Recenzovaný článek

Inovativní pohled na metodický proces čelení dezinformacím

Innovative View of the Methodical Process of Facing Disinformation

Martin Havlík

Abstrakt: Článek popisuje inovativní pohled na možný metodický proces přístupu a ochraně proti dezinformacím. Stále narůstající digitalizace a využívání kybernetického prostoru pro šíření veškerého druhu dat a informací poskytuje uživatelům neoddiskutovatelné množství výhod spojených s rychlým přístupem, distribucí nebo sdílením aktuálních sdělení. Tento vývojový trend však reciprocně generuje také množství souvisejících hrozeb, kterým je nutné čelit. Klíčovou úlohu zde hraje vlastní odolnost a účinné nástroje vůči informačním kampaním a informačnímu působení všech relevantních aktérů. Vlastní kritické myšlení a nastavené procesní mechanismy související s přístupem k informacím pak představují těžiště celkové odolnosti proti tomuto typu bezpečnostních hrozeb. Předkládaný metodický proces tak může pomoci širokému spektru čtenářů rozšířit pohled na komplexitu problému a částečně minimalizovat související bezpečnostní rizika.

Abstract: The article describes an innovative view of a possible methodical process of access and protection against disinformation. The ever-increasing digitization and use of cyberspace to disseminate all kinds of data and information provides users with an indisputable number of associated benefits associated with rapid access, distribution or sharing of current knowledge. However, this development trend also reciprocally generates a number of related threats that need to be faced. Our own resilience and effective tools against information campaigns and information actions of all relevant actors play the key role here. The critical thinking itself and the process mechanisms used to access information are the focus of overall resilience to this type of security threats. Thus, the methodical process can help a wide range of readers broaden their view of the complexity of the problem and partially minimize the associated security risks.

Klíčová slova: informace; dezinformace; hrozba; obrana; proces.

Key words: Information; Disinformation; Threat; Defence; Process.

ÚVOD

Cílem tohoto článku je poskytnout čtenářům inovativní pohled na možný procesní přístup k efektivnímu čelení dezinformacím, které jsou v současné době nedílnou součástí každodenního života celé naší společnosti. Značná nasycenost informačního prostředí nejrůznějšími informacemi, a potažmo i dezinformacemi, klade vysoké nároky na samotné konzumenty těchto informací. Klíčovým atributem je v této souvislosti kognitivní myšlení jednotlivců i odolnost společnosti jako celku, které se tak stává hlavním selekčním a absorpčním nástrojem. Zásadní je pak schopnost rozlišovat mezi informacemi sdělujícími reálná fakta a úmyslně šířenými dezinformacemi, ať je účel jejich šíření jakýkoliv. Kritický pohled (kritické myšlení) a nepřetržitá verifikace přijímaných informací se pak musí stát běžnou a automatickou činností každodenního života. Z uvedeného základního exkurzu do této problematiky lze usuzovat, že tato oblast je poměrně rozsáhlá a zahrnuje v sobě interdisciplinárně několik oborů (disciplín). Mezi tyto lze zařadit například neurovědu, psychologii, filosofii, okrajově také antropologii nebo v časné době často sklo-ňovanou umělou inteligenci a mnoho dalších. Ambicí toho článku není detailně popsat širší fundamenty té či oné disciplíny, ale předložit čtenářům inovativní pohled na bazální procesy, které lze bez komplikovaného a náročného úsilí aplikovat v praxi.

Na úvod je vhodné zdůraznit, že šíření dezinformací spočívá v úmyslném vytváření a šíření nepravdivých nebo zmanipulovaných informací, které mají příjemce oklamat nebo uvést v omyl. Účelem je buď způsobit škodu, nebo získat nějaký politický, osobní či finanční prospěch. Neúmyslné sdílení nepravdivých informací se označuje jako misinformace a tomuto problému se článek blíže věnovat nebude (jakkoliv jsou níže popsané postupy jistě aplikovatelné i na tuto charakteristickou skupinu informací). Dezinformační kampaně či masivní sdílení jednotlivých dezinformací se přesunuly primárně do prostředí internetu (obecně do kybernetického prostoru), kde klíčovou roli pro šíření hrají v současné době platformy sociálních sítí. Rovněž i intenzivnější vyžívání aplikací pro sdílení fotografií a videí (Instagram, Tik Tok) logicky akceleruje význam a využití nástrojů typu Deepfake, kterým bude v budoucnu nutné věnovat vyšší pozornost. Významnými nástroji šíření dezinformací na sociálních sítích jsou sady uživatelských účtů sloučených a spravovaných v rámci tzv. trollích farem, dále pak umělí boti řízení pomocí algoritmů a podobně. Přes akcentovaný význam sociálních sítí jako hlavního kanálu pro šíření dezinformací nelze však ani opomenout ani rozporuplné zpravodajské dezinformační weby a portály, a v souvislosti s válkou na Ukrajině také standardní média jako je například televize.

