovaného tlaku na politické představitele,
    - zahájení dezinformačních kampaní,
    - využití uplácených politiků ve vlastní prospěch. (Rácz, 2015, s. 59)

Útočná fáze bývá nejkratší. Skládá se z různých druhů útoků (vojenského či nevojenského charakteru). Tyto útoky jsou prováděny prostřednictvím vojenských nebo polovojenských operací či operací nevojenského charakteru. Spadají sem i různé politické kroky, teroristické akty, akty extremizmu a kybernetické útoky. Veškerá aktivita je prováděna s domácí podporou, která byla zajištěna prostřednictvím masivního šíření dezinformací a propagandou. (Hybrid Threats, 2015, s. 8-9)

Schematicky se útočná fáze dělí takto.

- Exploze napětí:
    - organizování masivních protivládních protestů v zemi,
    - infiltrace vojáků mezi protestanty a provedení prvotních násilných střetů a sabotážních činů,
    - provádění provokací a sabotáží po celé zemi s cílem rozptýlit státní orgány,

  - média útočící země zahajují masivní dezinformační kampaň,
  - prezentace síly armády útočící země za účelem odstrašení armády zasažené země.

- Odstranění vlády z cílového regionu:
  - obsazení administrativních budov,
  - znemožnění působení místních ozbrojených sil,
  - blokování místních médií a ovládání komunikačních kanálů,
  - pokračování diplomatického, politického a ekonomického tlaku na zasaženou zemi,
  - média útočící země se snaží dezorientovat zahraniční (mezinárodní) publikum.
- Ustavení alternativní politické moci:
  - vyhlášení nových politických reprezentací v zasažených regionech,
  - podpora nové vlády prostřednictvím médií útočící země,
  - zablokování možností protiútoku prezentací síly útočící armády. (Rácz, 2015, s. 63)

Finální fází útoku je **stabilizační fáze**, která zajišťuje uskutečnění vytyčených cílů hybridního útoku. Obsahuje většinou politické či diplomatické kroky uskutečněné v reakci na nastalou situaci za cílem uvolnění cesty k vítězství. Stabilizační fáze probíhá neprodleně po útočné fázi a není snadné ji identifikovat. (Hybrid Threats, 2015, s. 8-9)

Stabilizační fáze se rozděluje takto.

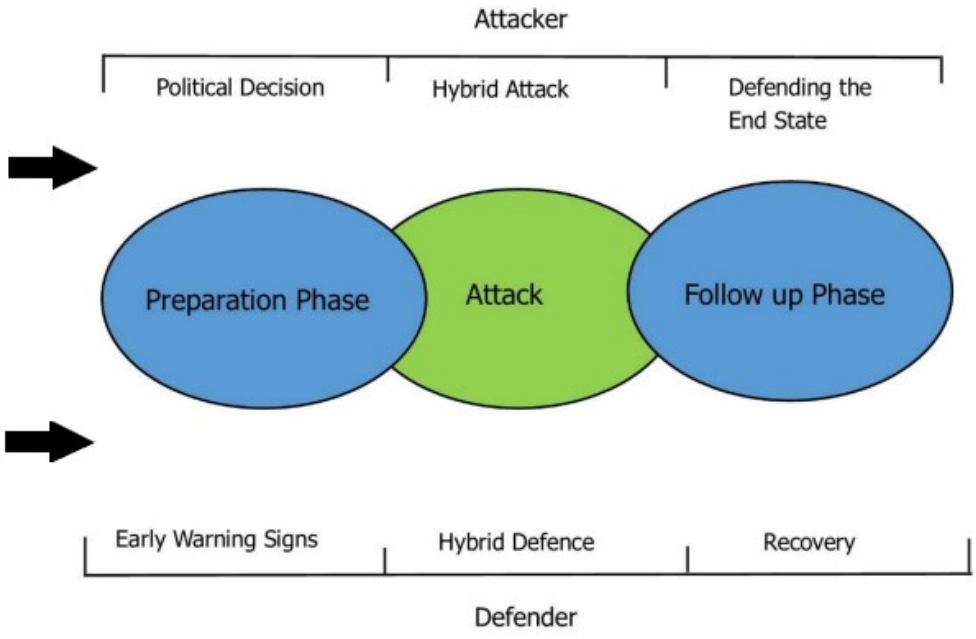
- Politická stabilizace:
  - uspořádání referenda a rozhodnutí o osamostatnění země,
  - nově vytvořený stát požádá o pomoc a ochranu útočící zemi.
- Oddělení území od cílové země:
  - anexe či včlenění získaného území,
  - zřízení vojenské základny a tím vytvoření sféry vlivu.

- Trvalé omezení svobody zasažené země:
    - ztráta území a tím narušení ekonomiky, infrastruktury či obyvatelstva,
    - prostřednictvím narušení hospodářství a domácí politiky vyvolat humanitární krizi,
    - tím zajistit nemožnost připojení zasažené země do jakéhokoliv paktu či organizace. (Rácz, 2015, s. 67)

Pro vedení hybridní války je nezbytné naplnění určitých podmínek. Zpravidla se jedná o tyto:

- Převaha v konvenčních vojenských prostředcích.
- Nízká úroveň vlády v cílové zemi.
- Dlouhodobé zanedbávání určitých regionů vládou a nízká legitimita vlády.
- Silná mediální podpora.
- Společná hranice s cílovou zemí či přítomnost ozbrojených složek.

V případě nenaplnění většiny podmínek, hybridní útok nebývá zpravidla úspěšný. (Rácz, 2015, s. 73-82)



Obrázek 1 Jednotlivé fáze z pohledu útočníka i „zasaženého"

Zdroj: Hybrid Threats, 2015, s. 10

Jak bylo popsáno výše v kapitole **2.3**, hybridní útok je možné rozdělit do tří fází **(Obr. 1)**, přípravná fáze, samotný útok neboli útočná fáze a následná stabilizační fáze. Výše uvedený obrázek znázorňuje a popisuje pohledy jak útočící, tak i napadené strany. Šipky vyznačují směr vývoje fází. Důvod útoku závisí na různých politických rozhodnutích, které se mohou konat ještě před nebo v průběhu přípravné fáze. Z toho důvodu musí být napadená strana velmi obezřetná, stále pozorovat a zkoumat situaci, aby zachytila i sebemenší varovné signály ohrožení nebo útoku. Ještě před ukončením přípravné fáze nastává fáze útočná. Napadená strana se musí útoku náležitě bránit a zamezit dalším aktivitám protější strany. Jak již bylo zmíněno, útočná fáze bývá nejkratší a před ukončením této fáze, nastává fáze stabilizační. Stabilizační fáze, nebo také následná, slouží pro útočníka jako prostor pro upevnění své pozice a zájmů v napadené zemi. Naopak zasažená země využívá tuto fázi k zotavení, přeskupení a komunikaci s útočící stranou ve snaze o ukončení konfliktu.

2.4 Bojiště hybridní války

Z historického pohledu bylo nejrušnější bojiště na poli hybridních válek období studené války. Obě velmoci bipolárního světa měli obavy ze vzájemné přímého vojenského konfliktu, a proto se jejich boje přesouvaly na pole dezinformací, špionáže a vedení bojů prostřednictvím jiných ozbrojených skupin. Mohlo by se zdát, že se skončením studené války a rozpadem bipolárního světa skončily i tyto hybridní války, avšak opak je pravdou. Spojené státy a Rusko dále pokračovaly v dosažení svých cílů zejména prostřednictvím vedení těchto skrytých válek. Mezi nejčastěji zmiňovaná místa dnešní doby, kde probíhá určitá forma hybridní války, patří Ukrajina. Avšak nelze to brát tak, že na jiných místech planety se tato válka neodehrává. Lze předpokládat, že určité formy hybridní války probíhají nepřetržitě v podstatě v každém státě. Jedním z největších aktuálních aktérů je tzv. Islámský stát. Bojištěm je tedy blízký východ a severní Afrika. Nelze se však soustředit pouze na fyzická bojiště, jak je známe z minulosti. Nejvíce hybridních bojů a válek probíhá v mediálním prostoru, neboť s příchodem digitalizace a internetu, se většina hybridních válek přenesla do online prostoru. Díky tomuto přesunu do online prostoru získali útočníci téměř neomezené pole působnosti, kdy s relativně nízkými náklady mohou vést boje ve větších rozměrech. De facto všichni uživatelé připojeni k internetu mohou být součástí či cílem hybridního útoku.

DÍLČÍ ZÁVĚR

Kapitola druhá pojednávala o problematice vedení hybridní války. Postupně bylo rozebráno užití konceptu hybridní války v minulosti. Byl prezentován koncept hybridní války a jednotlivé fáze hybridního útoku. V poslední řadě bylo pojednáno o bojištích hybridní války. Jednou z nejdůležitějších zbraní vedení hybridní války jsou dezinformace, neboť stále platí: kdo ovládá informace, ovládá svět.

3 DEZINFORMACE

Právě dezinformace představují jeden ze stěžejních prvků úspěšného vedení hybridní války. Prostřednictvím dezinformací je útočník schopen ovlivnit vnímání dané „operace“ u širší veřejnosti ve svůj prospěch. Prostřednictvím dezinformací si dokáže získat domácí obyvatelstvo.

Použití dezinformací pro vojenské použití není nic nového. Již v dávných dobách vysílali vojevůdci své vojáky v přestrojení na území, které chtěli dobýt, aby pomocí šíření nepravdivých zpráv jistým způsobem připravili půdu pro útok.

Pojem dezinformace se v dnešních médiích skloňuje v mnoha případech. Avšak značná část populace nedokáže pojem dezinformace formulovat a jako dezinformace označují takřka vše, co naleznou na internetu a odporuje jejich přesvědčení. Ať už se jedná o informace pravdivé či nepravdivé.

Uvěřitelnost jednotlivých zavádějících a dezinformačních zpráv se zvyšuje několika předpoklady:

1. Zpráva se zakládá, alespoň částečně, na pravdivých informacích.
2. Přizpůsobení informace dané oblasti.
3. Přijetí informace z několika kanálů. (Gregor a kol., 2018, s. 8, 9)

Především kvůli třetímu bodu obsahuje drtivá většina dezinformačních zpráv výzvu ke sdílení. Pokud totiž informaci obdrží příjemce z několika na sebe nevázaných zdrojů, je jednoduší jí uvěřit a tuto informaci přijmout za relevantní.

3.1 Trestněprávní úprava

Základem účinného boje vůči dezinformacím by měla být i efektivní legislativa. Avšak ta zde v současné době chybí, stejně tak jako účinná trestněprávní úprava. Nejenže není legislativně stanovena přesná definice pojmu *dezinformace*, neexistuje taktéž ani přesně popsaná skutková podstata trestného činu šíření dezinformací. Ukazuje to tak jistý druh neobratnosti a mezery v českém trestním právu, které není schopno účinně reagovat na současné hrozby. (Ministerstvo vnitra České republiky, c2022c)

Vytváří to tak komplikaci v aktivním boji vůči dezinformacím a postihování jejich šiřitelů. Příslušné orgány proto musí hledat skutkovou podstatu již uzákoněných trestných činů v zákoně č. 40/2009 Sb. trestní zákoník. Jedná se například o:

- §184 – pomluva,
- §355 – hanobení národa, rasy, etnické nebo jiné skupiny osob,
- §356 – podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod,
- §357 – šíření poplašné zprávy. (Ministerstvo vnitra České republiky, c2022c)

Bohužel i v tomto případě platí, že zločin je vždy o krok před zákonem. Organizované skupiny i jednotlivci se snaží vytvářet zprávy, které sice ovlivní veřejné mínění či názory, ale nenaplní skutkovou podstatu některého trestného činu.

3.2 Definice

Obecně se rozeznávají dva pojmy, které spolu souvisí a laickou veřejností jsou často zaměňovány. Jedná se o pojmy **dezinformace** a **misinformace.** V dnešní době se lze snadno setkat i s pojmem **fake news**, což není nic jiného než dezinformace.

V současnosti nejsou tyto pojmy legislativně ukotveny, ale jejich definice jsou převzaty z mezinárodně uznávaných pojmů.

Dezinformace

Dezinformace se definuje jako úmyslné a systematické šíření nepravdivých informací s cílem ovlivnit veřejné mínění či rozhodování. (Ministerstvo vnitra České republiky, c2022a)

Misinformace

Za misinformace se považuje nesprávná či zavádějící informace, která není šířena systematicky nebo úmyslně za účelem ovlivnění veřejného mínění. (Ministerstvo vnitra České republiky, c2022a)

Do kategorie misinformací spadají i takzvané městské legendy, „urban legends“. Tedy příběhy osob, kterým se stalo něco zajímavého. Často není cílem šíření těchto legend někoho poškodit nebo zmanipulovat, ale je zde snaha pouze o zviditelnění dané osoby. (Gregor a kol., 2018, s. 8, 9)

Tyto dva pojmy (*dezinformace* a *misinformace*) spolu úzce souvisí, často se prolínají a laická veřejnost je považuje za totožné. Neboť oba pojmy vyjadřují nesprávnou interpretaci informací. Pojem *dezinformace* značí záměrné šíření zavádějících informací

za účelem ovlivnění skupiny osob. Na druhou stranu pojem *misinformace* značí šíření nesprávných informací nevědomě bez snahy o ovlivnění skupiny osob. (Guess, 2020)

Problematika dezinformací není pouze „útok“ na konkrétní osobu, ale způsobení nedůvěry v systém či demokracii. V neposlední řadě zpochybnit co je vůbec pravda a čemu věřit.

3.3 Dezinformační kampaně

Jak již bylo řečeno, dezinformace jsou nezbytné k úspěšnému boji. Avšak ještě lepších výsledků se dosáhne, pokud je šíření dezinformací organizované, cílené a podpořené dalšími skutečnostmi. Právě všechno zmíněné obsahují dezinformační kampaně, které jsou promyšlené, organizované a přesně zacílené na určitou skupinu osob za určitým výsledkem.

Dezinformačních kampaní v minulosti proběhlo nespočet a další probíhají v současnosti. Následující výběr pouze ilustruje jednotlivé kampaně v historické době a způsoby jejich provedení.

3.3.1 Themistoklés

Používání dezinformací se užívá již od nepaměti. Jedno z nejstarších zdokumentovaných užití dezinformací s cílem vojenského vítězství sahá do období řecko-perské války, probíhající v letech 480-479 př. n. l. Řeckému vojevůdci Thémistoklovi se podařilo šířit falešné zprávy pomocí vysílání zdánlivě zběhlých otroků. Obsahem zpráv bylo připravované spiknutí řeckých vojáků v perských řadách, a tedy možnost zběhnutí obrněných oddílů zpět na řeckou stranu. Perský vojevůdce Xerxes těmto zprávám uvěřil a v nadcházejícím boji se rozhodl nenasadit do boje obrněné oddíly. Následkem tohoto rozhodnutí bylo řecké vítězství v bitvě zajištěno. (Gregor a kol., 2018. s. 10)

3.3.2 Vylodění v Normandii

Jedna z nejúspěšnějších a nejvýznamnějších dezinformačních kampaní druhé světové války byla součástí Operace Overlord. Němečtí generálové o snaze otevřít druhou frontu v Evropě věděli. Nevěděli však, kde k tomuto otevření dojde. Kvůli těmto obavám budovali tzv. Atlantický val[2]. Spojenecké velení vybralo jako místo vylodění oblast Normandie, avšak tato oblast byla těžce opevněna. Bylo tedy nutné přesvědčit Německou

[2] Soustava opevnění, která měla zastavit nebo zpomalit postup jednotek při vylodění. (Válka Revue, 2016)

armádu, že k vylodění dojde v jiné oblasti. Fiktivní místo vylodění mělo být Pas de Calais (místo s nejmenší vzdáleností z Anglie). (Gregor a kol., 2018. s. 12)

Pro přesvědčení německého velení byla spuštěna Operace Bodyguard. Soustava několika dalších menších (avšak neméně důležitých) operací. Jednou z nich byla i Operace Quicksilver. V rámci které byla zřízena fiktivní armáda umístěna v jihovýchodní Anglii připravující se na vylodění. Pro větší uvěřitelnost byla fingována i radiová komunikace. Na pobřeží byly umístěny nafukovací makety vyloďovacích člunů. (Fiala, 2018)

Spojenci se také snažili přesvědčit německou armádu, že k vylodění může též dojít v Norsku. Všechno s cílem co nejvíce roztříštit obranu v oblasti Normandie. V předvečer samotného vylodění provedli spojenci intenzivní bombardování oblasti Pas de Calais, s cílem odvrátit pozornost od vyloďovacích sektorů v Normandii.

Operace Bodyguard byla úspěšná do takové míry, že po provedení invaze v Normandii zůstala německá armáda ještě několik týdnů v oblasti Pas de Calais ze strachu před další invazí. (Gregor a kol., 2018, s. 12)

3.3.3 Operace Neptun

Úspěšné dezinformační kampaně měli na svědomí i členové československé StB. Jednou z takových akcí byla i Operace Neptun, která probíhala v letech 1964-1966 ve spolupráci se sovětskou KGB. Operaci měl na starosti nově vzniklý 8. odbor První správy ministerstva vnitra v čele s Ladislavem Bittmanem.

