# Dezinformace jako bezpečnostní hrozba v systému ochrany obyvatelstva

Kamila Šimíčková

Bakalářská práce
2024

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: 2023/2024

# ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

| | |
|---|---|
| Jméno a příjmení: | **Kamila Šimíčková** |
| Osobní číslo: | **L21668** |
| Studijní program: | **B1032A020002 Ochrana obyvatelstva** |
| Forma studia: | **Prezenční** |
| Téma práce: | **Dezinformace jako bezpečnostní hrozba v systému ochrany obyvatelstva** |

## Zásady pro vypracování

1. Na základě dostupných zahraničních a domácích zdrojů zpracujte teoretické poznatky a teoretická východiska k danému tématu.
2. Proveďte dotazníkové šetření u obyvatelstva na dané téma.
3. Na základě vyhodnocení dotazníkového šetření navrhněte případné změny a opatření ke zlepšení.

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

Seznam doporučené literatury:


1. BENNETT, W. Lance a LIVINGSTON, Steven (ed.). *The Disinformation Age.* Online. Cambridge: Cambridge University Press, 2020. ISBN 9781108914628. Dostupné z: https://doi.org/10.1017/9781108914628. [cit. 2023-10-14].
2. GREGOR, Miloš a VEJVODOVÁ, Petra. *Nejlepší kniha o fake news, dezinformacích a manipulacích!!!* Brno: CPress, 2018. ISBN 978-80-264-1805-4.
3. TÁBORSKÝ, Jiří. *V síti (dez)informací: proč věříme alternativním faktům.* Praha: Grada Publishing, 2020. ISBN 978-80--271-2014-7.


Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **Ing. Ivan Princ**
Ústav ochrany obyvatelstva

Datum zadání bakalářské práce: **1. prosince 2023**
Termín odevzdání bakalářské práce: **3. května 2024**

L.S.

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

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

V Uherském Hradišti dne 4. prosince 2023

# PROHLÁŠENÍ AUTORA
# BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že:

- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji bakalářskou 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 – bakalářskou 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 bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské 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 bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne: 3. 5. 2024

Jméno a příjmení studenta: Kamila Šimíčková

.....
podpis studenta

## ABSTRAKT

Na začátku teoretické části práce je definován systém ochrany obyvatelstva, základní pojmy z oblasti informování a informačního prostředí, ukotvení problematiky dezinformací ve strategických dokumentech včetně řešení problematiky dezinformací na národní a mezinárodní úrovni. V praktické části je první část věnována analýze dezinformací v internetovém prostředí. Na tuto část navazuje Ishikawa digram zabývající se možnými příčinami vybrané hrozby pro systém ochrany obyvatelstva a jednotlivá rizika jsou zpracovány maticí rizik. Dále je využita metoda dotazníkového šetření zabývající se zjištěním o povědomí občanů České republiky o oblasti dezinformací a mediální gramotnosti. Na konci praktické části práce jsou uvedeny návrhy ke zlepšení.



Klíčová slova: dezinformace, propaganda, informace, ochrana obyvatelstva



## ABSTRACT

At the beginning of the theoretical part of the thesis is defined the system of population protection, basic concepts from the field of information and information environment, anchoring of the issue of disinformation in strategic documents, including dealing with issue of disinformation at the national and international level. The practical part begins with the analysis of disinformation in the internet environment. This part is followed by Ishikawa diagram addressing possible causes of selected threat to the population protection system and individual risks are elaborated by risk matrix. The next method is questionnaire survey dealing with finding out about awareness of the citizen of the Czech Republic in the field of disinformation and media literacy. At the end of the practical part of the thesis, the suggestions for improvement are presented.



Keywords: disinformation, propaganda, information, population protection

*„An unexciting truth may be eclipsed by a thrilling falsehood“*

Aldous Huxley, 1958

Tímto bych chtěla velmi poděkovat vedoucímu bakalářské práce panu Ing. Ivanovi Princovi za jeho cenné rady a připomínky i trpělivost. Také bych chtěla poděkovat mé rodině a přátelům za podporu během psaní.

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

# OBSAH

# ÚVOD

Dezinformace je ve zkrácené definici informace, která je založena na lži a má za cíl manipulaci s jejím příjemcem. Oblast dezinformací je aktuálně velmi probírané téma. Tato oblast je velmi komplexní, jelikož zasahuje do mnoha sfér. Jednou z důležitých sfér, ve kterých jsou dezinformace současným problémem, je oblast bezpečnosti. Dezinformace ohrožují především demokratické zřízení země, ale mohou také poškodit pověst člověka, firmy a její prodej, veřejné instituce nebo mohou narušit stávající fungující systém. Problémem dezinformací je, že stačí, aby narušily důvěru svého příjemce v rámci svého cíle, i když se potvrdí, že daná dezinformace je falešná. Dalším rizikovým faktorem je jejich šíření. Často trvá až příliš dlouho, než se šíření dezinformace odhalí a mohou tak ovlivnit masy lidí. Pokud je dezinformační kampaň dobře nastavená a manipulativní obsah je šířen několika kanály, například přes dezinformační média a sociální sítě, tak může být jejich dopad obrovský. Největším dopadem dezinformací je manipulace s jejich příjemcem, který začne ztrácet důvěru v systém, především ten státní, a pak je velmi náročné si důvěru občana získat zpět.

Evropská unie i Česká republika si uvědomují, že dezinformace, dezinformační kampaně, propaganda a hybridní hrozby mohou ohrožovat jejich bezpečnost a narušovat důvěru veřejnosti a polarizovat ji. Za účelem ochrany proti těmto hrozbám identifikují rizika, nastavují si strategické cíle a snaží se najít taková opatření, aby bylo možné se těmto bezpečnostním hrozbám bránit.

Hlavním cílem bakalářské práce je na základě vyhodnocení dotazníkového šetření navrhnout případné změny a opatření ke zlepšení současného stavu. Ke splnění hlavního cíle byly stanoveny dílčí cíle: zpracovat teoretická východiska a teoretické poznatky na základě dostupných informací ze zahraničních a domácích zdrojů k danému tématu a provést dotazníkové šetření u obyvatelstva na dané téma.

V teoretické části jsou použity metody indukce a dedukce. V praktické části bakalářské práce je použito několik metod – dotazníkové šetření a Ishikawa diagram, na který navazuje matice rizik.

# I. TEORETICKÁ ČÁST

# 1 SYSTÉM OCHRANY OBYVATELSTVA

Ochrana obyvatelstva je definována v zákoně č. 239/2000 Sb., o integrovaném záchranném systému (dále v textu jen *„IZS“*) a o změně některých zákonů jako*: „plnění úkolů civilní ochrany, zejména varování, evakuace, ukrytí a nouzové přežití obyvatelstva a další opatření k zabezpečení ochrany jeho života, zdraví a majetku“*. Společně se zajišťováním svrchovanosti, územní celistvosti státu a ochranou demokratických základů České republiky je ochrana obyvatelstva základní funkcí a povinností státu. (Ministerstvo vnitra generální ředitelství Hasičského záchranného sboru České republiky, 2021)

Základním cílem ochrany obyvatelstva je ochrana osob prostřednictvím komplexního souboru opatření. Taková opatření vedou k ochraně zdraví a života osob i hospodářských zvířat, k ochraně majetku a životního prostředí. (Ministerstvo vnitra generální ředitelství Hasičského záchranného sboru České republiky, 2021) Součástí vnitřní bezpečnosti České republiky jsou kroky k zajištění ochrany obyvatelstva při mimořádných událostech živelní povahy, provozních haváriích nebo násilných konfliktech i při terorismu. Tato opatření vedou k zajišťování ochrany vnitřního pořádku, vnější bezpečnosti v případě vojenského ohrožení i ochranu ekonomiky státu. (Ministerstvo vnitra, 2021) Tyto činnosti jsou prováděny orgány veřejné správy, právnickými a podnikajícími fyzickými osobami i občany. Oblast varování, evakuace, ukrytí a nouzové přežití je v gesci Hasičského záchranného sboru České republiky (dále v textu jen *„HZS ČR“*), oblast veřejného pořádku je v gesci Policie České republiky (dále v textu jen *„PČR“*), ochranou života a zdraví je pověřeno Ministerstvo zdravotnictví České republiky a jednotlivé kraje a fungování státní správy a samosprávy při mimořádných událostech je v gesci orgánů veřejné správy. (hzscr.cz, ©2024) Ústředním orgánem pro oblast ochrany obyvatelstva je Ministerstvo vnitra České republiky. Úkoly ochrany obyvatelstva stanovené zákonem č. 239/2000 Sb., plní složky IZS, a dále se na nich podílejí orgány krajů a obcí, právnické i podnikající fyzické osoby i obyvatelstvo samotné. (Ministerstvo vnitra, 2021)

K účinnější ochraně obyvatelstva je důležitá informovanost veřejnosti o ochranných opatřeních. (Princ, nedatováno) Informování obyvatelstva při přípravě na mimořádné události je zakotveno v zákoně 239/2000 Sb., o integrovaném záchranném systému, kde z § 25 odst. 1 plyne, že má fyzická osoba pobývající na území České republiky právo: „*získat informace o opatřeních k zabezpečení ochrany obyvatelstva, poskytnutí instruktáže a školení ke své činnosti při mimořádných událostech*“. (Česko, 2000a)

Informování obyvatelstva je dále zakotveno v zákoně č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon) v § 31, ve kterém má fyzická osoba právo: „*na nezbytné informace o připravovaných krizových opatřeních k ochraně jejího života, zdraví a majetku*“. (Česko, 2000b) Formu informování obyvatelstva stanovuje Vyhláška Ministerstva vnitra č. 380/2002 Sb., k přípravě a provádění úkolů ochrany obyvatelstva. Z této vyhlášky vychází, že jsou právnické a fyzické osoby o charakteru možného ohrožení a připravovaných opařeních informovány těmito způsoby: „*hromadnými informačními prostředky, letáky a informačními brožurami, ukázkami činnosti IZS a besedami s obyvatelstvem*“.

Informace tohoto charakteru obsahují zejména možné zdroje rizik vzniku mimořádných událostí, preventivní opatření, jaké jsou činnosti IZS a jejich příprava na tyto aktivity, jaká jsou opatření ochrany obyvatelstva, informace o sebeochraně a poskytování vzájemné pomoci nebo jak by byla organizována humanitární pomoc. (Česko, 2002)

Informování probíhá ve třech fázích:

- Přípravná (preventivní) – seznámení obyvatelstva s charakterem a zdroji nebezpečí a jaké jsou způsoby ochrany, informování a varování.
- Akutní – při reálné hrozbě nebo probíhající mimořádné události. V této fázi probíhá tísňové informování následující po varování. Zde probíhá také komunikace orgánů krizového řízení s ohroženým obyvatelstvem.
- Obnova – probíhá během odstraňování následků a pokračuje až do přechodu do normálního stavu. (Princ, nedatováno)

Podle zprávy Národního kontrolního úřadu (dále jen *„NKÚ“*) má být základním prvkem systému ochrany obyvatelstva vzdělaný a informovaný občan. NKÚ našel několik nedostatků v plnění stanovených podmínek v oblasti ochrany obyvatelstva a po zveřejnění výsledků kontroly se Ministerstvo vnitra zavázalo, že od roku 2024 v oblasti výchovy a vzdělávání vytvoří v rámci základního a středoškolského vzdělávání oblast „*výchova k bezpečnosti*“, a také zprovozní aplikaci pro mobilní telefony pro informování obyvatelstva s funkcí hromadného rozesílání SMS zpráv a spustí webový portál ochrany obyvatelstva. (Nejvyšší kontrolní úřad, 2024)

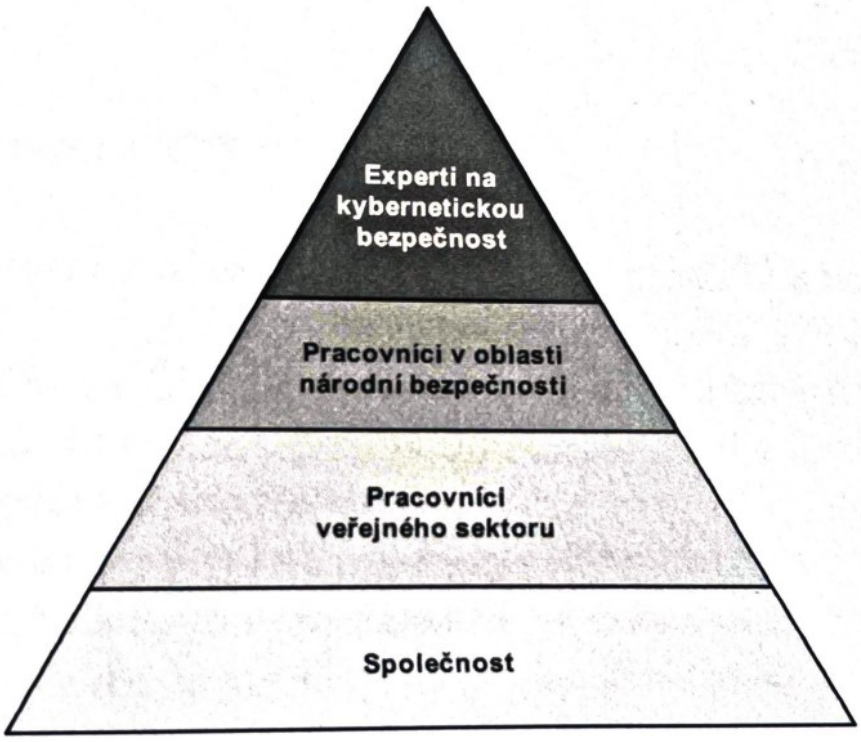
# 2 INFORMACE A INFORMAČNÍ PROSTŘEDÍ

Podle Dombrovské a Šidlichovské (2021) jsou **informace** v podstatě jakékoli sdělení, takže informací mohou být značky, nápisy nebo dokonce vůně. Zpravidla se ale v informačním prostředí rozlišují data, informace a znalosti. Data jsou shluky znaků, kterým nerozumíme, ale jakmile jim porozumíme, jedná se o informaci. Znalost je získána tehdy, kdy s těmito informacemi dokážeme dále pracovat. Podle Nonnemanna et al. (2022) není shoda na tom, co přesně informace je. Podle něj můžeme informaci chápat jako jakýkoli obsah sdělení, který můžeme předat někomu dalšímu, anebo informací může být údaj o prostředí, který snižuje jeho míru neurčitosti nebo to může být údaj využitelný příjemcem. Podle Jiráska et al. (2013) ve *„Výkladovém slovníku kybernetické bezpečnosti" je informace definována jako: „každý znakový projev, který má smysl pro komunikátora i příjemce"*.

**Kybernetický prostor** je dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) *„digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, službami a sítěmi elektronických komunikací"*. (Česko, 2014)

**Kybernetickou bezpečností** se rozumí *„souhrn právních, organizačních, technických a vzdělávacích prostředků, které směřují k zajištění ochrany kybernetického prostoru"* a **kybernetickou obranou** rozumíme obranu proti kybernetickým útokům a následnému zmírňování dopadů těchto útoků. (Sedlák a Konečný, 2021) Hlavními orgány zabývající se oblastí kybernetické bezpečnosti v České republice je Národní centrum kybernetické bezpečnosti (dále v textu jen *„NCKB"*) a Sekce strategických agend a spolupráce, které jsou výkonnými celky Národního úřadu pro kybernetickou a informační bezpečnost (dále v textu jen *„NÚKIB"*). Tyto orgány se zabývají především prevencí před kybernetickými hrozbami, koordinací řešení kybernetických bezpečnostních incidentů, osvětovou a vzdělávací činnost, spolupráci s národními a mezinárodními organizacemi, vývoj a výzkum v oblasti kybernetické bezpečnosti, pořádání a účast na kybernetických cvičeních, hodnocení a analýza rizik v kybernetické bezpečnosti. V rozsahu své působnosti také plní mezinárodní závazky a spolupráci na realizaci právních předpisů stanovené členstvím České republiky v mezinárodních organizacích, Severoatlantické alianci (dále v textu jen *„NATO"*) a Evropské unii (dále v textu jen *„EU"*). (nukib.gov.cz, nedatováno)

Na obrázku 1 je zobrazeno schéma odolného systému zajištění kybernetické bezpečnosti. Základem pro zajišťování tohoto druhu bezpečnosti je společnost, které se nazývá jako *„odolná společnost 4.0“*, která naplno využívá výhody, které poskytuje moderní společnost s minimalizací kybernetických rizik. (Sedlák a Konečný, 2021)




*Obrázek 1 Systém zajištění kybernetické bezpečnosti. (Sedlák a Konečný, 2021)*

**Informační**, nebo také **kybernetická**, **společnost** je taková společnost, která dokáže využívat informační a komunikační technologie a v jejím prostředí dochází k neustálé výměně informací a práce s nimi, kdy se předpokládá, že tato společnost je schopná jim rozumět. Informační společnost považuje vytváření, šíření a manipulaci s informacemi za nejvýznamnější ekonomické a kulturní aktivity. (Jirásek et al., 2013) Dombrovská a Šidlichovská (2021) také zmiňují **digitální společnost**, se kterou se pojí sociální sítě a rozvoj umělé inteligence. V této digitální společnosti máme přístup k množství informací, ale zároveň k němu můžeme přispívat vlastním obsahem. S tímto se pojí i tzv. **digitální smog**, protože se informacemi necháváme dobrovolně zahlcovat, pravidelně a opakovaně, i když většina z těchto informací nemá žádnou informační hodnotu. Tyto informace také mohou mít negativní dopad a mohou škodit.

**Informační a komunikační technologií** se rozumí: *„veškerá technika, která se zabývá zpracováním a přenosem informací, tj. zejména výpočetní a komunikační technika a její programové vybavení“*. (Jirásek et al., 2013) Podle Dombrovské a Šidlichovské (2021) má informační společnost prostřednictvím informačních a komunikačních technologií přístup k obrovskému množství zdrojů různých informací.

**Sociální síť** je podle Kožíška a Píseckého (2016) *„internetová služba, která umožňuje svým členům vytvářet veřejné, uzavřené nebo firemní profily, prezentace, diskusní fóra, a nabízí prostor ke sdílení fotografií, videí, obsahu a dalších aktivit“*.

## 2.1 Právní normy

Problematika informací, přístupu k nim a jejich rozšiřování, kybernetické bezpečnosti a postihy za šíření falešných zpráv je v českém právním prostředí zakotvena několika právními normami.

**Ústavní zákon č. 1/1993 Sb., Ústava České republiky**. Tento ústavní zákon je základním zákonem České republiky, a zároveň nejvyšší právní normou. Ústava České republiky pokládá základní pravidla výkonu státní moci a zaručuje lidská práva občanům České republiky. Základní lidská práva a svobody jsou pod ochranou soudní moci. (Česko, 1993b)

**Usnesení č. 2/1993 Sb., Usnesení předsednictva České národní rady o vyhlášení Listiny základních práv a svobod jako součástí ústavního pořádku České republiky**. Listina základních práv a svobod (dále v textu jen *„Listina“*) je součástí ústavního zákona č. 1/1993 Sb., Ústava České republiky. Listina pokládá základní práva svobody občana, kterou jsou zaručena všem bez rozdílu na pohlaví, rasy, barvy pleti, jazyka, víry a náboženství a všichni lidé jsou svobodní a rovní v důstojnosti i právech. Základní práva a svobody jsou podle Listiny nezcizitelná, nezadatelná, nepromlčitelná a nezrušitelná. Listina stanovuje, že *„každý má právo na svobodu myšlení, svědomí i náboženského vyznání. Dále také stanovuje, že je zaručena svoboda projevu a právo na informace a každý má právo vyjadřovat své názory slovem, písmem, tiskem, obrazem nebo jiným způsobem, jakož i svobodně vyhledávat, přijímat a rozšiřovat ideje a informace bez ohledu na hranice státu“*. Cenzura je podle Listiny nepřípustná. Na stranu druhou ale Listina zakotvuje, že svobodu projevu a právo na vyhledávání a šíření informací lze omezit zákonem. To ale pouze v případě, pokud jde o opatření pro ochranu práv a svobod druhých lidí, ochranu bezpečnosti státu a veřejnou bezpečnost, ale i ochranu veřejného zdraví a mravnosti v demokratické společnosti. (Česko, 1993a)

**Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky**. Tento ústavní zákon zakotvuje zajišťování vnitřní a vnější bezpečnosti v České republice, kdo ji zajišťuje a jaké orgány se na tomto zajišťování podílejí. Dále se dotýká i problematiky krizových stavů a Bezpečnostní tady státu. Stanovuje, že základní povinností sátu je *„zajištění svrchovanosti a územní celistvosti České republiky, ochrana demokratických základů a ochrana životů, zdraví a majetkových hodnot“*. (Česko, 1998)

**Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)**. Zákon o kybernetické bezpečností je základním právním dokumentem pro oblast zajišťování bezpečnosti v kybernetickém prostoru a upravuje práva a povinnosti osob i působnost a pravomoci veřejných orgánů v této oblasti. Tento zákon zpracovává příslušný předpis Evropské unie – Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti síti a informačních systémů v Unii. Zároveň také navazuje na přímo použitelný předpis Evropské unie – Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA (Agentura Evropské unie pro kybernetickou bezpečnost), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 (*„akt o kybernetické bezpečnosti“*). Zákon o kybernetické bezpečnosti vymezuje základní pojmy z této oblasti, orgány a osoby, kterým ukládá povinnosti v oblasti kybernetické bezpečnosti a jaký je systém zajištění kybernetické bezpečnosti. Uvádí, co je to národní CERT a vládní CERT, co je to stav kybernetického nebezpečí a výkon státní správy v této oblasti. Jaká je kontrola, nápravná opatření a přestupky. (Česko, 2014)

**Zákon č. 40/2009 Sb., trestní zákoník**. Tento zákon stanovuje působnost trestních zákonů, co je to trestní odpovědnost a kdy zaniká, jaké jsou trestní sankce a určuje konkrétní druhy trestných činů. Pro problematiku dezinformací je v trestním zákoníku důležitý **§ 357** týkající se trestného činu **šíření poplašné zprávy**. (Česko, 2009)

České právní prostředí nemá žádný právní dokument, který by se zabýval problematikou dezinformací nebo propagandou a ani tyto pojmy nejsou v žádném legislativním dokumentu zakotveny. V českém trestním právu tedy není definována skutková podstata trestného činu dezinformace nebo propagandy. (mvcr.cz, ©2024b) Zákon dotýkající se problematiky dezinformací na základě informací od poslanců vládní koalice nejspíš ani nevznikne. Dle poslanců se s dezinformacemi dá bojovat i jinak než právní úpravou, a to především tlakem na policii a státní zastupitelství, aby byly využívány již platné právní normy.

Například zákony postihující šíření poplašných zpráv. Návrh zákona o dezinformacích vznikl, vypracovalo ho Ministerstvo vnitra. Tento návrh ale vyvolal rozruch a debaty především v opozici. Opoziční politici tento návrh zákona o dezinformacích kritizovali, jelikož se obávají, že by ho vláda mohla použít k potlačování svobody slova. (Kryštofová, 2023) Předseda Stálé komise pro hybridní hrozby Ing. Lukáš Vlček se pro sever Aktuálně.cz vyjádřil, že je sám proti vytvoření nového zákona pro potlačování dezinformací, pokud by nebylo jisté, že bude funkční a vymahatelný. Tvrdí, že v legislativním prostředí již jsou právní normy zabývajících se potlačováním dezinformací, a proto podle něj je vhodnější cestou využívat nynější legislativu. (Bartoníček, 2023)

## 2.2 Problematika dezinformací ve strategických dokumentech České republiky

Oblast ochrany informací, kyberbezpečnosti, boj proti dezinformacím a hybridním hrozbám je dále řešena v několika strategických dokumentech, kterými Česká republika a její státní orgány nastavují nástroje pro zajištění bezpečnosti v oblasti hybridních hrozeb a dezinformací.