Významným akcelerátorem popisovaného fenoménu je také stupeň digitalizace a informační propojení obyvatel a připojených zařízení, který závratně rychle roste. V důsledku toho se paralelně zvyšují i odpovídající rizika, jako je zničení nebo kompromitace informačních systémů, únik osobních informací, neoprávněné nabývání a používání duševního vlastnictví a vlivové informační operace využívající sociálních sítí. Snahou autora tohoto článku je poukázat na inovativní metodický proces jak čelit dezinformacím, který tak může doplnit existující portfolio dalších možných metodických postupů. Níže popisovaný proces vychází z různých vydání publikace RESIST, a snaží se poskytnout nový náhled na řešení předmětné problematiky. Je vhodné v této části zdůraznit také tu skutečnost,

že se nejedná o dogmatický a jediný možný přístup, ale naopak je nutné existující procesy neustále přizpůsobovat vývoji okolního informačního prostředí a také vývoji nových komunikačních kanálů, nástrojů či technologií.

1 METODOLOGIE

Nosná metodologie vedoucí ke zpracování tohoto článku byla postavena na kvalitativním výzkumu a zejména na empirických zkušenostech autora. Kvalitativní výzkum je ve své obecné podstatě zaměřen na nalezení vysvětlení a příčinných mechanismů, které by nám umožnily zobecnit analyzované zákonitosti. Vzhledem k obsahovanému zaměření článku a ambicím autora je tento typ výzkumu příhodnější, protože poskytuje relevantnější předpoklady k provedení odpovídající analýzy bezpečnostních aspektů, ke kterým nejsou dostupné odpovídající kvantitativní údaje (zejména strukturální indikátory či jiné ukazatele, statistiky, průzkumy veřejného mínění atd.). Pro posouzení současného stavu a terminologické ukotvení byla při zpracování článku využita analýza vybraných zdrojů (dokumentů, literatury, webů apod.). Jak bylo uvedeno výše, klíčovou úlohu při zpracování hraje dlouhodobá empirie, tedy zkušenost získaná cílevědomým pozorováním problematiky ze strany autora. Uvedené argumenty jsou podpořeny výsledky vlastního pozorování a byly podrobeny několika expertním konzultacím. Pro doplnění kontextu je přínosné zmínit, že prezentovaný argumentační rámec není jediným a čtenář může zcela jistě nalézt v dalších zdrojích další možné postupy a vhodné procesy, jak efektivně bojovat proti dezinformacím.

2 TERMINOLOGICKÉ UKOTVENÍ

Pro uvedení do problému je vhodné nejdříve nastínit, co je z terminologického hlediska považováno za dezinformace. Většina relevantních zdrojů aktuálně rozlišuje mezi základními pojmy, jako jsou dezinformace (v angličtině *disinformation*), nepravdivé informace (v angličtině *misinformation*), případně „škodlivé“ informace (v angličtině *mal-information*) či také falešné zprávy (v angličtině *fake news*). Jakkoliv se mnohé definice ve svém popisu liší, lze nalézt některé společné atributy, které determinují jejich hlavní charakteristiku. Ambicí není komparovat existující definice, ale pouze demonstrovat základní odlišnosti preferované v nejrozšířenějších zdrojích. Například Oxfordská univerzita definuje dezinformaci následovně: *„Forma propagandy zahrnující* šíření nepravdivých informací s úmyslným záměrem oklamat nebo uvést v omyl. Není pravdou, že termín má ruské kořeny (дезинформация či *dezinformatsiya), ale je odvozena z francouzštiny (dés + information).“* Slovník The Britanica dezinformace definuje jako *„nepravdivé informace, které jsou poskytovány lidem proto, aby je přiměli něčemu uvěřit nebo zatajit pravdu“* a misinformace jako *„informace, které nejsou zcela pravdivé nebo přesné“.* Webový slovník Dictionary.com považuje dezinformace za *„nepravdivé informace,*

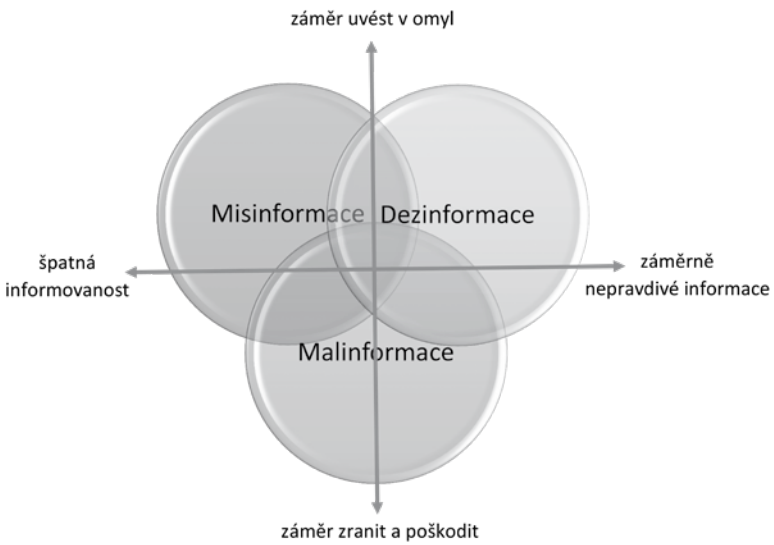
například o vojenské síle nebo plánech země, šířené vládou nebo zpravodajskou službou v nepřátelském aktu taktické politické subverze" či za *„záměrně zavádějící nebo zkreslené informace; zmanipulované narativy nebo fakta či propagandu".* Jednoduše lze shrnout, že dezinformace jsou vytvořeny a šířeny za účelem úmyslného poškození nějakého referenčního objektu či zásadního ovlivnění cílového publika (cílové skupiny).