Důvod přípravy této operace byl jednoznačný. Blížila se doba promlčení nacistických zločinů z druhé světové války. Cílem bylo toto promlčení odložit a připomenout zločiny a znejistit západní politiky. Toho mělo být dosaženo nalezením beden s vojenskými dokumenty na dně Čertova jezera na Šumavě. Avšak československá StB neměla k dispozici vhodné množství vojenských dokumentů, které by šly k tomuto účelu využít. Bylo proto rozhodnuto požádat o spolupráci sovětskou KGB, která v archivech tyto dokumenty měla a se spoluprací souhlasila. (Gregor a kol., 2018, s. 13) (Bittman, 2000, s. 176-180)

Po „nalezení“ dokumentů následoval projev tehdejšího ministra vnitra Lubomíra Štrougala. V projevu připomněl a zdůraznil, že podle nalezených dokumentů je politické vedení Rakouska a Německa spojeno s nacistickou minulostí. To mělo za následek odstoupení některých politiků z funkce, v několika případech došlo i k sebevraždě. Svou činnost také

obnovily organizace stíhající válečné zločince, které zveřejněním dokumentů dostaly nový impuls k činnosti. K prodloužení promlčení došlo také. (Bittman, 2000, s. 176-180)

3.3.4 Operace INFEKTION/DENVER

Jednu z nejvýznamnějších dezinformačních kampaní, které mají na mnoha místech přesah i do dnešních dnů, mají na svědomí členové sovětské KGB. Operace probíhala v 80. letech 20. století. V době, kdy se světem začaly šířit první nakažení virem HIV. Celý svět měl pochybnosti, kde se tento vir vzal. Těchto pochybností využila KGB ve svůj prospěch. (Gregor a kol., 2018, s. 13, 14)

Celá dezinformační kampaň byla odstartována otištěním článku v indických prosovětských novinách, že nový virus HIV je biologická zbraň vyvíjená americkou vládou. O dva roky později tuto zprávu znovu otiskly sovětské noviny. Následně byla obdobná zpráva vydána i ve východoněmeckém „pseudovědeckém“ časopise, v němž byl původ viru vystopován až do amerického Pentagonu. Poté začaly tuto zprávu citovat další sovětské a prosovětské časopisy a noviny, podpořené různými dalšími zprávami. (Gregor a kol., 2018, s. 13, 14)

Dezinformační kampaň byla nadmíru úspěšná hlavně v rozvojových zemích, především v Africe. Úspěchem byli ohromeni sovětští specialisté a začali šířit další dezinformace o nemoci AIDS, které pronikly na všechny kontinenty. (Bittman, 2000, s. 166)

Dezinformace měla úspěch i přesto, že odborníci ze Západu i Východu tuto zprávu vyvraceli, dokonce prokázali přírodní původ viru. (Gregor a kol., 2018, s. 13, 14)

K odhalení původu této zprávy došlo v roce 1991. Podle průzkumu provedeného téhož roku věřilo tomu, že je vir uměle vytvořen, 15 % Američanů. Z dalšího průzkumu provedeného roku 2005 vyplývá, že:

- 25 % Afroameričanů věří verzi, že je vir uměle vytvořen,
- 15 % Afroameričanů je přesvědčeno, že je vir nástrojem genocidy vůči občanům tmavé pleti. (Gregor a kol., 2018, s. 13, 14)

3.4 Dezinformace a média

Média představují stěžejní prvek v šíření dezinformací. Zvláště pak ta, která se vyloženě zaměřují na šíření dezinformačních zpráv. Taková média se nazývají dezinformační. Počínání těchto médií v České republice popsala i Bezpečnostní informační služba ve své výroční zprávě za rok 2019 takto:

„Poté, co se v ČR v posledních několika letech vytvořila a etablovala poměrně stabilní dezinformační scéna složená z médií, která se prezentují jako nezávislá či alternativní, jsou stále častěji patrné pokusy jejích protagonistů o očištění od přívlastku „dezinformační" a legitimizaci jejich názorů skrze tradiční a zavedená média. Tyto aktivity lze interpretovat jako přirozenou součást širšího trendu, který lze popsat jako snahu posunout konspirační teorie, proruské narativy a protizápadní postoje z okraje mediálního spektra do jeho středu." (Bezpečnostní informační služba, 2020, s. 11)

Dále ve výroční zprávě za rok 2020 se uvádí následující:

„V roce 2020 se dále stupňoval tlak, který dezinformační ekosystém vyvíjel na seriózní média včetně médií veřejné služby. Seriózní žurnalistika na manipulaci obsahu a problematiku dezinformací kontinuálně upozorňuje, čímž tvoří logický cíl verbálních útoků a diskreditace ze strany tzv. alternativní mediální scény. Kontinuální dezinformační tlak také podporuje rezignaci části společnosti na funkčnost státu v jeho současné ústavní podobě, což stát limituje ve schopnosti účinně komunikovat strategická témata zasažené části společnosti a v konečném důsledku zvyšuje zranitelnost státu a společnosti vůči vlivovým operacím cizí moci." (Bezpečnostní informační služba, 2021, s. 11)

Lze pozorovat trend stále se zvyšujících stránek šířících dezinformace. O tomto trendu svědčí i fakt, že se neustále rozšiřuje seznam vedený a aktualizovaný na webu *konspiratori.sk*. V době psaní této práce se na tomto seznamu nacházelo 230 webových stránek. (Konšpirátori.sk, c2022a)

Jak již bylo uvedeno, dezinformace slouží k získání určitého cíle. V příručce zpracované Pammentem, kterou využívá pro své potřeby i Centrum proti terorismu a hybridním hrozbám Ministerstva vnitra, se uvádí 5 nejčastějších cílů šíření dezinformací.

- Ekonomický – přímý finanční zisk. Zveřejňování zajímavých titulků za účelem přilákání čtenářů. Web je přitom finančně oceněn na základě počtu zobrazení, a tedy i zobrazení reklamy čtenářům.
- „Protože můžu" – cílem může být pokoření něčeho na první pohled nemožného, za účelem získání osobního respektu, osobního prospěchu či pokoření výzvy.
- Diskreditace – pomocí zveřejňovaných lží se médium snaží zdiskreditovat osobu či organizaci. Diskreditace patří k nejčastější dezinformační činnosti a vhodně doplňuje další cíle.

- Polarizace – šířením dezinformačních zpráv ještě více prohlubovat stávající rozpory ve společnosti. Vyostřením diskuzí se snaží vyprovokovat reakce a tím omezovat prostor na možný kompromis. Účely mohou být politické či společenské.
- Informační vlivové operace – cílem takové kampaně je podrývat národní prosperitu a bezpečnost. Za šířením většinou stojí nepřátelské subjekty, které k tomu využívají prostředníky uvnitř státu a vhodně tyto kroky kombinují s dalšími hybridními technikami (špionáž či získávání/zveřejňování kompromitujících materiálů). Dezinformace většinou souvisí s poškozováním národní pověsti a poškozováním pověsti dalších státních institucí. (Pamment, 2020, s. 7-9)

3.5 Moderní technologie a dezinformace

V současné době zažíváme prudký rozvoj moderních technologií ve smyslu umělých technologií apod. V podstatě každý mobilní telefon již dnes umožňuje ovládání pomocí hlasových pokynů, či převod textu na mluvenou řeč. Existuje možnost koupit si domácího asistenta, se kterým je možné vést konverzaci, kterou prakticky nelze odlišit od konverzace s živým člověkem.

Je také možnost nalézt různé editory, pomocí kterých můžeme upravit fotografii či video takovým způsobem, že si určíme text, který bude zakomponován do tohoto videa. U pokročilých softwarů je velmi obtížné určit, jestli se jedná o pravdu či podvrh.

Většina těchto softwarů byla vytvořena primárně pro pobavení. Avšak i tyto technologie lze zneužít ke tvorbě dezinformačních materiálů a hoaxů. Tyto materiály se nazývají **deepfake**. (Nasu, 2022)

Velké nebezpečí použití deepfakes je v současném období informačních válek. Není problém vytvořit video libovolného státníka, přednášejícího prohlášení v zájmu „útočníka“[3]. (Nasu, 2022)

Příležitost i nebezpečí v jednom je rozvoj moderních technologií. V dnešní době už je obtížné odlišit, zda po síti komunikujeme se skutečným člověkem, či pouze dobře naprogramovaným „chatbotem“.

Nutno podotknout, že nebezpečí dezinformačních chatbotů je v české republice menší než například v anglicky mluvících zemích. Jedním z důvodů je jistá složitost českého jazyka,

[3] Deepfake video ukrajinského prezidenta Volodymyra Zelenskeho, kde vyzývá občany ke složení zbraní https://www.youtube.com/watch?v=X17yrEV5sl4&ab_channel=TheTelegraph

kdy stroje mají problém se správným skloňováním apod. Také je pro „útočníky“ finančně náročné vyvíjet systém pouze pro použití v jednom státě. Proto je pro ně vhodnější připravit systém např. v anglickém jazyce, který je pro strojové systémy poněkud jednodušší (absence skloňování) a také mohou tento systém použít v řadě dalších zemí.

3.5.1 Sociální média a dezinformace

Sociálních médií existuje dnes několik druhů a každé má jiný cíl, obsah nebo funkce. Všechny mají však jeden společný cíl a tím je umožnit lidem budovat a udržovat vazby a vztahy s ostatními uživateli. V dnešní době jsou sociální média nedílnou součástí všech odvětví lidského života. Lidé je využívají pro zábavu, komunikaci se svými blízkými, sdílení zážitků a svých zájmů, nebo dokonce ke komunikaci ve firemních sférách. Sociální média jsou všude a celosvětově využívány. (Spišiaková, 2015)

Typy sociálních médií

Dělení a typů sociálních médií je spousta. Mohou být dělena podle jejich primárního určení nebo podle jejich funkcí.

- Osobní sítě – Facebook, Twitter, Whats App, Instagram atd.
- Sítě určené pro sdílení obsahu – Instagram, Pinterest, Reddit, Tumblr.
- Sítě sdružující uživatele se společnými zájmy – Linkedin, MeetUp, Flickr. (Spišiaková, 2015)

Při používání sociálních médií by měli být uživatelé obezřetní. Často si ani neuvědomují, co na svých sociálních mediích zveřejňují. Ať už se jedná o fotografie, příspěvky nebo komentáře, vždy to může pro útočníky sloužit jako vodítko a popud k útoku.

Jak již bylo řečeno, sociální sítě a média slouží ve velké míře k šíření dezinformací a propojování dezinformačních skupin. V některých případech se skupiny snaží tyto sítě zahltit jimi upravenými informacemi. Pokud k tomuto zahlcení dojde, pro běžného uživatele bude stále obtížnější ověřovat informace a v podstatě pro něj i ztrácet smysl informace ověřovat, pokud na každém médiu uvidí obdobné informace. Pomocí tohoto zahlcení mohou organizované skupiny ovlivnit veřejné mínění a názory veřejnosti.

Určitou formou obrany se může zdát cenzura. Avšak cenzuru veřejnost vnímá s nelibostí. Také to staví orgány rozhodující o cenzuře do role toho, kdo určuje, co pravda je a co není.

Také se tím umožní zablokovanému médiu stavět svoji popularitu na tom, že byl z vůle vlády zablokován, neboť jako jediný říkal pravdu.

3.6 Organizované šíření dezinformací

Na organizovaném a systematickém šíření dezinformací mají nemalý podíl i tzv. „trollí farmy“. Jedná se o organizovanou skupinu, která je financovaná či jiným způsobem odměněná za šíření zpráv ve prospěch zadavatele. Toto šíření zpráv spočívá především ve sdílení komentářů na sociálních sítích a přesvědčování komentujících. Činnost a existence těchto farem je velmi často spojovaná především s Ruskou federací, která je užívá jako jeden z mnoha prostředků vedení své hybridní války vůči „západu“. Avšak existence není vždy spojena se zájmy Ruské federace. Lze důvodně předpokládat, že jednotlivé trollí farmy vykazují činnost na podporu či proti různým politickým subjektům, či environmentálním kampaním. (Hrábek, 2017)

Základním principem funkce trollích farem je odepření občanům právo na informace založených na faktech, které jsou nezbytné pro utváření vlastních názorů.

Činnost trollí farmy často probíhá ve skupinách, kdy tato skupina „diskutuje“ mezi sebou na stránkách vybraného média. Vzájemně se přesvědčují a vyvrací své „argumenty“. Tuto diskuzi poté další skupina podporuje tzv. *likováním*[4] komentářů, pokud to dané médium podporuje. Obsahem těchto diskuzí je i sdílení zmanipulovaných obrázků, videí či odkazy na propagandistické a dezinformační stránky. (Vaj, 2015)

Cílem trollích farem je řešit témata politiky i na místech, která k tomu nejsou určená. Tím zasáhnout co možná největší spektrum lidí, děti, matky v domácnosti, dělníky, manažery apod. K tomu užívají již existující stránky, blogy a sociální sítě. Někdy zakládají různé nové internetové blogy a časopisy, které jsou na první pohled zaměřené např. na hobby a ve vhodný okamžik nějakým způsobem vložit informaci o politice. (Pomerantsev, 2020, s. 32-38)

[4] Algoritmus stránek doporučuje jednotlivé komentáře a vlákna na základě „oblíbenosti“ a tedy i důležitosti. Tato důležitost a „oblíbenost“ se vyhodnocuje na základě *liků*. Tímto si skupiny trollí farmy zajišťují, že se ke čtenářům dostane to, co tato skupina potřebuje.

DÍLČÍ ZÁVĚR

Třetí kapitola pojednávala o dezinformacích, jako o hlavní složce vedení hybridní války. Postupně byla rozebrána trestněprávní úprava v současné legislativě a samotná definice pojmu dezinformace. Dále byly popsány největší dezinformační kampaně v historii. V další části kapitoly bylo popsáno působení dezinformací na sociálních médiích a s moderními technologiemi. Závěrem kapitoly bylo popsáno šíření dezinformací organizovaným způsobem. Dezinformace jsou nepochybně velký problém, který působí také na bezpečnostní prostředí České republiky.

4 BEZPEČNOSTNÍ PROSTŘEDÍ ČESKÉ REPUBLIKY

Bezpečnostní prostředí je definováno jako prostor, ve kterém se realizují národní zájmy státu a také místo, kde se střetávají zájmy státu a jiných aktérů. Je také nedílnou součástí bezpečnostní politiky. Vyplývají z něj hrozby a rizika ohrožující dané státy a je třeba bezpečnostnímu prostředí věnovat dostatečně velkou pozornost, neboť se neustále vyvíjí a mění. (Frank, 2010) (Frank, 2003)

Bezpečnostní prostředí lze dělit na vnější a vnitřní. Vnějším bezpečnostním prostředím je myšlen prostor nacházející se za hranicemi České republiky. Ve vnějším prostoru se střetávají převážně zájmy našeho státu se zájmy jiných států, nebo aktérů a dochází k navazování mezinárodních vztahů. To vše má vliv na bezpečnost České republiky. Vnitřní bezpečnostní prostředí je geograficky vyhrazený prostor území České republiky. Zabývá se hrozbami a riziky, které ovlivňují bezpečnost státu uvnitř na jeho území. (Krásný, 2006)

Bezpečnostní strategie České republiky pohlíží na bezpečnostní prostředí jako na strategický kontext. Bezpečnostní prostředí našeho státu se neustále mění ve vztahu k bezpečnostní situaci v Evropě a ve světě. Na jeho stabilitu má vliv převážně rostoucí ctižádost ostatních aktérů, kteří se také snaží prosazovat své zájmy i vojenskou silou nebo hrozbami jejich použití. Nestabilita a konflikty daleko od hranic našeho státu, i přes svoji vzdálenost, nás stále ovlivňují a mohou mít také přímý dopad na bezpečnost České republiky. (Ministerstvo zahraničních věcí České republiky, 2015)

Aby se mohla Česká republika lépe chránit a zajistit spolehlivou bezpečnost pro své občany, musí znát bezpečnostní hrozby, které ji ovlivňují. Podle výsledků analýzy bezpečnostního prostředí lze identifikovat konkrétní hrozby ohrožující bezpečnost České republiky. Mezi tyto hrozby patří například terorismus, šíření zbraní hromadného ničení, kybernetické útoky, ale také oslabování mechanismu kooperativní bezpečnosti i politických a mezinárodněprávních závazků v oblasti bezpečnosti. Bezpečnostní strategie České republiky vymezuje jedenáct bezpečnostních hrozeb pro Českou republiku a pro každou hrozbu samostatně musí vytvořit strategii prevence a potlačování konkrétních bezpečnostních hrozeb. (Ministerstvo zahraničních věcí České republiky, 2015)

Samozřejmě od roku 2015 se některé bezpečnostní hrozby vyvinuly a přeměnily. Proto je nutné neustále situaci v bezpečnostním prostředí sledovat, monitorovat, analyzovat a pružně reagovat na každou změnu a vývoj přítomných rizik a hrozeb.

Nesmíme v žádném případě zapomenout na mezinárodní smlouvy a aliance, kterých je Česká republika součástí. Jako člen Evropské unie a Severoatlantické aliance, musí Česká republika k hrozbám přistupovat adekvátně a vycházet z aliančních závazků. Musí působit v širším strategickém prostředí, aby zainteresovala požadavky své, jakož i svých aliančních partnerů. To dává České republice značnou nevýhodu, protože musí plnit požadavky unie a aliance, a zároveň i závazky a opatření, které vyplývají z národních zájmů. Avšak na druhou stranu nesmíme opomenout ani výhody, které nám členství v aliancích přináší. Jedním z hlavních kladů je princip kolektivní obrany. Česká republika tudíž nemusí budovat velkou armádu, ale stačí mít velmi dobře vycvičenou a koordinovanou armádu i menších rozměrů, která bude oporou Alianci ve své odbornosti a profesionalitě. Také to dává prostor vládním orgánům soustředit se na vývoj uvnitř země a připravovat se na tyto vnitřní hrozby a rizika.

K obraně a prosazování bezpečnostních zájmů České republiky je nutné rozvíjet a podporovat spolupráci s právnickými a fyzickými osobami, orgány veřejné správy a samosprávy, ale také s občany.