**Obranná strategie České republiky** je jedním ze základních strategických dokumentů, jejíž cílem je stanovit možné hrozby pro Českou republiku a vysvětlovat, jaké činnosti jsou nutné provést, aby byla zajištěna obrana státu. Obranné strategie slouží k posílení zajišťování obranyschopnosti České republiky. (Česko, 2017 a Česko, 2023b) Obranná strategie České republiky 2017 se dotýká také dezinformací, a to konkrétně v souvislosti s aktivitami Ruské federace vůči členským zemím NATO a EU. Podle této Obranné strategie používá Ruská federace mnoha hybridních nástrojů, kterými jsou právě cílené dezinformační aktivity, ale také kybernetické útoky. V prvním pilíři *„Zodpovědný přístup státu k obraně České republiky a spojeneckým závazkům“* v odstavci 13 *„Systém obrany státu“* je zmíněno, že jednou ze základních funkcí systému obrany státu je také včasná identifikace a predikce vývoje hrozeb a jejich vyhodnocení, a to i těch hrozeb hybridních. (Česko, 2017) Obranná strategie České republiky 2023 rovněž zmiňuje hybridní hrozby a dezinformace. Podlé této Obranné strategie jsou pro Českou republiku hrozbou kybernetické útoky, dezinformační kampaně i zpravodajské aktivity, jelikož je Česká republika i její ozbrojené síly vystavována systematickému nepřátelskému působení. Obranná strategie České republiky 2023 dále zmiňuje, že hybridní působení a nepřátelská činnost může probíhat již v mírovém stavu, a proto se varovací doba velmi zkrátila. Jedním z nástrojů pro posilování odolnosti České republiky

a její společnosti je strategická komunikace a omezování nepřátelského informačního vlivu na českou společnost. (Česko, 2023b)

**Audit národní bezpečnosti** (dále v textu jen *„Audit“*) z roku 2016 má za cíl ověřit schopnost České republiky identifikovat bezpečnostní hrozby a učinit preventivní opatření proti těmto hrozbám a možným rizikům. Ověřuje, zda je současná legislativa dostatečná, jestli má Česká republika dostatečné kapacity na řešení krizí a zda je stát schopný na tyto hrozby reagovat okamžitě a efektivně. Na Auditu národní bezpečnosti se podílelo přes sto odborníků z různých oblastí s cílem vytvořit přehled a vyhodnotit nezávažnější hrozby pro Českou republiku. Problematika dezinformací, propagandy a hybridního působení je v Auditu zmíněna několikrát, především v kapitole *„Působení cizí moci“*. V této kapitole je propaganda a šíření dezinformací identifikována jako prostředek informační války, kterými se cizí mocnosti snaží působit na veřejné mínění. Identifikuje, že současná propaganda cizích mocností je zaměřovaná především na dezinformační kampaně, které cíli na narušování důvěry společnosti ve stát. Audit identifikuje dezinformační kampaň jako součást hybridních hrozeb, která je jedna z nejzávažnějších hrozeb pro Českou republiku. Audit hodnotí hrozbu ovlivňování veřejného mínění, která má za cíl narušování důvěry v právní demokratický stát, jako vysokou. Podotýká, že dezinformace jsou šířeny prostřednictvím mediálních platforem a sociálních sítí i „nezávislých“ nevládních organizací nebo známých osobností a politických příslušníků. Důsledkem této kampaně je radikalizace veřejnosti. Ve SWOT analýze v této kapitole je slabou stránkou České republiky slabá odolnost společnosti proti ovlivňování a snahám o narušení důvěry v demokratický stát prostřednictvím dezinformací. Další slabou stránkou je chybějící strategická komunikace státu v reakci na dezinformační kampaně a posilování důvěryhodnosti státu. Závěrem této kapitoly Audit doporučuje k posílení odolnosti analýzu stávající efektivnosti právních nástrojů, které by reagovaly v případě reakce na závažnou dezinformační vlnu. Problematika dezinformací je také zahrnuta v kapitole *„Hrozby v kyberprostoru“*. Identifikuje riziko v prostředí sociálních sítí, které mohou být využívány k šíření dezinformačních kampaní a nenávisti vůči různým skupinám obyvatel i státním orgánům. Další hrozbou jsou nepřátelské kampaně prostřednictvím dezinformačních aktivit v mediálním prostoru prováděných v kyberprostoru. Dezinformační kampaně jsou identifikovány jako hrozba i v kapitole *„Hybridní hrozby a jejich vliv na bezpečnost občanů ČR“*. Audit zmiňuje kybernetický prostor, který se může stát prostorem pro kybernetické útoky cílící na funkci veřejné správy, kritické infrastruktury a tento kybernetický prostor je prostředkem špionáže a dezinformačních kampaní. (Česko, 2016)

**Národní strategie pro čelení hybridnímu působení** je strategický dokument České republiky, který vymezuje cíle a určuje nástroje k ochraně životních, strategických a dalších významných zájmů České republiky. Vytvoření této Národní strategie bylo zadáno Auditem národní bezpečnostní z roku 2016. Národní strategie pro čelení hybridnímu působení vychází z Bezpečnostní strategie České republiky a je v souladu s dalšími strategickými dokumenty, například s Obrannou strategií České republiky a Národní strategií kybernetické bezpečnosti České republiky. Tato Národní strategie definuje bezpečnostní prostředí, ve kterém se Česká republika nachází a definuje hybridní působení a stanovuje strategické cíle pro efektivní odolnost České republiky proti hybridnímu působení. (Česko, 2021)

**Národní strategie kybernetické bezpečnosti České republiky** je jedním z dalších strategických dokumentů České republiky. Vymezuje bezpečnostní prostředí a strategický kontext a určuje systém zajišťování kybernetické bezpečnosti České republice. Určuje tři strategické cíle pro efektivní čelení kybernetickým hrozbám – sebevědomě v kyberprostoru, silná a spolehlivá spojenectví a odolná společnost 4.0. Národní strategie se dotýká i dezinformací, a to především v kapitole vzdělávání a osvěty. Označuje seniory za významnou skupinu populace, která je náchylnější na podléhání negativním vlivům moderních technologií a rozlišování dezinformací. (Česko, 2020)

**Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2021–2025**. Akční plán slouží k naplnění stanovených cílů v Národní strategii kybernetické bezpečnosti. Strategické cíle jsou rozděleny do třech oblastí – sebevědomě v kyberprostoru, silná a spolehlivá spojenectví a odolná společnost 4.0. V každé této oblasti je stanoven konkrétní úkol k dosažení cíle, odpovědný subjekt a časový rámec. Akční plán zadává celkem 105 úkolů pro naplnění strategických cílů. (Česko, 2021a)

# 3 DEZINFORMACE, PROPAGANDA, FAKE NEWS

Ministerstvo vnitra České republiky (©2023) označuje pojem *„dezinformace“* jako *„šíření záměrné nepravdivých informací, obzvláště pak státními aktéry nebo jejich odnožemi vůči cizímu státu nebo vůči médiím, s cílem ovlivnit rozhodování nebo názory těch, kteří je přijímají“*. Gregor a Vejvodová (2018) uvádí, že dezinformace jsou zavádějící nebo nepravdivé informace s cílem zmanipulovat a ovlivnit jejího příjemce, kterým může být široká veřejnost nebo specifická skupina. Souvisejícím termínem je také *„misinformace“,* česky *fáma*, kterou autoři popisují jako informace s nepravdivým základem, která je šířena nevědomě. Jako příklad misinformace uvádějí pomluvy a drby. Podle Kopeckého (2023) se samotná definice dezinformace skládá ze 3 základních částí – lži, záměru a prospěchu, takže při rozhodování, co dezinformace je a co naopak není, bychom se měli zaměřit právě na tyto tři složky – pravdivost, záměr a prospěch. Podle Gregora a Vejvodové (2018) musí dezinformace splňovat několik faktorů, aby naplnily svou funkci. Prvním je, že se musí zakládat na pravdivém jádru a věrohodných informacích. Dále se dezinformace musí přizpůsobit kulturnímu prostředí a kontextu, kde se použije a třetím faktorem je, aby byla dezinformace cílem přijímána z více kanálů.

Táborský (2020) uvádí, že nikdy v historii nebylo tak jednoduché šířit informace, jako právě v dnešní internetové době. Také se původce těchto informací i dezinformací může velmi jednoduše na internetu ukrýt, a zároveň v podstatě neexistuje žádná kontrola informačních zdrojů, tudíž jsme různými informacemi doslova zahlceni.

Informace byly a jsou v politickém a vojenském prostředí velmi zásadní a ti, kteří jsou původci těchto informací nebo s nimi dokáží manipulovat, jsou schopni zmást nepřítele nebo širokou veřejnost (Gregor a Mlejnková, 2021).

Dezinformace můžeme rozdělit do 4 kategorií podle jejich záměru:

- Podřízení se, nikoli víra – cílem je vytvořit, udržovat a zesilovat rozpory mezi soupeřícími politickými stranami, vládou nebo koalicí. V tomto případě jsou dezinformace strategií politické kontroly.
- Zasít rozpor – dezinformace zde slouží jako národní strategický nástroj se záměrem sabotovat mezinárodní konsenzus (zbraň proti nepřátelskému národu nebo koalici).
- Zasít zmatek – cílem dezinformací je zmást, tedy všechno a nic není uvěřitelné a důvěryhodné. Cílem není vytvářet věrohodnost, ale zmatek.

- Vzbuzovat pochybnosti – šíření pochybností je účinný způsob, protože věrohodné jevy lze jen zřídka absolutně prokázat. Vždy totiž existuje možnost pochybovat (Gregor a Mlejnková, 2021)

Na druhou stranu, ne každá lživá nebo nepravdivá informace je vždy dezinformací. V některých případech mohou různí aktéři, politici nebo propagandisté, označovat různé informace a zdiskreditovat tak uvěřitelnost takových informací. Některé informace mohou být falešné nebo nepravdivé, ale nenaplňují tu podstatu dezinformace – záměrně šířit falešnou zprávu. Sotva pravdivé informace také nemohou být považovány za dezinformace a falešné informace nemusí být vždy prezentovány se záměrem zmanipulovat příjemce této informace. Speciální kategorií jsou vtipy a satira, které jsou založeny na lživých nebo nekompletních informacích. Jejich záměr je ale pobavit publikum, nikoli s ním manipulovat. Pokud nebyly vytvořeny se záměrem manipulovat publikum, ale neznamená, že se z nich později nemohou stát prostředky dezinformačních akcí. Za dezinformaci se také mohou považovat altruistické falešné zprávy, které sice mají záměr konat dobro, ale stále manipulují s příjemcem (Gregor a Mlejnková, 2021). Přehled kategorií dezinformací je zobrazen v Tabulce 1.

*Tabulka 1 Kategorie dezinformací. (Gregor a Mlejnková, 2021)*

| Dezinformace | Není považováno za dezinformace |
|---|---|
| Zlomyslné lži | Pravdivá prohlášení |
| Audio-vizuální dezinformace | Náhodné nepravdy |
| Pravdivé dezinformace | Vtipy |
| Dezinformace s vedlejšími účinky | Sarkastické komentáře |
| Adaptivní dezinformace | Náhodné pravdy |
| Altruistické dezinformace | Nepravděpodobné lži |
| Škodlivé dezinformace | Satira |

**Propaganda**

Alvarová (2022) ve své knize uvádí, že propaganda není pouze šíření lží, ale jemná manipulace s veřejným míněním. Propaganda záměrně manipuluje s pravdou, ke které přidává různé významy, malé lži nebo polopravdy a společně například s mírně upravenou fotkou už nemusíme propagandu poznat. Dále také upozorňuje, že na internetu je velmi těžké rozeznat, co je fakt, jaké informace jsou ověřené nebo nepravdivé, a právě proto chycení se do pasti propagandy a dezinformací není otázkou rozumu, který na tomto poli hraje malou roli,

protože každý člověk má slabé místo. Oxfordský slovník definuje propagandu jako *„systematické šíření informací, především neobjektivních či zavádějících, s cílem podpořit věc nebo názor, anebo politický program“*. (oed.com, ©2023)

Ve dvacátém století si mohli propagandisté dovolit šířit i výslovné lží, protože v této době neexistovalo mnoho nástrojů, jak si rychle a přesně ověřovat informace. Toto se ale změnilo při nástupu a masivnímu rozvoji internetu ve dvacátém prvním století. Hlavním úkolem propagandisty je získat si důvěru, vytvořit důvěryhodnost a přesvědčit cíl, aby mohl zdroji věřit. V dnešní době lze výslovné lži velmi jednoduše ověřit a dostupnost mnoha zdrojů výrazně zredukovalo efektivitu šíření lží a jejich dopad na společnost. V současné době je strategie propagandy založena na výběru pravdy, která se smíchá s manipulativním obsahem. Takže finální produkt je lživý, ale v tomto případě se nikdo na okolní lži nedivá, když je přeci základ založen na pravdivé informaci. (Gregor a Mlejnková, 2021).

**Fake news**

Podle Kopeckého (2022) jsou termínem *fake news* označovány nepravdivé zprávy, ale také média, která tyto zprávy tvoří a šíří. V prostředí českého internetu se však více využívá názvů jako *„dezinformační web“* nebo *„dezinformační média“*. Mezi fake news ale nepatří satirická média. Gregor a Vejvodová (2018) popisují fake news jako úmyslně nepravdivé nebo zavádějící informace objevující se v médiích a na sociálních sítích. Podstatou fake news jsou informace, které jsou nepravdivé nebo zavádějící a mají za cíl zmanipulovat a ovlivnit publikum.

**Hoax**

Hoax jsou nepravdivá tvrzení, která jsou zcela záměrně zmanipulovaná jejichž cílem je oklamat příjemce. (Dombrovská a Šidlichovská, 2021) Hoax se dá také nazvat jako *poplašná zpráva*, která se pro svůj obsah snaží vytvořit dojem důvěryhodnosti. (Jirásek et al., 2013) Kopecký (2022a) definuje hoax jako: *„zprávu, která se snaží šířit paniku, vyděsit nás a přimět k unáhleným a často iracionálním reakcím. K hoaxům ale řadíme také žertovné nebo vtipné zprávy, jejichž cílem je především pobavit čtenáře“*. Hoaxy se velmi rychle šíří na sociálních sítích i prostřednictvím e-mailů a nabádají k dalšímu sdílení. Hoaxy mají několik druhů obsahů, například informace o hrozícím nebezpečí, falešné petice nebo žádosti o pomoc, anebo varují proti nějakému vymyšlenému ohrožení a používají citové vydírání. (Gregor a Vejvodová, 2018)

### Deep fake

Kopecký (2019) uvádí, že termínem deep fake se označuje velmi realistická úprava videa, která zobrazuje tváře osob a dokáže věrohodně změnit jejich mimiku na videu, měnit obličeje a upravit video tak, že osoba říká věty, které nikdy nepronesla. K vytvoření deep fake se využívá pokročilého počítačového zpracování dat a umělá inteligence.

### Hybridní hrozby

Hybridní hrozby jsou podle Ministerstva vnitra České republiky *„metody nebo způsoby, kterými je veden konflikt, tedy komplexní, adaptivní a integrovaná kombinace konvenčních i nekonvenčních nástrojů, otevřených i skrytých aktivit, které jsou prováděny vojenskými nebo civilními aktéry“*. (mvcr.cz, ©2024a) Definice NATO uvádí, že se hybridní metody používají ke stírání hranic mezi válkou a mírem a snaží se zasít pochybnosti do cílových skupin obyvatelstva s cílem destabilizovat společnost. (nato.int., 2024) Hybridní působení je podle Národní strategie pro čelení hybridnímu působení definováno jako: *„skýtá či zjevná činnost státních nebo nestátních aktérů namířená proti zranitelným prvkům demokratického státu a společnosti“*. Původci tohoto působení používají různé druhy nástrojů, například vojenské, politické, informační, zpravodajské, ekonomické nebo finanční. (Česko, 2021b)

# 4 ŘEŠENÍ DEZINFORMACÍ NA NÁRODNÍ A MEZINÁRODNÍ ÚROVNI

Hybridní působení, dezinformační kampaně, fake news nebo propaganda je aktuálním bezpečnostním tématem a státy i mezinárodní organizace nastavují systémy, jak proti takovým hrozbám bojovat.

Na shromáždění Světového ekonomického fóra v Davosu předsedkyně Evropské komise Ursula von der Leyen prohlásila, že misinformace a dezinformace jsou největším světovým problémem, dokonce větším než válečné konflikty a klimatická změna. Zmínila také, že tyto hrozby jsou úzce spojeny s polarizací společnosti. Podle von der Leynové je řešením spolupráce podniků a vlád zemí při potlačování dezinformací. (Duggan, 2024)

Světové ekonomické fórum (dále v textu jen *„WEF“* z angl. World Economic Forum) vydává každoročně řadu reportů, které mají detailně a široce zmapovat globální problémy a jsou zaměřeny na budoucí vývoj (Ministerstvo zahraničních věcí České republiky, nedatováno). Jedním z důležitých dokumentů, které WEF vydává, je The Global Risks Report, ten nejaktuálnější je k roku 2024. Tento report se zaměřuje na rizika v krátkodobém dvouletém měřítku a dlouhodobém desetiletém měřítku. Zpráva představuje zjištění průzkumu vnímání globálních rizik (GRPS, z angl. Global Risks Perception Survey), který zachycuje poznatky od asi 1 500 globálních expertů. Tato zpráva o globálních rizicích slouží ke zmapování nejzávažnějších současných rizik, a zároveň slouží jako podklad pro rozhodovací orgány v oblasti řešení aktuálních krizí. (World Economic Forum, ©2024)

Z výsledků tohoto průzkumu bylo seřazeno 10 největších rizik pro období následujících dvou a deseti let. Na obrázku 2 (viz níže) jsou uvedeny výsledky průzkumu WEF. Misinformace a dezinformace jsou podle odborníků největším rizikem pro následující dvouleté období a v desetiletém měřítku se dezinformace umístily na 5. místě z deseti. (World Economic Forum, ©2024)

V následujících dvou letech se očekává, že misinformace a dezinformace, jako nejzávažnější globální riziko, budou využívány státními i nestátními aktéry k dalšímu rozšiřování společenských a sociálních problémů. Tento problém také podporuje fakt, že manipulující a falešné informace se kvůli stále sofistikovanějším technologiím rozšiřují rychleji a efektivněji, a zároveň se důvěra v informace a instituce snižuje. Kvůli současnému rozvoji umělé inteligence se problém vytváření a šíření dezinformací bude nadále zhoršovat. Umělá inteligence umožňuje vytváření tzv. „syntetického“ obsahu, od sofistikovaného klonování hlasu až po

padělky webových stránek. V rámci boje proti dezinformacím vlády začínají zavádět nové, stále se vyvíjející nástroje a předpisy, které se zaměřují jak na návštěvníky, tak tvůrce webových stránek šířící dezinformace. Například v Číně požadují vodoznaky na obsah, který je generovaný umělou inteligencí, takže zavedení tohoto požadavku v jiných zemích by mohlo pomoct s identifikováním dezinformací, misinformací a manipulativního obsahu tvořené umělou inteligencí. Obecně ale platí, že rychlost a účinnost regulací takového obsahu s velkou pravděpodobností nebude odpovídat tempu vývoje v této oblasti (World Economic Forum, ©2024).

## 4.1 Boj proti dezinformacím na půdě Evropské unie

EU se zavazuje několika společnými strategickými dokumenty k řešení hybridních hrozeb a dezinformací v členských zemích. EU se snaží držet krok s neustále se vyvíjejícím digitálním prostředím a moderními technologiemi, které s sebou mohou nést bezpečnostní riziko.

Jedním ze strategických dokumentů je **Společné sdělení Evropskému parlamentu a Radě – Společný rámec pro boj proti hybridním hrozbám** (dále v textu jen *„Společný rámec“*). Stanovuje, že za boj proti hybridním hrozbám mají odpovědnost především členské státy, protože konkrétní slabiny jsou specifické především pro jednotlivé členské země. Státy EU se ale mohou potýkat se společnými hrozbami, kterým je ale možné efektivněji čelit pouze společnou koordinovanou reakcí. Zásadní roli v potlačování společných hrozeb je informovanost, která pomáhá členským státům zvyšovat schopnost reakce na hrozby. Cílem Společného rámce je vytvořit komplexní přístup EU a členských států bojovat proti hybridním hrozbám a zlepšení spolupráce mezi státy. Jedním z dalších cílů je také spolupráce s NATO v oblasti boje proti hybridnímu působení. Společný rámec pro boj proti hybridním hrozbám má několik cílů, ke kterým určuje konkrétní opatření. EU zřídila Středisko EU pro hybridní hrozby, které je řízené v rámci Střediska EU pro analýzu zpravodajských informací Evropské služby pro vnější činnost, které se zaměřuje na analýzu hybridních hrozeb. Jeho hlavní náplní je shromažďovat, analyzovat a sdílet utajované informace a další informace z otevřených zdrojů, jež se týkají varování před hybridními hrozbami. Tyto informace získává od členských států, Komise EU a dalších agentur EU a dalších zúčastněných stran v rámci Evropské služby pro vnější činnost. K této činnosti EU nařizuje opatření, aby si členské státy zřídily svá národní kontaktní místa pro hybridní hrozby, aby byla zajištěna komunikace a spolupráce se Střediskem EU pro hybridní hrozby.