Pojem misinformace pak můžeme obecně použít k zavádějícím informacím, které nebyly vytvořeny či šířeny se záměrným úmyslem způsobit škodu (jakkoliv tuto škodu mohou sekundárně neúmyslně generovat).

Další oblast informací označovanou jako malinformace lze popsat jako skupinu informací, které jsou většinou založeny na realitě, ale jsou určeny k ublížení osobě, organizaci, skupině obyvatel nebo zemi (např. někdo použije obrázek mrtvého dětského uprchlíka bez kontextu ve snaze podnítit nenávist ke konkrétní etnické skupině, proti které jsou apod.).

Skupinu fake news pak můžeme charakterizovat jako soubor zpráv či příběhů diseminovaných primárně na Internetu, které nejsou pravdivé a mohou svým atributy zapadat do kategorie dezinformací či misinformací.

Pro ucelení generalizace základních pojmů je přínosné ještě doplnit, že za dezinformaci nemůžeme obecně označovat odlišné názory, omyly či nepřesnosti, které nemají signifikantní vliv na podstatu sdělení. Průkaznější rozdělení uvedených hlavních skupin informací nám může podat teoretický rámec vymezený podle studie autorů WARDLE a DERAKSHAN z roku 2017, který je přehledně znázorněn na následujícím obrázku.



Obrázek č. 1: Tři základní typy informačních mutací[1]

[1] Vlastní zpracování na základě odborného článku HELVOORT, Jos van, HERMANS, Marianne. Effectiveness Of Educational Approaches To Elementary School Pupils (11 Or 12 Years Old) To Combat Fake News. Media Literacy and Academic Research. Vol. 3, No. 2, 2020. [online]. Available at: <https://www.mlar.sk/wp-content/uploads/2020/12/3_Helvoort_Hermans.pdf> [Accessed 6 April 2022].

3 VÝZNAMNÉ LEGISLATIVNÍ DETERMINANTY

Záměrem této podkapitoly je poskytnout čtenářům základní vhled do právní oblasti, který poukazuje na signifikantní faktory vztahující se na současné právní prostředí České republiky. Ambicí není nikterak diskutovat současnou legislativní stránku, ale zdůraznit klíčové vlivy, které s právní oblastí související a mohou zásadním způsobem ovlivnit procesy a dopady analyzovaného fenoménu.

S exponenciálním růstem digitálních informací a jejich téměř neregulovaným šířením (především na sociálních sítích a obecně v prostředí globální sítě Internet) narůstá také obtížnost rozpoznání původu obsahu či primárního zdroje těchto informací. Tato skutečnost tak logicky generuje související hrozby spojené zejména s uživateli všech možných komunikačních a informačních digitálních platforem. Tyto hrozby lze však z určité perspektivy považovat za rozporuplné a nelze je základními právními mechanismy komplexně regulovat a eliminovat. Zejména v případě snahy o minimalizaci šíření dezinformací je v demokratických systémech velmi problematické nalézt jednoznačné hranice a optimální vyvážení mezi svobodou projevu a protiprávním jednáním. Například v případě České republiky (pomineme-li jiné než mírové stavy) jsou pravidla šíření informací založena na listině základních práv a svob. Listina základních práv a svobod České republiky jako integrální součást českého ústavního pořádku determinuje, že svoboda projevu a právo na informace jsou zaručeny. Dále pak, že 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. Je zde zmíněna také nepřípustnost cenzury a také fakt, že svobodu projevu a právo vyhledávat a šířit informace lze omezit zákonem, jde-li o opatření v demokratické společnosti nezbytná pro ochranu práv a svobod druhých, bezpečnost státu, veřejnou bezpečnost, ochranu veřejného zdraví a mravnosti.[2]

Používané algoritmy současných sociálních sítí umožňují zásadním způsobem akcelerovat šíření dezinformací směrem k početnějšímu cílovému publiku, než tomu bylo před několika lety. Zásadní úlohu při adresné distribuci požadovaných informací uživatelům hrají takzvané soubory „cookie“. Zejména jejich podmnožina označovaná jako „profilové soubory cookie“[3] je využívána pro účely zasílání reklamních sdělení odpovídajících preferencím uživatelů. Tyto pak logicky mohou být zneužity pro intenzivnější šíření dezinformací, jakožto úmyslného marketingového produktu. Vzhledem k mimořádně invazivní povaze těchto souborů a svým dopadům, které mohou mít na soukromí širokého spektra uživatelů, stanovila evropská legislativa požadavek, aby byli uživatelé o používání

2 Usnesení předsednictva České národní rady ze dne 16. prosince 1992 o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky. Ústavní zákon č. 2/1993 Sb. ve znění ústavního zákona č. 162/1998 Sb. [online]. Available at: <https://www.psp.cz/docs/laws/listina.html> [Accessed 6 April 2022].