Teritoriální vymezení bezpečnostního prostředí

Teritoriální vymezení bezpečnostního prostředí je proměnlivé ve vztahu k subjektu, kterého se týká. Bezpečnostní prostředí České republiky je vzhledem k samotné rozloze státu úzké, avšak z jiného hlediska je bezpečnostní prostředí České republiky součástí bezpečnostního prostředí NATO. (Frank, 2003)

Bezpečnostní strategie České republiky

Základním dokumentem bezpečnostní politiky ČR je právě Bezpečnostní strategie České republiky, nejaktuálnější vydání z roku 2015. Navazuje na další strategie a koncepce našeho státu ve vztahu k bezpečnosti a zajišťování ochrany státu. Vládní dokument je zpracováván Kanceláří Prezidenta republiky a Parlamentu ve snaze vyhledat vhodná opatření proti hrozícím rizikům. Popisuje a analyzuje změny v bezpečnostním prostředí a zaměřuje se na klíčové hrozby v euroatlantickém prostoru a představuje nástroje pro zajišťování bezpečnosti svého státu. (Ministerstvo zahraničních věcí České republiky, 2015)

DÍLČÍ ZÁVĚR

Poslední kapitola, čtvrtá, teoretické části diplomové práce byla věnována popisu bezpečnostního prostředí České republiky.

5 DÍLČÍ ZÁVĚR TEORETICKÉ ČÁSTI

Záměrem teoretické části diplomové práce bylo objasnit pojmy hybridní hrozby, hybridní válka, dezinformace a bezpečnostní prostředí. Tato část práce je rozdělena do čtyř kapitol, kdy je každá kapitola věnována popisu jednoho pojmu.

První kapitola pojednávala o popisu hybridních hrozeb. Druhá kapitola práce prezentovala hybridní válku. Třetí kapitola byla zaměřena na rozbor pojmu dezinformace jako na jednu z hlavních hybridních hrozeb. Čtvrtá kapitola se zabývala problematikou bezpečnostního prostředí. Nutno podotknout, že ač byly principy hybridní války využívány již v historii, s rozvojem moderních technologií se jedná o rozvíjející se a aktuální hrozbu.

II. PRAKTICKÁ ČÁST

6 VNÍMÁNÍ DEZINFORMACÍ VEŘEJNOSTÍ

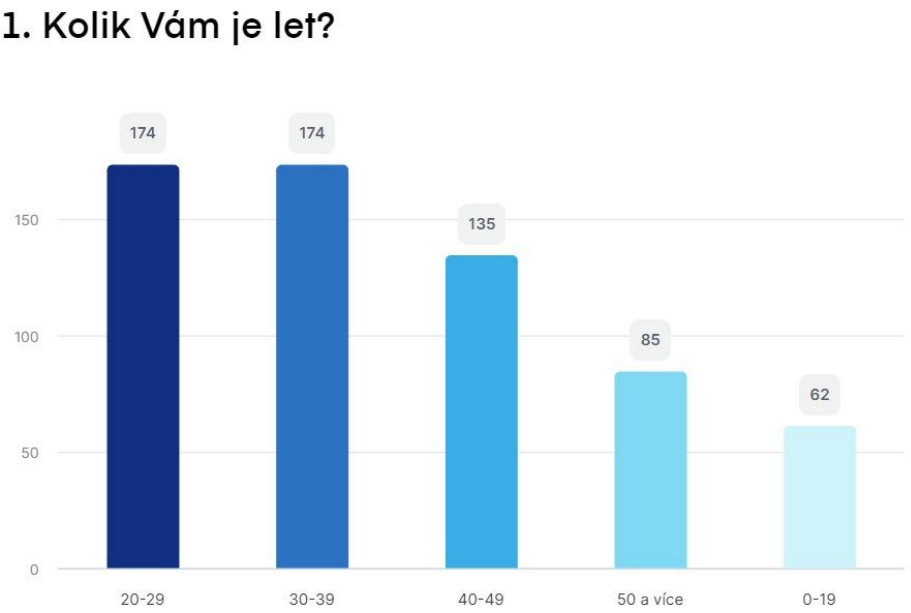
Za účelem posouzení vnímání dezinformací veřejností bylo provedeno dotazníkové šetření. Dotazník se skládá z 12 otázek, přičemž odpovědi na tyto otázky jsou převážně uzavřené, u dvou otázek byla možnost otevřené odpovědi. Dotazníkového šetření se zúčastnilo 717 respondentů, z toho 630 z nich dotazník úspěšně vyplnilo. Návratnost dotazníku byla tedy 87,9 %.

S cílem postihnout vnímání co nejširší skupiny obyvatelstva byl dotazník šířen mezi určité zájmové skupiny[5], odbornou veřejnost, jakož i mezi veřejnost laickou.

Přehled otázek dotazníkového šetření:

1. Kolik Vám je let?
2. Jaké je Vaše vzdělání?
3. Vnímáte rozdíl mezi pojmy „dezinformace“ a „misinformace“?
4. Vyberte vhodnou definici k pojmu „dezinformace“.
5. Vyberte vhodnou definici k pojmu „misinformace“.
6. Myslíte, že je Česká republika obětí šíření dezinformací?
7. Ohrožuje, podle Vás, šíření dezinformací bezpečnost České republiky?
8. Myslíte, že je blokování dezinformačních webů vhodná forma prevence?
9. Vyberte vhodné formy prevence vůči šíření dezinformací.
10. Považujete se za osobu schopnou rozeznat dezinformace?
11. Považujete sebe za osobu odolnou vůči dezinformacím?
12. Jakými kanály se, podle Vás, nejčastěji šíří dezinformace?

[5] Příslušníci PČR, internetová skupina Dezinformace a Hoaxy, uživatelé sociálních sítí

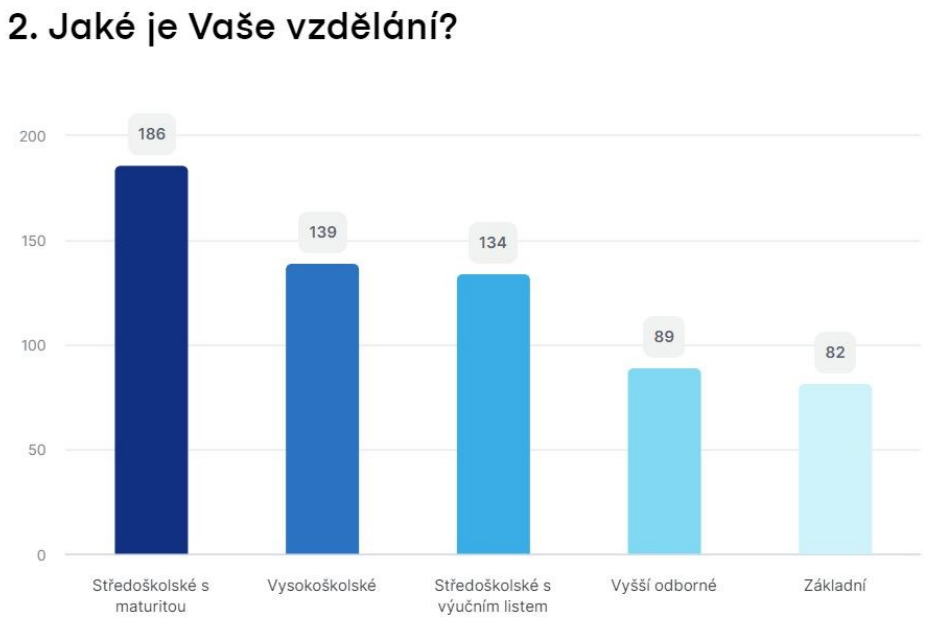


Obrázek 2 Dotazník, otázka č. 1

Zdroj: Vlastní zpracování, 2022

První otázka dotazníku **(Obr. 2)** sloužila ke generačnímu rozčlenění respondentů. Věkové kategorie byly rozděleny do pěti kategorií. Podle sesbíraných výsledků byly nejpočetnější skupiny respondentů ve věku 20–29 let a ve věku 30–39 let. Obě věkové kategorie byly zastoupeny 174 respondenty. Druhou nejpočetnější věkovou skupinou byly respondenti ve věku 40–49 let se 135 odpověďmi. Třetí v pořadí byla věková skupina 50 a více let s celkem 85 odpověďmi. Nejméně početnou skupinou s celkem 62 odpověďmi byly respondenti ve věku 0–19 let. Dotazník zasáhl veškeré věkové skupiny obyvatelstva, nejvíce však osoby od 20 do 39 let věku. Tato skupina osob je nejvíce ovlivněna prostřednictvím sociálních sítí, avšak nespadají do nejvíce ohrožené skupiny. Naopak nejvíce ohroženou skupinou jsou osoby ve věku 50 a více let. Neboť nedokáží efektivně vyhodnotit riziko dezinformačních a zavádějících zpráv. Právě z tohoto důvodu je potřeba této skupině věnovat více úsilí a chránit je.

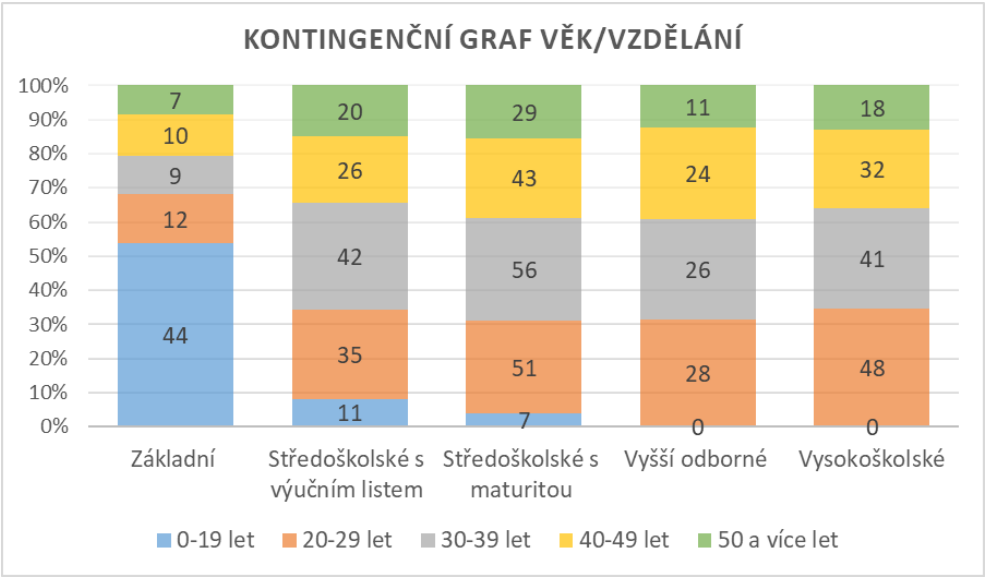
Zklamáním je také účast pouze 62 respondentů nejmladší věkové skupiny, do které lze zařadit osoby náctileté. Život těchto osob je plně ovlivněn a spjat s prostředím sociálních medií již od útlého věku. Kontakt s tímto prostředím od útlého věku, jim může do jisté míry znemožnit kriticky zhodnotit možná nebezpečí tohoto prostředí, a tak nejeví o tuto problematiku zájem.



Obrázek 3 Dotazník, otázka č. 2

Zdroj: Vlastní zpracování, 2022

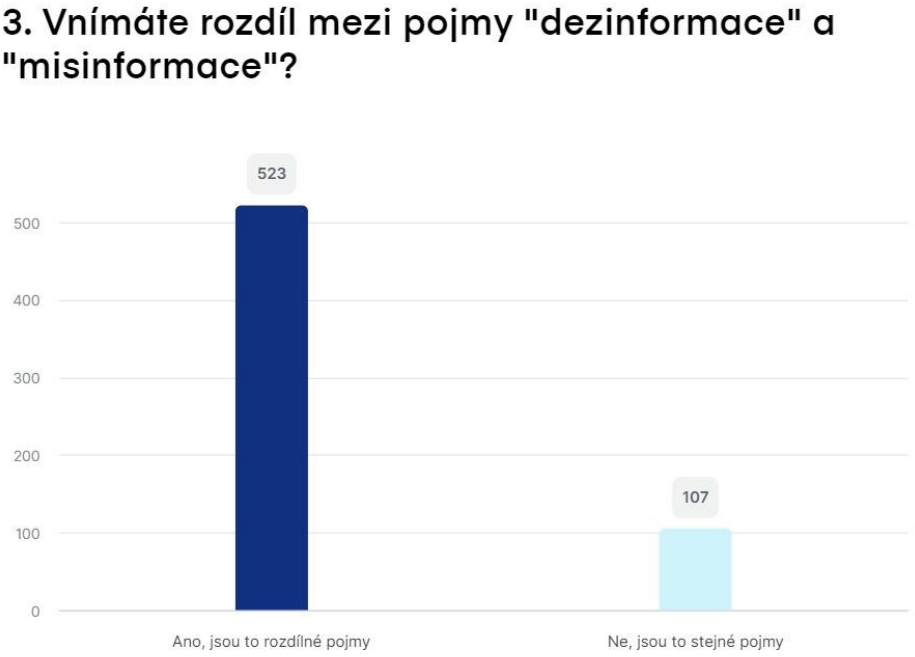
Dalším bodem pro rozdělení respondentů, je rozdělení podle vzdělání **(Obr. 3)**. Vzdělání je důležité pro utváření názorů. Širší rozhled nám umožňuje pochopit složitější témata a vidět jednotlivé spojitosti. Pro účely dotazníku bylo vzdělání rozděleno do pěti kategorií. Nejpočetnější skupinou byly osoby se středoškolským vzděláním zakončeným maturitou, celkem 186 respondentů. Druhou nejpočetnější skupinou byly osoby s vysokoškolským vzděláním, 139 respondentů. Pouze o pět méně, tedy 134 respondentů, mělo středoškolské vzdělání s výučním listem. Respondentů s vyšším odborným vzděláním bylo 89. Nejméně početnou skupinou bylo osob se základním vzděláním s celkovým počtem 82.



Obrázek 4 Kontingenční graf věk/vzdělání

Zdroj: Vlastní zpracování, 2022

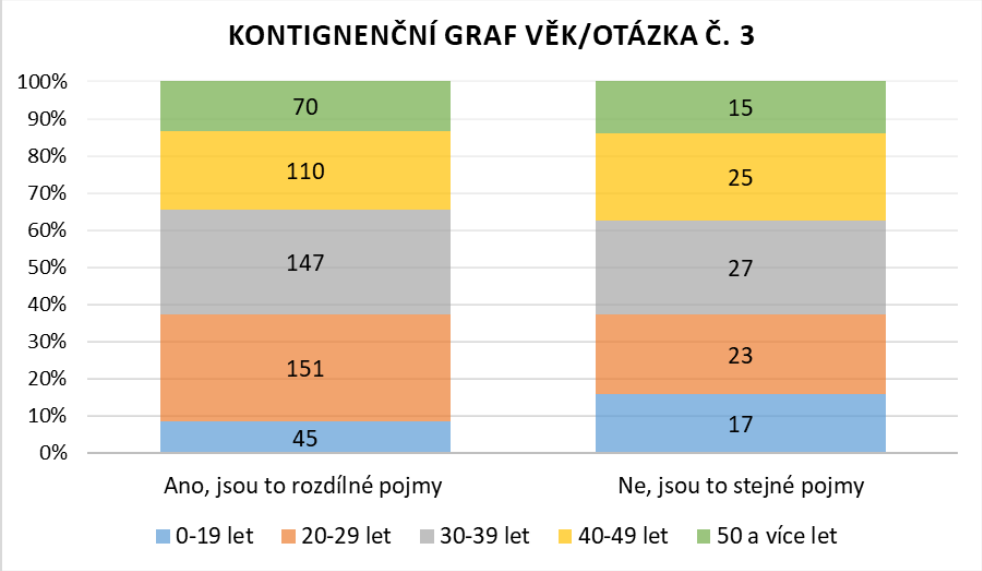
Kontingenční graf věk/vzdělání **(Obr. 4)** zobrazuje jednotlivé počty respondentů ve vztahu věku ke vzdělání. Je zjevné, že nejvíce osob se základním vzděláním bylo ve věkové skupině 0-19 let. Osoby se středoškolským vzděláním s výučním listem i maturitou byly nejvíce zastoupeny ve věkové skupině 30-39 let. Vyšší odborné a vysokoškolské vzdělání měly nejvíce osoby ve věkové skupině 20-29 let.



Obrázek 5 Dotazník, otázka č. 3
Zdroj: Vlastní zpracování, 2022

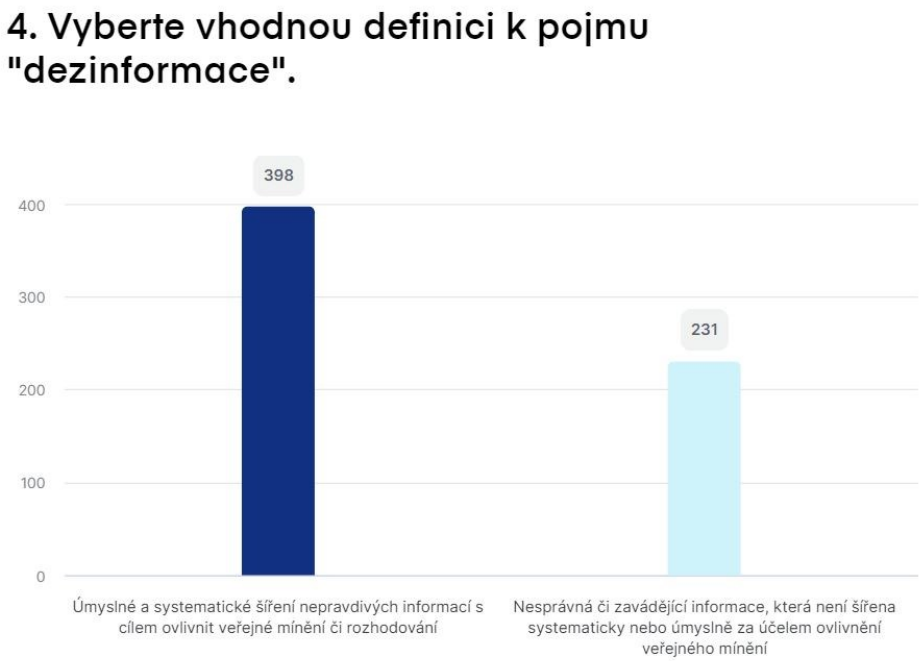
Základním kamenem k úspěšnému boji s dezinformacemi je schopnost rozlišit nebezpečné dezinformace od misinformací. Celkem 523 respondentů se označilo za osobu schopnou rozlišit tyto dva pojmy, zbylých 107 respondentů považují tyto dva pojmy za stejné **(Obr. 5)**.