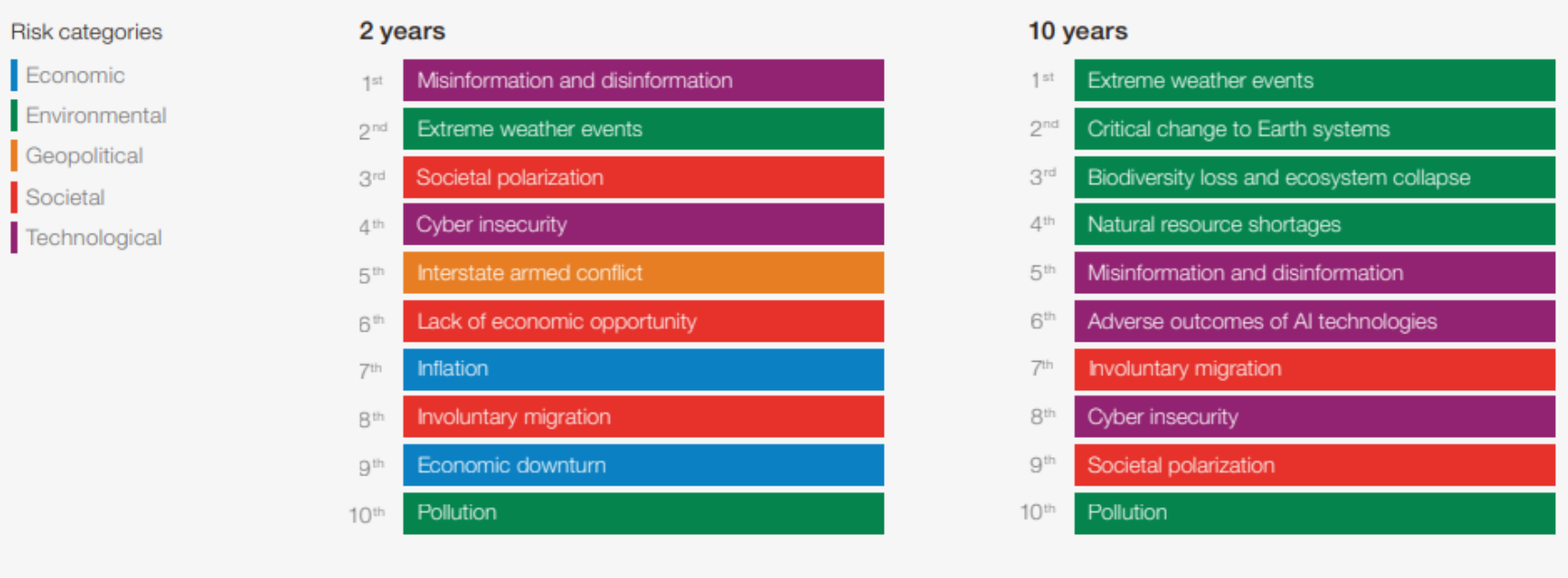
Strategická komunikace EU by měla využívat nástroje sociálních médií, ale také audio-médií a video-médií i internetových médií. Členské státy EU by měly vypracovávat koordinované mechanismy pro strategickou komunikaci, která by podporovala zjišťování původu falešných informací a jak takovému šíření předcházet. Zaměřuje se na posílení spolupráce s třetími zeměmi v rámci Východního partnerství a jižního sousedství. Rovněž klade důraz na prevenci, reakci na krize a následné zotavení. Rychlá reakce na události vyvolané hybridními hrozbami jsou zásadním opatřením v boji proti tomuto druhu hrozeb. Důležitá je spolupráce členských států a Evropského střediska pro koordinaci odezvy na mimořádné události, který by mohl být účinným mechanismem pro informovanost mezi členskými státy. Dalším důležitým aspektem při boji proti hybridním hrozbám je posilování spolupráce zejména s NATO, ale i dalšími mezinárodními organizacemi, jako je Organizace spojených národů (dále v textu jen *„OSN“*), Organizace pro bezpečnost a spolupráci v Evropě (dále textu jen *„OBSE“*). Užší spolupráce především na politické a operační úrovni mezi EU a NATO by umožnila efektivněji reagovat na hybridní hrozby. (Evropská Unie, 2016)

**Sdělení Komise Evropskému parlamentu, Radě Evropskému hospodářskému a sociálnímu výboru a Výboru regionů – Boj proti dezinformacím na internetu: evropský přístup**. Tento strategický dokument se zaměřuje na strategii EU pro boj proti šíření dezinformací na internetu. Evropská komise zde navrhuje opatření a inciativy ke zvýšení transparentnosti, podpoře rozmanitost médií, posílení spolupráce s platformami sociálních sítí a zlepšení mediální gramotnost veřejnosti. Toto Sdělení je součástí snah EU o ochranu demokratických procesů a ochranu veřejného prostoru před škodlivými informacemi a manipulacemi. (Evropská komise, 2018)

Evropská komise vydala dokument s pokyny pro učitele a pedagogické pracovníky ve výchově a vzdělávání na základních a středních školách k podpoře digitální gramotnosti ve třídách, a jak řešit dezinformace. Publikace s názvem *„**Guidelines for teachers and educators on tackling disinformation and promoting digital literacy through education and training**“* poskytuje návody a doporučení, jak efektivně bojovat proti dezinformacím a podporovat digitální gramotnost ve vzdělávání. Obsahuje pokyny, jak do výuky integrovat prvky rozpoznávání a kritického hodnocení informací online s cílem posílit odolnost žáků a studentů vůči dezinformacím a manipulativnímu obsahu na internetu. (European Commission, 2022)

**Evropské centrum excelence pro čelení hybridním hrozbám,** anglicky European Centre of Excellence for Countering Hybrid Threats (dále v textu jen *„Hybrid CoE"*) se sídlem v Helsinkách je mezinárodní autonomní síťová organizace podporující celovládní a celospolečenský přístup k boji proti hybridním hrozbám. Hybrid CoE bylo založeno v roce 2017 prvními devíti zúčastněnými státy (Finsko, Švédsko, Spojené království, Lotyšsko, Litva, Polsko, Francie, Německo a Spojené státy americké). Posláním Hybrid CoE je posilování bezpečnosti zúčastněných států a poskytování odborných znalostí a školení pro čelení hybridnímu působení. Hlavním úkolem Hybrid CoE je budování schopnosti zúčastněných států předcházet hybridním hrozbám a čelit tomuto působení. Cíle je dosahováno sdílením ověřených postupů, poskytování doporučení a testování nových přístupů. Hybrid CoE buduje operační kapacity zúčastněných států školením odborníků z praxe a pořádá praktická cvičení. Na činnosti Hybrid CoE se mohou podílet státy z celé EU a NATO. V současné době je počet zúčastněných států 35. (hybridcoe.fi, nedatováno a; hybridcoe.fi, nedatováno b)

Jedním z nástrojů pro boj s dezinformacemi na evropské úrovni je také internetový portál **EUvsDisinfo**. Tento portál je vlajkovým projektem pracovní skupiny East StratCom Evropské služby pro vnější činnost. Jeho činnost běží od roku 2015 s cílem potírat dezinformace a dezinformační kampaně cílené proti EU, především řeší dezinformační kampaně Ruské federace. (Evropská komise, nedatováno) Portál spravuje tým odborníků z oblasti komunikace, žurnalistiky, sociálních studií a expertů na Rusko. Hlavním cílem projektu je zvyšovat informovanost veřejnosti o dezinformačních kampaních Kremlu a pomoct evropským občanům i lidem mimo EU rozvíjet odolnost vůči digitálním informacím a mediální manipulaci. Od roku 2019 se jejich monitorovací kapacity přesunuly i na západní Balkán a do jižního sousedství EU, kde odhalují dezinformace. Tyto případy a reakce na ně jsou shromažďovány v databázi na webu a je to jediné prohledávatelné úložiště s otevřeným zdrojem svého druhu. Nachází se zde asi 12 000 vzorků prokremelských dezinformací. Dále také publikují články a analýzy o vývoji v oblasti dezinformačních metod a shromažďují mezinárodní výzkum, který přináší další inovace. Zaměřují se také na školení v institucích EU, vlád členských států, novinářů a organizací občanské společnosti a vystupují na mezinárodních konferencích. (euvsdisinfo.eu, nedatováno)




*Obrázek 2 Globální rizika seřazená podle závažnosti ve dvouletém a desetiletém horizontu. (World Economic Forum, ©2024)*

## 4.2 Boj proti dezinformacím v českém prostředí

Česká republika se v posledních letech zaměřila kromě tradičních hrozeb i na bezpečnostní hrozby plynoucí především z prostředí informačních technologií a internetu. V nové bezpečnostní strategii z roku 2023 jsou dezinformace a dezinformační aktivity řešeny několikrát. Dezinformace jsou zmiňovány především v souvislosti s působením cizích států a jejich dezinformační kampaně cílící na oslabování demokratických základů České republiky a ovlivňování jejího obyvatelstva. Tato oblast je zmiňována především v souvislosti s působením Ruska a Číny na českém území.

V odstavci 38 **Bezpečnostní strategie České republiky 2023** je podotknuto, že: *„Státní i nestátní aktéři mohou ohrozit bezpečnost České republiky prostřednictvím hybridního působení, které se soustředí zejména na zranitelná místa demokratické společnosti. Kybernetické, **dezinformační**, ekonomické ale i politické, diplomatické, vojenské, zpravodajské a jiné nástroje jsou synergicky využívány s cílem narušit demokratické procesy a chod demokratických institucí, mechanismy právního státu, vnitřní bezpečnost i společenskou soudržnost.“* Podle tohoto odstavce lze usuzovat, že si Česká republika uvědomuje možné plynoucí bezpečnostní hrozby, které dezinformace a hybridní působení přináší a ohrožuje tak demokracii a náladu ve společnosti. V kapitole V. *„Strategie prosazování bezpečnostních zájmů České republiky“* Bezpečnostní strategie v odstavci 52 uvádí, že *„zásadní součástí posilování společenské odolnosti představuje čelení **dezinformacím**, informačním operacím a snahám o manipulaci informačního prostoru, zejména těch, které jsou prováděny ve prospěch cizích státních aktérů usilujících o narušení demokratického charakteru státu a jeho bezpečnosti.“* V tomto odstavci je dále zmíněno, že pro úspěšnou obranu proti dezinformacím a informačním operacím je nutné, aby nástroje pro boj byly komplexní a kombinovaly podporu vzdělávání v oblasti mediální a informační gramotnosti. Zároveň ale musí být posilována občanská soudržnost a stát by měl v této oblasti strategicky komunikovat. Dalšími nástroji by mělo být budování kapacit pro detekci a analýzu těchto hrozeb a mezinárodní spolupráce a koordinace v boji proti dezinformacím a informačním operacím, především pak na půdě EU a NATO. Boj proti dezinformacím je v Bezpečnostní strategii také komentován v posledním odstavci 130 v souvislosti s řádným fungováním institucí právního státu, aby nedošlo k narušení rovnováhy mezi soudní, výkonnou a zákonodárnou mocí, jelikož by narušení této rovnováhy mohlo vést ke ztrátě důvěry veřejnosti a k destabilizaci demokratického zřízení státu. Z toho důvodu by měl stát bojovat proti dezinformacím, jež tyto zásady zpochybňují. (Česko, 2023)

Bezpečnostní strategie České republiky 2023 se od té předchozí z roku 2015 liší především v přístupu k dezinformacím. V **Bezpečnostní strategii České republiky 2015** jsou dezinformační akce uvedeny pouze jednou, a to v souvislosti s bezpečnostní hrozbou *„oslabování mechanismu kooperativní bezpečnosti i politických a mezinárodněprávních závazků v oblasti bezpečnosti“*, která byla umístěna na první místo v bezpečnostních hrozbách. Dezinformace jsou zde zmíněny jako pomocná forma propagandy v hybridním válčení. (Česko, 2015)

V Programovém prohlášení vlády České republiky z roku 2022 se současná vláda zavazuje k boji s dezinformacemi. V odstavci *„bezpečnost“* uvádí, že do konce roku 2022 zřídila při Úřadu vlády české republiky *„Poradce pro národní bezpečnost“*. Tento poradce je hlavním nadresortním koordinátorem v prostředí dezinformací a hybridních hrozeb. Na Úřadu vlády měla vzniknout platforma pro koordinaci a komunikaci mezi subjekty, které se zabývají bezpečnostní problematikou se zaměřením na větší spolupráci mezi bezpečnostními a zpravodajskými službami, které mají zajistit efektivní postup v boji s hybridními hrozbami a dezinformacemi. (Programové prohlášení vlády České republiky, 2022) Usnesením vlády České republiky č. 1078 dne 21. prosince 2022 vytvořila funkci poradce pro národní bezpečnost a Usnesením vlády České republiky č. 1103 ze dne 21. prosince 2022 jmenovala Tomáše Pojara, MA poradcem pro národní bezpečnost s účinností od 1. ledna 2023. (Česko, 2022a a Česko, 2022b) Poradce pro národní bezpečnost (dále v textu jen *„Poradce“*) je poradním orgánem vlády v rámci bezpečnosti České republiky a je zařazen do organizační struktury Úřadu vlády České republiky. Jeho hlavním úkolem je podílet se na koordinaci činnosti státních orgánů v rámci zajišťování bezpečnosti České republiky. Tento Poradce je také tajemníkem Bezpečností rady státu a může se účastnit jednání vlády, která se týkají bezpečnosti České republiky. Zpracovává připomínky k návrhům, které se dotýkají oblasti zajišťování bezpečnostní státu, spolupracuje s dalšími příslušníky vlády a jinými vedoucími ústředních správních orgánů. (Česko, 2022c) Poradce pro národní bezpečnost v současné době také zastává funkci zmocněnce pro média a dezinformace, jelikož toto místo bylo Úřadem vlády v únoru roku 2023 zrušeno. Tuto funkci zastával odborník na média Michal Klíma necelý rok (místo bylo vytvořeno v březnu roku 2022), který se vyjádřil, že důvodem zrušení funkce zmocněnce pro média a dezinformace je skutečnost, že vláda chce oblast nově řešit prostřednictvím Bezpečnostní rady státu. (Pika a Kubant, 2023)

**Centrum proti hybridním hrozbám** (dále v textu jen *„CHH"*) je odborné analytické akoncepční pracoviště se zamřením na hrozby ohrožující bezpečnost České republiky, které spadají do oblasti vnitřní bezpečnosti. Takovou hrozbou je například působení cizí moci, bezpečnostní dopady migrace, dezinformace, ale do jejich činnosti spadá také zvyšování odolnosti veřejné správy a dalších orgánů proti působení cizí moci. CHH vzniklo na základě doporučení Auditu národní bezpečnosti z roku 2016. O zřízení CHH rozhodl ministr vnitra a pracoviště zahájilo své působení 1. ledna 2017 s názvem Centrum proti terorismu a hybridním hrozbám, ale od 1. července 2022 se oddělila agenda boje proti terorismu a v současné době se toto centrum nazývá pouze jako Centrum proti hybridním hrozbám. (mvcr.cz, ©2024c)

Podle Obranné strategie 2023 je jedním z nástrojů pro posilování odolnosti České republiky a její společnosti strategická komunikace, která by měla probíhat formou transparentní komunikace strategických cílů v obraně bezpečnosti státu, ale i omezování nepřátelského informačního vlivu na českou společnost. Klíčovou roli v koordinaci čelení hybridním hrozbám a strategickou komunikaci státu má Úřad vlády České republiky a jednotlivá ministerstva se na tomto zajišťování bezpečnosti podílí v rámci své působnosti. (Česko, 2023b)

Vláda České republiky stanovuje v Národní strategii pro čelení hybridnímu působení tři strategické cíle:

- **Odolná společnost, odolný stát, odolná kritická infrastruktura** – vytvoření společnosti, která je schopná včasně detekovat hybridní působení a efektivně na něj reagovat. Stát musí snižovat svou strategickou závislost na ostatních zemích s jinou ideovou a hodnotovou orientací a bude využívat transparentní systém prověřování investic do průmyslové sektoru se strategickými komoditami. Součástí tohoto cíle je zvyšování povědomí o existenci hybridního působení prostřednictvím vzdělávacích programů a osvětových akcí a systému strategické komunikace.
- **Systémový a celostátní přístup v rámci České republiky** – posílení meziresortní spolupráce a zvýšení schopnosti koordinace a sdílení informací mezi odpovědnými orgány a institucemi. Optimalizace platforem v rámci Bezpečnostní rady státu ke sdílení informací a nové poznatky budou pravidelně sdíleny mezi experty. Součástí je provádění prověřovacích cvičení na národní a mezinárodní úrovni pro čelení hybridnímu působení.

- **Schopnost adekvátní a včasné reakce** – aktivní účast České republiky v činnostech a aktivitách mezinárodních organizací, kterých je členem. Posilování rozvoje spolupráce s NATO a EU a přispívání k činnosti Evropského centra excelence pro čelení hybridním hrozbám. Česká republika má nadále pokračovat v práci na indikátorech hybridního působení pro včasnou reakci a musí být připravena na nepřátelskou hybridní činnost a zavádět odvetná opatření a další nástroje národní i nadnárodní úrovně. (Česko, 2021b)

**Kybernetická bezpečnost v České republice**

Kybernetická bezpečnost je v České republice zajišťována několika orgány a úřady, které jsou odpovědné za ochranu kybernetického prostoru. Gestorem kybernetické bezpečnosti a ústředním správním orgánem pro tuto oblast je Národní úřad pro kybernetickou a informační bezpečnost (dále v textu jen *„NÚKIB“*). Působnost NÚKIB je dána zákonem číslo 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) a působí v oblasti ochrany utajovaných informací v prostředí informačních a komunikačních systémů a kryptografické ochrany. (Česko, 2020)

V české republice existuje několik projektů, které se zaměřují na ověřování tvrzení a obsahu na internetu s cílem předcházení šíření nepravdivých informací a dezinformací. Jedním z těchto projektu je i **Demagog.cz,** který má za cíl kultivovat veřejnou debatu v České republice prostřednictvím ověřování tvrzení politiků a politických stran. Toto neziskové dobrovolnické sdružení funguje od roku 2012. Jejich činnost se zabývá především v poukazování na nepravdivá a manipulativní vyjádření ve veřejném prostoru. Analyzuje faktické výroky politiků, podrobuje je zkoumání a dohledává primární zdroje takových informací. Za dobu, co fungují již ověřili tisíce výroků českých politiků a poukazují, zda mluví pravdu nebo veřejně klamou. (Demagog.cz, nedatováno)

Dalším z publicistických webů je **Manipulátoři.cz**. Tento web funguje už od roku 2015, v roce 2021 vznikl sesterský web se zaměření na fact-checking Faktické.info a v roce 2023 se tyto dva projekty spojily. Tento projekt se věnuje především politickému marketingu, public relations a komunikačním strategiím. Uvádí, že podtitulem jejich webu je „*na faktech záleží*“ a svá tvrzení staví na ověřitelných a zdrojovaných faktech. Cílem tohoto projektu je vytvořit otevřenou neideologickou platformu, která má sloužit pro faktickou diskuzi. Podporuje nezávislá a otevřené myšlení, ale také otevírá kritické debaty o společenském a politickém dění v České republice. (Manipulátoři.cz, nedatováno)

# 5 ŠÍŘENÍ DEZINFORMACÍ

Digitální revoluce, která se začala rozvíjet na začátku jednadvacátého století potvrzovala myšlenku optimistického vyprávění o technologickém pokroku a jeho politických důsledcích. Nové komunikační prostředky rozšířily přístup ke zprávám a informacím, které poskytovaly mnohem rychleji a spolehlivěji a nabízely tak mnohem širší možnost svobodného vyjadřování a veřejné diskuse. S velmi snadným přístupem k internetu kdykoli člověk chtěl, měl jednotlivec na dosah ruky neomezené množství informací. (Bennett a Livingston, 2020)

Šíření dezinformací na internetu se v průběhu let rapidně změnilo. Online fámy a dezinformace se v polovině 90. let na internetu se šířily pouze málo způsoby. Pomluvy se mohly šířit prostřednictvím přeposílání e-mailů, vymyšlené příběhy se daly zveřejňovat na webových stránkách a nepravdivá tvrzení se mohla uvádět v online chatu. Každá z těchto možností je pro šíření nepravdivých informací online omezující. Řetězové e-maily jsou snadno dohledatelné, víme, kdo nám je přeposlal a komu je posíláme my. V současné době je takové přeposílání velmi časově náročné, protože přeposílání e-mailů s falešnými informacemi sto přátelům dá mnohem více práce než současné *„lajkování“* a *„retweetování“*, kdy výrok sdílíme se všemi ve své síti. (Bennett a Livingston, 2020) Podle výzkumu uvedeném ve Sdělení Komise Evropskému parlamentu, Radě Evropskému hospodářskému a sociálnímu výboru a Výboru regionů – Boj proti dezinformacím na internetu agregátory informací a vyhledávače sociálních médií v roce 2016 představovaly hlavní zdroj online zpráv až pro 57 % uživatelů v EU a až třetina osob ve věku od 18 až 24 let uvedla, že sociální média jsou jejich hlavním zdrojem informací (Evropská komise, 2018) Audit národní bezpečnosti uvádí, že jsou dezinformace šířeny prostřednictvím mediálních platforem a sociálních sítí i „*nezávislých*“ nevládních organizací nebo známých osobností a politických příslušníků. Důsledkem této kampaně je radikalizace veřejnosti. (Česko, 2016)

Dezinformace se šíří vzájemně propojenými hospodářskými, technologickými, politickými a ideologickými příčinami. Rychlé změny ve společnosti vedou k pocitu nejistoty a obavy. Ekonomická nestabilita, nárust extremismu a kulturní proměny vytvářejí prostředí, které usnadňuje dezinformačním kampaním dosáhnout svého cíle. Tímto cílem bývá zvýšit napětí ve společnosti, rozdělovat ji a podkopávat důvěru. Důsledky šíření dezinformací jsou různé v závislosti na každé společnosti, což souvisí s úrovní vzdělání, demokratickou kulturou, důvěrou v instituce, účasti občanů ve volbách, vlivem peněz v politice a mírou sociálních a ekonomických nerovností. (Evropská komise, 2018) Například efekt dopadu propagandy je větší, když je základ manipulativní informace založen na pravdě nebo faktu.

Pokud si publikum ověří tu část propagandy, která je faktem, má pak tendenci uvěřit i té lživé části, a zároveň je také větší pravděpodobnost, že v budoucnu bude zdroji této informace věřit další a jiné lži. (Gregor a Mlejnková, 2021) Stejné podmínky se vztahují i na šíření dezinformací. Studie *„Šíření pravdivých a falešných informací online“* autora Vosoughi et al. (2018) zkoumala rozdíl v rychlosti šíření pravdivých a ověřených informací a těch falešných na Twitteru (dnes platforma X) v letech 2006–2017. Data zahrnují asi 126 000 příspěvků, který byly sdíleny asi 3 miliony uživatelů více než 4,5 milionkrát. Autoři studie klasifikovali zprávy jako pravdivé nebo nepravdivé na základě ověřování pomocí šesti nezávislých fact-checkingových organizací. Z výsledků této studie vychází, že nepravdivé informace se šíří výrazně déle, rychleji a hlouběji než pravda ve všech kategoriích informací. Tento efekt byl výraznější při šíření nepravdivých politických zpráv než nepravdivých zpráv o terorismu, přírodních katastrofách, vědě nebo financích.

Misinformace se na sociálních sítích šíří jinak než v klasických podobách médií, jako je televize, rádio nebo noviny. Mainstreamové zpravodajské servery mají totiž své nástroje, aby zabránily šíření nepravdivých a falešných informací. Naopak sociální sítě umožňují a podporují šíření virálního obsahu s nízkým dohledem. Rychlé zveřejňování a přímé sdílení umožňuje uživatelům rychle rozšiřovat informace velkému publiku. (American Psychological Association, 2023) Falešné informace a misinformace mohou být také šířeny pomocí tzv. *„kruhového zpravodajství“* (z angl. *„circular reporting“*). Takové zpravodajství znamená, že noviny A vydají dezinformační článek, noviny B ji přetisknou a noviny A pak citují noviny B a označí ji za zdroj této informace. Když je taková falešná informace opakovaně zveřejňována, dochází tedy ke kruhovému či falešnému potvrzování zpráv, která je dalšími autory následně považována za ověřenou mnoha zdroji. Jako příklad tohoto falešného potvrzování je uváděno vydání článku v roce 1998 v pseudovědeckém plátku, který tvrdí, že očkování dětí způsobuje autismus, což vedlo ke vzniku hnutí proti očkování bez ohledu na to, že původní zpráva byla několikrát zpochybněna vědeckou obcí. (TED-Ed, 2015)

**Dílčí závěr z teoretické části:** Teoretická část je zaměřena na položení základu v oblasti dezinformací. Popisuje systém ochrany obyvatelstva a důležitost informování, definuje používané pojmy a charakterizuje informace, informační prostředí a jejich zakotvení v českém právním prostředí. Dále uvádí, jak probíhá boj s dezinformacemi na národní a mezinárodní úrovni. V teoretické části práce je také popsáno šíření dezinformací na internetu a sociálních sítích.