3 Netbox – Co jsou cookies? 2022. [online]. Available at: <https://www.netbox.cz/cookies> [Accessed 6 April 2022].

souborů "cookie" náležitě informováni a aby udělili souhlas s jejich používáním.[4] Tento souhlas v podobě velmi jednoduché praktické akceptace (jedno kliknutí či potvrzení POP-Up okna[5]) však není zásadní ochranou před příjmem někdy poměrně toxických dezinformací.[6]

V případě úspěšného čelení dezinformacím je nutné podotknout, že tento fenomén není jen odpovědností státu a jeho institucí (zejména bezpečnostního charakteru), ale také celé společnosti, včetně jednotlivců. Jakkoliv můžeme v posledních měsících pozorovat intenzivnější veřejnou debatu na toto aktuální téma mezi politickou reprezentací, v informačním prostředí rezonuje také snaha dalších nestátních či nevládních subjektů (think-tanky, univerzitní spolky či pracoviště apod.) zabývat se tímto problémem. Záměrem všech zainteresovaných subjektů (od státních institucí, přes nestátní subjekty až po samotné jednotlivce) by měl komplexní přístup v posilování odolnosti celé společnosti jako celku vůči dezinformacím. Dalším následným celospolečenským úkolem by mělo být přispívání k eliminaci dalšího šíření dezinformací.

4 INOVATIVNÍ PROCESNÍ MODEL ČELENÍ DEZINFORMACÍM

V této kapitole bude blíže popsán inovativní procesní model čelení dezinformacím, který je ve svém základu rozdělen na pět fundamentálních fází, které zahrnují postupně detekci (zjištění), analýzu (rozbor), verifikace (ověření), reakci (odezvu) a následnou evaluaci (vyhodnocení). Celý popsaný cyklus je graficky znázorněn na následujícím obrázku.

Obrázek č. 2: Procesní schéma dílčích fází obrany proti dezinformacím[7]

4 Ibidem.

5 Vyskakovací POP-Up okno je jednou z nejstarších metod zobrazení dalšího dokumentu uživateli. Vyskakovací okna existují již od starověku. Původní myšlenkou bylo zobrazit jiný obsah bez zavření hlavního okna. V současnosti existují i jiné způsoby, jak toho dosáhnout. Vyskakovací okna mohou být záludná zejména na mobilních zařízeních, která nezobrazují více oken současně. Více informací k předmětné problematice lze nalézt například na webu Java Script.info (https://javascript.info/popup-windows) nebo PC Encyclopedia (https://www.pcmag.com/encyclopedia/term/popup) a mnoha dalších.

6 Více informací specifikované zejména pro jednotlivé členské státy Evropské unie lze nalézt na webu Your Online Choice - a guide to online behavioural advertising (www.youronlinechoices.com).

7 Vlastní zpracování.

Jednotlivé fáze celého procesu budou následně blíže popsány, a to zejména formou grafických modelů, které pomohou potenciálním čtenářům efektivněji absorbovat klíčové kroky. Ambicí je sdílet zejména procesní mechanismy a nikoliv unifikovat přesné kroky, které jsou použitelné pouze pro přesně definovaný vzorek informací či jejich některé specifické sady. Ve vztahu k dezinformacím a jejich široké škále je vhodným přístup založen na generalizaci přístupů a nikoliv na dogmatické aplikace velmi detailních schémat na každou jednotlivou informaci. Na druhou stranu je logické, že určité zobecňování přináší také odpovídající úskalí v chybějící míře detailu, která nemusí všem zainteresovaným plně vyhovovat. Pro tyto případy lze však doporučit zevrubnější materiály (studie, příručky, publikace atd.) uvedené v poznámkovém aparátu, které mohou pomoci nalézt odpovědi na případné související otázky či hypotézy.

a) Detekce

Fáze detekce se má zaměřit na odhalení potenciálně škodlivých, zavádějících či zkreslených informací, které uživatelé přijímají. Primárním účelem je identifikovat dostupnými prostředky a vlastním kritickým myšlením odlišnosti ve sdělení, které nejsou založeny na relevantních faktech. Za hlavní skupiny detekčních mechanismů můžeme považovat procesy rozpoznání:

- zájmových informací a sdělení speciálními on-line nástroji;
- zájmových informací a sdělení specifickými systémy s prvky umělé inteligence;
- zájmových informací a sdělení vlastní činností (s využitím kritického myšlení);
- zájmových informací a sdělení partnery, spolupracovníky apod.

V rámci detekce je možné zaměřit použité techniky a postupy na britský model FIRST zahrnující klíčové dezinformační principy a techniky. Tento mnemotechnický model se jeví jako vhodný pro široké spektrum uživatelů a je blíže rozpracován v dostupné metodice[8],[9], včetně ilustrativních případových studií.