Vnímání rozdílu mezi dezinformacemi a misinformacemi se liší také podle vzdělání respondentů. Jak již bylo řečeno, vzdělání je jedním z hlavních předpokladů k utváření názorů a vytvoření širšího rozhledu. Rozdíl v pojmech vnímá 50 osob se základním vzděláním, 108 se středoškolským vzděláním s výučním listem, 158 osob se středoškolským vzděláním s maturitou, 79 osob s vyšším odborným vzděláním a 128 osob a vysokoškolským vzděláním. Naopak 32 osob se základním vzděláním v těchto pojmech rozdíl nevnímá. Stejně tak jako 26 osob se středoškolským vzděláním ukončené výučním listem, 28 osob se středoškolským vzděláním ukončeným maturitní zkouškou, 10 respondentů s vyšším odborným vzděláním a 11 osob s vysokoškolským vzděláním.



Obrázek 6 Kontingenční graf věk/otázka č. 3
Zdroj: Vlastní zpracování, 2022

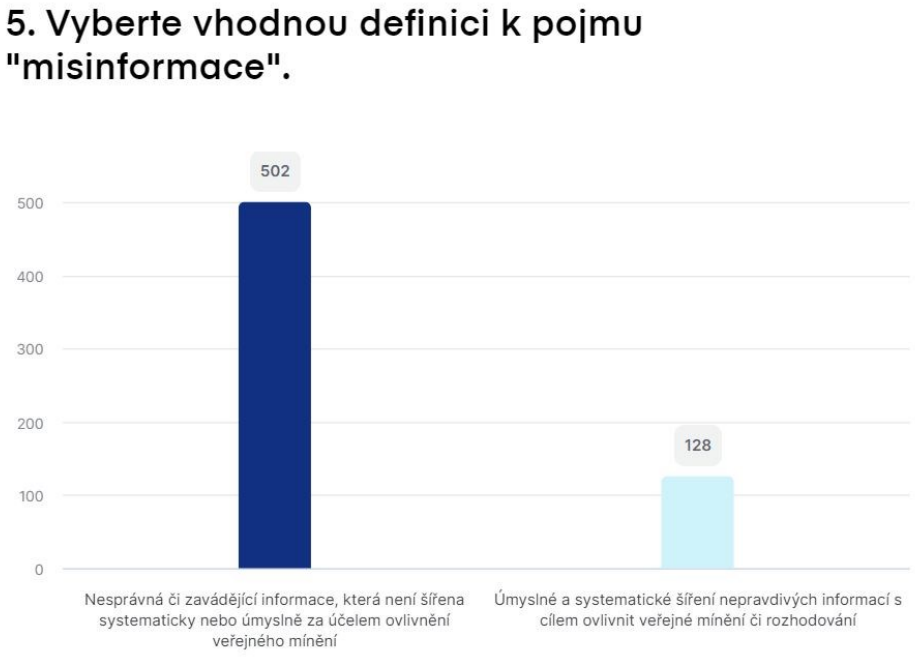
Z uvedeného grafu **(Obr. 6)** vyplývá, že ve věkové kategorii 0-19 let 45 respondentů považuje tyto pojmy za rozdílné, 17 dotazovaných stejné věkové kategorie v těchto pojmech nevidí rozdíl. 151 osob ve věkové kategorii 20-29 let považuje za rozdílné a 23 dotazovaných ze stejné kategorie rozdíl nevnímá. Druhou nejpočetnější skupinou dotazovaných, vnímající rozdíl mezi těmito pojmy, byla skupina ve věku 30-39 let s celkovým počtem 147, 27 respondentů označilo, že pojmy jsou stejné. Respondenti ve věku 40-49 let označili, že jsou pojmy rozdílné ve 110 případech a ve 25 případech, že jsou pojmy stejné. Polední věková kategorie 50 a více let považuje pojmy za rozdílné v 70 případech a v 15 případech je považuje za stejné.



Obrázek 7 Dotazník, otázka č. 4

Zdroj: Vlastní zpracování, 2022

Podle Ministerstva vnitra České republiky je pojem dezinformace definován jako *„Úmyslné a systematické šíření nepravdivých informací s cílem ovlivnit veřejné mínění či rozhodování.“* Správnou definici označilo 63,3 % respondentů. Nesprávnou definici označilo 36,7 % dotazovaných a 1 osoba tuto otázku nezodpověděla **(Obr. 7)**. (Ministerstvo vnitra České republiky, c2022a)

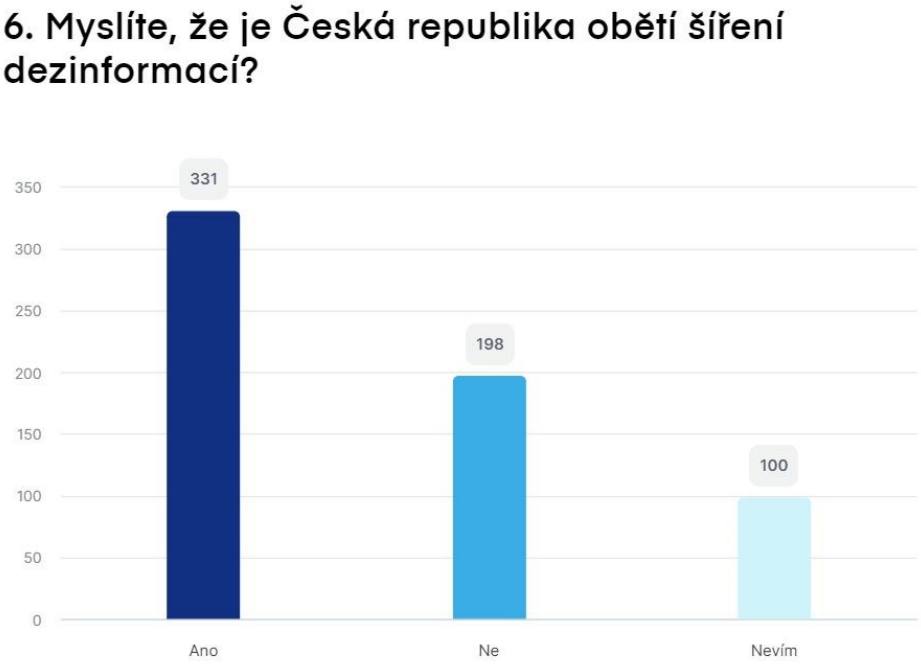


Obrázek 8 Dotazník, otázka č. 5

Zdroj: Vlastní zpracování, 2022

Pojem misinformace lze definovat jako *„Nesprávná či zavádějící informace, která není šířena systematicky nebo úmyslně za účelem ovlivnění veřejného mínění.“* Správnou odpověď označilo 79,7 % dotázaných **(Obr. 8)**. Obecně je překvapující procento správných odpovědí, neboť pojem misinformace je v mediálním prostoru méně užíván. (Ministerstvo vnitra České republiky, c2022a)

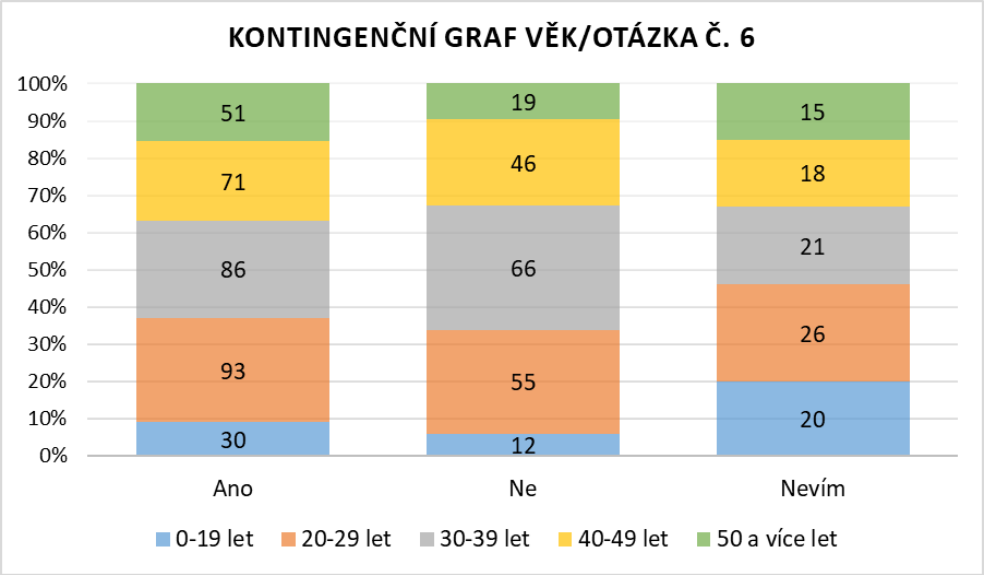
Pro doplnění lze uvést, že respondenti ve věku 20-39 let volili u obou otázek nejčastěji správnou odpověď.



Obrázek 9 Dotazník, otázka č. 6

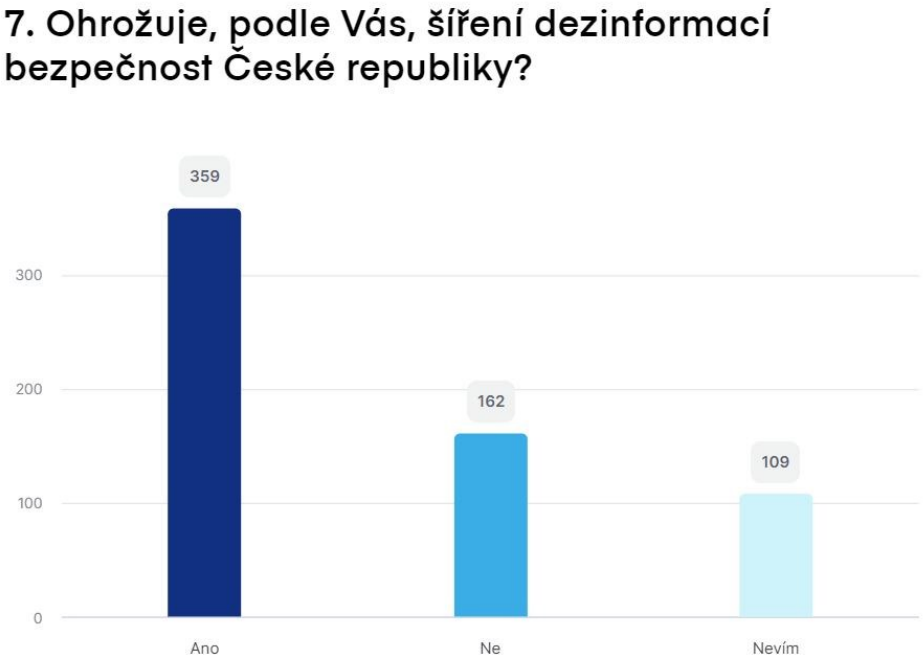
Zdroj: Vlastní zpracování, 2022

Na otázku, zda je Česká republika obětí šíření dezinformací odpovědělo kladně 331 respondentů, 198 respondentů odpovědělo, že ČR není obětí šíření dezinformací a 100 dotazovaných neví **(Obr. 9)**. Jeden respondent tuto otázku nezodpověděl. Ve společnosti jsou dezinformace a různé jiné zavádějící zprávy přítomny již dlouhou dobu. V českém internetovém prostoru je velké procento mediálních stránek, které šíří dezinformační zprávy a pomocí řetězových emailů se dále dostávají do společnosti a jsou rozšířené v takové míře, že se již staly součástí českého mediálního prostoru a lidé před nimi posupně ztrácí obranyschopnost.



Obrázek 10 Kontingenční graf věk/otázka č. 6
Zdroj: Vlastní zpracování, 2022

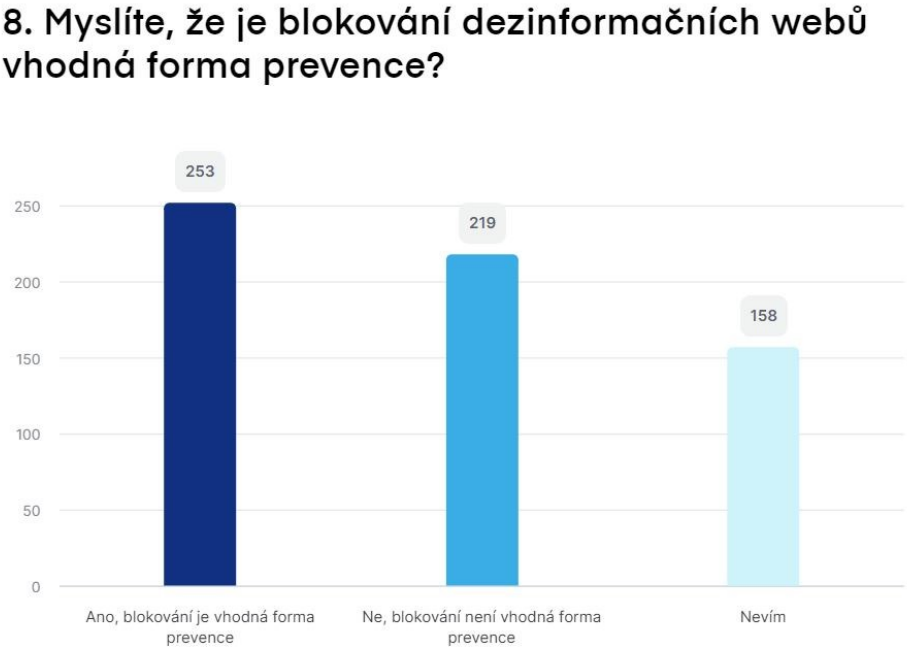
Co se týče rozdělení podle věkových skupin ve vztahu k otázce č. 6, kladnou a neutrální odpověď volili nejvíce osoby ve věku 20-29 let. Negativně hodnotila převážně věková skupina 30-39 let **(Obr. 10)**.



Obrázek 11 Dotazník, otázka č. 7
Zdroj: Vlastní zpracování, 2022

Výsledky otázky č. 7 podporují tvrzení BIS, která dlouhodobě upozorňuje na šíření zahraničních narativů v českém prostoru. Neboť 359 respondentů uvedlo, že šíření dezinformací ohrožuje bezpečnost České republiky **(Obr. 11)**. Pouze 162 respondentů uvedlo nesouhlasné stanovisko a zbývajících 109 odpovědělo neutrálně. I když si to mnozí

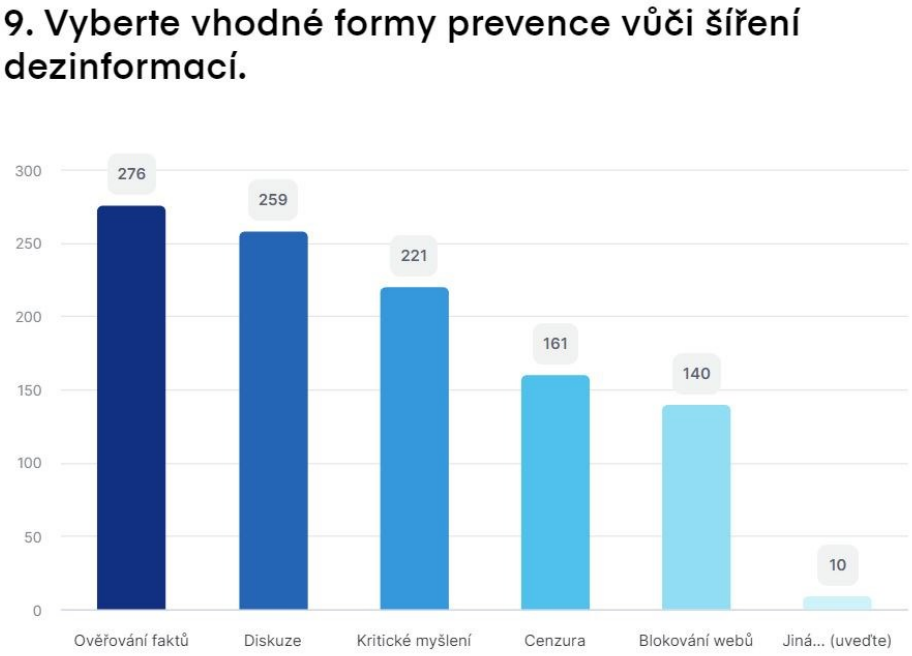
z nás neuvědomují, šíření dezinformací probíhá dnes a denně. Různé zahraniční agentury se snaží o vnitřní rozklad společnosti, upevnění své pozice v našem státu a hájení svých zájmů. V mnoha případech k tomu dochází prostřednictvím zpochybňování kroků vlády, nevhodné výklady prohlášení, upozorňování na chyby provedené v minulosti či prosté šíření pomluv a lží.



Obrázek 12 Dotazník, otázka č. 8
Zdroj: Vlastní zpracování, 2022

Ze všech perspektiv, na tuto otázku neexistuje obecně správná odpověď. Z každé možnosti **(Obr. 12)**, jsou šiřitelé schopni dojít zisku a stále napadat jejich cíl. Jedním z nejvhodnějších způsobů, jak se vypořádat s přítomností dezinformačních webů v internetovém prostoru, je všeobecná diskuze, pomocí které se může mezi obyvatelstvo šířit vysvětlení, proč a co je špatné a proč těmto informacím nevěřit. Pokud by vláda zakázala nebo nařídila blokování těchto webů, bude se sama stavět do pozice soudce, který určuje, co je pravda a co lež. Při snaze blokovat tyto weby, se provozovatelé těchto stránek mohou prezentovat prohlášením, že oni jediní šíří pravdu a z toho důvodu je chtějí vládnoucí strany umlčet. Pokud se těmto webům nechá příliš velký prostor k operování, budou se nekontrolovaně rozšiřovat, získávat více a více popularity a ovlivňovat myšlení ostatních. Existují osoby, které budou za každou cenu zastávat tato média a bezmezně jim důvěřovat. Z tohoto důvodu, je nejlepším řešením, diskuze na celospolečenské úrovni či osvětová kampaň, která by lidi učila ověřovat si zprávy z více zdrojů. Pokud by ale byla kampaň vedena a propagována vládou, lze předpokládat, negativní ohlas provozovatelů

dezinformačních webů. Z výše popsaných důvodů vyplývá složitost tohoto tématu a komplikovanost nalezení správného řešení, neboť jednoduchá odpověď neexistuje.