# II. PRAKTICKÁ ČÁST

# 6 DEZINFROMACE NA ČESKÉM INTERNETU

Mainstreamová média jsou podle Cambridge Dictionary definována jako forma médií, především ty tradiční jako jsou noviny, televize nebo rádio a mají velký vliv na masy lidí a prezentují obecně přijímané myšlenky a názory. (Cambridge University Press & Assessment, ©2024)

Veřejnoprávní média jsou definována Tulinskou (©2024) jako *„média placená z daní vázány specifickými povinnostmi“*. Protiváhou veřejnoprávních médií jsou komerční média, která jsou orientována především na zisk a vydělávají na reklamě. Oba typy médií jsou regulovány zákonem. Mezi veřejnoprávní média patří Česká televize a Český rozhlas, které mají několik úkolů – *„vysílat nezávislé a svobodné programy, vytvářet rozmanitou programovou nabídku, přispívat k porozumění ve společnosti a k poznání kultury a kulturního dědictví, vytvářet prostor k veřejné diskuzi a přinášet nezávislé a nestranné informace a zpravodajství“*. V roce 2017 byla důvěra veřejnosti v Českou televizi 63 %, ve srovnání s rokem 2016, kdy byla důvěra 65 % a v roce 2015 byla důvěra dokonce 68 %. V těchto letech můžeme tedy demonstrovat, že se důvěra veřejnosti v Českou televizi snižuje. Podle Výroční zprávy 2017 je na tom Česká republika ještě dobře, jelikož uvádí, že se s důvěrou veřejnosti ještě držela nad ORF, BBC nebo ARD. Tento výzkum pro Českou televizi provedla nadnárodní agentura Kantar v roce 2017. (Česká televize, 2018) Ve Výroční zprávě České televize za rok 2023 dosáhla důvěryhodnost ČT24 hodnoty 65 %, což Česká televize přisuzuje tomu, že *„informace předkládané českou televizí jsou objektivní a vyvážené“*. V rámci České republiky jsou ČT24 a Český rozhlas ve srovnání s jinými zpravodajskými zdroji označovány jako nejdůvěryhodnější v zemi. ČT24 dosáhlo lepšího hodnocení než řecká či španělská televize veřejné služby a ve srovnání s německou ZDF nebo francouzskou FT dosáhla podobných výsledků. (Česká televize, 2024)

V posledních letech se v souvislosti s dezinformacemi zmiňují tzv. alternativní média, která nabízejí alternativní (jiný) zdroj informací. Tyto weby a média se stavějí do opozice k běžným zdrojům informací a celkovému převládajícímu názoru společnosti. Ve většině případech se tyto alternativní weby a média považují za šiřitele dezinformací. (Gregor a Vejvodová, 2018) Řada webů, které se označují jako dezinformační, mají často velmi malý dezinformační charakter. Některé weby svým obsahem nasycují touhu čtenářů po konspiračních teoriích, jiné prezentují ideologické a politické názory, část webů má na šíření dezinformací a falešných zpráv postavený svůj business model a jen malou část těchto serverů můžeme označit jako skutečné šiřitele dezinformací a nástroje propagandy. (Bernard a Daniel, 2019)

Podle zprávy o extremismu vydané Ministerstvem vnitra České republiky v roce 2023 dezinformační média dlouhodobě vydávají obsah se stereotypními nenávistnými sděleními a jejich potenciál v radikalizování veřejnosti začíná klesat. Čtenáři těchto dezinformačních médií začínají dávat přednost takovým sdělením šířící se na sociálních médiích, které mají kratší a údernější titulky, ale čtenáři se také zaměřují na streamovaná videa. (Ministerstvo vnitra České republiky, 2023) Z tohoto lze usuzovat, že dezinformace se v českém internetovém prostředí šíří především přes sociální média, na kterých se rozšiřují snadněji.

## 6.1 Dezinformační weby na českém internetu

V České republice od roku 2014 stále narůstá počet dezinformačních médií a na internetu můžeme najít stovky různých zahraničních i českých webů, které záměrně sdílejí dezinformace a používají manipulační techniky. Cílem těchto médií a webů je kritika klasických a mainstreamových médií ze zatajování informací nebo lhaní. Tyto dezinformační weby pak samy nabízejí novou formu reality, která bývá založena na lžích a je vytvořena pomocí manipulačních technik. (Gregor a Vejvodová, 2018)

Spolek Nelež na svých webových stránkách uvádí metodiku, kterou posuzuje jednotlivé weby a hodnotí je, zda jsou dezinformační či nikoli. Na jejich seznamu se nachází 51 webů, které označují za dezinformační. U některých webů také uvádí měsíční průměr návštěvnosti v roce 2019. Například web *„novarepublika.cz“* měl v roce 2019 měsíční průměr návštěvnosti více jak 5 000 návštěv, web *„protiproud.cz“* okolo 566 000, *web „cz.sputniknews.com“* už měl přes 2 000 0000 návštěv a web *„parlamentnilisty.cz“* dokonce přes 7 000 000 návštěv za měsíc. Podle tohoto spolku jsou dezinformační weby základnou pro dezinformace i manipulativní obsah, které se šíří efektivně díky algoritmům na sociálních sítích i řetězovými e-maily. Tímto se dosah manipulativního obsahu násobí a může oslovit i statisíce uživatelů internetu. (nelez.cz, nedatováno)

Dalším webem, který se zaměřuje na dezinformace a manipulativní obsah, je **Nadační fond nezávislé žurnalistiky**. Od roku 2016 podporují svobodnou diskusi o společenských, politických a ekonomických tématech a pomáhají nezávislým médiím a novinářům. Jejich projekt MediaRating je zaměřen na hodnocení důvěryhodnosti zpravodajsko-publicistických médií. Dále bojují proti dezinformacím, konspiračním teoriím i fake news, mediálně vzdělávají děti i dospělé a podporují investigativní novinařinu formou grantů. V projektu MediaRating mají vlastní metodiku, kterou posuzují jednotlivá média a weby a rozdávají

*„známky“* podle výsledků. Mezi kritéria patří – původní obsah, transparentnost média a redakce a práce s obsahem. Po vyhodnocení celkový počet bodů určuje kategorii, do které médium patří: A (85 bodů a více) – splňuje základní kritéria novinářských standardů a důvěryhodnosti; A- (80–84,9 bodů); B+ (70–79,9 bodů), B (60–69,9), B- (50–59,9 bodů) a C (méně než 49,9 bodů), kdy médium nesplňuje základní kritéria. (nfnz.cz, nedatováno)

## 6.2 Mediální gramotnost

Mediální gramotnost je *„soubor znalostí a dovedností umožňující orientaci v mediálním prostoru a kriticky hodnotit mediální obsah“*. Sem patří znalosti mediální logiky, jakou mají roli média ve společnosti a jak jsou významné pro demokracii. Jsou to schopnosti analýzy informací a posouzení jejich důležitosti a důvěryhodnosti. (jsns.cz, nedatováno) Mediálně gramotný člověk je ten, který dokáže pracovat se zdroji informací a dokáže porozumět obsahu mediálních zpráv (Gregor a Vejvodová, 2018) Zásadním plánem státu by mělo být klást důraz na vzdělávání veřejnosti v oblasti mediální gramotnosti, aby každý jedinec věděl, jak fungují média a jedinec, který zná princip informační války, co jsou to dezinformace a propaganda. *„Vyvrátíte-li jednu dezinformaci, ochráníte člověka jeden den před lží. Když ho naučíte, jak lež a dezinformace odhalit, uchráníte ho před nesmysly celý život.“* (Nutil, 2018)

V České republice fungují projekty, které se zaměřují na zvyšování mediální gramotnosti v České republice. Jedním z projektů je *„Zvol si info“* založený v roce 2016 na Katedře politologie Masarykovy univerzity. Tento projekt se zaměřuje na vzdělávání středoškolských studentů v oblasti mediální gramotnosti a kritického myšlení. Dalším projektem je *„Jeden svět na školách“* pod neziskovou organizací Člověk v tísni. Tento projekt funguje již od roku 2001 a také se zaměřují na mediální gramotnost veřejnosti. Lekce mediální gramotnosti a orientaci v digitálním prostoru jsou veřejně přístupné na jejich stránkách po registraci. (Gregor a Vejvodová, 2018) Mohou být také využívány ke vzdělávání dospělé populace České republiky.

Fact-checking je proces ověřování informací v textu, zda jsou pravdivé nebo ne. Tento proces je nestranný s cílem posoudit pravdivost psaného textu a zda je v souladu s ověřitelnými fakty. (Kopecký, 2022b)

Myslet kriticky je podle Nutila (2018) myšlení nezávislé a analytické, které vede k určitému závěru a je to vědomý a racionální proces. V Cambridgeském slovníku je kritické myšlení definováno jako proces pečlivého přemýšlení o myšlence nebo tématu, aniž by se daná osoba nechala ovlivnit pocity nebo názory. (Cambridge University Press & Assessment, ©2024a)

Dombrovská a Šidlichovská (2021) uvádí, že je několik faktorů, které jsou pro kritické myšlení typické – *„nezávislé přemýšlení se zodpovědností za důsledky rozhodování; informace jsou pro přemýšlení a rozhodování východiskem, nikoliv argumentem; stojí na otázkách; hledá nejen důvody, ale také důkazy a připouští i podporuje dialog“*. Autorky dále tvrdí, že je kritické myšlení tou nejúčinnější pomocí proti dezinformacím.

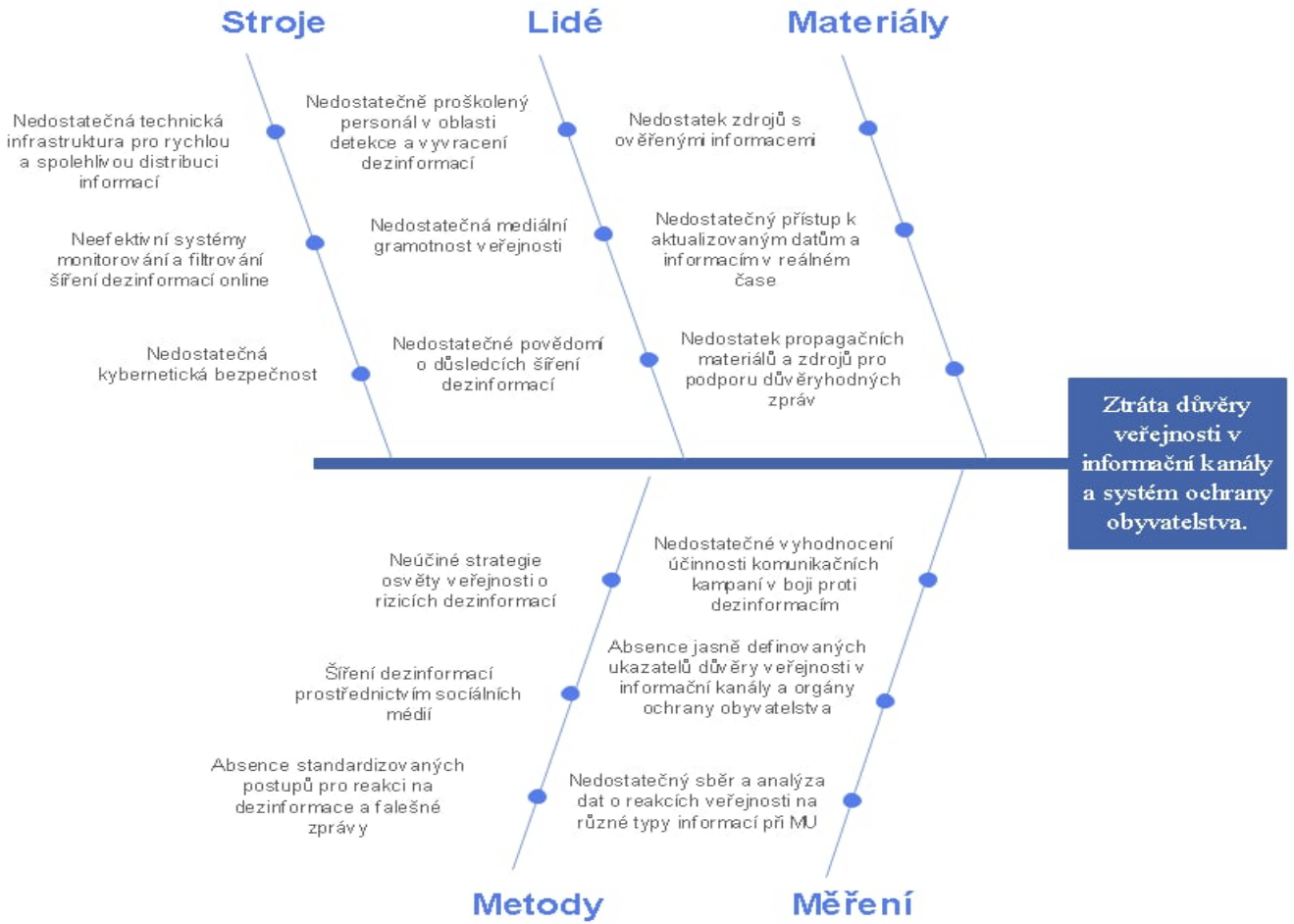
# 7 ISHIKAWA DIAGRAM A MATICE RIZIK

V práci je využita metoda Ishikawa digramu k nalezení kořenových příčin problému, na kterou navazuje matice rizik k posouzení závažnosti rizika.

Ishikawa diagram nebo také digram rybí kosti je metoda příčin a následků. Tento diagram slouží k identifikaci co nejvíce možných příčin zkoumaného problému. Často jsou příčiny získávány technikou brainstormingu, které jsou pak tříděny do jednotlivých kategorií. (asq.org, ©2024) Tato analytická metoda se díky své univerzálnosti používá v několika oblastech. Jednou z takových oblastí jsou i rizika a řešení problémů. Tento digram rybí kosti lze použít pro hledání příčin problému zpětně nebo naopak do budoucna pro návrh preventivních opatření a eliminaci možných příčin. Příčiny se hledají v základních oblastech nazývaných jako 5M nebo 8M – *„Man power (lidé), Methods (metody), Machines (stroje), Materials (materiál), Measurements (meření), Mother nature (prostředí), Management a Maintenance“*. (ManagementMania.com, 2015)

V této práci byla použita oblast Ishikawa digramu 5M – Stroje, Lidé, Materiály, Metody a Měření. V každé oblasti byly zvoleny celkem tři příčiny, které mohou způsobit zkoumaný problém – *„ztráta důvěry veřejnosti v informační kanály a orgány ochrany obyvatelstva“*. Na obrázku č. 4 je zobrazen celý digram rybí kosti. Na základě teoretických poznatků o dezinformacích a dalších souvislostech s touto oblastí bylo identifikováno několik možných příčin problému ztráty důvěry veřejnosti v informační kanály a systém ochrany obyvatelstva. Tento problém byl stanoven na základě povahy a charakteru dezinformací, jelikož jejich hlavním úkolem je zasít nedůvěru veřejnosti ve fungující systém nebo veřejné instituce a polarizovat společnost, což by mohlo vést ke snižování efektivnosti stanovených opatření během mimořádných událostí. Takovou velkou mimořádnou událostí, ve které je třeba spolupráce a důvěra společnosti v bezpečnostní systém České republiky, jsou epidemie, pandemie, ale také úniky nebezpečných látek či kybernetické útoky. Identifikace možných příčin je použita do budoucna pro návrh preventivních opatření ke snižování nalezených rizik a hrozeb pro zkoumaný problém.

Na obrázku 3 níže je zobrazen vytvořený digram rybí kosti s celkem patnácti příčinami rozdělených do jednotlivých oblastí




*Obrázek 3 Ishikawa diagram. (zdroj: vlastní zpracování)*

### Matice rizik

Maticí rizik rozumíme grafické znázornění identifikovaných rizik, která jsou rozdělena do prioritních skupin. Matice rizik se nejčastěji používá ke stanovení velikosti rizika a určit, zda je riziko dostatečně kontrolováno. Umožňuje vyhodnotit a zhodnotit stanovená rizika, nejčastěji, podle dvou kritérií – dopadu a pravděpodobnosti. Rizika se poté roztřídí do třech skupin podle jejich míry. Nízká rizika jsou taková, která mají nízký dopad i pravděpodobnost a u takových rizik žádné kroky k jejich eliminaci neprovádíme. Další skupinou jsou střední rizika, která se řeší po vyřešení rizik vysokých. Vysoká rizika jsou taková rizika s velkým dopadem i velkou pravděpodobností výskytu a musí se řešit ihned. (Aptien.com, 2023; wolterskluwer.com, ©2024)

V tabulce 2 je zobrazen přehled stanovených stupnic dopadu a pravděpodobnosti rizik, kterými byli posuzovaný jednotlivá rizika. Dopad na zkoumaný problém je dle stupnice malý, mírný, střední, významný nebo kritický. Co se týče pravděpodobnosti vzniku či rozvinutí daného rizika je stanovena od jedné do pěti jako velmi malá, malá, střední, velká a velmi velká.

*Tabulka 2 Přehled stanovených stupnic dopadu a pravděpodobnosti rizika. (zdroj: vlastní zpracování)*

| Stupnice | Dopad | Pravděpodobnost |
|---|---|---|
| **1** | malý | velmi malá |
| **2** | mírný | malá |
| **3** | střední | střední |
| **4** | významný | velká |
| **5** | kritický | velmi velká |

V tabulce 3 je zobrazena matice rizik, která rozděluje výslednou hodnotu rizika do třech kategorií na rizika nízká, střední a vysoká. Hodnota 1–9 je určena pro nízká rizika označena zelenou barvou, hodnoty 10–19 pro rizika střední označena žlutou barvou a hodnoty 20–25 jsou rizika vysoká označena červenou barvou. Tato tabulka se barevně prolíná s tabulkou 4 (viz. níže).

*Tabulka 3 Matice rizik – rizika nízká, střední a vysoká. (zdroj: vlastní zpracování)*

Matice rizik – tabulka

| Pravděpodobnost | | | | | | |
|---|---|---|---|---|---|---|
| 5 | 5 | 10 | 15 | 20 | 25 | |
| 4 | 4 | 8 | 12 | 16 | 20 | |
| 3 | 3 | 6 | 9 | 12 | 15 | |
| 2 | 2 | 4 | 6 | 8 | 10 | |
| 1 | 1 | 2 | 3 | 4 | 5 | |
| | 1 | 2 | 3 | 4 | 5 | |
| | | | Dopad | | | |

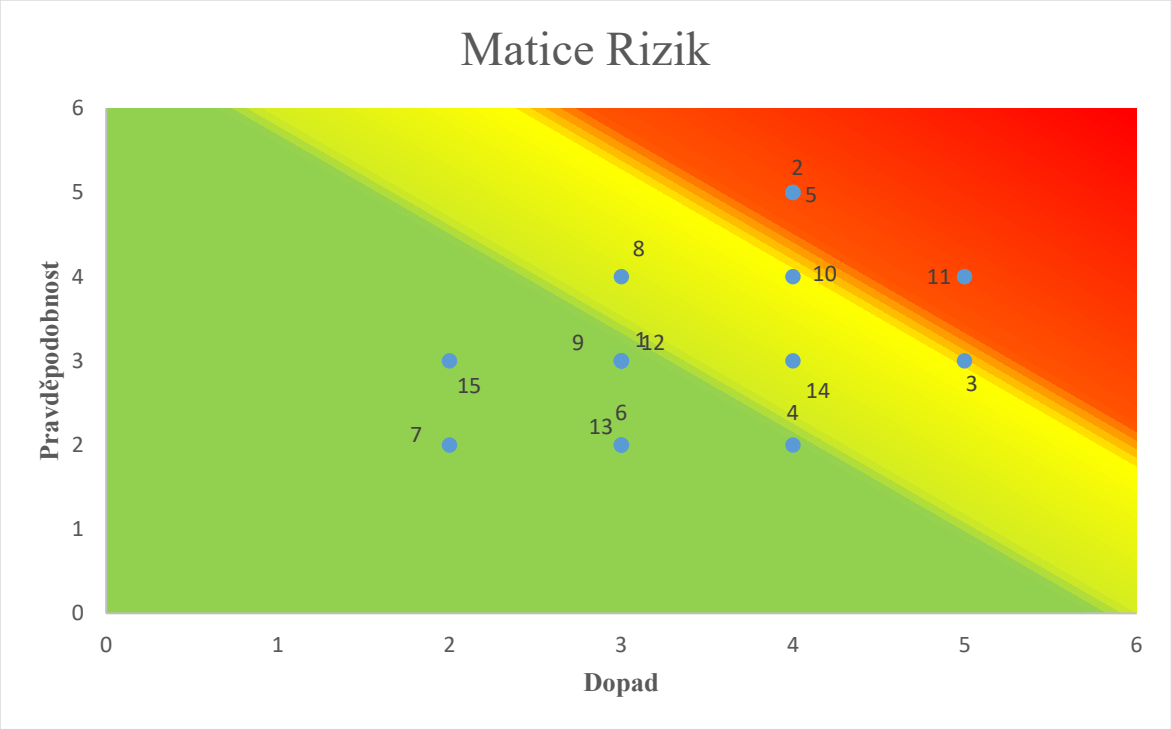
Jednotlivá rizika byla posuzována z pohledu jejich dopadu a pravděpodobnosti. Značka *„D“* značí dopad, značka *„P“* značí pravděpodobnost a značka *„R“* výslednou hodnotu rizika. Rizika stanovené v Ishikawa digramu na obrázku 3 byly hodnoceny podle stupnice dopadu a pravděpodobnosti v tabulce 2. Celkové hodnocení rizik je zobrazeno v tabulce 4. Hodnota přiřazeného dopadu a hodnota přiřazené pravděpodobnosti se mezi sebou vynásobí a vyjde výsledná míra rizika.

*Tabulka 4 Matice rizik. (zdroj: vlastní zpracování)*

| Pořadové číslo | Kategorie | Příčina | D | P | R |
|---|---|---|---|---|---|
| **1** | Stroje | Nedostatečná technická infrastruktura pro rychlou a spolehlivou distribuci informací. | 3 | 3 | 9 |
| **2** | Stroje | Neefektivní systémy monitorování a filtrování šíření dezinformací. | 4 | 5 | 20 |
| **3** | Stroje | Nedostatečná kybernetická bezpečnost. | 5 | 3 | 15 |
| **4** | Lidé | Nedostatečně proškolený personál v oblasti detekce a vyvracení dezinformací. | 4 | 2 | 8 |
| **5** | Lidé | Nedostatečná mediální gramotnost veřejnosti. | 4 | 5 | 20 |

| Pořadové číslo | Kategorie | Příčina | D | P | R |
|---|---|---|---|---|---|
| **6** | Lidé | Nedostatečné povědomí o důsledcích šíření dezinformací. | 3 | 2 | 6 |
| **7** | Materiály | Nedostatek zdrojů s ověřenými informacemi. | 2 | 2 | 4 |
| **8** | Materiály | Nedostatečný přístup k aktualizovaným datům a informacím v reálném čase. | 3 | 4 | 12 |
| **9** | Materiály | Nedostatek propagačních materiálů a zdrojů pro podporu důvěryhodných zpráv. | 3 | 3 | 9 |
| **10** | Metody | Neúčinné strategie osvěty veřejnosti o rizicích dezinformací. | 4 | 4 | 16 |
| **11** | Metody | Šíření dezinformací prostřednictvím sociálních médií. | 5 | 4 | 20 |
| **12** | Metody | Absence standardizovaných postupů pro reakci na dezinformace a falešné zprávy. | 4 | 3 | 12 |
| **13** | Měření | Nedostatečné vyhodnocení účinnosti komunikačních kampaní v boji proti dezinformacím. | 3 | 2 | 6 |
| **14** | Měření | Absence jasně definovaných ukazatelů důvěry veřejnosti v informační kanály a orgány ochrany obyvatelstva. | 3 | 3 | 9 |
| **15** | Měření | Nedostatečný sběr a analýza dat o reakcích veřejnosti na různé typy informací při MU. | 2 | 3 | 6 |

Podle tabulky 4 matice rizik vyšlo 8 příčin s nízkým rizikem, 4 příčiny jako střední riziko a 3 příčiny s vysokým rizikem, u kterých je nutné navrhnout opatření k okamžitému zlepšení. Rizika jsou také graficky zobrazena na obrázku 4 v mapě matice rizika, kde vystupují pod pořadovým číslem.




*Obrázek 4 Mapa matice rizik. (zdroj: vlastní zpracování)*

**Dílčí závěr kapitoly 7**: Ishikawa diagram byl využit pro určení možných příčin zkoumaného problému – ztráta důvěry veřejnosti v informační kanály a systém ochrany obyvatelstva. Jednotlivá rizika byla dále posuzována podle jejich dopadu a pravděpodobnosti. Rizika, kterým je dle své hodnoty přiřazena zelená barva, jsou rizika nízká. Tato rizika nepotřebují okamžité nebo zvláštní opatření k jejich snižování. Rizika označena žlutou barvou mají střední závažnost a měla by být přijata opatření ke zlepšení – riziko č. 3, 8, 10 a 12. Rizika označena červenou barvou jsou vysoká rizika, která potřebují okamžité ošetření a musí být přijata opatření k jejich snížení. Vysokými riziky jsou – č. 2 *„neefektivní systémy monitorování a filtrování šíření dezinformací“,* č. 5 *„nedostatečná mediální gramotnost veřejnosti“* ač. *11 „šíření dezinformací prostřednictvím sociálních sítí“*. Jednotlivá navržená opatření jsou určena v kapitole 9.