8 Resist 2 – Counter-disinformation Toolkit. Government Communication Service. UK. 2021. [online]. Available at: <https://gcs.civilservice.gov.uk/publications/resist-2-counter-disinformation-toolkit/> [Accessed 6 April 2022].

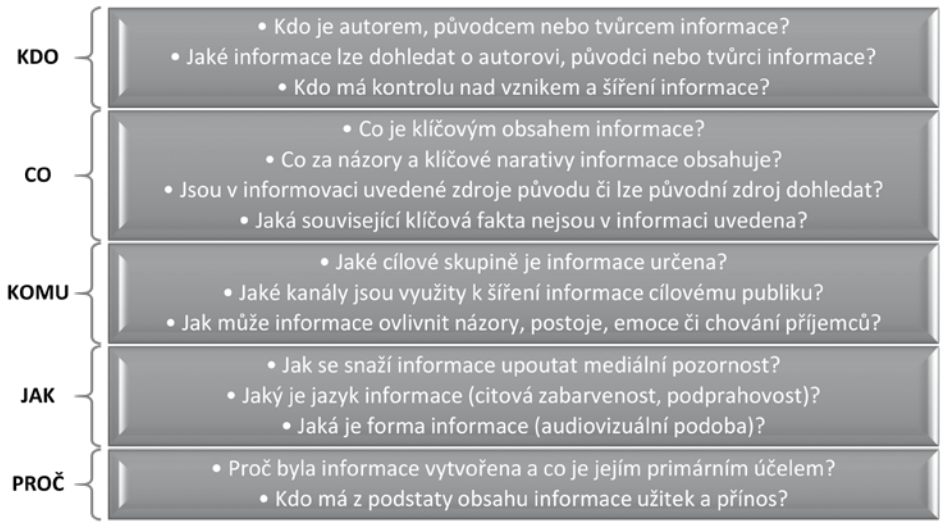
9 Pro zájemce je aktuálně dostupná také modifikovaná česká metodika, kterou zpracovalo Centrum proti terorismu a hybridním hrozbám společně s odborem komunikace britského úřadu vlády (UK Government Communication Service). Více viz Ministerstvo vnitra ČR. Centrum proti terorismu a hybridním hrozbám. 2022. [online]. Available at: <https://www.mvcr.cz/cthh/clanek/ke-stazeni-resist-prirucka-pro-boj-s-dezinformacemi.aspx> [Accessed 6 April 2022].

Obrázek č. 3: Dezinformační principy modelu FIRST[10]

b) Analýza

Po detekci podezřelých sdělení dezinformačního charakteru by měla následovat fáze analytická. V této části je potřeba provést dílčí analýzy zaměřené na původ, klíčové atributy či cíle šíření a zejména na potenciální dopady. S ohledem na uvedené argumenty je vyžadován hlubší rozbor zkoumaného sdělení s cílem nalézt odpovědi na klíčové otázky determinující povahu, původ a záměr té či oné informace (sdělení). K tomuto účelu může posloužit hloubková analýza obsahu s využitím sady pomocných otázek, které jsou znázorněny na následujícím obrázku.

10 Vlastní zpracování s využitím údajů z metodické příručky Ministerstva vnitra ČR. Viz Ministerstvo vnitra ČR. Centrum proti terorismu a hybridním hrozbám. 2022. [online]. Available at: <https://www.mvcr.cz/cthh/clanek/ke-stazeni-resist-prirucka-pro-boj-s-dezinformacemi.aspx> [Accessed 6 April 2022].



Obrázek č. 4: Soustava klíčových analytických otázek[11]

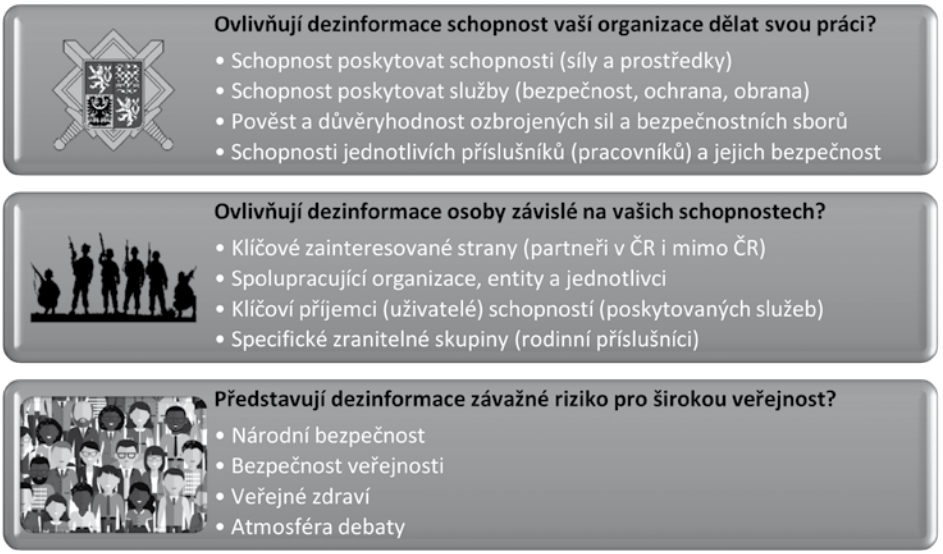
Další analytickým krokem by měla být formulace klíčových zjištění a argumentačního rámce pro další fáze celého procesu. Formulace klíčových zjištění v analytické fázi obsahuje také identifikaci nejpravděpodobnějšího cíle. V této souvislosti lze doporučit následující kategorizaci se zaměřením na:

- cíle ekonomické (finanční zisk, clickbaity atd.);
- cíle diskreditační (kompromitace aktéra – organizace, skupiny, jednotlivce);
- cíle polarizační (politická, společenská, náboženská, národnostní atd.);
- cíle vlivové – informační (podrytí bezpečnosti, suverenity, prosperity atd.);
- cíle výzvově motivované (hackerská a hráčská mentalita, výzva a získání respektu).[12]

Důležitou součástí analytické fáze by měla být rovněž dílčí analýza dopadů na vlastní důležitá aktiva (referenční objekty). Je přínosné vědět, jaké případné škody mohou jednotlivé dezinformace či závadová sdělení způsobit v souvislosti s našimi individuálními zájmy, zájmy společnosti, zájmy organizace a podobně. Klíčové oblasti, které bychom měli vzít na zřetel při posuzování dopadů, jsou demonstrativně uvedeny na následujícím obrázku. Pro potřeby tohoto článku a s ohledem na primární čtenáře byly klíčové determinanty modifikovány do bezpečnostně-obranné oblasti a rezortu obrany.

11 Vlastní zpracování s využitím údajů z metodické příručky Ministerstva vnitra ČR. Viz Ministerstvo vnitra ČR. Centrum proti terorismu a hybridním hrozbám. 2022. [online]. Available at: <https://www.mvcr.cz/cthh/clanek/ke-stazeni-resist-prirucka-pro-boj-s-dezinformacemi.aspx> [Accessed 6 April 2022].

12 Ministerstvo vnitra ČR. Centrum proti terorismu a hybridním hrozbám. 2022. [online]. Available at: <https://www.mvcr.cz/cthh/clanek/ke-stazeni-resist-prirucka-pro-boj-s-dezinformacemi.aspx> [Accessed 6 April 2022].



Obrázek č. 5: Klíčové argumenty pro analýzu dopadů[13]

Výše uvedenou sadu analytických činností nemůžeme logicky považovat za komplexní a pokrývající všechny související aspekty. Lze je však pokládat za primární k dosažení minimální efektivity v rámci čelení dezinformacím. Klíčovým doporučením je provedení analýzy původu a identifikaci možných dopadů, jakkoliv může odborná veřejnost a experti nalézt celou další škálu účinných nástrojů aplikovatelných na předmětnou problematiku.

c) Verifikace

Výše popsaná analytická fáze je úzce propojena s fází verifikace nebo-li ověřování. Zjištěné argumenty při analýze předmětné informace či sdělení by se měly stát základním vstupem pro komparaci obsahu, místa či data původu, zdroje a účelu šíření posuzované informace.

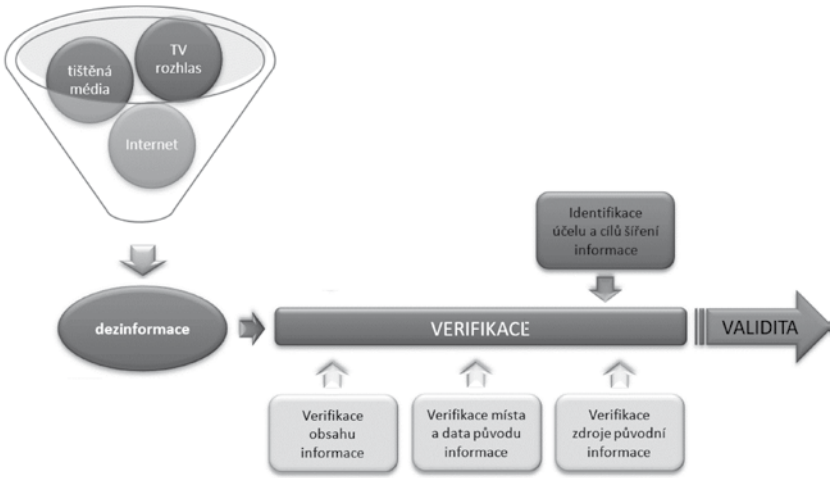
Při ověřování a porovnávání identifikovaných argumentů a základních faktů každé potenciální dezinformace či zásadního a podezřelého sdělení je vhodné vlastní úsilí zaměřit na následující oblasti:

- verifikace obsahu informace;
- verifikace místa a data původu informace;
- verifikace zdroje původní informace;
- potvrzení identifikace účelu a cílů šíření informace.