Obrázek 13 Dotazník, otázka č. 9

Zdroj: Vlastní zpracování, 2022

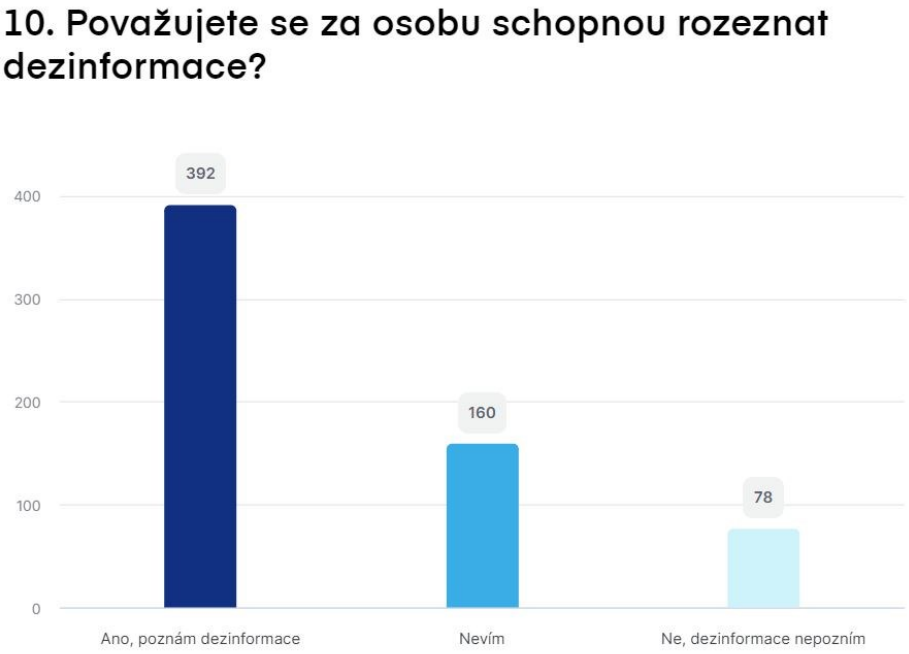
Mezi nejvhodnější formy prevence vůči šíření dezinformací patří ověřování faktů, pro které hlasovalo 276 respondentů **(Obr. 13)**. Co se týče ověřování faktů, v současné době existuje několik webových stránek, které se zabývají monitorováním a vyvracením nejčastěji se šířících manipulativních zpráv a hoaxů. Pro možnost diskuze, jako dalšího způsobu prevence hlasovalo 259 respondentů. Třetí nejčastěji volenou možností je kritické myšlení, pro které hlasovalo 221 dotázaných. Možnost cenzury volilo 161 respondentů. Blokování webů jako nejlepší formu prevence zvolilo 140 dotázaných.

Dále byly k této otázce uvedeny i jiné možnosti odpovědi, které jsou:

- Edukace.
- Osvěta, edukace, informační kampaně.
- Vzdělávaní.
- Výuka kritického myšlení a mediální gramotnosti ve školách.
- Zřízení příslušného úřadu, spolehlivá legislativa, silný státní aparát.
- Přidělení účtu na sociálních sítích oproti dokladu.
- Osvěta.

- Legislativa.
- Odsouzení šiřitelů jakožto zrádců ;-) lobotomie.
- Logika.

Některé, respondenty uvedené, možnosti lze reálně využít. Patří mezi ně především osvěta, vzdělávání a výuka kritického myšlení a mediální gramotnosti. Výuka mediální gramotnosti by byla dobrým doplněním osnov informatiky na základních a středních školách.

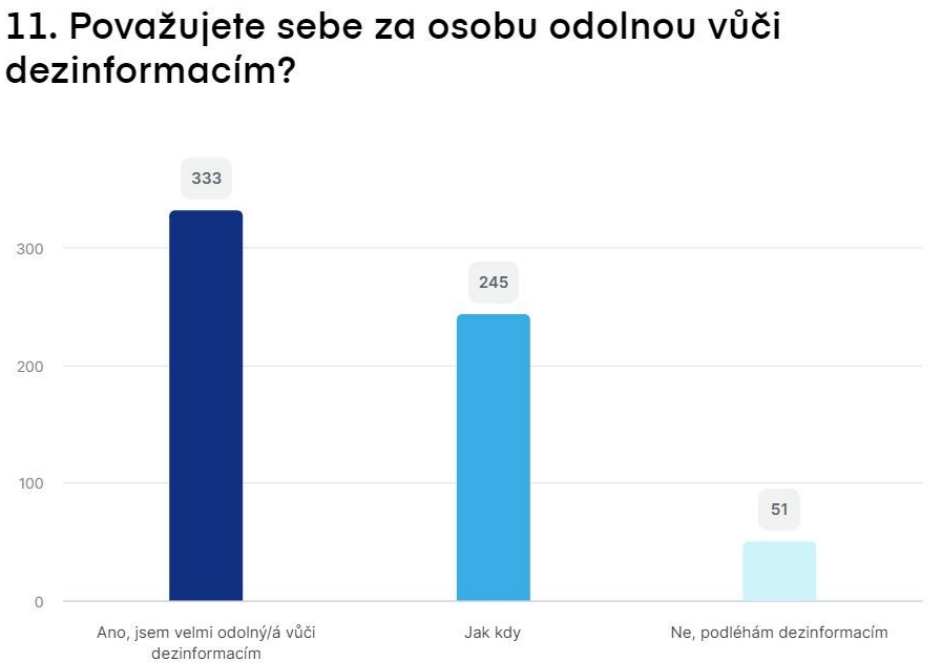


Obrázek 14 Dotazník, otázka č. 10

Zdroj: Vlastní zpracování, 2022

Ke schopnosti rozeznat dezinformace je také nutno mít přehled o aktuálním dění v mediálním prostoru. Nestačí si pouze informaci přečíst, je také nutné znát její kontext. Dezinformační zprávy nikdy nevznikají nahodile, ale většinou se skrývají ve zprávách o aktuálním dění. Podle výsledku se 392 respondentů považuje za osobu schopnou rozeznat dezinformace **(Obr. 14)**. Možnost nevím zvolilo 160 dotázaných a 78 respondentů se považuje za osobu, která dezinformace nepozná. I když je většina výsledků pozitivní, realita se může lišit, a i osoba, která se považuje za schopnou dezinformace rozeznat, se může zmýlit. V dnešní uspěchané době je stále obtížnější najít si čas zprávu vyhodnotit, a proto předkládanou zprávu přijme a neověří si její správnost. K tomu nepomáhá ani fakt, že šiřitelé dezinformačních zpráv přichází stále s novými způsoby, jak

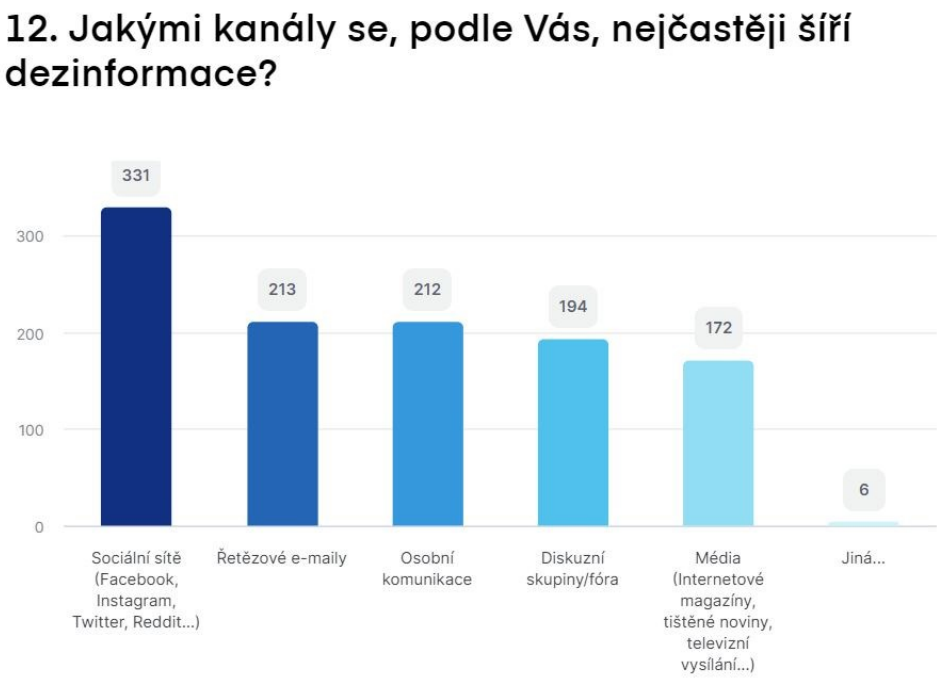
věrohodně předkládat dezinformace. Proto je stále obtížnější a časově náročnější informace kriticky vyhodnocovat a ověřovat z více zdrojů.



Obrázek 15 Dotazník, otázka č. 11

Zdroj: Vlastní zpracování, 2022

Nestačí pouze dezinformace poznat či identifikovat, ale nesmíme se jimi nechat ovlivňovat. Jedinci, kteří dezinformaci vyhodnotí a poznají, ji mohou z legrace sdělit ostatním kolegům či známým, kteří tuto informaci mohou přijmout za reálnou. Nejlepší ochrana a prevence je nevěnovat těmto informacím pozornost a nešířit je dál. Podle výsledků průzkumu se 333 dotázaných považuje za osobu odolnou vůči dezinformacím **(Obr. 15)**. Na druhou stranu 245 dotázaných uvedlo, že jim částečně podléhají. Nelze zapomenout ani na 51 respondentů, kteří dezinformacím podléhají. Jeden respondent otázku nezodpověděl. Lze předpokládat, že procento osob podléhajících dezinformacím může být vyšší. Řada osob totiž přebírá informace z dezinformačních webů a medií a tyto informace pokládá za pravdivé a relevantní. Dále vyplývá, že osoby, považující se za odolné vůči dezinformacím byly převážně osoby s vysokoškolským a středoškolským vzděláním s maturitou. Osoby převážně se základním vzděláním se považují za osoby podléhající dezinformacím.



Obrázek 16 Dotazník, otázka č. 12

Zdroj: Vlastní zpracování, 2022

Pro šíření dezinformačních zpráv a informací se používá mnoho různých kanálů. Často se tyto způsoby kombinují navzájem. Kdy například zveřejní zprávu na svém webu a k šíření této zprávy využívají řetězových emailů či sociálních sítí. V poslední době se lze setkat i s šířením dezinformací za úplatu tzv. influencery[6].

Tomu v podstatě odpovídají i výsledky 12. otázky dotazníku **(Obr. 16)**. Nejvíce volenou odpovědí bylo šíření pomocí sociálních sítí, tato možnost získala 331 hlasů. Dále následovaly řetězové e-maily s 213 hlasy, osobní komunikace s 212 hlasy, diskuzní skupiny/fóra se 194 hlasy, média se 172 hlasy a šestkrát byla zvolena i možnost jiná.

Sociální sítě jsou dlouhodobě v oblibě mezi šiřiteli dezinformací a tzv. internetovými trolly, protože prostředí sociálních sítí poskytuje dobrou anonymitu, vyřízení profilu je bezplatné, umožňuje kontakt s velkou skupinou uživatelů a pokud „útočníci“ postupují podle různých algoritmů chování jednotlivých sociálních sítí, tato skupina uživatelů se snadno zvětší. Ochrana před takovými uživateli je obtížná a zpočátku je obtížné také odhalení jejich opravdových úmyslů. Snaží se totiž chovat co možná nejvíce nenápadně a postupně do komunikace vkládat i nejrůznější narativy. Často také diskutují různé dezinformační skupiny mezi sebou, aby si ostatní uživatelé mohli následně tuto komunikaci přečíst a přijmout jednotlivé argumenty za své.

[6] Deník *The Guardian* přinesl zjištění, že různé PR agentury napojené na Rusko nabízely francouzským a německým influencerům peníze za šíření nepravdivých informací ohledně úmrtí po aplikaci vakcín na COVID-19. (Henley, 2021)

Řetězové e-maily se mohou zdát podceňované a více méně neškodné. Opak je ale pravdou. Manipulativní řetězové e-maily zasahují desetitisíce občanů a svou formou i způsobem šíření jsou zacílené především na seniory. Tudíž ovlivňují ne zrovna malou část české populace. Podle průzkumů provedených v roce 2018 se s manipulativními řetězovými e-maily setkalo přes 90 % českých seniorů a 20 % z nich se přiznalo k aktivnímu přeposílání těchto zpráv. (Čeští elfové, c2021)

Respondenti uvedli následující další odpovědi:

- Spd.
- Komentářové sekce.
- Projevy bývalého premiéra A.B.
- Dezinformační letáky vhozené do schránky.
- Televizní a rádiové vysílání podléhající cenzorským úřadům.
- Pošta, vylepené plakáty na veřejných místech.

6.1 Celkové vyhodnocení dotazníku

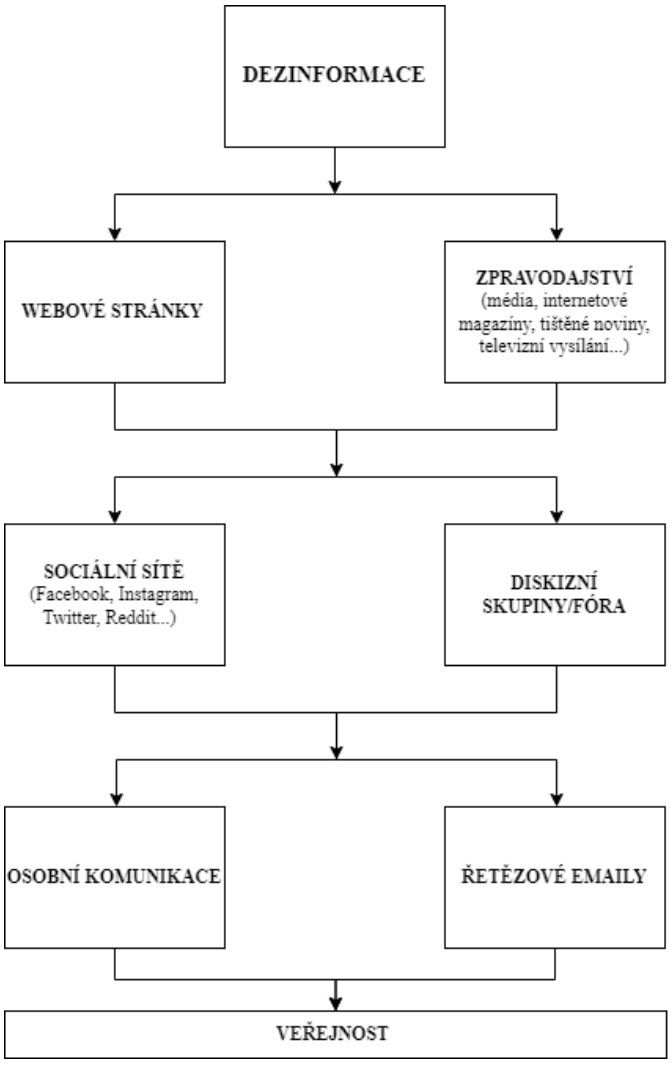
Dotazník obsahoval 12 otázek, které dotázaní postupně vyplňovali. První dvě otázky byly obecného charakteru na zjištění složení skupiny respondentů. Rozdělení bylo podle věku a vzdělání. Následující otázky již byly zaměřeny na samotnou problematiku dezinformací. Po celkovém vyhodnocení dotazníku lze konstatovat, že vybraný vzorek obyvatelstva je ve zkoumané problematice znalý a dokáže se orientovat. Povědomí o základech problematiky a zájem mají v podstatě všechny zkoumané věkové kategorie.

Dotazníkového šetření se zúčastnilo 630 respondentů, kteří úspěšně tento dotazník ukončili a odeslali. Lze tedy usoudit, že i samotný zájem o problematiku dezinformací vcelku vysoký. Takto vysokému počtu respondentů napomohla i vhodná distribuce mezi respondenty. Šetření se účastnili příslušníci bezpečnostních sborů, jakož i odborná a laická veřejnost. O zájmu o tuto problematiku vypovídá i skutečnost, kdy někteří respondenti poslali i zpětnou vazbu s doporučením pro případné opakování šetření a projevovali zájem i před vyplněním samotného dotazníku.

6.2 Postup šíření dezinformací

Samotná tvorba dezinformací je vcelku prostý proces. Vše se zakládá na převzetí reálné informace, či reakce na aktuální dění a upravení této informace za účelem ovlivnění určité

skupiny obyvatelstva. Ať už se jedná o jednotlivce, který chce uplatnit svůj vnitřní zájem, nebo o organizovanou skupinu, která plní vyšší cíle. Proces přijetí dezinformační zprávy není v současnosti nic složitého. Dezinformacím je veřejnost vystavena dnes a denně a jejich šíření ve velké míře závisí i na samotných příjemcích. Samotní příjemci informací jsou svým způsobem misinformátoři, protože si tyto přijaté informace upravují podle svého za účelem většího šokování dalších příjemců. Lidé si mnohdy tuto skutečnost ani neuvědomí, a tak jednoduše dochází ke zbarvení pravdivé události. Následně čím více se informace předává mezi lidmi, tím větší je šance, že si každý interpret informaci upraví. Je velice pravděpodobné, že možný desátý posluchač se dozví zcela jinou informaci. V současnosti čtenáři různých internetových médií čtou pouze titulky zpráv a celý obsah sdělení si domyslí na základě tohoto titulku. Tohoto faktu využívají samotní tvůrci dezinformací a upravují tak titulky článků pro větší atraktivitu čtenářů.