# 8 DOTAZNÍKOVÉ ŠETŘENÍ

Dotazníkové šetření je metoda terénního sběru informací, ve kterém se potřebná data získávají od oslovených osob prostřednictvím předem daných otázek. Dotazníkové šetření je charakterizována několika znaky – *„odpovědi jsou získávány zprostředkovaně prostřednictvím subjektivních odpovědí, není zde přímá interakce mezi výzkumným pracovníkem a respondentem a je to metoda vysoce standardizovaná a formalizovaná“.* Výhodou dotazníkového šetření je právě nepřímá interakce výzkumníka s tázanou osobou, jelikož to respondentovi dává větší důvěru v anonymitu šetření a nemůže dojít ke kladení sugestivních nebo nejednoznačných otázek od výzkumného pracovníka. Také je velkou výhodou, že prostřednictvím dotazníku můžeme za relativně krátký čas získat data od velkého počtu jedinců, i přesto, že jsou respondenti rozptýlení na velkém prostoru. Nevýhodou této metody je, že odpovědi respondentů mohou být zkresleny. To může být například tím, že respondent neodpoví pravdivě, nepochopí otázku nebo pokud není o problematice informován. (Disman, 2018)

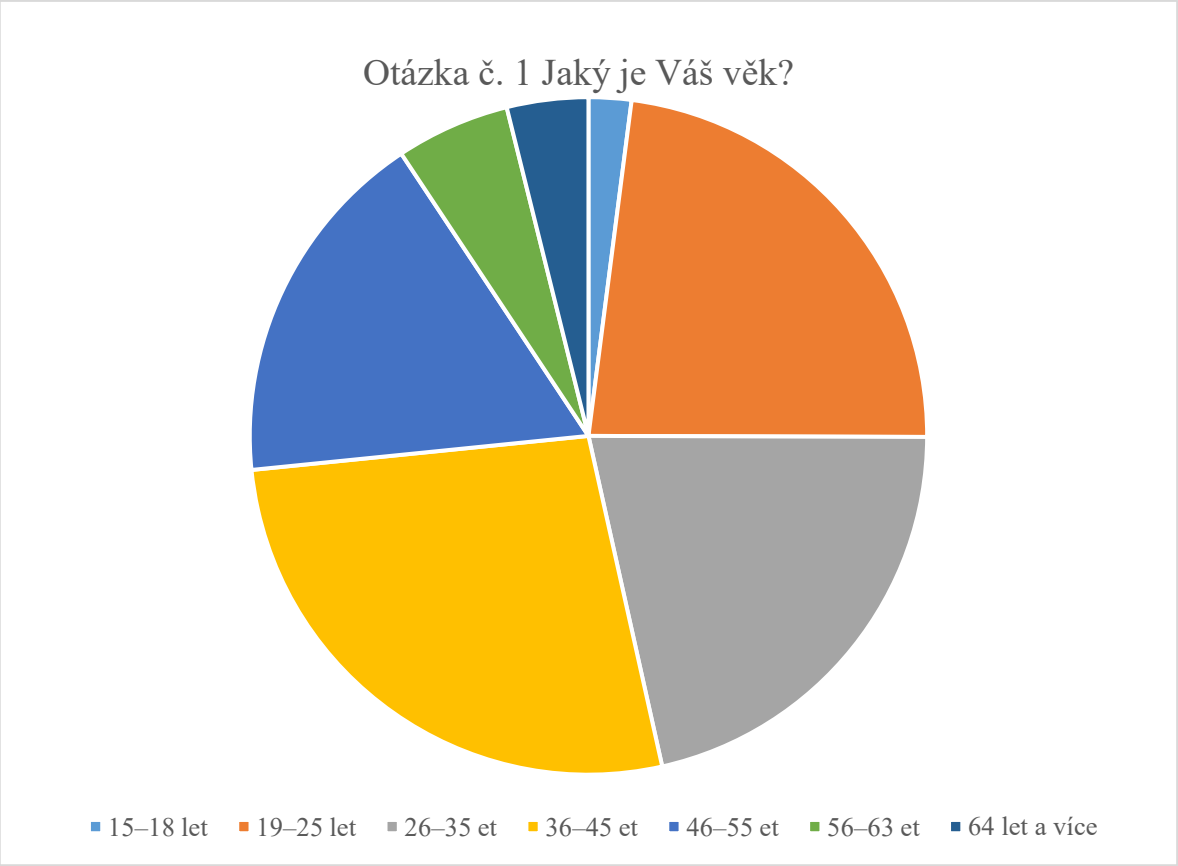
Výzkumná otázka: Jaké je povědomí obyvatelstva České republiky o oblasti dezinformací?

Cíle výzkumu: zjištění informací od obyvatelstva České republiky o jejich povědomí v oblasti dezinformací a mediální gramotnosti.

Dotazníkové šetření probíhalo v období od 9. března 2024 do 9. dubna 2024. Dotazník byl vytvořen v Google Forms v elektronické podobě a respondenti byli oslovování prostřednictvím sociálních sítí Facebook a Instagram. Dotazník vyplnilo celkem 376 respondentů. Dotazník je složen z 15 povinných otázek a 1 nepovinné otázky, která navazovala na povinnou otázku. Celkem dotazník obsahuje 16 otázek. Dotazník zahrnuje 9 uzavřených otázek, 3 polouzavřené otázky a 4 otevřené otázky. První tři otázky se zaměřují na získání dat o respondentech – jejich věk, pohlaví a dosažené vzdělání. První sada otázek se soustředí na sběr dat o povědomí v dané problematice, odkud termín dezinformace znají, prvním setkání s tímto pojmem, zda si asociují tento pojem i s jinými termíny a otázky se také týkají mediální gramotnosti dotázaných. Druhá část otázek se zaměřuje především na názory respondentů na danou problematiku a boj proti dezinformacím v České republice.

**Otázka č. 1 Jaký je Váš věk?** (uzavřená otázka)

Věkové rozpětí bylo rozděleno do 7 kategorií, viz. obrázek 5 V procentech bylo zastoupení 15–18 let (2,1 %), 19–25 let (23,7 %), 26–35 let (22,1 %), 36–45 let (27,7 %), 46–55 let (17,8 %), 56–63 let (5,6 %) a 64 let a více (4 %). Věkové zastoupení respondentů bylo více méně vyvážené, především v kategoriích 19–25 let, 26–35 let, 36–45 let a 46–55 let.




*Obrázek 5 Graf k otázce č. 1 Jaký je Váš věk? (zdroj: vlastní zpracování)*

**Otázka č. 2 Jste žena nebo muž?** (uzavřená otázka)

Dotazníkového šetření se zúčastnilo celkem 73,4 % žen a 26,6 % mužů.

**Otázka č. 3 Jaké je Vaše nejvyšší dosažené vzdělání? (**uzavřená otázka)

Záměrem této otázky je zjisti nejvyšší dosažené vzdělání dotázaného kvůli následnému porovnání s dalšími otázkami. Vzdělání je často zmiňováno v souvislosti s odolností a schopností rozlišit falešné informace od pravdivých. Ve strategických cílech je zmiňováno, že důležitým aspektem v boji proti informačním hrozbám je právě vzdělanost obyvatel, a také se šíří názor, že vysoce vzdělaný člověk má vyšší předpoklad pro úspěšné rozlišování manipulativního obsahu a takový občan je méně náchylný k podléhání lžím a falešným zprávám. Tato tvrzení budou na konci této kapitoly prověřena porovnáním otázky 3 s otázkou 9 a otázkou 15. Největší zastoupení v nejvyšším dosaženém vzdělání měli respondenti střední školu s maturitní zkouškou (45,5 %), následovalo vysokoškolské vzdělání (35,4 %), dále pak střední s vyučením (9,8 %), vyšší odborné vzdělání (5,3 %) a základní vzdělání (4 %).

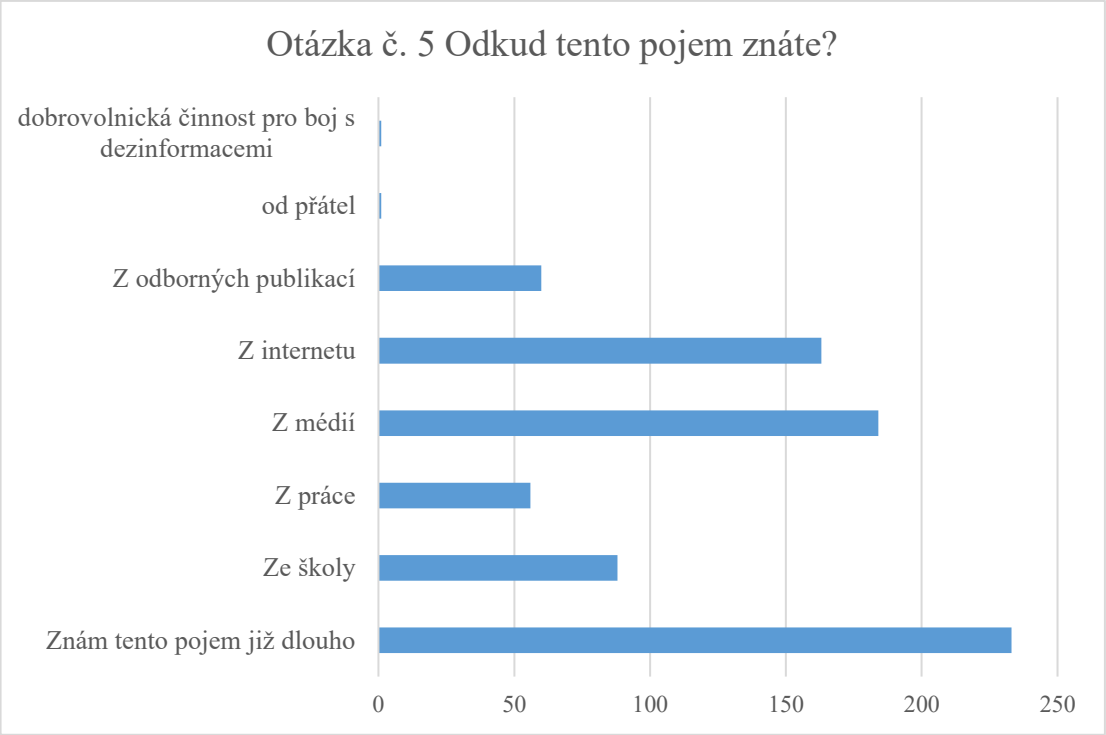

*Obrázek 6 Graf k otázce č. 3 Jaké je Vaše nejvyšší dosažené vzdělání? (zdroj: vlastní zpracování)*

**Otázka č. 4 Znáte pojem dezinformace?** (uzavřená otázka)

Záměrem této otázky je zjistit, zda respondent zná termín dezinformace či nikoli. Pojem dezinformace zná 98,1 % respondentů (369 osob) a 1,9 % (7 osob), pojem dezinformace nezná.

**Otázka č. 5 Pokud ano, odkud tento pojem znáte?** (nepovinná polouzavřená otázka)

Otázka navazuje na předchozí otázku č. 4 *„Znáte pojem dezinformace?“*. V této otázce mohli respondenti zaškrtnou více odpovědí, odkud pojem *„dezinformace“* znají nebo bylo umožněno v poli *„jiné“* odpovědět podle sebe, co v nabídce respondentovi chybělo. Nejvíce odpovědí (celkem 233) bylo, že dotázaný zná tento pojem již dlouho. Dále pak tento pojem znají z médií (184 odpovědí), z internetu (163 odpovědí), ze školy (88 odpovědí), z odborných publikací (60 odpovědí), z práce (56 odpovědí) nebo od přátel (1 odpověď) a dobrovolnická činnosti pro boj s dezinformacemi (1 odpověď).




*Obrázek 7 Graf k otázce č. 5 Odkud tento pojmem znáte? (zdroj: vlastní zpracování)*

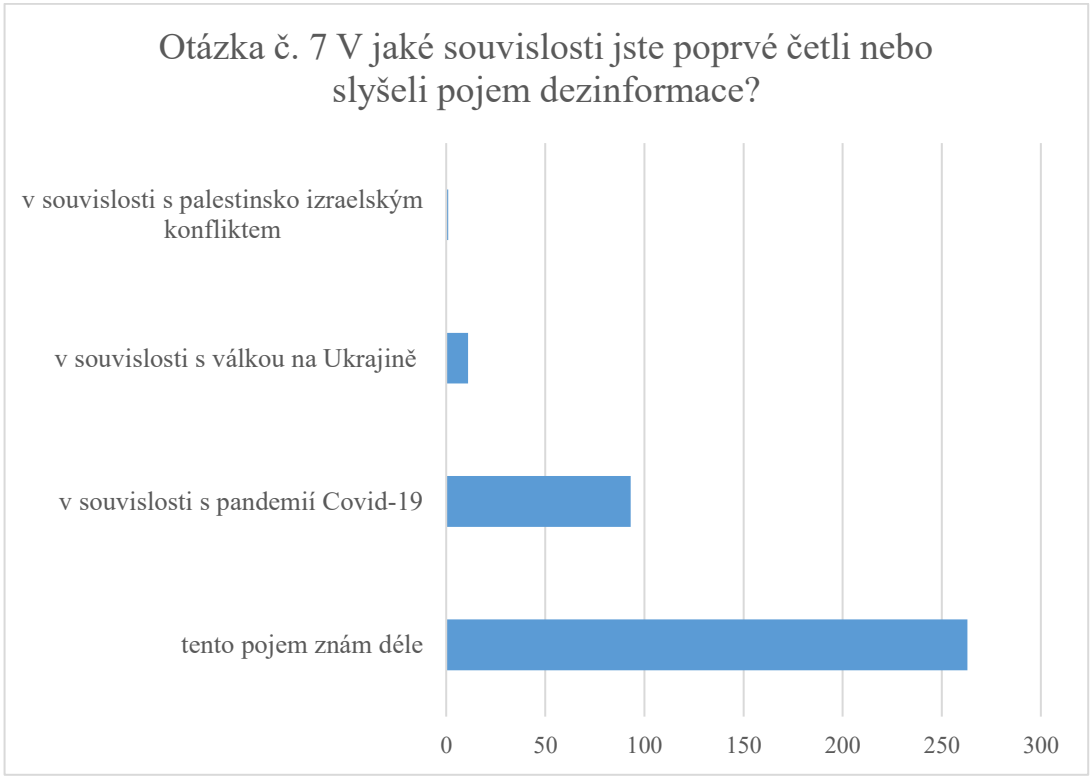
**Otázka č. 6 Znáte některé další pojmy, které mohou souviset s pojmem dezinformace? Vypište je.** (otevřená otázka)

Tato otázka byla do dotazníkového šetření zahrnuta z důvodu ověřit, zda si dokáží lidé s pojmem dezinformace spojit i některé další termíny používané v této oblasti. Předpokladem bylo, že si lidé dezinformace spojují s termínem *„fake news“*, *„propaganda“*, *„deepfake“*, *„lži a manipulace“* a *„hoax“*. Nejčastější odpovědí byly pojmy *„hoax“*, *„fake news“*, „*propaganda*“ a *„misinformace“*. Velmi často zmiňovali manipulace a lži, ale také se hojně objevoval pojem *„maliinformace“*. Často asociovaným termínem byly dezinformační weby, dezinformátor a hybridní válka. Dotázaní si dezinformace spojují také s panikou, vyvoláváním strachu, ohýbáním pravdy, neinformovaností a nevědomostí nebo anarchismem. V odpovědích zazněla také kyberkriminalita, AI (z angl. *„artificial intelligence“*, česky umělá inteligence) a *„deepfake“*. Někteří respondenti pochopili otázku jinak a odpověděli *„greendeal“*, *„plochozemci“* nebo *„antivaxer“*. Celkem 58 respondentů na otázku neodpovědělo nebo napsalo, že neví.

**Otázka č. 7 V jaké souvislosti jste poprvé četli nebo slyšeli pojem dezinformace?** (polouzavřená otázka)

Tato otázka se zaměřovala na zjištění, v jaké souvislosti se respondent poprvé setkal s pojmem dezinformace. Bylo na výběr z několika odpovědí a také možnost „jiné“, kam mohl

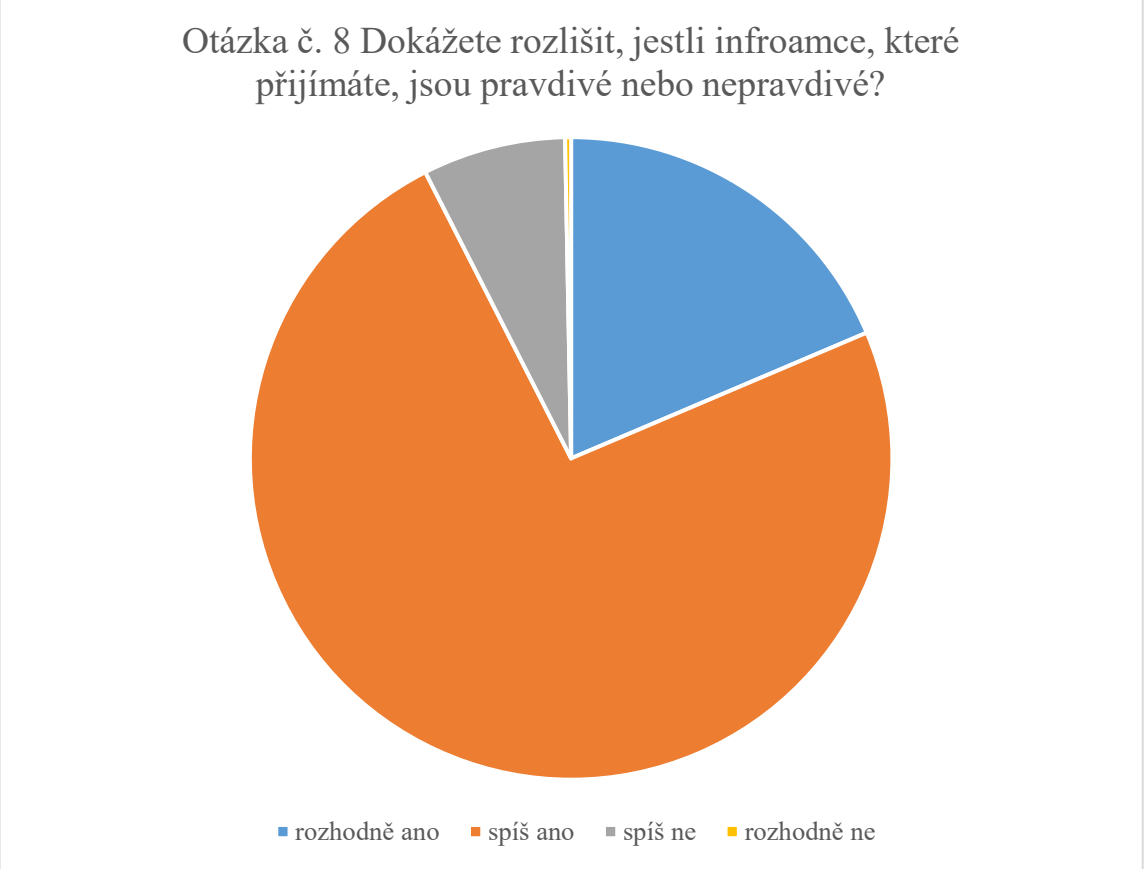
respondent napsat svou odpověď, která mu chyběla v předem dané nabídce. Celkem 263 dotázaných tento pojem zná delší dobu, 93 respondentů se s tímto pojmem poprvé setkalo během pandemie Covid-19, 11 dotázaných dezinformace poprvé slyšelo v souvislosti s válkou na Ukrajině a jeden respondent pak v souvislosti s palestinsko-izraelským konfliktem. V poli „jiné“ byly pak odpovědi následovné – v souvislosti s politikou v Americe (1 odpověď), migrační krize v roce 2015 a Syrská občanská válka (1 odpověď), anexe poloostrova Krym (2 odpovědi), vláda Petra Fialy (1 odpověď), volby (1 odpověď), „*s oficiálním určením vedoucí role KSČ ve společnosti před rokem 89´“* (1 odpověď) a vzdělávání dospělých (1 odpověď).




*Obrázek 8 Graf k otázce č. 7 V jaké souvislosti jste poprvé četli nebo slyšeli pojem dezinformace? (zdroj: vlastní zpracování)*

**Otázka č. 8 Dokážete rozlišit, jestli informace, které přijímáte jsou pravdivé nebo nepravdivé?** (uzavřená otázka)

Záměrem této otázky bylo zjistit, zda respondenti zvládnou rozlišit přijímané falešné informace od těch pravdivých. Celkem 18,6 % dotázaných dokáže rozhodně rozlišit, zda jsou informace, které přijímají, pravdivé nebo ne. Spíše dokáže rozlišit takové informace 73,9 % respondentů, spíše nedokáže rozlišit celkem 7,2 % dotázaných a 0,3 % rozhodně nedokáže rozlišit pravdivé a falešné informace.



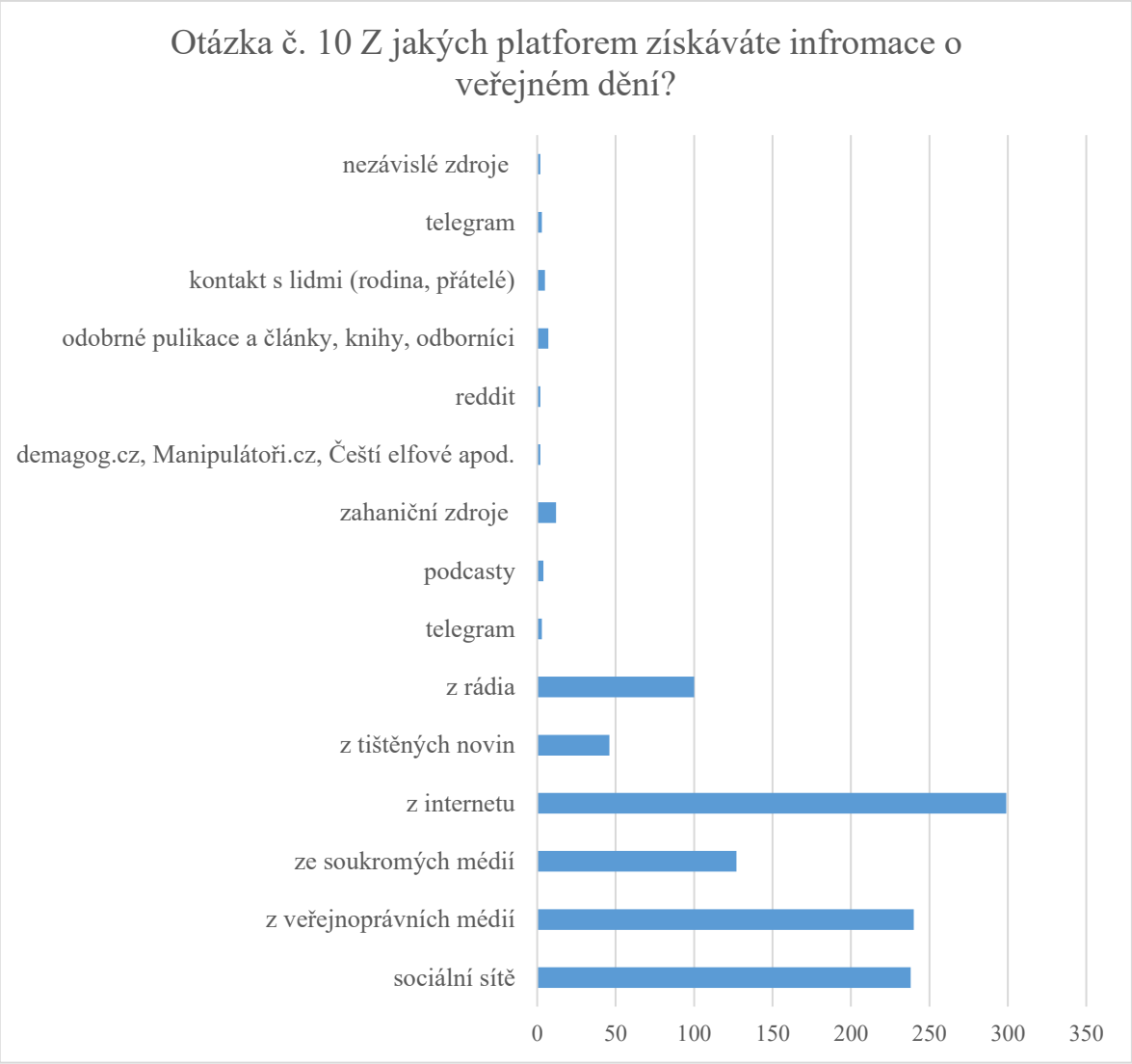

*Obrázek 9 Graf k otázce č. 8 Dokážete rozlišit, jestli informace, které přijímáte, jsou pravdivé nebo nepravdivé? (zdroj: vlastní zpracování)*

**Otázka č. 9 Ověřujete si informace, které přijímáte, z více zdrojů?** (uzavřená otázka)

Cílem této otázky bylo zjistit, zda si respondenti ověřují přijímané informace z více zdrojů či nikoliv. Tato otázka souvisí s mediální gramotností veřejnosti a 93,1 % respondentů (350 osob) si informace ověřuje z více zdrojů a 6,9 % (26 osob) si informace neověřuje.