Praktické provedení této fáze může být v mnoha případech sloučeno s předešlou analytikou fází, ačkoliv jejich teoretické přístupy jsou odlišné.

13 Vlastní zpracování s využitím údajů z metodické příručky Ministerstva vnitra ČR. Viz Ministerstvo vnitra ČR. Centrum proti terorismu a hybridním hrozbám. 2022. [online]. Available at: <https://www.mvcr.cz/cthh/clanek/ke-stazeni-resist-prirucka-pro-boj-s-dezinformacemi.aspx> [Accessed 6 April 2022].

Při ověřování informací je nutná jistá dávka kritického myšlení. Je důležité se vždy zamyslet, co je samotným obsahem sdělení, kdo toto sdělení sdílel, kdo je jeho zdrojem, kde a kdy byl obsah vytvořen a za jakým účelem je toto sdělení šířeno mezi adresáty. Validita informací se nejsnáze posuzuje jejím srovnáním s nastalou skutečností. Toto však mnohdy není procesně jednoduché a v některých případech je toto téměř nemožné. Pro hodnocení validity informace proto může posloužit rozdělení procesu ověřování (verifikace) na dílčí fáze, které mohou cílovému uživateli informace vždy posloužit. Obecný proces verifikace je znázorněn na následujícím obrázku.



Obrázek č. 6: Procesní schéma verifikace informací[14]

d) Reakce

Další fází v procesu čelení dezinformacím je pak určitá odezva, jejíž forma a intenzita je závislá na mnoha faktorech. Tyto determinanty jsou propojeny zejména s dosahem, cílovým publikem či potenciálem a rozsahem možných škod (které mohou být nejrůznějšího charakteru). Na základě vyhodnocení zmíněných klíčových ukazatelů lze pak přistoupit k celé škále reaktivních opatření. S ohledem na fundamentální přesah článku do oblasti bezpečnosti byla pro základní pochopení této specifické fáze vybrána následující skupina opatření a aktivit, která svým charakterem představují možnou odezvu související s riziky šíření dezinformací a závadových sdělení. Mezi signifikantní mechanizmy odezvy můžeme zařadit:

- včasné varování klíčových osob s rozhodovací pravomocí (rozhodovací manažerská, velitelská a operační linie), a to na základě funkčních varovných systémů;[15]

[14] Vlastní zpracování s využitím odborného článku. Více viz HAVLÍK, Martin. Dissemination of misleading Information and elimination of risks resulting from them. 2017. [online]. Available at: <https://1url.cz/Pr1Cn> [Accessed 6 April 2022].

[15] V zahraničních zdrojích se varovné systémy velmi často označují termínem Rapid Alert System.

- posilování odolnosti individuálního personálu, skupiny, organizace či celé společnosti (včetně ozbrojených sil a bezpečnostních sborů či nejrůznějších resortů);
- šíření efektivních metodik a postupů pro čelení dezinformacím;
- praktické procvičování metodických postupů v rámci nejrůznějších cvičení;
- konfrontace nesrovnalostí a vyvrácení zavádějících informací;
- korekce nepravdivých informací a sdělení;
- národní regulace dezinformačních médií (webů, blogů, sítí apod.);
- publikování relevantních argumentů a fakt (příprava a podpora prohlášení);
- podpora interní a strategické komunikace (na všech úrovních);
- atribuce původního zdroje či aktéra a identifikace záměru šiřitele;
- vedení vlastních reaktivních ofensivních informačních operací apod.

e) Evaluace

Poslední fází celého procesu, ačkoliv bývá velmi často vypouštěna, je také následné hodnocení. Ačkoliv samotná evaluace procesu nemá bezprostřední vliv na šíření dezinformací a jejich dopady, může být velmi užitečná pro budoucí zefektivnění. Zejména pro střednědobé a dlouhodobé procesní mechanismy je pravidelná evaluace velmi důležitá a může včas odhalit interní, systémové či další nedostatky. Navíc může také reagovat na veškeré změny bezpečnostního prostředí (někdy velmi dynamické), může reflektovat rozvoj moderních technologií a také nových komunikačních kanálů i nástrojů.

Činnosti v rámci evaluační fáze by měly být zaměřeny především na:

- hodnocení dopadu vlastních reaktivních opatření;
- aktualizaci metodických postupů;
- tvorbu a aktualizaci odpovídajících výukových osnov pro posilování odolnosti;
- šíření povědomí o významu kritického myšlení;
- přípravu a implementaci nových nástrojů typu „Fact-checking“[16] (on-line);
- zavádění moderních detekčních nástrojů s prvky umělé inteligence;
- aktualizaci relevantních strategických a řídících dokumentů;
- využití a modifikaci postupů v rámci systému Lessons Learned;
- přípravu nových scénářů pro následná praktická cvičení;
- přípravu vhodných střednědobých a dlouhodobých komunikačních linií (narativů).

Kontinuální provádění této poslední fáze celého metodického procesu čelení dezinformacím může být velmi klíčovým akcelerátorem celkové úspěch v boji s předmětným fenoménem.