Obrázek 17 Postup šíření dezinformací
Zdroj: Vlastní zpracování, 2022

Jak již bylo zmíněno, šíření dezinformací je závislé na samotných příjemcích. Pokud se totožné informace dostanou k dalšímu příjemci z více stran nebo zdrojů, stává se tak lépe uvěřitelnou a v jeho očích reálnou informací. Z tohoto důvodu obsahuje většina dezinformačních zpráv výzvu ke sdílení. V takovémto případě je ověřování informací a zpráv daleko složitější a člověk tak snáze uvěří dezinformačním zprávám, potažmo je pak dále šíří sám.

Samotný postup šíření dezinformací začíná vznikem dezinformace jako takové. Ať už má dezinformace pravdivý základ anebo je zcela vymyšlená, na způsobu šíření se nic nemění. Prvním krokem po vytvoření samotné dezinformační zprávy je uveřejnění této zprávy nejčastěji na „zpravodajských“ webech či jiných internetových stránkách. Návštěvníci těchto stránek tuto informaci přijmou a dále ji šíří prostřednictvím sociálních sítí. Nezáleží na tom, zda tyto zprávy šíří za účelem satiry nebo z přesvědčení, sami se stávají hnacím motorem šíření těchto dezinformačních zpráv. Příjemci mohou dále zprávy a informace rozebírat na různých diskuzních fórech nebo v komentářových sekcích na sociálních sítích. To směřuje k dalším desítkám nebo stovkám úprav přijímané informace, podle povahy čtenáře. Následně je jen otázkou času kdy se tyto informace a zprávy přesunou z internetového prostředí reálného světa. Samotní příjemci o těchto informacích rádi diskutují v zaměstnání se svými kolegy, s přáteli nebo rodinou. Podstatnou roli v šíření dezinformačních zpráv hrají i řetězové emaily. Řetězové emaily jsou primárně zaměřeny na příjemce vyšších věkových kategorií, kteří těmto zprávám snadněji podléhají. Většina těchto škodlivých emailů obsahuje výzvu k dalšímu sdílení a šíření tak více závisí na samotných příjemcích.

6.3 Kontrolní seznam (Checklist) ověření informací

Při prohlížení novinových článků a zpráv můžeme snadno narazit na nejrůznější texty, pomocí kterých nás chtějí autoři ovlivnit. Takové texty se nazývají manipulativní. Abychom byli odolnější vůči manipulacím prostřednictvím těchto textů, je dobré myslet na základní znaky a pravidla. Takové texty se dají, některé snadno a jiné obtížněji, odhalit.

Manipulativní novinové články mají titulky psané často s použitím velkých písmen ve snaze nás upoutat a vytvořit pocit naléhavosti sdělení. Také je vhodné nevytvářet si názory na základě přečtených titulků, neboť obsah titulku ve velké míře často ani nesouvisí s obsahem samotného článku. Autoři používají zajímavé titulky pouze ve snaze o zvýšení popularity daného média. (Nelež, c2020)

Dalším krokem k odhalení manipulativního textu je kontrola zdrojů, které autor použil. Pokud u textu nejsou zveřejněné použité zdroje, či tyto zdroje odkazují na závadné stránky, s velkou pravděpodobností je závadný i obsah samotného článku. Dalším krokem je ověření, kdo je autor textu. Pokud autor nepřísluší k některé ze zavedených redakcí, za jeho články nese odpovědnost pouze sám autor a není tedy žádná záruka za relevantnost obsahu. (Nelež, c2020)

Datum uveřejnění textu nám také může pomoci. Často dochází ke sdílení článků se starším datem vydání pouze na základě podobnosti s aktuálním děním. Tyto články jsou sdíleny buď celkově, tedy s textem i doprovodnými obrázky, nebo jsou sdíleny pouze obrázky. V současnosti si můžeme ověřit pravdivost data pořízení daného obrázku díky funkci „vyhledat podobnou fotografii“. Ve velice krátké době tedy získáme výčet článků a stránek, které danou fotografii použily spolu s datem zveřejnění. (Nelež, c2020)

Je také nutné sledovat, zda článek obsahuje emoce. Pokud již titulek článku vyvolává agresi či rozčilení a článek samotný v tomto pokračuje, pak je velké riziko, že byl článek napsán pouze za účelem vyvolání konkrétní emoce bez snahy o pravdivost uveřejněných informací. (Nelež, c2020)

V poslední řadě nesmíme zapomínat na ověřování informací. Pokud se informace v článku zdají až moc přesvědčivé či jednostranně zaměřené, je vždy vhodné najít články nebo zdroje, které nabízí pohled i z druhé strany či rozebírají stejné téma. Poté si můžeme posoudit relevantnost informací pro naši potřebu. (Nelež, c2020)

Pokud si čtenáři a příjemci zpráv chtějí ověřit její pravdivost, mohou si ji ověřit pomocí několika kontrolních otázek uvedených v následujícím kontrolním seznamu neboli Checklistu. Dezinformace a různé zavádějící zprávy lze poznat podle několika varovných signálů.

Tabulka 1 Kontrolní seznam (Checklist) ověření informací

P.č.	Otázka	ANO	NE	Pozn.
1	Obsahuje informace výrok: *„tohle před námi tají*…?			
2	Obsahuje informace fráze: *„nezávislost“*, *„svoboda“*, *„bez cenzury“*, *„nekorektní“*, apod.?			
3	Je informace přeposlána jako kopie emailu s desítkou dalších příjemců?			
4	Vybízí informace ke sdílení s dalšími čtenáři, uživateli nebo známými?			
5	Je informace psána nespisovnou češtinou a obsahuje gramatické chyby?			
6	Obsahuje text pasáže psané velkými písmeny?			
7	Obsahuje text opakovaně několik vykřičníků za sebou?			
8	Jsou v textu obsaženy fráze typu: *„tohle si nenecháme líbit“*, *„jakou budoucnost připravují pro naše děti“*, *„tohle už nikdo nezastaví“*, apod.?			
9	Vybízí text k zaslání peněz nebo provedení nákupu?			
10	Obsahuje text instrukce k rozkliknutí internetového odkazu?			

Zdroj: Upraveno podle Malý, 2021

Uvedené otázky v kontrolním seznamu jsou pouze jedny z mnoha dalších, které by mohly být použity při kontrole správnosti sdělení. Otázky se mohou samozřejmě lišit ve vztahu ke zkoumanému tématu, a proto se podoba kontrolního seznamu může kdykoliv pozměnit. Uvedené otázky **(Tab. 1)** mohou sloužit jako vodítko, znázorňující, jak útočníci zprávy vytváří. Jak již bylo popsáno, dezinformační weby vydělávají na zveřejňování reklamy či provádění nákupu přes jejich odkazy. Proto je důležité nepodléhat skrytému nátlaku

těchto stránek a vyvarovat se otevírání těchto internetových reklam a odkazů. Nejen že nás reklamy mohou přesměrovat na stránky se závadným obsahem, ale také v některých případech v nich mohou být skryté hrozby v podobě počítačových virů. V takovýchto případech už nejsme dezinformacemi ohroženi pouze my, ale i náš majetek a soukromí. Podobný kontrolní seznam může být použit při ověření či kontrole věrohodnosti osobností. Už jen otázka *„Je tato osoba věrohodná?“* nebo *„Mohu této osobnosti plně důvěřovat?“* v nás může jednoduše vzbouzet negativní emoce, tudíž negativní odpověď, nebo naopak.

DÍLČÍ ZÁVĚR

Kapitola šestá pojednávala o zjištění, jak veřejnost vnímá dezinformace. Toto zjištění bylo provedeno formou dotazníkového šetření, kterého se zúčastnilo 630 respondentů. Všechny dotazníkové otázky byly okomentovány, vyhodnoceny a některé otázky byly doplněny kontingenčními grafy pro upřesnění. Výsledky šetření prokázaly, že se veřejnost v oblasti dezinformací orientuje a je schopna dezinformace rozeznat. Následně byla řešena problematika šíření dezinformací a jejich postup šíření byl graficky zaznamenán v diagramu. V poslední řadě byl vytvořen kontrolní seznam neboli Checklist, sloužící jako průvodce nebo rádce při ověřování relevantnosti a pravosti informace.

7 VLIV DEZINFORMACÍ NA SOCIÁLNÍ A BEZPEČNOSTNÍ PROSTŘEDÍ

Šíření dezinformací a konspirací má také velmi velký dopad na sociální prostředí České republiky. Sociální prostředí má samo o sobě nejasnou definici. Pojem se často zaměňuje nebo ztotožňuje se společenským prostředím nebo sociálním světem. Lze říci, že se jedná o souhrn společenských aspektů, nebo také o společenství, ve kterém člověk žije, navazuje vztahy a vyvíjí se. (Šilhánová, Nešpor, 2017) (Kohoutek, c2005-2022)

Dezinformace stále více ovlivňují společenské hodnoty, mění názory na kritické problémy a témata a vytváří nové názory na fakta, pravdy a přesvědčení. Negativní působení dezinformací v sociálním prostředí se může projevit konflikty mezi občany, spory na pracovišti, rozpory v rodinách nebo mezi přáteli, pouze z důvodu zastávání jiných názorů. Jedním z jasných příkladů mohou být uvedeny například prezidentské volby. Jednotlivé strany jsou často napadány oponenty nebo voliči zastávající názory jiné strany, za účelem je pošpinit a vytvořit tak dojem, že nejsou jako kandidáti vhodní. To má řetězový vliv na voliče, kteří jsou přímo ovlivněni rozšiřujícími se dezinformacemi. Dochází ke střetu konfliktů zastánců různých kandidátů, ve snaze ospravedlnit a vyvrátit tvrzení dezinformací. Trpí tím tak celá společnost a mezilidské vztahy. (Mooney, 2018)

Bezpečnostní prostředí, jakožto vymezený prostor zabývající se možnými hrozbami a riziky, působící na území České republiky, je samozřejmě existencí dezinformací velmi ohroženo. Ve vztahu vnitřního bezpečnostního prostředí šíření dezinformací obrací občany jednoho státu proti sobě, tvrzením pouhých názorů. Dobře zmanipulovaná informace by mohla vést až ke vzniku konfliktu mezi občany. Nebo činnosti, kterým se dezinformační weby a skupiny zabývají primárně, jako ponížit a vyvolat nedůvěru vlády a představenstva České republiky. Stejným způsobem by mohl být vytvořen konflikt mezi sousedními, nebo dvěma rozdílnými státy. Za použití a rozšíření dezinformací o jednom státě ohrožující druhý a naopak. Bezpečnost států by pak byla ohrožena. Občané dotčených a napadených států se mohou dožadovat vyjádření, které se může pod nátlakem velmi lehce zmanipulovat a dát prostor k vytvoření nových dezinformací, které mohou situaci ještě více zhoršit.

DÍLČÍ ZÁVĚR

V sedmé kapitole byl popsán pojem sociální prostředí a vliv dezinformací na toto prostředí. Dále byl popsán vliv dezinformací na bezpečnostní prostředí.

8 NÁVRHY NA ZLEPŠENÍ STÁVAJÍCÍHO STAVU

Ve snaze zlepšení stávajícího stavu je nutné si uvědomit, že dezinformace nejsou pouze bezpečnostní hrozbou. Šíření dezinformací ohrožuje jak bezpečnost samotnou, tak narušuje například sociální vazby, v nejhorším případě může dojít i k ohrožení samotného života, pokud se budeme řídit zveřejňovanými šarlatánskými radami. Souhrnně lze jako návrhy označit například:

- zvýšení úrovně mediální gramotnosti,
- apel na kritické myšlení,
- osvětová kampaň,
- vymáhání práva v online prostoru,
- fact-checking.

Tyto popsané možnosti jsou pouze část možností, pomocí kterých lze zvýšit a zlepšit úroveň odolnosti obyvatel proti působení dezinformací. Způsobů, jakými zvýšit odolnost je nepochybně více, avšak již zmíněné možnosti jsou nejzásadnější. Pokud si totiž obyvatelé osvojí některé schopnosti, budou disponovat již akceptovatelnou úrovní odolnosti.

Zvýšení úrovně mediální gramotnosti

Mediální gramotnost je v dnešní době asi nejvíce důležitou schopností. Každý musí být schopen se orientovat v psaném textu, najít zde skryté významy, popřípadě odhalit manipulující techniky. Výuku mediální gramotnosti je vhodné zařadit do výuky na základních a středních školách. Právě tito žáci již vyrůstají ve světě zcela ovlivněném světem médií a sociálních sítí. Velkou část svého volného času tráví před obrazovkou svého mobilního telefonu, proto právě na tuto skupinu je třeba zaměřit co nejvíce úsilí.

Vzdělávání mladších generací v problematice hybridních hrozeb a dezinformací je základem pro možné snížení počtu dezinformačních webů a jejich vlivu. V případě, kdy si bude každý umět informace a zprávy ověřit a nebude slepě věřit pouze jednomu zdroji, brát to tak, že „co je psáno, to je dáno“, dezinformační weby budou ztrácet svoji popularitu a smysl. S nástupem modernějších technologií, bude pro budoucí generace daleko snazší si informace dohledat a ověřit na mnoha jiných internetových stránkách, nebo diskuzních fórech. Je možné, že se o problematiku dezinformací bude zajímat daleko více lidí a snažit

se ji vymýtit z mediálního světa. Nic těmto osobám nebude bránit v zakládání dalších internetových webů a stránek, které budou uvádět dezinformace na pravou míru a objasňovat jejich nepravost.

Nelze však zapomínat ani na starší generace. Právě u příslušníků těchto generací lze pozorovat jistou neobratnost ve vztahu k moderním médiím. Jsou snadno ovlivnitelní pomocí manipulativních a emočně zabarvených zpráv. Navíc vyrůstali v době, kdy platilo, že co vyšlo v novinách, byla pravda. Proto je dnes obtížné je naučit, že ne vše, co je napsáno je pravda.

Kritické myšlení

Pojem kritické myšlení je často využíván. Avšak ne každý dokáže toto myšlení vhodně využívat. Nejčastěji se jako kritické myšlení označuje schopnost nepodléhat prvním dojmům, nepřebírat obecné mínění či názory, a hlavně schopnost utvořit si vlastní názor na základě vlastních zkušeností a odborných poznatků. Pokud se obyvatelé naučí a osvojí si první jmenovanou schopnost, tedy nepodléhat prvním dojmům, pak se vliv dezinformací sníží. Většina dezinformačních a konspiračních webů totiž právě spoléhá na rychlé utvoření názoru na základě prvního dojmu. Často proto do článků implementují přemíru emocí, které poté přenáší na čtenáře. A pokud čtenář, pod tíhou emotivního článku, zaujme stejné stanovisko, a to poté dále šíří, činí přesně podle zájmu dezinformační skupiny.

Avšak schopnost kritického myšlení je do jisté míry ne zrovna snadno osvojitelná. Člověk je již od přírody naučen rozhodovat se na základě emocí a prvního dojmu. Je proto potřeba se části těchto schopností vzdát za účelem osvojení si těchto základních principů, které jsou nezbytné k utváření vlastních racionálních názorů.

Osvětová kampaň v médiích

Jak již bylo mnohokrát popsáno, dezinformace se nejčastěji šíří v mediálním a online prostoru. Jedním z řešení by mohla být osvětová kampaň, pomocí které by autoři apelovali na obyvatele jako na základní skladební kámen obrany proti dezinformacím a v pomyslném duchu přenesli zodpovědnost právě na občany. Tím by se mohlo docílit toho, že by občané začali více přemýšlet nad přebíraným obsahem.

Součástí této osvětové kampaně mohou být reklamy v televizním vysílání upozorňující na nebezpečí dezinformací, sdělení základních principů, jak dezinformace odhalit či jak se vůči nim bránit. Avšak tuto kampaň je, mimo televizní vysílání, nezbytné provést

i v online prostoru. Zde by formou „pop up“ reklam mohly být zobrazovány informace týkajících se dezinformací.

Je však nutné myslet na fakt, že pokud bude tato kampaň prováděna pod záštitou vládních úřadů, strhne se na dezinformačních webech masivní anti kampaň s cílem pošpinit a poškodit zájmy této osvětové kampaně. Také je nezbytné vše pečlivě připravit, aby nedošlo k nedorozuměním v interpretaci či reklamě na kampaň.

Vymáhání práva

Prostředí internetu je svobodné a do jisté míry anonymní místo. Mnoho útočníků a šiřitelů dezinformací se sem uchyluje ve snaze zamaskovat svou identitu, či se cíleně vydávat za někoho jiného a pod tímto pseudonymem pokračovat ve své nekalé činnosti. Je však nezbytné vytyčit jasné hranice, co lze tolerovat a co je již za hranou. Také stát musí posílit svoji pozici v kyberprostoru a aktivně s co největší pozorností zasahovat proti těmto jedincům či organizovaným skupinám. Šiřitelé pomluv a nenávistných či manipulativních zpráv musí převzít osobní zodpovědnost za tyto zprávy, a ne se stále schovávat za roušku anonymity poskytnuté online prostředím. Stejný díl viny ale musí nést i celý řetězec dalších stránek a institucí, které se na tyto zavádějící články odkazují. (Eberle, 2022)

Také je potřeba zasáhnout proti všem, kteří nadužívají pojem *dezinformace* a tím přispívají k zevšednění onoho pojmu. Řada lidí jako dezinformace označuje v podstatě vše, co nesouhlasí s jejich názory. Avšak tento pojem ve velké míře používají i různé instituce či novináři, kteří tak informace označují i navzdory chybějící argumentaci. (Eberle, 2022)

Fact-checking

Dalším způsobem prevence může být Fack-checking, neboli ověřování faktů. V současnosti existuje množství internetových stránek, které se zabývají ověřováním pravdivosti informací, které jsou zveřejňovány v online prostoru či na ověřování výroků politiků. Avšak tyto stránky spolu ve větší míře nespolupracují a každý projekt jde vlastní cestou. Problém těchto projektů je menší propagace. Tedy pokud se člověk v dané oblasti nepohybuje či nehledá cíleně, existuje relativně malá šance, že je člověk odhalí.