**Otázka č. 10 Z jakých platforem získáváte informace o veřejném dění?** (polouzavřená otázka)

Cílem otázky bylo zjistit, které platformy dotázaní nejčastěji využívají jako svůj zdroj informací. Na výběr bylo z 6 předem daných odpovědí a byla otevřená odpověď „jiné“, kam mohli respondenti dopsat odpověď, která jim v základním výběru chyběla. Odpovědi v otázce č. 10 byly zaškrtávací, takže dotázaný mohl vybrat více odpovědí. Nejvíce respondenti získávají informace z internetu (299 odpovědí), veřejnoprávních médií (240 odpovědí) a sociálních sítí (238 odpovědí). Dále pak dotázaní získávají informace ze soukromých médií a rádia, tištěných novin a v poli *„jiné“* pak respondenti uvedli, že získávají informace primárně ze zahraničních zdrojů (BBC, The Guardian, CNN, New York Times) a odborných publikací.

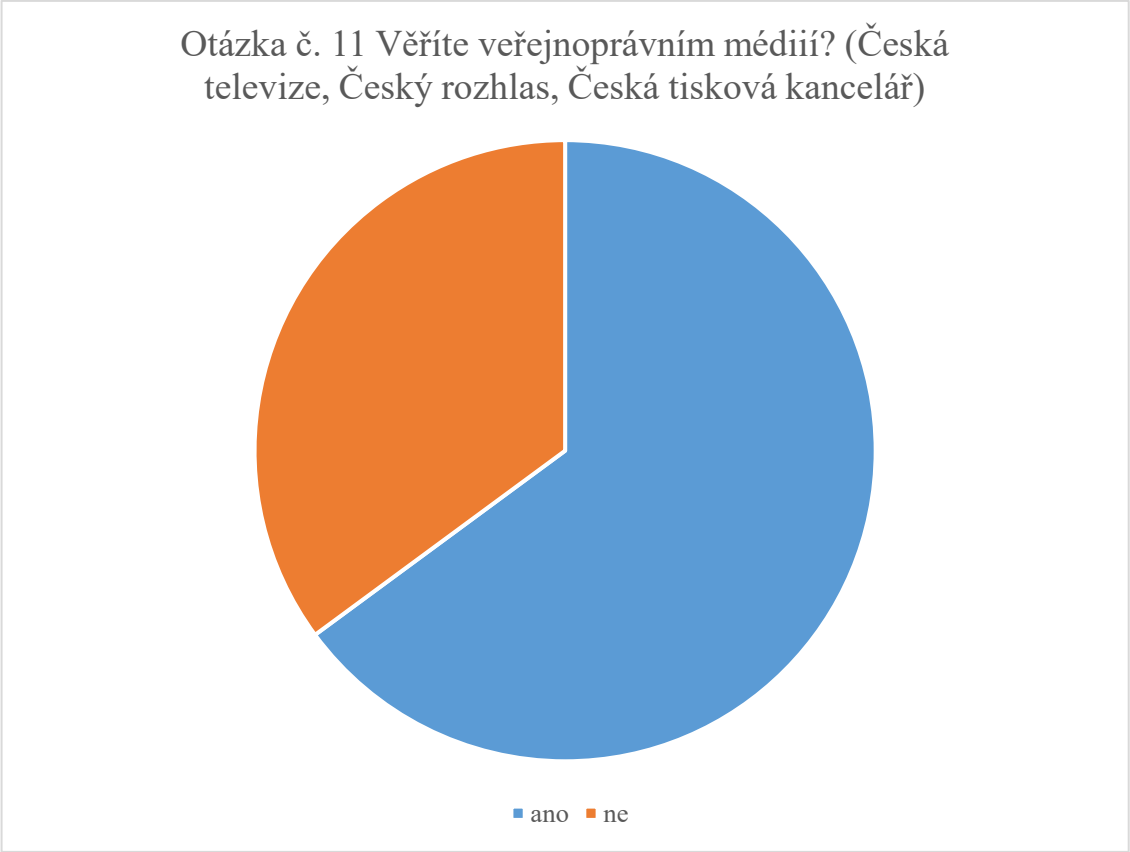



*Obrázek 10 Graf k otázce č. 10 Z jakých platforem získáváte informace o veřejném dění? (zdroj: vlastní zpracování)*

**Otázka č. 11 Věříte veřejnoprávním médiím?** (Česká televize, Český rozhlas, Česká tisková kancelář) (uzavřená otázka).

Záměrem této otázky bylo zjistit, jestli respondenti věří veřejnoprávní médiím v České republice, jelikož tato média jsou hlavním zdrojem ověřených informací během mimořádných událostí.

Celkem 64,9 % (244 osob) věří veřejnoprávním médiím a 35,1 % (132 osob) ne. Výzkum důvěry české veřejnosti v Českou televizi zveřejněný ve Výroční zprávě České televize za rok 2023 byla důvěra veřejnosti 65 %. Podle získaných dat v tomto dotazníkovém šetření 64,9 % důvěry ve veřejnoprávní média odpovídají získaným datům přímo od České televize.




*Obrázek 11 Graf k otázce č. 11 Věříte veřejnoprávní médiím (Česká televize, Český rozhlas, Česká tisková kancelář)? (zdroj: vlastní zpracování)*

**Otázka č. 12 Proč jim věříte/nevěříte?** (otevřená otázka)

Otázka č. 12 navazuje na předchozí otázku č. 11 ohledně důvěry ve veřejnoprávní média. Cílem této otázky bylo zjistit, proč respondent těmto médiím věří nebo proč v ně nemá důvěru

Respondenti veřejnoprávním médiím věří nejčastěji proto, že si tato média ověřují informace, mají velké zkušenosti se zpravodajstvím a mají své know-how i historii. Těmto médiím věří, protože jim přijdou důvěryhodné a nezávislé a jsou financovány veřejností, takže mají zodpovědnost za poskytování korektních informací. Jejich zpravodajství je vyvážené, pracují zde profesionální, inteligentní a vzdělaní reportéři i další zaměstnanci a zachovávají si svou úroveň. Kontrola a ověřování informací v těchto médiích je na vysoké úrovni a jejich práce je dozorována. Pokud uveřejní nějaké nepravdivé nebo neúplné informace, vždy obratem vše uvedou na pravou míru a omluví se za chybu. Informace zveřejněné v těchto médiích se dají nezávisle ověřit na jiných tuzemských i zahraničních platformách. Respondenti těmto médiím věří také proto, že jsou státní, základem důvěry ve stát, podléhají zákonům a jsou vázány pravidly pro zpravodajství a mají svůj kodex, je to základ pro ověřování

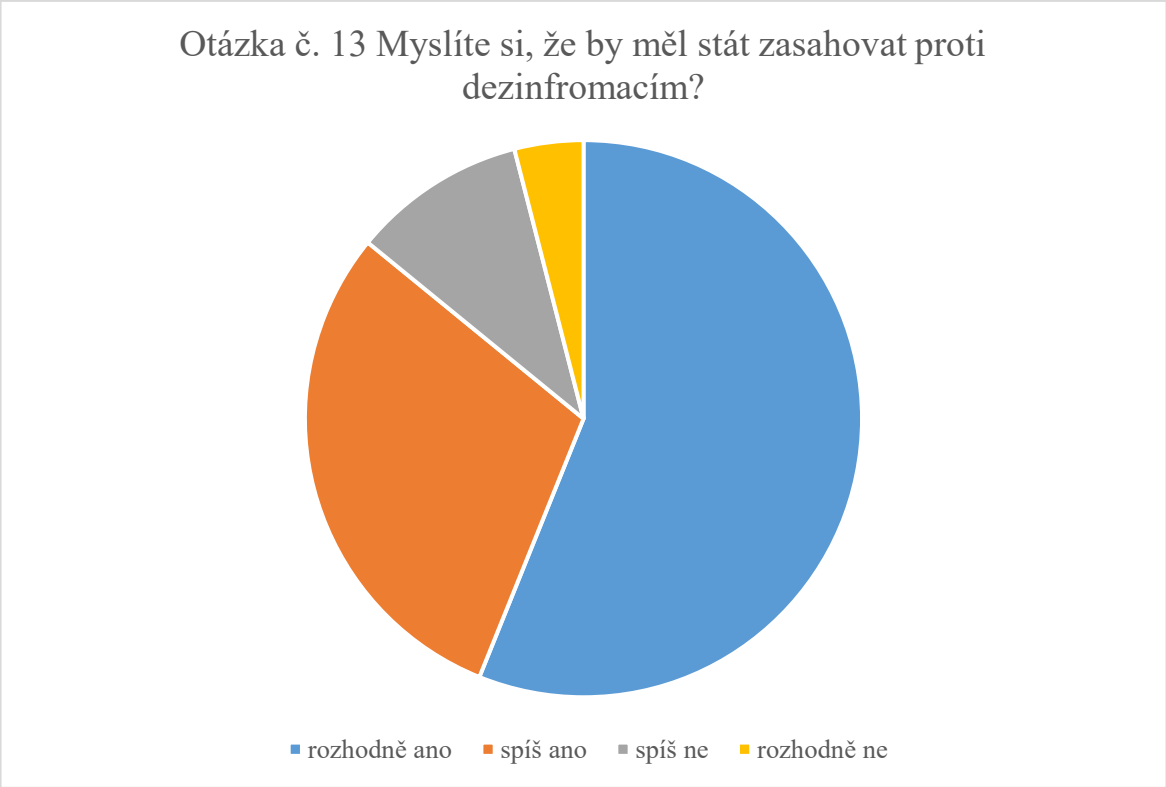
informací odjinud a podávají přesné a nezabarvené informace. Jednou z odpovědí také bylo, že jsou veřejnoprávní média důležitá pro bezpečnost státu a vždy udávají zdroj informace a vše se dá nezávisle ověřit. Věří také proto, že se domnívají, že se v těchto médiích nešíří dezinformace a čerpají z oficiálních tiskových agentur.

Respondenti také uváděli, že těmto médiím sice věří, ale ověřují si informace na jiných platformách (tuzemských i zahraničních), anebo jim věří *„tak na půl“, věří „jen něco a částečně“* a *„jak kdy“*.

Respondenti veřejnoprávním médiím nevěří nejčastěji z důvodu, že tato média nejsou důvěryhodná, jsou zaujatá, neobjektivní, neodráží realitu, zveřejňují zkreslené informace, lžou, popisují události pouze z jedné strany a nedodávají celý kontext (například co se stalo před tím), jsou nevyvážená, jsou provládní a zveřejňují pouze to, co se jim hodí. Těmto médiím nevěří také z důvodu, že dělají tzv. „*z komára velblouda*“, manipulují s veřejností a jejich názory, zkrášlují si svou pravdu, jejich informace jsou chybné, přibarvují si informace pro sledovanost, velmi často jsou jejich reportáže negativní a zaměřují se na emoce veřejnosti. Některé odpovědi také uvádí, že veřejnoprávní média záměrně vyvolávají paniku, nafukují nepravdivé informace, jsou zaprodaní, jsou řízeny státem, zatajují a nesdělují důležité informace a jejich pravda je vždy „*tak na půl cesty*“. Někteří respondenti veřejnoprávní média označují přímo za dezinformátory, anebo že jsou pro dezinformace tato média využívána či dezinformace šíří a veřejnost jenom straší. Novináři jsou podle některých odpovědí nevzdělaní, je zde rozsáhlá korupce a šíří jednostrannou propagandu. Respondenti také odpovídají, že od dob pandemie Covid-19 těmto veřejnoprávním médiím nevěří a spíše se jim v současné době vyhýbají, protože se nechtějí zahlcovat informacemi. Jeden respondent dokonce odpověděl, že od té doby, co nesleduje zpravodajství, tak se cítí mnohem lépe, protože má pocit, že jsou všechny poskytované informace negativní. Stejně jako u respondentů, kteří veřejnoprávním médiím věří, tak ti, co v ně nemají důvěru, uvádějí, že věří jen něčemu.

**Otázka č. 13 Myslíte si, že by měl stát zasahovat proti dezinformacím?** (uzavřená otázka)

Záměrem této otázky bylo zjistit, jaký názor mají dotázaní na to, že by měl stát zasahovat a bojovat proti dezinformacím. Celkem 56,1 % (211) respondentů si myslí rozhodně ano, 29,8 % (112) spíše ano, 10,1 % (38) spíše ne a 4 % (15) si myslím, že by se stát v tomto boji rozhodně neměl angažovat.




*Obrázek 12 Graf k otázce č. 13 Myslíte si, že by měl stát zasahovat proti dezinformacím? (zdroj: vlastní zpracování)*

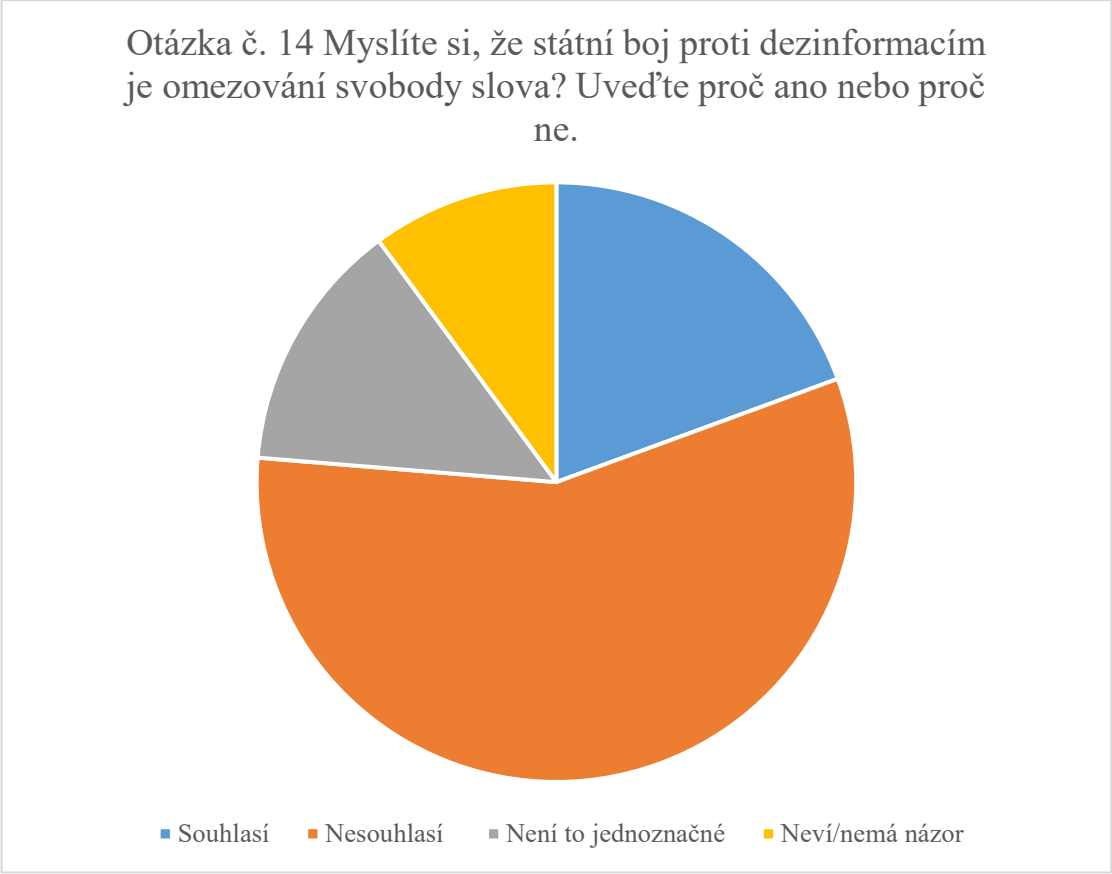
**Otázka č. 14 Myslíte si, že státní boj proti dezinformacím je omezování svobody slova? Uveďte proč ano nebo proč ne.** (otevřená otázka)

Otázka č. 14 navazuje na předchozí otázku č. 13 ohledně zasahování státu v boji proti dezinformacím. Cílem otázky bylo zjistit, jak respondenti vnímají státní boj proti dezinformacím a jestli je takový boj ze strany státu omezování svobody slova či nikoli, jelikož takový problém se vyskytl, když stát začal s dezinformacemi bojovat. Odpovědi jsou zobrazeny na koláčovým grafu na obrázku 13. Celkem 19,4 % respondentů souhlasí s tím, že je státní boj proti dezinformacím omezování svobody slova, 56,9 % dotázaných s tímto nesouhlasí, 13,6 % odpovědělo, že to není jednoznačné a je to tzv. „*tak na půl*“ a 10,1 % respondentů neví nebo nemá názor.

Nejčastějším odůvodněním, proč si respondent myslí, že státní boj proti dezinformacím je omezování svobody slova byl odkaz na Ústavu a Listinu základních práv a svobod, kde je deklarovaná svoboda slova a vyjádření názoru, a také na dezinformace není zákon ani paragraf. Někteří respondenti se obávají, že by takový zásah státu mohl vést k cenzuře a totalitě a stát by tedy neměl v této oblasti přímo zasahovat a určovat, kdo si má co myslet. Také si myslí, že výroky dříve označovány za dezinformace se dnes ukazují jako pravdivé.

Jiní respondenti ale mají názor, že státní boj by byl omezování svobody slova, ale je to nutné k potírání dezinformací. Zazněl zde také názor, že „*přímé omezování dezinformací jen podpoří jejich sílu*“, proto má tedy stát spíš systematicky vzdělávat obyvatelstvo a usměrňovat tok dezinformací, než je přímo potírat a zákoně trestat.

Důvodů, proč státní boj proti dezinformacím omezování svobody slova není, bylo mnoho. Především ten, že dezinformace nejsou názor, ale lži s účelem manipulovat společností a vytvářet nedůvěru veřejnosti ve státní instituce a „*svoboda jednoho končí tam, kde začíná svoboda druhého*“. Dezinformace podle této skupiny ohrožují bezpečnost státu, vyvolávají paniku a je proto nutné je regulovat. Taková regulace se nedá brát za omezování svobody slova, ale naopak jako chránění práv všech občanů. Dále si myslí, že tento boj je naopak důležitý pro zabránění šíření dezinformací a je to součást bezpečnostní politiky státu a systému vzdělávání a je to zásah proti systematické hybridní válce. Je důležité, aby všechny informace byly tříděné a ověřované a oblast dezinformací by měla být zahrnuta v právních normách. Jeden respondent si také myslí, že boj proti dezinformacím v České republice není dostatečný.

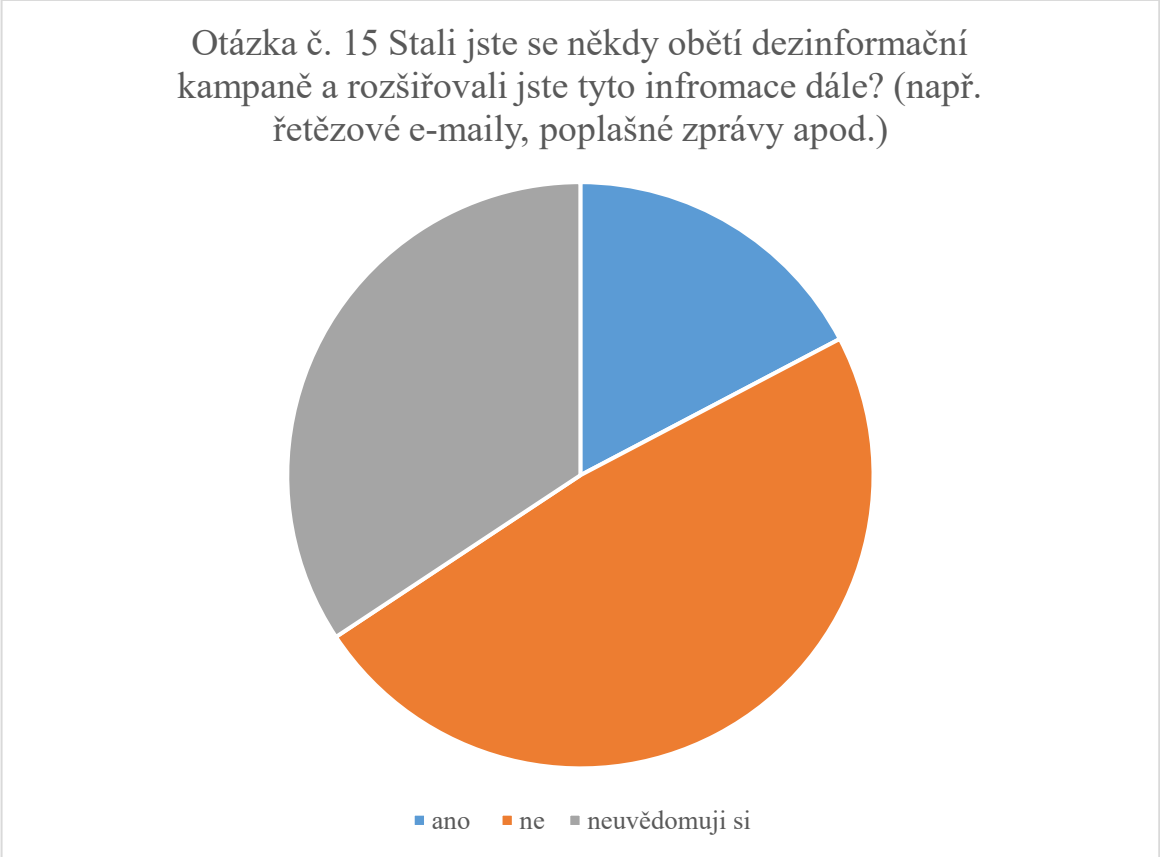



*Obrázek 13 Graf k otázce č. 14 Myslíte si, že státní boj proti dezinformacím je omezování svobody slova? Uveďte proč ano nebo proč ne. (zdroj: vlastní zpracování)*

Dotázaní zařazeni do skupiny „není to jednoznačné“ mají takový názor, že by stát neměl dezinformace omezovat, ale regulovat skrz vzdělávací a osvětovou činnost. Dalším názorem bylo, že za účelem ochrany bezpečnosti to omezování svobody slova není, ale v politických kruzích a dění ve státě by to omezování už mohlo být. Respondenti v této skupině jsou toho názoru, že by takový státní boj proti dezinformací měl být spíš formou zvyšování mediální gramotnosti, kritického myšlení u obyvatelstva a účinnou strategickou komunikací státu. V tomto případě by to omezování svobody slova nebylo.

**Otázka č. 15 Stali jste se někdy obětí dezinformační kampaně a rozšiřovali jste tyto informace dále? (např. řetězové e-maily, poplašné zprávy apod.)** (uzavřená otázka)

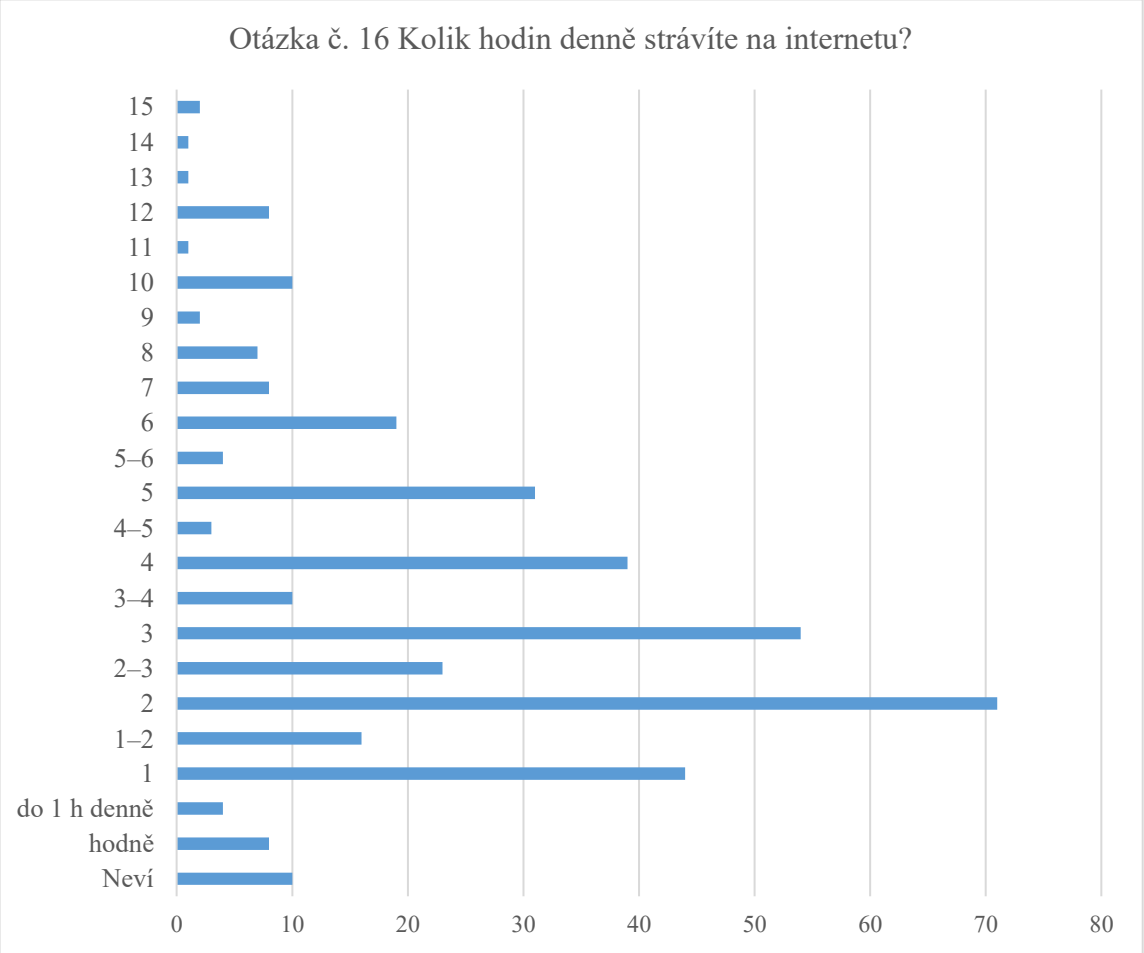
Záměrem této otázky bylo zjistit, jestli si respondenti uvědomují, že se stali či nestali součástí dezinformační kampaně nebo se s dezinformacemi přímo setkali. Celkem 17,3 % (65) odpovědělo, že se stali součástí takové kampaně, 48,4 % (182) ne a 34,3 % (129) si takovou skutečnost neuvědomuje. Poměrně mnoho respondentů, asi třetina dotázaných, si ani neuvědomuje, že mohli být někdy součástí nějaké dezinformační kampaně.




*Obrázek 14 Graf k otázce č. 15 Stali jste se někdy obětí dezinformační kampaně a rozšiřovali jste tyto informace dále? (např. řetězové e-maily, poplašné zprávy apod.)*

**Otázka č. 16 Kolik hodin denně průměrně strávíte na internetu?** (otevřená otázka)

Cílem této otázky bylo zjistit, kolik hodin dotázaní stráví na internetu, jelikož dezinformace se nejčastěji šíří právě přes tento kanál. Respondenti tráví na internetu od 20 minut denně až po 15 hodin za den. Průměrně ale stráví na internetu okolo 4 denně. Podle doplňkových odpovědí, které dotázaní přikládali ke svému konečnému číslu, jsou ty vyšší hodnoty strávených hodin na internetu často způsobeny tím, že internet potřebují k práci či studiu. Do grafu zobrazeném na obrázku 15 byly také zahrnuty odpovědí „*nevím*“ a „*hodně*“.




*Obrázek 15 Graf k otázce č. 16 Kolik hodin denně strávíte na internetu? (zdroj: vlastní zpracování)*

Ve společnosti se často spojuje odolnost proti manipulativnímu obsahu a vzdělanost. Z tohoto důvodu bude posouzena otázka č. 3 zahrnující nejvyšší dosažené vzdělání a další vybrané otázky. V otázce č. 9 se ptá, zda si respondent ověřuje informace z více zdrojů, či nikoliv. Celkem 6,9 %, tedy 26 osob si informace, které přijímá neověřuje z více zdrojů. Podle odpovědí bylo zjištěno, že si informace z více zdrojů neověřuje 42,3 % respondentů s nejvyšším dosaženým vzděláním – střední škola s maturitní zkouškou, 24,6 % respondentů s vysokoškolským vzděláním, 11,5 % střední škola s vyučením, 7,7 % s vyšším odborným

vzděláním a 3,8 % se základním vzděláním. Otázka č. 15 se ptá, zda byl dotázaných někdy obětí dezinformační kampaně. I tato otázka je porovnána s otázkou č. 3 nejvyššího dosaženého vzdělání. Celkem 65 respondentů odpovědělo, že se stalo obětí dezinformační kampaně. Celkem 44,6 % dotázaných má nejvyšší dosažené vzdělání střední škola s maturitní zkouškou, 43,1 % má vysokoškolské vzdělání, 6,2 % základní vzdělání, 3,1 % vyšší odborné vzdělání a 3,1 % střední škola s vyučením. Z porovnání těchto znaků vyplývá, že rozpoznání manipulativního obsahu, falešné zprávy a dezinformace nemusí souviset s vysokým vzděláním a obětí dezinformační kampaně a šíření takových informací se může stát i člověk, který je společností brán jako vysoce vzdělaný.

Porovnání otázky č. 4 „*Znáte pojem dezinformace*“ s otázkou č. 2 a 3 týkající se věku respondenta a jeho vzdělání. Celkem 7 respondentů odpovědělo, že pojem dezinformace nezná, z toho jsou 2 osoby ve věku 15–18 let, 3 osoby ve věku 19–25 let, 1 osoba ve věku 26–35 let a 1 osoba ve věku 56–63 let. Zajímavostí je, že všechny tyto osoby jsou ženy. Co se týče nejvyššího dosaženého vzdělání, tak 1 osoba má základní vzdělání, 2 osoby středoškolské s maturitní zkouškou a 4 osoby vysokoškolské vzdělání. Mohlo by se předpokládat, že osoby s vyšším vzděláním budou tento termín znát, ale podle získaných dat tomu tak není. Předpokládá se, že pojem dezinformace nebudou znát osoby ve vyšším věku, ale z těchto dat vyplývá, že termín neznají dotázaní především ve věkovém rozpětí 15–35 let.

**Dílčí závěr z dotazníkového šetření**: Z dat získaných prostřednictvím dotazníkového šetření u obyvatelstva České republiky bylo zjištěno, že oslovení znají pojem dezinformace a zvládnou ho asociovat i s jinými pojmy, které s touto oblastí souvisejí. Dále vyplývá, že si dotázaní ověřují informace u několika zdrojů, což je znakem dobré mediální gramotnosti. Ze získaných údajů také vyplývá, že první kontakt s termínem dezinformace se respondenti měli již dříve a znají tento pojem dlouho. Důvěru ve veřejnoprávní média má 64,9 % dotázaných, což odpovídá nejaktuálnějším datům České televize a jejich průzkumu důvěry v roce 2023, kde číslo dosahuje 65 %. Nadpoloviční důvěra v tyto média je důležitá, jelikož veřejnoprávní média jsou využívána k předávaní ověřených informací o probíhajících mimořádných událostech, takže důvěra občanů v tento informační kanál je důležitá. Ze získaných dat vyplývá, že si respondenti myslí, že by stát měl zasahovat proti dezinformacím, jelikož ohrožují bezpečnost státu, šíří paniku, manipulují s veřejností a myšlením občanů, polarizují společnost a přispívají ke zhoršování konfliktů ve společnosti a zvyšují nedůvěru ve veřejné instituce a systém. Tento boj proti dezinformacím by měl být prováděn především prostřednictvím osvětových a vzdělávacích činností a neměl by užívat přímou represi.

Podle údajů získaných v poslední otázce tráví dotázaní poměrně mnoho času na internetu. Časové rozpětí je od 1 hodiny denně, přes 5 hodin denně a sahá až k 15 hodinám denně. Po porovnání získaných dat mezi sebou bylo zjištěno, že obětí dezinformační kampaně může být i vysoce vzdělaný člověk, u kterého by se předpokládalo, že není tak ovlivnitelný. Zároveň znalost problematiky hrozeb a kybernetické bezpečnosti nezáleží na věku.

# 9 NÁVRHY ŘEŠENÍ

Na základě získaných dat z dotazníkového šetření, digramu rybí kosti a matice rizik bylo navrženo několik opatření ke zlepšení současného stavu.

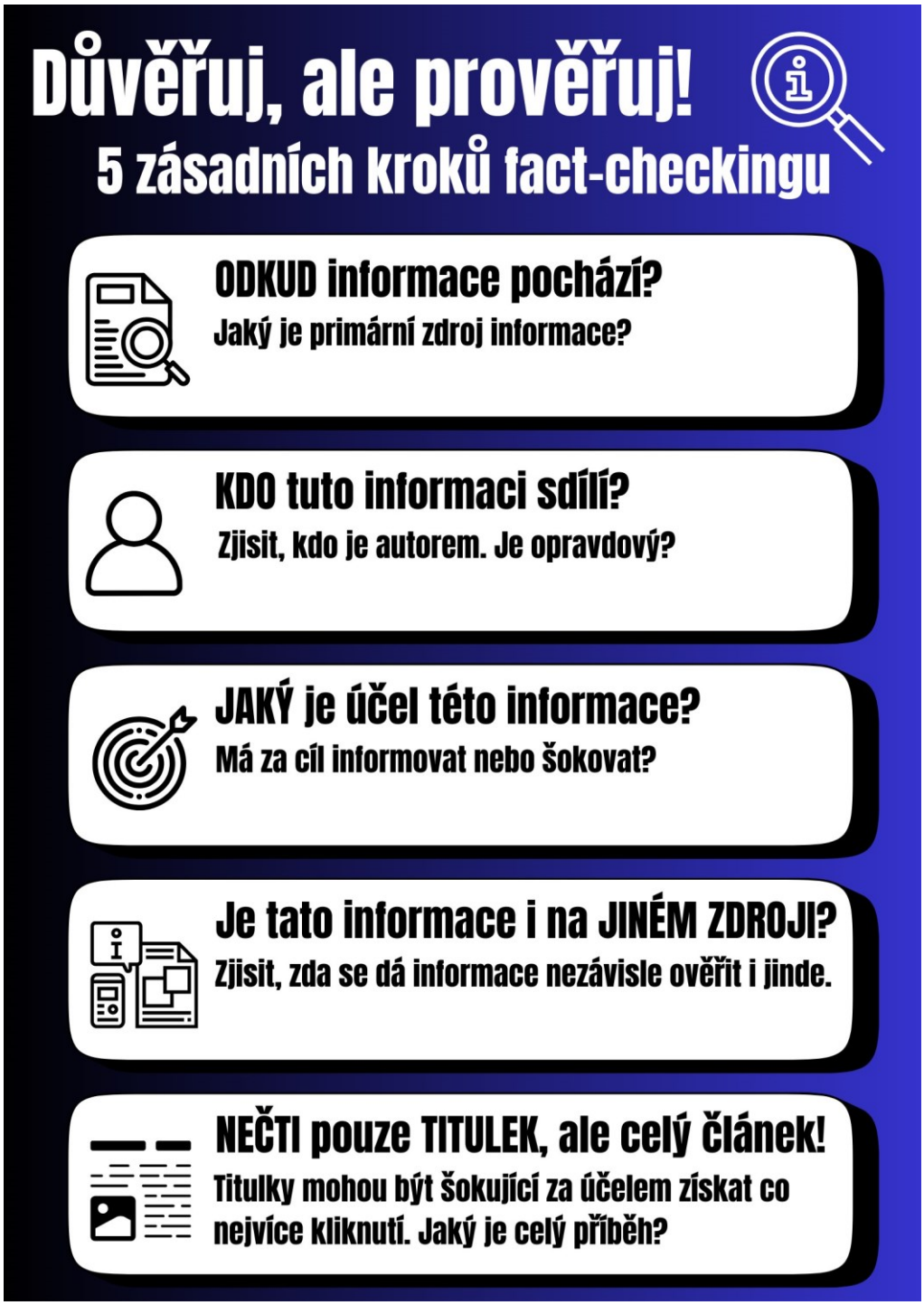
Na základě získaných poznatků o oblasti dezinformací bylo zjištěno, že základem boje proti dezinformacím je odolná společnost, která je mediálně gramotná a dokáže kriticky přemýšlet. Dezinformace cílí především na jedince či skupiny, které svým obsahem manipulují a zasívají do nich nenávist, nedůvěru nebo agresi. I přes to, že se dezinformační zpráva objasní a vyvrátí se její falešný obsah, i tak může vzbudit nedůvěru v cíl této falešné zprávy. Podle studie *„Šíření pravdivých a falešných informací online“* autora Vosoughi et al. (viz kapitola 5 teoretické části) se nepravdivé informace šíří mnohem rychleji než ty pravdivé, takže než k zacílené osobě dojde zpráva s pravdivým a vyvráceným obsahem, může být už pozdě. Tento obsah sdílí právě uživatelé sociálních sítí a internetu. Podle obrázku 1 (viz. kapitola 2 teoretické části) je pro kybernetickou bezpečnost základním pilířem odolná společnost. Odolná společnost, stát a kritická infrastruktura je také prvním ze tří strategických cílů České republiky v Národní strategii pro čelní hybridním hrozbám. Společnost a široká veřejnost je klíčovým faktorem pro boj s dezinformacemi, propagandu a působení manipulativního obsahu, jelikož takový obsah cílí právě na veřejnost, kterou má za cíl polarizovat a destabilizovat stávají systém státu, včetně její bezpečnosti. Proto je posilování odolnosti společnosti tak důležité. Základním faktorem pro to, aby veřejnost byla odolná je seznámit ji s takovým druhem hrozby, vysvětlit jí možné následky a jak takovým falešným informacím a manipulaci nepodlehnout.

Pro ošetření rizik z matice rizik v tabulce 5 byly nastaveny následující opatření. Jako opatření pro řešení rizika vysokého č. 2 *„Neefektivní systémy monitorování a filtrování šíření dezinformací.“*, a rizik středních č. 11 *„Šíření dezinformací prostřednictvím sociálních sítí.“* a č. 12 *„Absence standardizovaných postupů pro reakci na dezinformace a falešné zprávy.“* Pro opatření těchto středních a vysokých rizik je nutné, aby byl nastaven systém, který by se zaměřoval pouze na dezinformace, jejich šíření a dopady na společnost. Tento systém by měl obsahovat tým odborníků z oblasti kyberbezpečnosti, médií a analytiků, jejichž prací by bylo dohlížet na bezpečnost na internetu. Dezinformace se masivně šíří přes sociální sítě, takže by se jejich práce zaměřovala na facebookové skupiny a veřejně sdílený obsah, který by mohl být potenciálně nebezpečný. Měli by pevně nastavený metodický postup, kterým by se řídili při monitorování, filtrování a analyzování dat. Byli by také hlavním koordinátorem pro další veřejné instituce, kterým by radili, jak reagovat na dezinformace a falešné

zprávy. Pro ošetření středního rizika s č. 3 *„Nedostatečná kybernetická bezpečnost“* je nutné, aby stát kladl větší důraz na kybernetickou bezpečnost ve veřejných institucích pracujících s citlivými daty (např. univerzity s bezpečnostním zaměřením) a soukromé firmy a instituce (digitální firmy apod.). K ošetření středního rizika s č. *8 „Nedostatečný přístup k aktualizovaným datům a informacím v reálném čase“* je nutné, aby byl zřízen systém, který by shromažďoval aktualizovaná data a informace v reálném čase, především pro případ mimořádných událostí s veřejným přístupem. Takový portál by pro případ mimořádných událostí mohlo spravovat Národní operační a informační středisko. K ošetření vysokých rizik č. 5 *„Nedostatečná mediální gramotnost veřejnosti“* a středního rizika č. *10 „Neúčinné strategie osvěty veřejnosti o rizicích dezinformací.“* Pro boj s těmito rizika je nutné, aby byla zvyšována mediální gramotnost veřejnosti. Zvyšování mediální gramotnosti by probíhalo prostřednictvím osvěty a vzděláváním obyvatelstva. Mediální gramotnost by měla být zahrnuta do osnov pro vzdělávání na základních školách, kde by se již od mladého věku děti naučily, jak s informacemi pracovat, jak se jimi nezahlcovat a jak rozpoznat manipulativní obsah od toho informačního. K tomuto se dá využít již probíhajících projektů např. Zvol si info nebo vzdělávací program *„Jeden svět na školách“* od Člověka v tísni. Jedním příspěvkem k opatření jsou také zásady fact-chcekingu.

Na obrázku 16 je vytvořen fact-checkingový postup, jak si může každý občan ověřovat informace, než je bude sdílet dále nebo na něj začnou působit. Fact-checking se skládá z 5 základních kroků k ověření zdroje a záměru informace. Je to přispění k mediální gramotnosti občanů České republiky. Tento fack-checkingový leták nese název *„Důvěřuj, ale prověřuj! 5 zásadních kroků fact-checkingu“* a mohl by být využit systémem ochrany obyvatelstva jako jedním z nástrojů ke snížení tohoto rizika. Švédská civilní nouzová agentura vydala v roce 2018 brožuru s názvem *„If Crisis or War Comes“* (ve švédském originálu *„Om krisen eller kriget kommer“),* která má připravit všechny žijící ve Švédsku na možné mimořádné události, extrémní počasí, kybernetické hrozby nebo válečné konflikty. V této brožuře je jedna strana věnována také dezinformacím a falešným zprávám a jak se bránit propagandě cizí moci. (Swedish Civil Contigencies Agency (MSB), revidováno 2022) Taková brožura by mohla být vytvořena i pro celostátní ochranu obyvatelstva v České republice, ve které by byla, podobně jako ve Švédsku, zahrnuta oblast dezinformací. Podle Výroční zprávy Národního kontrolního úřadu by mělo Ministerstvo vnitra během roku 2024 spustit webové stránky ochrany obyvatelstva, kde by mohla být zveřejněna taková brožura s komplexními informa-

cemi ke všem mimořádným událostem, kybernetickým hrozbám i hrozbám hybridním. Součástí této brožury by měly být informace, jak se bránit manipulativnímu obsahu a dezinformacím v digitálním světě. V této kapitole by měl být zahrnut i informační leták se zásadami fact-checkingu na obrázku 16.




*Obrázek 16 Fact-checking. (zdroj: vlastní zpracování)*

Jednou z možných cest, jak může systém ochrany obyvatelstva přispět v ochraně před hrozbami dezinformací a manipulativního obsahu je podílet se na osvětových činnostech, pořádat přednášky a vzdělávat občany. Jednou z možností, jak plošně vzdělávat obyvatelstvo v této oblasti je již výše zmíněný web ochrany obyvatelstva, na kterém by byly zveřejněny informace, co jsou to dezinformace, fake news, propaganda nebo deepfake, jak je rozlišit a jak se jim občan může bránit. Základní složka IZS, Policie České republiky, působí na Instagramu, kde zveřejňuje důležité i zajímavé informace o jejich práci, působnosti i dění ve společnosti. Tento profil sleduje okolo 214 tisíce lidí. Tento profil by mohl sloužit právě k osvětové činnosti v oblasti dezinformací na sociálních sítích. V tzv. „highlights“ na tomto profilu, by mohly být jednoduchou formou vysvětleny základní pojmy v oblasti dezinformací a zásady fact-checkingu, který je právě na sociálních sítích důležitý.

Zásadní otázkou v oblasti dezinformací je, kdo a jak může vůbec určit, co dezinformace je a co naopak není? V současné době, kdy má přístup k internetu skoro každý, a může tak kdokoli cokoli na publikovat, je mnohem těžší regulovat falešné a manipulativní informace. Debata o určování dezinformací je aktuálně častým probíraným tématem a ve veřejném prostoru je mnoho souhlasných i právě nesouhlasných názorů. V politickém i veřejném prostředí zaznívají názory, že by potírání dezinformací a blokování dezinformačních webů mohlo vést k cenzuře a omezování svobody slova. Je tomu ale vážně tak? Mnoho odpůrců se odvolává na Listinu základních práv a svobod, která garantuje, že mají všichni lidé právo na vlastní názor, politické, náboženské vyznání a svobodně se vyjádřit. Tento ústavní zákon ale dále zmiňuje, že stát může omezit a přijmout taková opatření, pokud tyto názory ohrožují lidské životy, zdraví nebo bezpečnost země. Z dat získaných prostřednictvím dotazníkového šetření u obyvatelstva České republiky vyplývá, že si občané uvědomují absenci zákona či jiné právní normy, která by jasně definovala dezinformace a postihovala jejich šíření. Takové právní norma v České republice chybí. Také vznikla otázka, kdo je vůbec kompetentní určovat, co dezinformace je a co není a jak toho dosáhne. Z povahy a charakteru dezinformací by to musel být celý tým odborníků z různých oblastí (média, bezpečnost, politika, marketing, kybernetická bezpečnost a mnoho dalších) a tým analytiků, kteří by veškeré takto označované informace museli prověřovat a kontrolovat. Takové označování nemůže dělat pouze jeden pověřený člověk. Proto by měla být jasně nastavená metodika a tým odborníků, kteří by se věnovali oblasti informací a potírání dezinformací a osvětové činnosti.

# ZÁVĚR

Jednoduché nástroje proti šíření dezinformací a jejich dopadům neexistují. Dezinformace, propaganda nebo fake news nemají stejné dopady jako například požár, dopravní nehoda nebo únik nebezpečné látky. Šíření dezinformací je často skryté, pomalé a na první pohled nerozpoznatelné. Takové bezpečnostní hrozby ale s sebou nesou vážné bezpečnostní dopady, především na demokratické zřízení státu, ale také mohou zapříčinit pokles důvěry ve veřejné instituce i IZS.

Dle Ishikawa diagramu a navazující matice rizik bylo zjištěno, že důvěra veřejnosti v informační kanály a systém ochrany obyvatelstva, jako veřejné instituce zajišťující bezpečnost České republiky, může být narušena několika faktory. Pro střední a vysoká rizika byla navržena opatření pro jejich ošetření tak, aby informační kanály a systém ochrany obyvatelstva jako takový mohl být důvěryhodný pro veřejnost. Bylo zjištěno, že dezinformace nemusí být přímou hrozbou pro systém ochrany obyvatelstva, ale může narušit jeho fungování a důvěru veřejnosti v tento systém. Z dat dotazníkového šetření vyplývá, že znalost respondentů v této oblasti je vysoká a mediální gramotnost je na dobré úrovni. Z nasbíraných údajů bylo zjištěno, že více jak polovina dotázaných věří veřejnoprávním médiím, která hrají důležitou roli pro v informování obyvatelstva při mimořádných událostech. Ze získaných dat bylo zjištěno, že dosažené vzdělaní nemusí znamenat vysokou mediální gramotnost nebo větší odolnost vůči dezinformacím. Obětí dezinformací se může stát každý. Proto je důležité, aby se rozšiřovalo povědomí o oblasti dezinformací. Dezinformace se totiž nedají zastavit pouze rušením dezinformačních webů, cenzurou nebo trestními sazbami. Dezinformace je komplexní téma, které musí být řešeno celou společností.