Všechny výše popsané fáze procesu čelení dezinformacím můžeme považovat za integrální součást komplexního mechanismu. Jakkoliv se přístupy a použité postupy jednotlivých uživatelů informací mohou lišit, lze při jejich zobecnění nalézt určité společné parametry. Tyto kritéria pak mohou být základním stavebním kamenem souhrnného

16 Oxfordský slovník definuje Fact-checking jako termín, jehož účelem je prozkoumat problém za účelem ověření faktů. Ověřování faktů je proces, který se pokouší potvrdit nebo vyvrátit tvrzení učiněná v řeči, tištěných médiích nebo online obsahu. 2022. [online]. Available at: <https://www.lexico.com/definition/fact-check> [Accessed 6 April 2022].

celospolečenského systému zaměřeného na boj proti dezinformacím a ochranu vlastních zájmů.

ZÁVĚR

V rámci komplexního procesu čelení dezinformacím není až tak podstatné separovat jednotlivé fáze a důsledně dodržovat nastíněné postupy, ale vždy podrobit obsah a souvislosti hodnotícímu pohledu. Tento pohled může být založen jak na určitém procesním mechanismu, tak rovněž na vlastním kritickém posouzení. Nesystémový a automatizovaný přístup však klade obecně nároky na hlubší praktické zkušenosti, zvláštní edukaci či vlohy a není bohužel efektivně aplikovatelný většinou cílového publika. Pouze intenzivní a nepřetržitá osvěta, částečná změna myšlení, posilování celospolečenské odolnosti a další související opatření mohou být zárukou úspěšnosti v rámci boje proti dezinformacím. K tomuto účelu lze tak využít dostupné metodické procesy, které mohou být účinným vodítkem pro celou škálu uživatelů.

Šíření dezinformací, misinformací, malinformací a dalších všemožných informačních derivátů může ve svém důsledku způsobit značné škody. Tyto nemusí být směřovány pouze na jednotlivce, ale v posledních letech je trendem ovlivnit mnohem širší cílové publikum a změnit pohled celé cílové společnosti a manipulovat tím veřejné mínění. Je nutné také zdůraznit, že se uvedené informační techniky staly nedílnou součástí vlivových informačních operací, bez kterých si aktuálně nelze představit žádné konflikty či krizové situace nejrůznějšího charakteru. V kontextu hlavních argumentů uvedených v tomto článku tak nelze tedy význam dezinformací vnímat pouze v kontextu ohrožení individuálních zájmů či osobní diskreditace, ale je nutné zvažovat i neoddiskutovatelné silové efekty. K těmto lze přiřadit nutnou adaptaci nových způsobů vedení operací, které mají v posledních letech multidoménový charakter a staly se nedílnou součástí všech konfliktů či krizových situací.

Dodatek autora:

V rámci rozšíření pohledu na zkoumanou problematiku je na závěr článku úmyslně zařazen také následující krátký exkurz popisující současný stav v Evropské unii. Významné iniciativy a přístup EU k dezinformacím lze nalézt v obsáhlé příručce[17]*. Evropská unie (konkrétně Evropská komise) financuje celou řadu projektů, které se zabývají problematikou boje proti dezinformacím (včetně aktuálního fenoménu sociálních sítí).*[18] *Mimo uve-*

17 Automated tackling of disinformation. Brussels. European Union - European Parliamentary Research Service. 2019. ISBN 978-92-846-3945-8.

18 Evropská komise. Financované projekty zabývající se bojem proti dezinformacím. 2022. [online]. Available at: <https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/fighting-disinformation/funded-projects-fight-against-disinformation_cs#jin-vsouasn-dob-pouvan-nstroje> [Accessed 6 April 2022].

dené projekty se Evropská unie angažuje plošně v boji proti šíření dezinformacím (nejen na Internetu), aby zajistila ochranu evropských hodnot a demokratických systémů. Šíření dezinformací i *misinformací* může mít řadu důsledků, jako je ohrožení evropských demokracií, polarizace diskusí, ohrožení zdraví, bezpečnosti a životního prostředí občanů unie.[19]

Autor: ***Plk. gšt. PhDr. Ing. Martin Havlík, Ph.D., MBA, Msc., LL.M.****Pracovník Ministerstva obrany České republiky. Specializuje se na zpravodajskou problematiku, zejména pak na oblast technických zpravodajských disciplín, informačních a kybernetických operací jakožto nedílné součásti hybridního působení státních i nestátních aktérů. Mimo uvedené se dlouhodobě zaměřuje na analýzy bezpečnostních hrozeb a rizik v oblastech konfliktů (především v Asii) s dopadem na obranu a bezpečnost České republiky.*

Jak citovat: HAVLÍK, Martin. Inovativní pohled na metodický proces čelení dezinformacím. *Vojenské rozhledy*. 2022, 31 (4), 023-036. ISSN 1210-3292 (print), 2336-2995 (on-line). Available at: www.vojenskerozhledy.cz.

19 European Commission. Tackling online disinformation. 2022. [online]. Available at: <https://digital-strategy.ec.europa.eu/en/policies/online-disinformation> [Accessed 6 April 2022].