Pokud by se tedy tyto projekty rozhodly ke spolupráci, usnadnilo by to zajištění lepšího financování a reklamy. Tyto projekty by se lépe dostaly do lidského podvědomí a postupně by se s nimi lidé naučili pracovat. Je logické, že některé projekty nemají zájem spolupracovat s ostatními a chtějí vše řešit vlastní cestou. Řešením tohoto individualismu by mohlo být vytvoření jakési webové brány, která by sloužila jako rozdělovač

či přeřazovač. Pokud by občan hledal informace o řetězových e-mailech, otevřel by tuto příslušnou stránku, díky níž by byl jedním či dvěma kliknutími přesměrován na stránky příslušného projektu. Tím by byl zaručen individualismus jednotlivých projektů spolu s prezentací jejich sponzorů a partnerů.

Ne všechna řešení a opatření musí být systémového charakteru, či organizována vládou nebo příslušnými úřady. Na poli odolnosti proti dezinformacím zveřejňovaných v prostředí internetu, je nejlepší ochrana vzdělaný uživatel. Některé varovné signály mohou být již na pohled zřejmé, jiné mohou být odhaleny při podrobnějším zkoumání.

Některé webové stránky, které vydávají závadný obsah, mohou na první pohled vypadat relevantně a nezkušený uživatel internetu by je mohl přijmout za relevantní zdroj informací. Základní body k ověření relevantního zdroje mohou být tyto. (Ohio University, 2022)

Vydavatel: Na webové stránce by měly být k dispozici informace o vydavateli konkrétní stránky, kontakty a také kvalifikace autora či vlastníka.

Účel: Mělo by být jasné, za jakým účelem jsou konkrétní stránky provozovány. Ať už při prohlížení zveřejňovaného obsahu, či v popisu konkrétní stránky. U zahraničních stránek lze sledovat i doménu konkrétního webu. Například *„.gov“* značí vládní stránky nebo *„.edu“* označují stránky vzdělávacích institucí.

Zdroje/odkazy: Příspěvky na webové stránce by měly obsahovat i odkazy na zdroje. Pokud stránka na zdroje neodkazuje, či odkazuje na stránky pochybné kvality, pravděpodobně se bude jednat o stránku se závadným obsahem.

Aktuálnost: Vydané příspěvky by měly obsahovat informaci o vydání, či publikování daného článku. Také by měly informovat o případných aktualizacích a doplněních.

Přesnost: Zveřejňované informace by měly být snadno ověřitelné u jiných internetových či tištěných zdrojů. (Ohio University, 2022)

8.1 Čelení hybridním hrozbám

Výše popsaný text je zaměřen primárně na zlepšení stavu v případě působení dezinformací. Je však nutné se zaměřit také na obranu vůči působení hybridních hrozeb, neboť šíření dezinformací je právě jednou formou hybridních hrozeb.

Inspirací nám mohou být již zavedené modely čelení hybridním hrozbám. Například *Nizozemský*. Jistě můžeme namítat, že obě zmíněné země mají jiné přístupy, myšlení či možnosti. Avšak cílem stále zůstává ochránit obyvatelstvo a zemi před působením zvenčí.

Nizozemský model

Česká republika si je s Nizozemskem podobná. Sdílí některé podobné parametry, jako například velikost, otevřená a na zahraniční napojená ekonomika, či fakt, že nesousedíme s žádným z nepřátelských států.

Na druhé straně, v některých ohledech již ČR postoupila v designu systému čelení hybridnímu působení dále než Nizozemsko. Přesto i zde lze nalézt užitečný zdroj inspirace pro rozvoj českého systému, především v oblasti spolupráce s nestátními experty a institucemi expertního vědění. (Bahenský, 2021)

V nizozemském prostředí tato spolupráce sahá až do sedmdesátých let dvacátého století, kdy vznikla *Nizozemská vědecká rada pro vládní politiky*[7]. Tato rada původně připravovala podklady pro vládní úředníky a parlament, avšak v posledních desetiletích se více zaměřuje i na komunikaci s veřejností. Její význam vychází z faktu, že svou působností překlenují jednotlivá vládní období a stanovuje a udržuje dlouhodobé trendy vývoje na poli bezpečnosti. Avšak tato rada představuje pouze jednu skupinu z rozsáhlého systému vládního poradenství. V nizozemských podmínkách tyto expertní a poradní skupiny koordinuje Ministerský bezpečnostní výbor, tedy obdoba naší Bezpečnostní rady státu (BRS). Avšak četnost a pravidelnost setkání je na rozdíl od BRS vyšší. (Bahenský, 2021)

V bezpečnostní oblasti je tím nejstěžejnějším *Národní síť analytiků v oblasti bezpečnosti*[8], která vznikla v roce 2011 a sdružuje šest dalších institucí. Hlavním cílem této instituce je příprava Profilu národních rizik. Tento Profil představuje souhrn možných rizik a hrozeb, které mohou ohrozit národní zájmy. Avšak přínos Profilu národních rizik je vyšší. Přispívá k překlenování rozdílů hranic mezi vnitřní a vnější bezpečností, primárně kvůli důrazu na mezinárodní rozměry, a tedy čelení hybridním hrozbám.

Dalším prvkem v oblasti čelení hybridním hrozbám jsou rozsáhlá a poměrně častá cvičení. Tato cvičení slouží k posilování robustnosti celého bezpečnostního systému a v praxi připravují na schopnost řešit otázky typu *„Co se stane, když…?“*. (Bahenský, 2021)

[7] Wetenschappelijke Raad voor het Regeringsbeleid
[8] Analistennetwerk Nationale Veiligheid

DÍLČÍ ZÁVĚR

V osmé kapitole byly popsány metody a opatření na zlepšení stávajícího stavu v oblasti vnímání dezinformací a ochrany před nimi. Byla navržena jednotlivá opatření. Dále byl popsán nizozemský model čelení hybridním hrozbám jako možná inspirace pro Českou republiku.

9 INTERNETOVÉ STRÁNKY ZAMĚŘENÉ NA OVĚŘOVÁNÍ INFORMACÍ

Určitým pomocníkem při boji proti dezinformacím se mohou stát i různé webové stránky. Autoři a provozovatelé těchto stránek si vzali za svůj cíl bojovat proti šíření nepravdivých a dezinformačních zpráv na internetu. Vkládají úsilí do sběru, archivaci i vyhledávání spojitostí s šířenými informacemi a vyvracejí je či uvádějí na pravou míru. Uživatel internetu tedy má o něco jednodušší ověřování informací. Postačuje otevřít některou z vybraných stránek a najít zprávu, která ho zaujala. Během chvilky se dozví, jestli je informace pravdivá či nikoliv. V případě nepravdivé informace se zde nachází i vysvětlení, proč tomu tak je a nabízí i vysvětlení spojitostí.

Nabízený výběr z níže uvedených webových stránek je pouze část z dostupných možností.

Občanské hnutí *Čeští elfové*[9] se jako jedno z mála věnuje primárně monitoringu řetězových e-mailů. Pod svou záštitou také udržuje databázi řetězových e-mailů.[10] Avšak mimo to se věnuje i sledování zahraničních dezinformačních kampaní, které u nás probíhají. Pokud nějaké dezinformační aktivity zaznamená, ihned na ně reaguje. Vydává texty, které samo zveřejňuje, či je přebírají jiná média. Aktivně přistupuje i k činnostem na sociálních sítích. Dle jeho slov infiltruje každou dezinformační skupinu a pozoruje dění zevnitř. (Čeští elfové, c2021)

Každý měsíc vydává pravidelný přehled dezinformační scény. V tomto katalogu zveřejňuje souhrnné informace, např. počty zachycených řetězových e-mailů, nejčastěji hájené i napadané subjekty apod. Také uvádí nejčastěji citované dezinformační weby, spolu s počty zveřejněných článků. Závěrem každé zprávy uvádí nejčastěji opakované a sdílené narativy. (Čeští elfové, c2021)

Projekt *Manipulároři.cz z.s.*[11] je zaměřen především na vyvracení šířících se HOAXů a dezinformací. Každý zachycený HOAX za pomoci dostupných dat a zveřejněných informací vyvrací logickými argumenty. (Manipulátoři.cz)

Projekt Manipulátoři.cz z.s. se potýká s určitými kontroverzemi. Často je mu vytýkána neschopnost pracovat s informacemi. Také místo logického vyvracení informací pouze určuje, co je správné a co ne. A dokonce se někdy sám dopouští šíření dezinformací, kvůli

[9] https://www.cesti-elfove.cz/
[10] https://www.eldariel.cesti-elfove.cz/
[11] https://www.manipulatori.cz/

nedostatečnému ověření informací. Proto je vhodné v tomto případě brát zveřejněné informace a argumenty pouze orientačně a dál si informaci ověřit. (Kremlík, 2019)

Nelze opomenout, že projekt spolupracuje a podílí se na vytvoření metodického plánu mediální výchovy určeného pro učitele základních a středních škol. (Burešová, 2020)

Server *HOAX.cz*[12] je jeden z nejstarších českých webů takového zaměření. Je k dispozici již od roku 2000 a má širší záběr než jenom vyvracení HOAXů. Internetová stránka je rozdělena do několika sekcí. Kdy jsou sekce věnovány zvlášť:

- HOAXům,
- podvodným loteriím,
- tzv. Scam419[13],
- malwarům,
- řetězovým e-mailům. (HOAX, c2000-2022a)

Schéma každé kategorie je obdobné bez ohledu na zaměření. Je zde, mimo jiné, stručné vysvětlení daného pojmu a aktuality z dané oblasti. Konkrétně v kategorii HOAXů zde nalezneme také pravidla tzv. netikety, tedy pravidla chování v síti. Popis, čím a jak HOAXy škodí, diskuze k tématu a aktuality zde také nechybí. (HOAX, c2000-2022a)

Jedno z negativ zmiňované stránky může být poněkud starší webdesign a nepříliš aktuální zveřejňované informace. Avšak nespornou výhodou daných stránek je vedená databáze. Zveřejněné informace jsou přehledně rozděleny podle kategorií a u každé archivované zprávy se nachází vyjádření redaktora a také vyjádření odborníka na dané téma. (HOAX, c2000-2022a)

Projekt *Demagog.cz z.s.*[14] se zaměřuje na odlišnou činnost než ostatní nabízené stránky. Předmětem činnosti je především ověřování pravdivosti tvrzení českých politiků. Každý den jsme svědky mnoha politických vyjádření a prohlášení. Řada politických představitelů, v zájmu zvýšení své popularity a volitelnosti, přichází s prohlášeními, která se ne vždy zakládají na pravdě. Právě proto má projekt *Demagog.cz* své nezastupitelné místo na „českém“ internetu. (Demagog.cz, c2012—2022)

[12] https://www.hoax.cz/hoax/
[13] Podvody typu dopis Nigerijského prince (HOAX, c2000-2022b)
[14] https://www.demagog.cz/

Každé vyjádření představitele politické strany, ať už na Twitteru, Facebooku, ale i při rozhovorech v TV či rádiích, je ověřováno. Ke každému takovému prohlášení nabízí Demagog.cz vyjádření, zda se jedná o pravdu či nikoliv. V každém případě přidá i odůvodnění, jak k takovému vyjádření došlo. Informace vyhledává a porovnává s informacemi z mediálního prostoru, v programových prohlášeních jednotlivých politických stran či s předvolebními postoji. (Demagog.cz, c2012—2022)

Za zmínku také stojí, že projekt Demagog.cz ctí kodex zásad Mezinárodní fact-checkingové organizace (IFCN) a ověřuje pravdivost části obsahu pro společnost Facebook. Projekt je také držitelem několika prestižních ocenění, za zmínku stojí Křišťálová lupa. (Demagog.cz, c2012—2022)

Stránky projektu také obsahují přehledy jednotlivých českých politiků, kdy je u každého jednoho politika uvedeno celkové množství zkoumaných výroků a každý výrok je zařazen do jedné z kategorií: Pravda, Nepravda, Zavádějící nebo Neověřitelné. Dalším zajímavým přehledem může být soupis vládních slibů jednotlivých vlád a zhodnocení, zda byly sliby splněny, částečně splněny či porušeny. Tyto přehledy vládních slibů jsou vedeny od vzniku projektu, tedy od roku 2012. (Demagog.cz, c2012—2022)

Projekt *Atlas konspirací*[15] je veden na pracovišti Studia nových médií při Ústavu informačních studií a knihovnictví Filozofické fakulty Univerzity Karlovy v Praze. Velmi přehledně a moderně zpracované stránky projektu nabízejí, na rozdíl od ostatních stránek a projektů, pouze přehled konspirací. Nesnaží se tedy o jejich vyvracení a slouží jenom jako katalog či již zmíněný atlas. Mimo to zde můžeme nalézt vyčerpávající a snadno pochopitelné definice konspirací, tzv. populistického rámování a dezinformací. Na poli konspirací zde můžeme nalézt dělení do několika hlavních kategorií, které se dále podrobněji dělí a rozvětvují. Ke každé konspiraci je uveden popis a hlavní zdroje na české scéně. (Atlas konspirací, c2022)

Figuruje zde také seznam hlavních konspiračních a dezinformačních médií. Ke každému zveřejněnému webu autoři projektu dokládají „vlastnickou strukturu“, tedy komu patří doména, na které je web provozován, nejčastěji šířené narativy či nejčastěji přebírané a zveřejňované zdroje. V neposlední řadě je ke každému webu uvedena návštěvnost a stránky, z nichž nejčastěji návštěvníci přichází. Dále zde můžeme nalézt i rozdělení konspirací podle země, proti které jsou zaměřeny. (Atlas konspirací, c2022)

[15] https://atlaskonspiraci.cz/Hlavn%C3%AD_strana

Projekt *NELEŽ*[16] vznikl v roce 2020 za podpory společnosti T-Mobile s cílem omezit šíření dezinformací v online prostoru. Za podpory mnoha velkých firem každý den kontroluje množství internetových stránek a příspěvků s cílem odhalit možné dezinformace. Vypracovává a spravuje seznam dezinformačních webů. Na svých internetových stránkách přehledně vysvětluje, co jsou to dezinformace, jak je odhalit či popisuje způsoby, jakými mohou škodit společnosti. (Nelež, c2020)

Zaměřuje se hlavně na ochranu společností, které chtějí šířit svou reklamu v online prostoru. Snadno se totiž může stát, že nevhodně umístěnou reklamou může být poškozena pověst samotné značky. Tohoto hodnocení mohou využít i uživatelé, kteří nemají zájem šířit svou reklamu. Pokud totiž není internetová stránka vhodná k umístění reklamy z důvodu možnosti poškození pověsti, dá se důvodně předpokládat, že obsah této internetové stránky bude jistým způsobem závadný. (Nelež, c2020)

Nemusíme se omezovat pouze na prostředí „českého“ internetu, ale jako inspiraci si můžeme vzít i stránky **slovenského sdružení *o.z. Konšpirátori.sk***[17]**,** provozujícího stejnojmenný projekt. Členové tohoto sdružení se zabývají monitoringem stránek se závadným obsahem, jejich vyhodnocením a zveřejněním. Velkou výhodou tohoto projektu je, že se neomezuje pouze na domácí prostředí „slovenského“ internetu, ale zabývá se i monitornigem českého internetového prostředí. (Konšpirátori.sk, c2022b)

Pro vyhodnocení míry „závadnosti“ určité stránky používají autoři projektu stupnici pěti bodů. Pokud stránka splňuje alespoň jeden bod, je zařazena mezi závadné. Avšak projekt není zaměřen pouze na monitoring stránek šířící dezinformace, ale je zaměřen na hledání závadného obsahu na internetu obecně. K tomu slouží následující hodnotící stupnice.

1. Stránka obsahuje informace šarlatánského charakteru, který odporuje objektivním vědeckým poznatkům. Uvedené informace mohou svým charakterem způsobit zanedbání potřebné léčby či ublížit na zdraví.
2. Stránka obsahuje nepravdivé, podvodné či dezinformační informace, které odporují faktům. Například fotografie použité v zavádějícím kontextu.
3. Stránka obsahuje konspirační teorie, které pokud nebudou kriticky vyhodnoceny, mohou mít vážný politický, sociální či zdravotní dopad.

[16] https://www.nelez.cz/
[17] https://www.konspiratori.sk/

4. Stránka obsahuje extremistický obsah, vulgarismy, šíření poplašných zpráv či hanobení menšin, ras, národností apod.
5. Stránka nerespektuje zásady novinářské etiky. Nezveřejňuje opravné zprávy či vyjádření u zpráv, které se ukázaly jako nepravdivé. Ale také pokud stránka nemá jasnou vlastnickou strukturu nebo publikuje šokující informace za účelem zvýšení návštěvnosti a tyto zprávy poté upraví. (Konšpirátori.sk, c2022b)

Projekt je primárně zaměřen na vyhodnocení závadnosti a ochranu zadavatelů internetové reklamy. Avšak podle tohoto vyhodnocení se můžeme také řídit. Pokud totiž není webová stránka, vzhledem ke svému obsahu, vhodná pro inzerenty, pravděpodobně se zde nebude nacházet vhodný a relevantní obsah pro běžné uživatele internetu.