Důležitými opatřením pro ochranu před dezinformacemi je odolný a uvědomělý občan se schopností kritického myšlení. Právě kritické myšlení a schopnost fact-checkingu je důležitým faktorem pro zabránění šíření manipulativního obsahu v digitálním prostředí. Tyto schopnosti musí získat právě veřejnost, bez níž se nedokáže bránit před působením dezinformačních kampaní a manipulaci s jejich myšlením. Důležitým faktorem pro zvyšování mediální gramotnosti je vzdělávání dětí a mládeže na školách, ale také je důležité provádět osvětovou činnosti mezi dospělým, a především starším obyvatelstvem. K tomuto vzdělávání lze využít již probíhajících projektů, které mají s touto problematikou zkušenosti.

Hlavním cílem bakalářské práce bylo na základě vyhodnocení dotazníkového šetření navrhnout případné změny a opatření ke zlepšení současného stavu.

Ke splnění hlavního cíle byly stanoveny dílčí cíle: zpracovat teoretická východiska a teoretické poznatky na základě dostupných informací ze zahraničních a domácích zdrojů k danému tématu, provést dotazníkové šetření u obyvatelstva na dané téma a navrhnout opatření ke zlepšení. V teoretické části byly použity metody indukce a dedukce s využitím mnoha aktuálních domácích i zahraničních zdrojů pro položení základu k pochopení dané problematiky. V praktické části byl zpracován Ishikawa diagram s navazující maticí rizik pro odhalení možných rizik pro systém ochrany obyvatelstva a posouzení závažnosti těchto hrozeb. Dále bylo zpracováno a vyhodnoceno dotazníkové šetření a vypracovány návrhy možného zlepšení. Cíle stanovené v úvodu práce byly splněny.

# SEZNAM POUŽITÉ LITERATURY

ALVAROVÁ, Alexandra, 2022. *Průmysl lží: propaganda, konspirace a dezinformační válka.* 3., rozšířené vydání. Praha: Stanislav Juhaňák – Triton. ISBN 978-80-7684-056-0.

AMERICAN PSYCHOLOGICAL ASSOCIATION, 2023. *How and why does misinformation spread?* Online. In: AMERICAN PSYCHOLOGICAL ASSOCIATION. apa.org. 2024. Dostupné z: https://www.apa.org/topics/journalism-facts/how-why-misinformation-spreads. [cit. 2024-04-04].

APTIEN.COM. *Co je matice rizik*. Online. In: APTIEN. Aptien.com. Dostupné z: https://aptien.com/cs/kb/articles/what-is-risk-matrix. [cit. 2024-04-16].

ASF.ORG, ©2024. *Fishbone Diagram*. Online. In: ASQ. Asf.org. Dostupné z: https://asq.org/quality-resources/fishbone. [cit. 2024-04-15].

BARTONÍČEK, Radek, 2023. *Zákon proti dezinformacím zřejmě nevznikne. Stačí bojovat pravdou, míní Benda z ODS*. Online. In: aktualne.cz. Dostupné z: https://zpravy.aktualne.cz/domaci/zakon-proti-dezinformacim/r~739a7c12c71611ed8b4e0cc47ab5f122/. [cit. 2024-03-16].

BENNETT, W. Lance a LIVINGSTON, Steven (ed.), 2020. *The Disinformation Age*. Online. United Kingdom: Cambridge University Press. ISBN 9781108914628. Dostupné z: https://doi.org/10.1017/9781108914628. [cit. 2024-03-18].

BERNARD, Josef a DANIEL, Jan, 2019. *Hybridní válka, dezinformace a evropská bezpečnost: Hledání alternativních chápání v prostředí České republiky*. Online. In: INSTITUTE OF INTERNATIONAL RELATIONS (IRR). Irr.cz. Dostupné z: https://www.iir.cz/en/hybridni-valka-dezinformace-a-evropska-bezpecnost-hledani-alternativnich-chapani-v-prostredi-ceske-republiky. [cit. 2024-04-11].

CAMBRIDGE UNIVERSITY PRESS & ASSESSMENT, ©2024a. *Critical thinking*. Online. In: CAMBRIDGE UNIVERSITY PRESS & ASSESSMENT. Dictionary.cambridge.org. Dostupné z: https://dictionary.cambridge.org/dictionary/english/critical-thinking. [cit. 2024-04-03].

CAMBRIDGE UNIVERSITY PRESS & ASSESSMENT, ©2024b. *Mainstream media*. Online. In: CAMBRIDGE UNIVERSITY PRESS & ASSESSMENT. Dictionary.cambridge.org. Dostupné z: https://dictionary.cambridge.org/dictionary/english/mainstream-media. [cit. 2024-04-14].

CANVA. Online. In: Canva.com. Dostupné z: https://www.canva.com/cs_cz/. [cit. 2024-04-21].

ČESKÁ TELEVIZE, 2018. *Výroční zpráva o činnosti České televize v roce 2017*. Česká televize. Dostupné z: https://www.ceskatelevize.cz/rada-ct/vyrocni-zpravy/. [cit. 2024-04-14].

ČESKÁ TELEVIZE, 2024. *Výroční zpráva o činnosti České televize v roce 2024*. Česká televize. Dostupné z: https://www.ceskatelevize.cz/rada-ct/vyrocni-zpravy/. [cit. 2024-04-14].

ČESKO, 1993a. Usnesení č. 2/1993 Sb., předsednictva České národní rady o vyhlášení LISTINY ZÁKLADNÍCH PRÁV A SVOBOD jako součástí ústavního pořádku České republiky – znění od 1. 10. 2021. In: Zákony pro lidi.cz [online]. © AION CS 2010–2024. Dostupné z: https://www.zakonyprolidi.cz/cs/1993-2?text=2%2F1993. [cit. 2024-03-16].

ČESKO, 1993b. Ústavní zákon č. 1/1993 Sb., ústava České republiky – znění od 1. 6. 2013. In: Zákony pro lidi.cz [online]. © AION CS 2010–2024. Dostupné z: https://www.zakonyprolidi.cz/cs/1993-1#f1471021. [cit. 2024-03-16].

ČESKO, 1998. Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky – znění od 1. 12. 2000. In: Zákony pro lidi.cz [online]. © AION CS 2010–2024. Dostupné z: https://www.zakonyprolidi.cz/cs/1998-110#f1861164. [cit. 2024-03-16].

ČESKO, 2000a. Zákon č. 239/2000 Sb., o integrovaném záchranném systému a o změně některých zákonů – znění od 1. 1. 2024. In: Zákony pro lidi.cz [online]. © AION CS 2010–2024. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-239#p2-1-e. [cit. 2024-04-06].

ČESKO, 2000b. Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon) – znění od 1. 1. 2024. In: Zákony pro lidi.cz [online]. © AION CS 2010–2024. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-240#f2059821. [cit. 2024-04-130.].

ČESKO, 2002. Vyhláška č. 380/2002 Sb., Ministerstva vnitra k přípravě a provádění úkolů ochrany obyvatelstva – znění od 22. 8. 2002. In: Zákony pro lidi.cz [online]. © AION CS 2010–2024. Dostupné z: https://www.zakonyproldi.cz/cs/2002-380#f2356160. [cit. 2024-04-13].

ČESKO, 2009. Zákon č. 40/2009 Sb., trestní zákoník – znění od 1. 7. 2023. In: Zákony pro lidi.cz [online]. © AION CS 2010–2024. Dostupné z: https://www.zakonypro-lidi.cz/cs/2009-40#f3921443. [cit. 2024-03-16].

ČESKO, 2014. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) – znění od 6. 8. 2022. In: Zákony pro lidi.cz [online]. © AION CS 2010–2024. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181#f5278856. [cit. 2024-03-16].

ČESKO, 2015. *Bezpečnostní strategie České republiky 2015*. Praha: Ministerstvo zahraničních věcí České republiky. ISBN 978-80-7441-005-5.

ČESKO, 2016. *Audit národní bezpečnosti*. Praha: Ministerstvo vnitra České republiky.

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

ČESKO, 2020. *Národní strategie kybernetické bezpečnosti České republiky*. Národní úřad pro kybernetickou bezpečnost.

ČESKO, 2021a. *Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2021 až 2025*. Online. In: Národní úřad pro kybernetickou a informační bezpečnost. Dostupné z: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/. [cit. 2024-04-01].

ČESKO, 2021b. *Národní strategie pro čelení hybridnímu působení – National strategy for countering hybrid interference*. 1. vydání. Praha: Ministerstvo obrany České republiky – VHÚ Praha. 10, 11 stran. ISBN 978-80-7278-827-9.

ČESKO, 2022a. *Usnesení vlády České republiky o jmenování poradce pro národní bezpečnost.*

ČESKO, 2022b. *Usnesení vlády České republiky o vytvoření funkce poradce pro národní bezpečnost.*

ČESKO, 2022c. *Statut poradce pro národní bezpečnost*. In: Usnesení vlády ze dne 21. prosince 2022.

ČESKO, 2023a. *Bezpečnostní strategie České republiky 2023*. Vydání první. Praha: Ministerstvo zahraničních věcí České republiky. 35 stran. ISBN 978-7441-097-0.

ČESKO, 2023b. *Obranná strategie České republiky*. Praha: Ministerstvo obrany České republiky – VHÚ Praha.

DEMAGOG.CZ, nedatováno. *O nás: Co je to Demagog.cz?* Online. In: Demagog.cz. Dostupné z: https://demagog.cz/stranka/o-nas. [cit. 2024-04-02].

DISMAN, Miroslav, 2018. *Šetření dotazníkové (MSgS)*. Online. In: SOCIÁLNÍ ENCYKLOPEDIE. Encyklopedie.soc.cas.cz. Dostupné z: https://encyklopedie.soc.cas.cz/w/%C5%A0et%C5%99en%C3%AD_dotazn%C3%ADkov%C3%A9_(MSgS). [cit. 2024-04-16].

DOMBROVSKÁ, Michaela a ŠIDLICHOVSKÁ, Zuzana, 2021. *Informační detox: jak si zjednodušit život v digitální době*. Praha: Grada. ISBN 978-80-271-2920-1.

DUGGAN, Laurel, 2024. *Ursula von der Leyen: misinformation is world's gravest problem*. Online. In: Unherd.com. Dostupné z: https://unherd.com/thepost/ursula-von-der-leyen-misinformation-is-worlds-gravest-problem/. [cit. 2024-02-03].

EUROPEAN COMMISSION, 2022. *Guidelines for teachers and educators on tackling disinformation and promoting digital literacy through education and training*. Online. Luxembourg: European Union. ISBN 978-92-76-55108-9. Dostupné z: https://doi.org/10.22766/28248. [cit. 2024-04-02].

EUVSDISINFO.EU, nedatováno. *About*. Online. In: EUVSDISINFO. Euvsdisinfo.eu. Dostupné z: https://euvsdisinfo.eu/about/. [cit. 2024-04-02].

EVROPSKÁ KOMISE, 2018. Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů – Boj proti dezinformacím na internetu: evropský přístup. Online. Brusel. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A52018DC0236&qid=1700300738680. [cit. 2024-04-02].

EVROPSKÁ KOMISE, nedatováno. *Na pravou míru*. Online. In: EVROPSKÁ KOMISE. Europa.eu. Dostupné z: https://czechia.representation.ec.europa.eu/novinky-udalosti/na-pravou-miru_cs. [cit. 2024-04-02].

EVROPSKÁ UNIE, 2016. *Společné sdělení Evropskému parlamentu a Radě – Společný rámec pro boj proti hybridním hrozbám – Reakce Evropské unie*. Online. Brusel. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A52016JC0018&qid=1700300738680. [cit. 2024-04-01].

GREGOR, Miloš a MLEJNKOVÁ, Petra, 2021. *Challenging online propaganda and disinformation in the 21st century*. Political campaigning and communication. Cham: Palgrave Macmillan. ISBN 978-3-030-58623-2.

GREGOR, Miloš a VEJVODOVÁ, Petra, 2018. *Nejlepší kniha o fake news, dezinformacích a manipulacích!!!*. Brno: CPress. ISBN 978-80-264-1805-4.

HYBRIDCOE.FI, nedatováno a. *Establishment*. Online. In: HYBRID COE. hybridcoe.fi. Dostupné z: https://www.hybridcoe.fi/establishment/. [cit. 2024-04-04].

HYBRIDCOE.FI, nedatováno b. *What is Hybrid CoE?* Online. In: HYBRID COE. hybridcoe.fi. Dostupné z: https://www.hybridcoe.fi/who-what-and-how/. [cit. 2024-04-04].

HZSCR.CZ, ©2024. *Úvodní stránka*. Online. In: GENERÁLNÍ ŘEDITELSTVÍ HASIČSKÉHO ZÁCHRANNÉHO SBORU ČR. Hzscr.cz. Dostupné z: https://www.hzscr.cz/clanek/ochrana-obyvatelstva-uvodem.aspx. [cit. 2024-04-10].

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

JSNS.CZ, nedatováno. *Slovníček pojmů k mediálnímu vzdělávání: Mediální gramotnost*. Online. In: JEDEN SVĚT NA ŠKOLÁCH. Jsns.cz. Dostupné z: https://www.jsns.cz/projekty/medialni-vzdelavani/materialy/slovnicek-medialniho-vzdelavani. [cit. 2024-04-21].

KOPECKÝ, Kamil, 2019. *Deep fake – stručný úvod do problematiky*. Online. *E-Bezpečí*. Roč. 4, č. 1, s. 23–25. ISSN 2571-1679. Dostupné z: https://www.e-bezpeci.cz/index.php/70-projekt-fake-news/1417-deep-fake-strucny-uvod-do-problematiky. [cit. 2024-03-12].

KOPECKÝ, Kamil, 2022a. *Co je to vlastně ten hoax, dezinformace, misinformace nebo třeba fake news? Čím se tyto termíny liší a co mají společného?* Online. *E-Bezpečí*. ISSN 2571-1679. Dostupné z: https://www.e-bezpeci.cz/index.php/clanky-komentare/2864-co-je-to-vlastne-ten-hoax-dezinformace-misinformace-nebo-treba-fake-news-cim-se-tyto-terminy-lisi-a-co-maji-spolecneho. [cit. 2024-01-31].

KOPECKÝ, Kamil, 2022b. *Fact-checking vs. debunking*. Online. *E-bezpečí*. ISSN 2571-1679. Dostupné z: https://www.e-bezpeci.cz/index.php/clanky-komentare/2854-fact-checking-vs-debunking. [cit. 2024-04-03].

KOPECKÝ, Kamil, 2023. *Kdo rozhoduje o tom, co je a co není dezinformace?* Online. *E-bezpečí*. ISSN 2571-1679. Dostupné z: https://www.e-bezpeci.cz/index.php/clanky-komentare/3149-kdo-rozhoduje-o-tom-).%20co-je-a-co-neni-dezinformace. [cit. 2024-01-30].

KOŽÍŠEK, Martin a PÍSECKÝ, Václav, 2016. *Bezpečně n@ internetu: průvodce chováním ve světě online*. Praha: Grada Publishing. ISBN 978-80-247-5595-3.

KRYŠTOFOVÁ, Vendula, 2023. *Právně definovat dezinformaci je nemožné. Platí ‚když ji vidím, tak ji poznám', říká redaktor Koubský*. Online. In: ČESKÝ ROZHLAS. Irozhlas.cz. Dostupné z: https://www.irozhlas.cz/zpravy-domov/dezinformace-novy-zakon-koubsky_2303242250_krp. [cit. 2024-03-16].

MANAGEMENTMANIA.COM, 2015. *Ishikawův diagram*. Online. In: MANAGEMENTMANIA. Managementmania.com. Dostupné z: https://managementmania.com/cs/ishikawuv-diagram. [cit. 2024-04-15].

MANIPULÁTOŘI.CZ, nedatováno. *Vydavatel a transparentní financování: Něco o nás*. Online. In: Manipulatori.cz. Dostupné z: https://manipulatori.cz/finacovani/. [cit. 2024-04-02].

MINISTERSTVO VNITRA, 2021. *Krizové řízení při nevojenských krizových situacích, ochrana obyvatelstva, kritická infrastruktura: modul A; C; I*. Praha: Ministerstvo vnitra. ISBN 978-80-7616-097-2.

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY, 2023. *Projevy extremismu a předsudečné nenávisti: Souhrnná situační zpráva 1. pololetí roku 2023*. Online. Dostupné z: https://www.mvcr.cz/clanek/pololetni-zprava-mv-o-extremismu-556073.aspx. [cit. 2024-04-15].

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY, ©2023. *Definice dezinformací a propagandy: Dezinformace: systematické a úmyslné klamání*. Online. In: mvcr.cz. Dostupné z: https://www.mvcr.cz/chh/clanek/definice-dezinformaci-a-propagandy.aspx. [cit. 2023-12-26].

MINISTERSTVO VNITRA GENERÁLNÍ ŘEDITELSTVÍ HASIČSKÉHO ZÁCHRANNÉHO SBORU ČESKÉ REPUBLIKY, 2021. *Krizové řízení při nevojenských krizových situacích, ochrana obyvatelstva, kritická infrastruktura: modul A; C; I*. Praha: Ministerstvo vnitra. ISBN 978-80-7616-097-2.

MINISTERSTVO ZAHRANIČNÍCH VĚCÍ ČESKÉ REPUBLIKY, nedatováno. *Světové ekonomické fórum*. Online. In: mzv.gov.cz. Dostupné z: https://mzv.gov.cz/mission.geneva/cz/svetovy_obchod/svetove_ekonomicke_forum/index.html. [cit. 2024-02-03].

MVCR.CZ, ©2024a. *Co jsou hybridní hrozby*. Online. In: MINITERSTVO VNITRA ČESKÉ REPUBLIKY. Mvcr.cz. Dostupné z: https://www.mvcr.cz/chh/clanek/co-jsou-hybridni-hrozby.aspx. [cit. 2024-04-01].

MVCR.CZ, ©2024b. *Trestněprávní úprava*. Online. MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. mvcr.cz. Dostupné z: https://www.mvcr.cz/chh/clanek/dezinformacni-kampane-trestnepravni-uprava-trestnepravni-uprava.aspx. [cit. 2024-03-16].

MVCR.CZ, ©2024c. *FAQ: Odpovědi na nejčastější dotazy ohledně CHH a jeho práce*. Online. In: CENTRUM PROTI HYBRIDNÍM HROZBÁM. Mvcr.cz. Dostupné z: https://www.mvcr.cz/chh/clanek/specialni-dokumenty-faq.aspx. [cit. 2024-04-02].

NATO.INT, 2024. *Countering hybrid threats*. Online. In: NORTH ATLANTIC TREATY ORGANIZATION. Nato.int. Dostupné z: https://www.nato.int/cps/en/natohq/topics_156338.htm. [cit. 2024-04-01].

NFNZ.CZ, nedatováno. *O nás*. Online. In: NADAČNÍ FOND NEZÁVISLÉ ŽURNALISTIKY. Nfnz.cz. Dostupné z: https://www.nfnz.cz/o-nas/. [cit. 2024-04-02].

NEJVYŠŠÍ KONTROLNÍ ÚŘAD, 2024. *Výroční zpráva o činnosti NKÚ za rok 2023*: Sp. zn.:79/2024-NKU45/86/24. Nejvyšší kontrolní úřad.

NELEZ.CZ, nedatováno. *Postav se za pravdu proti dezinformacím*. Online. In: NELEŽ. Nelez.cz. Dostupné z: https://www.nelez.cz/. [cit. 2024-04-15].

NONNEMANN, František; ČERVENÝ, Vlastimil a VÍTEK, Dominik, 2022. *Kybernetický bezpečnostní incident 3D: IT, právo a compliance*. Právní monografie (Wolters Kluwer ČR). Praha: Wolters Kluwer. ISBN 978-80-7676-515-3.

NUKIB.GOV.CZ, nedatováno. *Kybernetická bezpečnost*. Online. NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. Nukib.gov.cz. Dostupné z: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/. [cit. 2024-03-16].

NUTIL, Petr, 2018. *Média, lži a příliš rychlý mozek: průvodce postpravdivým světem*. Praha: Grada. ISBN 978-80-271-0716-2.

NUTIL, Petr, 2020. *Jak neztratit rozum v nerozumné době: o falešných představách, iluzích a předsudcí*ch. Praha: Grada. ISBN 978-80-271-1796-3.

OED.COM, ©2023. *Propaganda*. Online. In: OXFORD ENGLISH DICTIONARY. Oed.com. Dostupné z: https://www.oed.com/dictionary/propaganda_n?tl=true. [cit. 2024-04-01].

PIKA, Tomáš a KUBANT, Vít, 2023. *Vláda zrušila funkci vládního zmocněnce pro média Klímy. Agendu dezinformací převezme poradce Pojar*. Online. In: Irozhlas.cz. Dostupné z: https://www.irozhlas.cz/zpravy-domov/michal-klima-zmocnenec-media-dezinformace-vlada-konec-tomas-pojar_2302151348_pik. [cit. 2024-03-16].

PRINC, Ivan, nedatováno. *Téma 13: Nástroje a prostředky komunikace a informování veřejnosti v rámci prevence mimořádných událostí – systém varování a vyrozumění*. Powerpoint. Univerzita Tomáše Bati ve Zlíně – Fakulta logistiky a krizového řízení.

*Programové prohlášení vlády České republiky*, 2022. Online. Dostupné z: https://vlada.gov.cz/cz/programove-prohlaseni-vlady-193547/. [cit. 2024-03-14].

SEDLÁK, Petr a KONEČNÝ, Martin, 2021. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. Brno: CERM, akademické nakladatelství. ISBN 978-80-7623-068-2.

SWEDISH CIVIL CONTIGENCIES AGENCY (MSB), revidováno 2022. *If Crisis or War Comes*. Online. Karlstad: Swedish Civil Contingencies Agency (MSB. ISBN 978-91-7927-334-7. Dostupné z: https://www.msb.se/en/rad-till-privatpersoner/the-brochure-if-crisis-or-war-comes/. [cit. 2024-04-10].

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

TULINSKÁ, Hana. *Veřejnoprávní média*. Online. In: MASARYKOVA UNIVERZITA. ©2024. Dostupné z: https://kisk.phil.muni.cz/onlife/temata/media-a-obcanstvi/verejnopravni-media. [cit. 2024-04-14].

TED-ED, 2015. *How false news can spread – Noah Tavlin*. Online. 2016. Dostupné z: YouTube, https://www.youtube.com/watch?v=cSKGa_7XJkg. [cit. 2024-04-04].

VOSOUGHI, Soroush; ROY, Deb a ARAL, Sinan, 2018. The spread of true and false news online. Online. *Science*. Article 359. Dostupné z: https://doi.org/10.1126/science.aap9559. [cit. 2024-04-04].

WOLTERSKLUWER.COM, ©2024. *Risk matrix*. Online. In: WOLTERS KLUWE. Wolterskluwer.com. Dostupné z: https://www.wolterskluwer.com/en/solutions/enablon/bowtie/expert-insights/barrier-based-risk-management-knowledge-base/risk-matrices. [cit. 2024-04-16].

WORLD ECONOMIC FORUM, ©2024. *The Global Risks Report 2024*. Online. 19th Edition. Ženeva. ISBN 978-2-940631-64-3. Dostupné z: https://www.weforum.org/publications/global-risks-report-2024/. [cit. 2024-02-03].

# SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

| | |
|---|---|
| CHH | Centrum proti hybridním hrozbám |
| EU | Evropská unie |
| GRPS | Global Risks Perception Survey (Průzkum vnímání globálních rizik) |
| HZS ČR | Hasičský záchranný sbor České republiky |
| IZS | Integrovaný záchranný systém |
| NATO | Severoatlantická aliance (z angl. North Atlantic Treaty Organization) |
| NCKB | Národní centrum kybernetické bezpečnosti |
| NKÚ | Nejvyšší kontrolní úřad |
| NÚKIB | Národní úřad pro kybernetickou a informační bezpečnost |
| OBSE | Organizace pro bezpečnost a spolupráci v Evropě |
| OSN | Organizace spojených národů |
| PČR | Policie České republiky |
| WEF | World Economic Forum |

# SEZNAM OBRÁZKŮ

# SEZNAM TABULEK