Projekt podporuje přes 60 subjektů, mezi kterými nechybí společnosti jako například mobilní operátor O_2 a společnost Seznam. Ale také ambasády Holandského království, Spojeného království Velké Británie a Severního Irska či Spojených států amerických. (Konšpirátori.sk, c2022b)

Prostředí internetu se velmi dynamicky vyvíjí a rozvíjí. Anonymita umožňuje různým subjektům šířit a publikovat závadný obsah a přitom se vydávat za solidního publikovatele. Pokud se chceme aktivně těmto nepravdám bránit a nepřijímat tyto nepravdivé narativy za své, můžeme k tomu využít některou z prezentovaných webových stránek. Každá přispívá k odhalení dezinformací či HOAXů. Některé pouze nabízí zpracovaný přehled dezinformací, které se šíří a některé pomocí faktů přímo vyvrací tyto nepravdy. Je tak pouze na nás, uživatelích internetu a sociálních sítí, jak se k této hrozbě postavíme.

DÍLČÍ ZÁVĚR

Devátá kapitola pojednávala o jednotlivých webech, jako o možnosti čelení dezinformacím. Tyto popsané weby slouží jako pomůcka ke snadnému ověření dostupných informací a vyhodnocení stránek, které sdílí tyto informace.

ZÁVĚR

Diplomová práce pojednávala o problematice hybridních hrozeb a dezinformací. Teoretická část byla zaměřena na objasnění pojmů hybridní hrozby, hybridní válka, dezinformace a bezpečnostní prostřední. V praktické části diplomové práce bylo provedeno dotazníkové šetření za účelem zjištění vnímání problematiky veřejností. Dotazníkové šetření bylo vyhodnoceno, okomentováno a byla navržena opatření ke zlepšení stávajícího stavu. Provedeným dotazníkovým šetřením bylo zjištěno, že se obyvatelstvo v oblasti dezinformací orientuje a tyto dezinformace je schopné odhalit. Prostřednictvím diagramu byl popsán způsob šíření dezinformací k veřejnosti. Za pomoci kontrolního seznamu (Checklist) byl navržen postup ověřování informací. Následně bylo popsáno působení dezinformací na sociální a bezpečnostní prostředí České republiky. Závěrem diplomové práce byly představeny internetové stránky zabývající se bojem proti šíření dezinformací v internetovém prostoru. Jako pomocné body při sepisování diplomové práce byly určeny dílčí cíle a výzkumné otázky, které jsou následně popsány.

Výzkumná otázka první: *Lze zabránit šíření dezinformací?* Šíření dezinformací jako takových zastavit nelze. Může se pouze do určité míry omezit.

Výzkumná otázka druhá: *Lze spolu se zapojením médií omezit šíření dezinformací?* Omezit šíření dezinformací ze strany médií lze docílit pouze tehdy, pokud redakce budou zveřejňovat relevantní a ověřitelné články. Pokud budou v honbě za vyšší sledovaností sdílet titulky neodpovídající obsahu článku, vydávat nepravdivé články apod., nemůže se podíl dezinformací v mediálním prostoru snížit.

Výzkumná otázka třetí: *Jakými způsoby si může veřejnost ověřit informace?* Způsobů a možností k ověření pravdivosti a relevance informací je hned několik. Lze využít některé ze jmenovaných internetových stránek, které se zabývají ověřováním informací či ověřováním pravdivosti politických diskuzí. Dále je možné využít i běžného internetového vyhledávače, který umožní najít podobné zprávy. V neposlední řadě lze využít funkce vyhledávání obrázků. Pokud jsou tedy v článku použity obrázky, pomocí uvedené funkce lze zjistit, kdy a kdo tento obrázek zveřejnil nebo použil. Nutno dodat, že současnost poskytuje mnoho možností k ověření informací, avšak mnoho uživatelů internetu tyto možnosti ověření nevyužívá, neboť představují pomyslný krok navíc při získávání informací, a tedy způsobují jistý diskomfort.

SEZNAM POUŽITÉ LITERATURY

Atlas konspirací [online], c2022. Praha: Univerzita Karlova v Praze [cit. 2022-07-18]. Dostupné z: https://atlaskonspiraci.cz/

BAHENSKÝ, Vojtěch a Ondřej DITRYCH, 2021. Nizozemský model čelení hybridnímu působení: inspirace pro Českou republiku. Ústav mezinárodních vztahů Praha [online]. Praha: Ústav mezinárodních vztahů Praha [cit. 2022-07-21]. Dostupné z: https://www.iir.cz/nizozemsky-model-celeni-hybridnimu-pusobeni-inspirace-pro-ceskou-republiku

BARTOŠÍK, Jan, 2022. Hybridní hrozby jsou s námi od nepaměti. Znali je už ve starověku. Deník.cz [online]. Praha: VLTAVA LABE MEDIA [cit. 2022-07-18]. Dostupné z: https://www.denik.cz/veda/hybridni-hrozby-strach-valka-cina-rusko-amerika.html

BEZPEČNOSTNÍ INFORMAČNÍ SLUŽBA. Výroční zpráva Bezpečnostní informační služby za rok 2019. Praha: Bezpečnostní informační služba. 2020. Dostupné také z: https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2019-vz-cz.pdf

BEZPEČNOSTNÍ INFORMAČNÍ SLUŽBA. Výroční zpráva Bezpečnostní informační služby za rok 2020. Praha: Bezpečnostní informační služba. 2021. Dostupné také z: https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2020-vz-cz-2.pdf

BITTMAN, Ladislav, 2000. Mezinárodní dezinformace: černá propaganda, aktivní opatření a tajné akce. Praha: Mladá fronta. Archiv (Mladá fronta). ISBN 80-204-0843-6.

BUREŠOVÁ, Lenka, 2020. Weby HOAX.CZ, MANIPULATORI.CZ a DEMAGOG.CZ aneb uvádění podezřelých tvrzení na pravou míru. Děti a media [online]. Praha: Rada pro rozhlasové a televizní vysílání [cit. 2022-07-18]. Dostupné z: https://www.deti-a-media.cz/art/3258/weby-hoax-cz-manipulatori-cz-a-demagog-cz-aneb-uvadeni-podezrelych-tvrzeni-na-pravou-miru.htm

Čeští elfové [online], c2021. Česká republika: Čeští elfové [cit. 2022-07-18]. Dostupné z: https://cesti-elfove.cz/

ČEŠTÍ ELFOVÉ, c2021. Řetězové e-maily. Čeští elfové [online]. Česká republika: Čeští elfové [cit. 2022-07-15]. Dostupné z: https://cesti-elfove.cz/retezove-maily/

Demagog.cz [online], c2012—2022. Praha: Demagog.cz [cit. 2022-07-18]. Dostupné z: https://demagog.cz/

EBERLE, Jakub, 2022. Desatero pro lepší porozumění a čelení dezinformacím. Ústav mezinárodních vztahů Praha [online]. Praha: Ústav mezinárodních vztahů Praha [cit. 2022-07-21]. Dostupné z: https://www.iir.cz/desatero-pro-lepsi-porozumeni-a-celeni-dezinformacim

FIALA, Jan, 2018. Operace "bodyguard"? Němci do poslední chvíle věřili podvodu. EuroZprávy.cz [online]. INCORP [cit. 2022-02-23]. Dostupné z: https://eurozpravy.cz/magazin/230896-operace-bodyguard-nemci-do-posledni-chvile-verili-podvodu/

FRANK, Libor a Richard STOJAR, 2010. Charakteristiky a trendy vývoje bezpečnostního prostředí: Implikace pro ozbrojené síly. Brno. Dostupné také z: https://is.muni.cz/el/1423/jaro2016/BSS151/um/Charakteristiky_a_trendy_vyvoje_bezpecnostniho_prostredi.pdf. Dílčí podkladová pracovní studie projektů obranného výzkumu. Univerzita obrany.

FRANK, Libor, 2003. Bezpečnostní prostředí České republiky. Obrana a strategie (Defence and Strategy) [online]. Brno: Univerzita obrany, 2003(1), 7-14 [cit. 2022-07-18]. ISSN 1802-7199. Dostupné z: doi:10.3849/1802-7199

GREGOR, Miloš a Petra VEJVODOVÁ, 2018. Nejlepší kniha o fake news, dezinformacích a manipulacích!!!. 1. Brno: CPress. ISBN 978-802-6418-054.

GUESS, Andrew M. a Benjamin A. LYONS, 2020. Misinformation, Disinformation, and Online Propaganda. In: PERSILY, Nathaniel a Joshua A. TUCKER, ed. Social Media and Democracy: The State of the Field, Prospects for Reform. Cambridge: Cambridge University Press, s. 10-33. ISBN 9781108890960. Dostupné z: doi:10.1017/9781108890960

HENLEY, Jon, 2021. Influencers say Russia-linked PR agency asked them to disparage Pfizer vaccine. The Guardian [online]. Londýn: Guardian News & Media Limited [cit. 2022-07-15]. Dostupné z: https://www.theguardian.com/media/2021/may/25/influencers-say-russia-linked-pr-agency-asked-them-to-disparage-pfizer-vaccine

HOAX [online], c2000-2022a. Česká republika: HOAX.cz [cit. 2022-07-21]. Dostupné z: https://www.hoax.cz/cze/

HOAX, c2000-2022b. CO JE TO SCAM419. HOAX [online]. Česká republika: HOAX.cz [cit. 2022-07-21]. Dostupné z: https://www.hoax.cz/scam419/co-je-to-scam-419

HRÁBEK, Lukáš, 2017. Falešné profily a nenávistné komentáře. Uhlobaron Tykač manipuluje propagandou. Deník Referendum [online]. Vydavatelství Referendum [cit. 2022-03-09]. Dostupné z: https://denikreferendum.cz/clanek/25143-falesne-profily-a-nenavistne-komentare-uhlobaron-tykac-manipuluje-propagandou

Hybrid Threats: NATO, 2015. Background Report [online]. Praha: Asociace pro mezinárodní otázky (AMO), (3) [cit. 2022-5-24]. Dostupné z: https://www.studentsummit.cz/wp-content/uploads/2019/02/PSS-Hybrid-Threats-NATO.pdf

JASPER, Scott a Scott MORELAND, 2014. The Islamic State is a Hybrid Threat: Why Does That Matter?. Small Wars Journal [online]. Washington: Small Wars Foundation [cit. 2022-07-15]. Dostupné z: https://smallwarsjournal.com/jrnl/art/the-islamic-state-is-a-hybrid-threat-why-does-that-matter

KARTUSOVÁ, Alžběta, 2021. Hybridní hrozby – fenomén v oblasti válek 21. století. In: VOSTRÁ, Zuzana. Nestandardní bezpečnostní situace ve státě – ústavní, evropský a mezinárodní pohled. Plzeň: Západočeská univerzita v Plzni, s. 89-102. ISBN 978-80-261-0922-8. Dostupné také z: https://dspace5.zcu.cz/bitstream/11025/45495/1/e-verze-95-108.pdf

KOHOUTEK, Rudolf, c2005-2022. Pojem sociální prostředí. Slovník cizích slov [online]. Ostrava: ABZ knihy [cit. 2022-07-21]. Dostupné z: https://slovnik-cizich-slov.abz.cz/web.php/slovo/socialni-prostredi

Konšpirátori.sk [online], c2022b. Bratislava: o.z. Konšpirátori.sk [cit. 2022-07-18]. Dostupné z: https://konspiratori.sk/

KONŠPIRÁTORI.SK, c2022a. Zoznam stránok so sporným obsahom [online]. o.z. Konšpirátori.sk [cit. 2022-05-25]. Dostupné z: https://konspiratori.sk/zoznam-stranok

KRÁSNÝ, Antonín a Oldřich SOCHA, 2006. Možné vlivy bezpečnostního prostředí na Českou republiku a její ozbrojené síly. Obrana a strategie (Defence and Strategy)

[online]. Brno: Univerzita obrany, 2006(1), 7-18 [cit. 2022-07-18]. ISSN 1802-7199. Dostupné z: doi:10.3849/1802-7199

KREMLÍK, Vítězslav, 2019. KLIMA: Jak manipuluje dezinformační web Manipulatori.cz. Neviditelný pes [online]. Praha: Neviditelný pes [cit. 2022-07-18]. Dostupné z: https://neviditelnypes.lidovky.cz/klima/klima-jak-manipuluje-dezinformacni-web-manipulatori-cz.A190326_214739_p_klima_wag

KŘÍŽ, Zdeněk, Zinaida SHEVCHUK a Peter ŠTEVKOV, 2015. Hybridní válka jako nový fenomén v bezpečnostním prostředí Evropy. Praha: Pro Informační centrum o NATO vydalo Jagello 2000. ISBN 978-80-904850-2-0.

MALÝ, Martin, 2021. Dezinformace a my. Bez pochopení toho, jak se šíří a jak účinkují, je každý odpor předem prohraná fraška. Info.cz [online]. Praha: CMI News [cit. 2022-07-22]. Dostupné z: https://www.info.cz/nazory/virus-dezinformace

Manipulátoři.cz [online]. Praha: Manipulátoři.cz [cit. 2022-07-18]. Dostupné z: https://manipulatori.cz/

MAREŠ, Miroslav. Hybridní hrozby v České republice a jak jim čelit. Natoaktual.cz: Portál informačního centra o NATO v Praze [online]. 2016 [cit. 2022-05-20]. Dostupné z: https://www.natoaktual.cz/analyzy-a-komentare/hybridni-hrozby-v-ceske-republice-a-jak-jim-celit.A161020_164518_na_nazory_m02

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY, c2022a. Definice dezinformací a propagandy. Ministerstvo vnitra České republiky [online]. Praha: Ministerstvo vnitra České republiky [cit. 2022-07-14]. Dostupné z: https://www.mvcr.cz/chh/clanek/definice-dezinformaci-a-propagandy.aspx

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY, c2022b. Co jsou hybridní hrozby. Ministerstvo vnitra České republiky [online]. Praha: Ministerstvo vnitra České republiky [cit. 2022-05-23]. Dostupné z: https://www.mvcr.cz/cthh/clanek/co-jsou-hybridni-hrozby.aspx

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY, c2022c. Trestněprávní úprava. Ministerstvo vnitra České republiky [online]. Praha: Ministerstvo vnitra České republiky [cit. 2022-07-19]. Dostupné z: https://www.mvcr.cz/chh/clanek/dezinformacni-kampane-trestnepravni-uprava-trestnepravni-uprava.aspx

MINISTERSTVO ZAHRANIČNÍCH VĚCÍ ČESKÉ REPUBLIKY, 2015. Bezpečnostní strategie České republiky: 2015. 1. Praha: Ministerstvo zahraničních věcí České republiky. ISBN 978-80-7441-005-5. Dostupné také z: https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf

MOONEY, Hailey, 2018. "Fake News" and the Sociological Imagination: Theory Informs Practice. LOEX Quarterly [online]. Eastern Michigan University, 44(4), 4-16 [cit. 2022-07-21]. ISSN 1547-0172. Dostupné z: https://commons.emich.edu/loexquarterly/vol44/iss4/3/

NASU, Hitoshi, 2022. Deepfake Technology in the Age of Information Warfare. Liber Institute West Point [online]. West Point: United States Military Academy [cit. 2022-05-25]. Dostupné z: https://lieber.westpoint.edu/deepfake-technology-age-information-warfare/

Nelež [online], c2020. Česká republika: Nelež [cit. 2022-07-18]. Dostupné z: https://www.nelez.cz/

OHIO UNIVERSITY, 2022. Guide to Misinformation and Fact-Checking. Ohio University: Online Master of Public Administration [online]. Ohio: Ohio University [cit. 2022-07-21]. Dostupné z: https://onlinemasters.ohio.edu/masters-public-administration/guide-to-misinformation-and-fact-checking/

PAMMENT, James, 2020. Resist: Příručka pro boj s dezinformacemi. Praha: Centrum proti terorismu a hybridním hrozbám Ministerstva vnitra. Dostupné také z: https://www.mvcr.cz/cthh/clanek/ke-stazeni-resist-prirucka-pro-boj-s-dezinformacemi.aspx

POMERANTSEV, Peter, 2020. Tohle není propaganda: válka proti realitě. Praha: Dokořán. ISBN 978-807-3639-990.

RÁCZ, András, 2015. Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist. Helsinki: The Finnish Institute of International Affairs. ISBN 978-951-769-453-7. ISSN 2323-5454. Dostupné také z: https://www.fiia.fi/wp-content/uploads/2017/01/fiiareport43.pdf

ŠILHÁNOVÁ, Hana, NEŠPOR, Zdeněk R., ed., 2017. Prostředí sociální. SOCIOLOGICKÝ ÚSTAV AV ČR. Sociologická encyklopedie [online]. Praha: Sociologický ústav AV ČR [cit. 2022-07-21]. Dostupné z:

https://encyklopedie.soc.cas.cz/w/Prost%C5%99ed%C3%AD_soci%C3%A1ln%C3%AD

VAJ, 2015. Továrna na propagandu. Šířením názorů Kremlu se dá slušně vydělat. E15 [online]. CZECH NEWS CENTER [cit. 2022-03-09]. Dostupné z: https://www.e15.cz/magazin/tovarna-na-propagandu-sirenim-nazoru-kremlu-se-da-slusne-vydelat-1175587

VÁLKA REVUE, 2016. Atlantický val: Jak vypadalo opevnění na jednotlivých plážích?. 100+1 zahraniční zajímavost [online]. Brno: Extra Publishing [cit. 2022-07-27]. Dostupné z: https://www.stoplusjednicka.cz/atlanticky-val-jak-vypadalo-opevneni-na-jednotlivych-plazich

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AIDS	Acquired Immune Deficiency Syndrome (tj. syndrom získaného imunodeficitu).
BIS	Bezpečnostní informační služba.
BRS	Bezpečnostní rada státu.
ČR	Česká republika.
HIV	Human Immunodeficiency Virus (tj. virus způsobující ztrátu obranyschopnosti).
IFCN	International Fact-Checking Network (tj. mezinárodní fact-checkingová síť).
KGB	Výbor státní bezpečnosti (hlavní sovětská tajná služba).
o.z.	Občianske združenie.
Obr.	Obrázek.
PR	Public relations (tj. vztahy s veřejností).
př. n. l.	Před naším letopočtem.
StB	Státní bezpečnost.
Tab.	Tabulka.
TV	Televize.
z.s.	Zapsaný spolek.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK