Kybernetická bezpečnost v prostředí hybridní války

David Šikuta

Bakalářská práce
2023

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

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

Akademický rok: 2022/2023

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**David Šikuta**
Osobní číslo:	**L20659**
Studijní program:	**B1022A020002 Management rizik**
Forma studia:	**Kombinovaná**
Téma práce:	**Kybernetická bezpečnost v prostředí hybridní války**

Zásady pro vypracování

1. Definujte základní pojmy, fenomény zkoumané problematiky a proveďte řešerši relevantní literatury.
2. U vybraných fenoménů diskutujte rizika a hrozby spojené s kybernetickou bezpečností v kontextu armádních procesů.
3. Vhodnou formou navrhněte technická a organizační opatření k ošetření identifikovaných nedostatků.

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

Seznam doporučené literatury:

1. ŘEHKA, Karel. *Informační válka*. Praha: Academia, 2017. XXI. století. ISBN 978-80-200-2770-2.
2. SEDLÁK, Petr a Martin KONEČNÝ. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. Brno: CERM, akademické nakladatelství, 2021. ISBN 978-80-7623-068-2.
3. SMEJKAL, Vladimír, Tomáš SOKOL a Jindřich KODL. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-765-8.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **Ing. Pavel Valášek**
Ústav krizového řízení

Datum zadání bakalářské práce: **1. prosince 2022**
Termín odevzdání bakalářské práce: **5. května 2023**

L.S.

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

Ing. et Ing. Jiří Konečný, Ph.D.
ředitel ústavu

V Uherském Hradišti dne 2. prosince 2022

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: 5.5.2023

Jméno a příjmení studenta: David Šikuta

.....
podpis studenta

ABSTRAKT

Bakalářská práce se zabývá kybernetickou bezpečností při vedení hybridní války se zaměřením na informační bezpečnost a ovlivnění vojáků a obyvatelstva. Na zkoumanou problematiku bylo nahlíženo jak v mírových podmínkách, tak ve válečném stavu a přímém operačním nasazení vojáků. Byla použita analýza rizik PHN, návrh základní struktury školení, vytvořena pomůcka pro chování na sociálních sítích a příklady použití a dopadů útoků k ovlivnění vojsk a obyvatel.

Klíčová slova: Kybernetická bezpečnost, hybridní válka, kyberprostor, dezinformace, propaganda.

ABSTRACT

The bachelor's thesis deals with cyber security in the conduct of hybrid warfare with a focus on information security and influencing soldiers and the population. The researched issue was looked at both in peacetime conditions and in a state of war and the direct operational deployment of soldiers. A PHN risk analysis, design of a basic training structure, a tool for social media behavior and examples of the use and impact of attacks to influence troops and populations were used.

Keywords: Cybersecurity, hybrid warfare, cyberspace, disinformation, propaganda.

Děkuji mému vedoucímu práce Ing. Pavlu Valáškovi za jeho věcné rady, pomoc, přístup a odborné vedení. Poděkování také patří kolegům, kteří si našli čas a pomohli s vypracováním týmových částí práce. Velké poděkování patří i mé manželce Kláře, která mi byla velkou oporou.

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

OBSAH

ÚVOD

Problematika útoků v kybernetickém prostoru proniká do povědomí jak armád, tak obyvatel po celém světě. Stává se fenoménem moderního boje a z pohledu bezpečnosti obrovskou výzvou. Armády postupně uznávají kybernetický prostor jako bojiště a zavádí různá opatření. Vznikají nové jednotky se specializací pro informační válku a boj v kybernetickém prostoru. Nicméně informační válka probíhá na všech frontách po boku válečného úsilí již po tisíciletí. S časem se mění jen médium a prostředky dopravy na cíl.

V této práci je cílem popsat prostředky pro boj a obranu v kybernetickém prostoru, důsledky útoků a rizika spojená s hybridní válkou se zaměřením na dvě problematiky. V první části zaměření na únik, nebo zisk informací v kybernetickém prostoru, zejména přes nejrozšířenější platformy pro sdílení informací, vyhodnocení rizika a důsledků a následné zhodnocení ohrožení vlastních jednotek. V druhé části na ovlivnění vlastních i cizích vojsk a obyvatel. Návrh určitých řešeních založených na přípravě jak v době míru, tak v bojových situacích.

K ošetření rizik v provázaném systému kybernetického prostoru a skutečného bojiště musíme kombinovat jak prvky přípravy v podobě školení, tak prvky tvrdšího přístupu, například v podobě fyzické bezpečnosti, kdy je ohrožení na spadnutí, jednotka v pohybu, nebo již v prostoru operace a selhání jednotlivce reálné. Mírová doba a válečný stav se zásadně liší v přístupu. V přední linii dotyku s nepřítelem je školení spíše nereálné, v době míru zase destrukce mobilní sítě zbytečná. Mezi oběma stavy silně osciluje práce velitelů na nižších stupních, jejich práce s lidmi, schopnost pojmenovat a odhalit konkrétní rizika a zvolit správný postup k ošetření rizika.

První část struktury práce je teoretická s vysvětlením pojmů, seznámením s analýzou, vysvětlením a trochou historie hybridního válčení, až k seznámení s prostředky používanými k boji a obraně. Druhá část je praktická s vyhodnocením rizik a dopadů, návrhem opatření a několika příklady použití jak vůči nepříteli, tak vůči vlastním vojskům a obyvatelstvu.

I. TEORETICKÁ ČÁST

1 DEFINICE ZÁKLADNÍCH POJMŮ

Pro zvládnutí obrany, tedy zabezpečení a ovládnutí kyberprostoru jako bojiště, je důležité definovat, vymezit a pochopit jak samotný kyberprostor, tedy místo, kde se střet odehrává, tak prostředky pro vedení boje a definovat si cíle útoků, možnosti obrany a určit si obrannou linii.

V dnešní době, která plně využívá ICT (informační a komunikační technologie) se hrozba kybernetického útoku neustále zvyšuje a stává se moderním nástrojem zločineckých skupin, teroristických organizací a jednotlivých států. Zatím co zločinci a zločinecké organizace útočí za vidinou peněz na státní správu, nebo soukromý sektor, teroristé útočí na státní infrastrukturu a objekty za účelem dosažení svých cílů, tak státy jako takové začleňují kybernetický prostor do obranných doktrín a mluví se o něm jako o pátém bojišti. Kyberprostor tak po zemi, vzduchu, vodě a vesmíru zastává pátou dimenzi bojových operací. Přitom před pár lety byl kyberprostor z pohledu bojových operací považován jen za nějakou spojnici původních čtyř bojišť. K oficiálnímu uznání došlo až v roce 2016 na summitu NATO (Severoatlantická aliance) ve Varšavě, kde všechny členské státy NATO označily kyberprostor jako pátou operační doménu. (Pačka, 2019)

1.1 Kyberprostor

Definování kyberprostoru se napříč odbornou literaturou vcelku liší. První použití pojmu kyberprostor použil již v roce 1982 William Gibson v povídce „Jak vypálit Chrom“. Následně v románu „Neuromancer“ popsal kyberprostor následovně:

„Konsensuální halucinace každý den zakoušena miliardami oprávněných operátorů všech národů, dětmi, které se učí základy matematiky… Grafická reprezentace dat abstrahovaných z bank všech počítačů lidského systému. Nedomyslitelná komplexnost. Linie světla seřazené v neprostoru mysli, shluky a souhvězdí dat. Jako světla města, … William Gibson: Neuromancer (1984).“ (Kolouch a Bašta, 2019, s. 35)

V Oxfordském slovníku již najdeme modernější definování kyberprostoru, nicméně velmi strohé. K pojmu „*cyberspace“* uvádí:

„Fiktivní prostředí, ve kterém dochází ke komunikaci skrze počítačové sítě.“ (Kolouch a Bašta, 2019, s. 35)

Český výkladový slovník defacto kyberprostor nedefinuje, jen uvádí pojem *„Český kyberprostor“*, což nás odkazuje dále na definici *„kyberprostor pod jurisdikcí České republiky.“* (Kolouch a Bašta, 2019, s. 35)

Výstižnou a moderní definici lze nalézt například v knize cybersecurity (2019) od pánů Koloucha a Bašty, který zní následovně:

„Kyberprostor je virtuální realitou, nemající konec ani začátek. Tato virtuální realita je však zcela závislá na materiální podstatě, tedy technologiích nacházejících se ve světě reálném.“ (Kolouch a Bašta, 2019, s. 36)

Za zmínku jistě stojí i zákonná definice, se kterou se v odvětví kybernetické bezpečnosti můžeme setkat velmi často:

„Kybernetickým prostorem je digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, službami a sítěmi elektronických komunikací.“ (Jirásek, Novák a Požár, 2022, s. 100)

Definic je spousta, některé rozsáhlejší, některé velmi strohé. Každá je vyložena v kontextu literatury a témat různých autorů a jejich pohledu na problematiku. Na jednu stranu je kyberprostor popisován jednoduše jen do základní úrovně, což je snadno vstřebatelné a pro představu dostačující. Na druhou stranu se dá popsat do hloubky, jako například v dokumentu armády USA „Cyberspace Operations: Concept Capability Plan 2016-2028“, který jej rozděluje do tří vrstev, a to do fyzické, logické a sociální. Každou z nich poté popisuje a skládá do dalších pěti komponent. Zmíněný dokument definuje pojem kyberprostor takto:

"A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.“ (Cyberspace Operations Concept Capability Plan 2016-2028, 2010, s. 6)

Což lze přeložit následovně:

„Globální doména v informačním prostředí sestávající ze vzájemně závislé sítě infrastruktur informačních technologií, včetně internetu, telekomunikačních sítí, počítačových systémů a řídících jednotek.“ (Cyberspace Operations Concept Capability Plan 2016-2028, 2010, s. 6)

V dnešním pojetí se tedy kyberprostor nejčastěji uvádí v prostoru informačních sítí, i když přesná definice a vymezení aktuálně neexistuje a každá literatura k tomuto pojmu přistupuje individuálně dle konkrétní problematiky, kterou se zabývá a řeší.

1.2 Bezpečnost v kyberprostoru

Díky přesahu do různých bezpečnostních sfér a také ve stínu různých incidentů v kyberprostoru se v posledním desetiletí zesílil význam kybernetické bezpečnosti jak na úrovni široké veřejnosti, tak na úrovni státu a jeho bezpečnostní politiky. S tím je spjata potřeba o zachování komplexní bezpečnosti České republiky. Kybernetická bezpečnost se tak dotýká každého uživatele, který využívá ICT v každodenním životě, jak k soukromým účelům, tak k těm pracovním. Každý uživatel může svým chováním způsobit bezpečnostní incident a umožnit, nebo ulehčit útočnou akci v kyberprostoru. Tyto slabé články v zabezpečení útočníci vyhledávají a snaží se je využít pro své účely, ať už pro prolomení zabezpečení pomocí technologií a postupů, nebo díky sociálnímu inženýrství.

1.3 Aktivum

Jako aktivum označujeme vše, co má pro daný subjekt nějakou hodnotu. Tato hodnota může být snížena působením hrozby. Aktiva dělíme do dvou základních skupin:

Hmotná – do této kategorie patří například budovy, pozemky, peněžní hotovost, vybavení.

Nehmotná – pod nehmotná aktiva zařadíme například informace, morálku, know-how, autorská práva.

1.4 Bezpečnost

Tento pojem, ač všeobecně známý, není napříč literaturou a různými vědními obory definován zcela jednotně. Většina definic se však shodne, že se jedná o určitý stav, ať už jednotlivců, skupin, společností, či států, kdy se tito necítí ohroženi hrozbami, nebo se považují před možnými hrozbami dostatečně chráněni. (Smejkal, Sokol a Kodl, 2019)

Security a safety

Velmi často české pojetí slova „bezpečnost“ zahrnuje dva anglické pojmy. V zahraniční literatuře se zpravidla setkáváme s rozdělením pojmu na „security“ a „safety“. Na obě anglická slova můžeme velmi často narazit i v české literatuře nejen o kybernetické bezpečnosti.

- **Security** – Tento pojem se používá ve smyslu aktivní ochrany a zabezpečení.
- **Safety** – Tento pojem se využívá v případě vyjádření pasivní bezpečnosti nebo charakteristice stavu.

Neurčitost pojmů lze vidět například mezi knihami CyberSecurity (Kolouch a Bašta, 2019) a Bezpečnost informačních systémů (Smejkal, Sokol a Kodl, 2019), kdy první uvádí u pojmu bezpečnost anglický název security a druhá u stejného pojmu safety. Druhá zmíněná security překládá jako zabezpečení.

1.5 Fyzická bezpečnost

Obecně se jí rozumí systém technických, organizačních a režimových opatření. (Smejkal, Sokol a Kodl, 2019)

1.6 Hrozba

„Potenciální příčina nechtěného incidentu, jehož výsledkem může být poškození systému nebo organizace.“ (Jirásek, Novák a Požár, 2022, s. 73)

1.7 Riziko

Výkladový slovník kybernetické bezpečnosti riziko definuje následovně:

- *„Nebezpečí, možnost škody, ztráty, nezdaru.*
- *Účinek nejistoty na dosažení cílů.*
- *Možnost, že určitá hrozba využije zranitelnosti aktiva nebo skupiny aktiv a způsobí organizaci škodu.“* (Jirásek, Novák a Požár, 2022, s. 154)

1.8 Kybernetické riziko

Je rizikem, které způsobuje hrozba v kyberprostoru. (Jirásek, Novák a Požár, 2022)

1.9 Zranitelnost

Jedná se o slabé místo aktiva, nebo nedostatek v jeho ochraně. Zranitelnost může hrozba využít pro působení svého negativního vlivu na dané aktivum, subjekt, případně jeho části. Zranitelnost vyjadřuje citlivost aktiva na určitou hrozbu. (Smejkal a Rais, 2013)

1.10 Protiopatření

„Protiopatření je postup, proces, procedura, technický prostředek nebo cokoliv, co bylo speciálně navrženo pro zmírnění působení hrozby (její eliminaci), snížení zranitelnosti nebo dopadu hrozby. Protiopatření se navrhují s cílem předejít vzniku škody nebo s cílem usnadnit překlenutí následků vzniklé škody.“ (Smejkal a Rais, 2013, s. 449)

1.11 Cookies

Anonymita v kybernetickém prostoru končí už při prvním otevření webové stránky používající tzv. cookies, česky přeloženo jako sušenky. Ty obsahují malé množství dat stažené z navštívené internetové stránky do zařízení. Jakmile internetovou stránku navštívíme znovu, zařízení odešle data zpět a díky tomu může stránka identifikovat uživatele a zpětně dostává uložené informace. (Král, 2015)

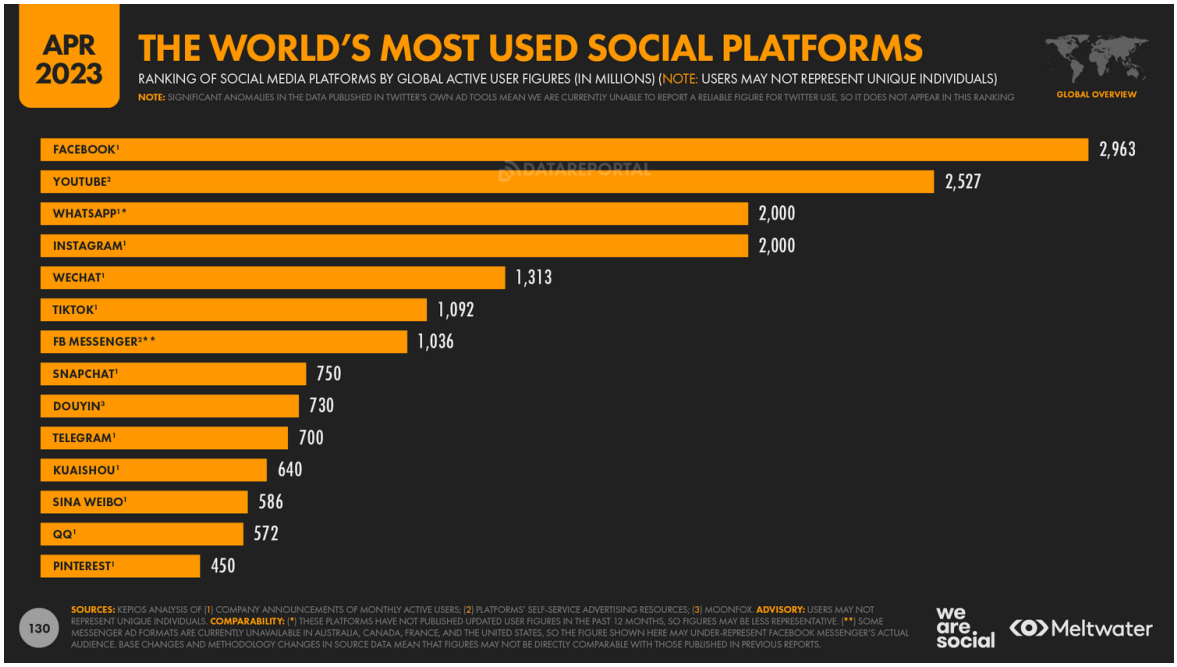
Výhody cookies spočívají v uložení informací, které nemusí uživatel zadávat opakovaně, jako jsou například různá nastavení stránky, uložení přihlašovacích údajů, zvýraznění již zobrazených odkazů, uchování nákupního košíku a uložení polohy výdejního místa. Pro běžné použití se jedná o výborného pomocníka. Nicméně jak bývá často zvykem, i tento dobrý sluha může být zlým pánem. Pokud si internetová stránka stáhne cookies, zjistí o uživateli veškerou uloženou historii. (Petrowski, 2014)

V běžném životě se zpravidla používají na jedné straně právě pro uchování určitých nastavení tak, aby uživatel nemusel vše vyplňovat znovu a ulehčují mu život, na straně druhé pro cílenou reklamu. V případě bezpečnosti můžou vyzradit například přibližnou polohu, a to nejen přesnou podle GPS (globální poziční systém), ale i podle připojeného uzlu mobilní sítě.

1.12 Sociální sítě

Jedná se o internetové služby, které jsou určené pro vytváření profilů umožňujících sdílet fotografie, videa, informace a jiné aktivity mezi svými členy. Můžou být například uzavřené, veřejné, firemní, sloužit jako diskusní fóra apod. Zpravidla obsah tvoří sami uživatelé, kdy poskytují buď informace o své osobě, svém životě a práci, nebo jsou součástí různých skupin na kterých si vzájemně vyměňují tematické informace. (Kožíšek a Písecký, 2016)

Data ukazují stálý nárust uživatelů a dle údajů k dubnu 2023 používá sociální sítě 4,8 miliardy uživatelů, což odpovídá 59,9% světové populace. Za poslední rok vzrostl počet uživatelů o 150 miliónů. (DataReportal, 2023)



Obrázek 1: Počet uživatelů sociálních sítí – duben 2023 (DataReportal, 2023)

1.13 Aplikace s možností sdílení informací

Mezi běžnými uživateli převládá sdílení informací a polohy v mobilních aplikacích jako jsou například:

- aplikace sociálních sítí,
- chatovací aplikace,
- aplikace pro záznam sportovních aktivit.

Přes tyto aplikace lze zveřejňovat informace, multimédia, polohu apod. Všechny tyto aplikace vyžadující přístup k poloze často dokážou polohu uložit a následně sdílet na profilu uživatele včetně dalších doprovodných informací, jako je třeba datum, kdy se daném místě nacházel.

Novým trendem je nositelná elektronika, která sdílí například i sportovní aktivity a na ně navázanou polohu.

2 ANALÝZA RIZIK

Pokud chceme nějaké riziko snížit, musíme jej nejprve analyzovat. Toho docílíme definováním hrozeb, míru pravděpodobnosti a to, jaký bude reálný dopad na aktiva. V první fázi musíme rizika identifikovat, což zahrnuje zpravidla tyto činnosti:

- identifikaci aktiv,
- stanovení hodnoty aktiv,
- identifikaci hrozeb a slabin,
- stanovení závažnosti hrozeb a míry zranitelnosti.

Po identifikaci rizik můžeme přejít k jejich vyhodnocení, což zpravidla zahrnuje tyto kroky:

- Posoudit, jaký bude mít dopad uskutečněná hrozba na dané aktivum.
- Nastavit si úrovně rizik.
- Určit, zda jsou rizika akceptovatelná, či neakceptovatelná.

Aby se rizika dala správně vyhodnotit, je potřeba zvážit tyto aspekty:

- Jaká aktiva budou poškozena při naplnění hrozeb a jaké potencionální důsledky mohou nastat.
- Jaká je reálná pravděpodobnost příchodu takového rizika, a to jak z pohledu hrozeb, které převažují, tak míry zranitelnosti aktiva a situace po aplikaci opatření ke snížení rizika. (Smejkal a Rais, 2013)

Metody analýzy rizik dělíme do tří skupin:

- **Kvalitativní metody –** popisuje závažnost a pravděpodobnost, že daná událost nastane. Rizika vyjadřuje například bodovým ohodnocením, pravděpodobností, případně i slovně. Používají se například stupnice 1-10 k bodovému ohodnocení, nebo stav 1-0 k určení pravděpodobnosti, případně nízké, střední, vysoké jako slovní ohodnocení. Jedná se o metodu, která je více subjektivní a tvoří se kvalifikovaným odhadem. Tyto metody se používají pro jejich jednoduchost a rychlost, nebo v případě nedostatku kvality či kvantity číselných údajů.
- **Kvantitativní metody –** zakládají se na matematickém výpočtu a používají stejné způsoby číselného ohodnocení jako metody kvalitativní. Hlavní rozdíl je v jejich výstupu. Tím je nějaké číselné ohodnocení dopadu, zpravidla ve financích, jako jsou

Kč, nebo EUR. Jedná se o více exaktní metodu, která je složitější a náročnější na čas než metoda kvalitativní. Přesnost výstupů je přímo závislá na přesnosti vstupních dat.

- **Kombinované metody –** vycházejí z kvantitativních vstupů, ale mají kvalitativní neboli slovní výstup. (Smejkal a Rais, 2013)

2.1 Metody identifikace rizik

V současné době není jediný správný způsob identifikace rizik. Ta se řeší různě dle zkušeností, oboru, prostředí a hloubky identifikace. Pro správnou analýzu rizik je potřeba určit kontext a definovat mantinely, poté je možné identifikovat buď dílčí, nebo komplexní soubor rizik. K identifikaci rizik se nejběžněji používají tyto metody:

- pozorování,
- brainstorming,
- delphi,
- analýza incidentů,
- procesní analýza,
- analýza aktiv,
- rozhovory,
- kontrolní seznamy,
- analýza hrozeb a zranitelností,
- afinity diagramy,
- diagramy příčin a následků. (Clever and smart, 2010)

2.1.1 Pozorování

Jedná se o základní metodu používanou pro určitý start analýzy, nebo jako určitý výchozí bod založený na praxi, anebo pro částečnou analýzu konkrétní skupiny rizik. Dále se dá uplatnit v případech, kdy neexistuje registr, či již nějaká zpracovaná analýza, která by se dala o pozorovaná rizika rozšířit. (Znalostní systém prevence rizik v BOZP, 2023)

2.1.2 Brainwriting

Metoda podobná brainstormingu, jen s tím rozdílem, že nápady se zapisují na lísteček. Menší skupina lidí, zpravidla 3-12, ohraničená časem většinou několika málo jednotek minut a počtem návrhů, které má účastník uvést. (Doležal, Máchal a Lacko, 2012)

2.2 Metody hodnocení rizik

V dalším kroku se identifikovaná rizika ohodnotí a zjistí se tak jejich závažnost. Správné hodnocení vychází ze zkušenosti a znalostí analytika. Hodnocení určí přijatelnost či nepřijatelnost rizika, případně míru daného rizika. K hodnocení rizik je k dispozici opravdu velké množství metod. Různé metody jsou určeny pro různé obory či rizika. Z tohoto důvodu se různé metody zpravidla nedají porovnávat mezi sebou. Mezi rozšířené metody hodnocení rizik patří například:

- checklist,
- bodová metoda,
- FMEA (Analýza možného výskytu a vlivu vad),
- what – If,
- bezpečnostní prohlídka. (Znalostní systém prevence rizik v BOZP, 2023)

2.2.1 Bodová metoda PNH

Tato metoda hodnotí míru rizika podle kombinace pravděpodobnosti výskytu rizika a možné závažnosti následku. Chráněným zájmem v této metodě bude lidský život a zdraví. V prvotní fázi lze vytvořit matici rizik ze vzorce R = P x Z, kdy nám součin pravděpodobnosti **P** a závažnosti **Z** určí míru rizika **R**. Tím si kategorizujeme a ujasníme akceptovatelnost rizika. Dále lze použít metodu analýzy rizik PNH se vzorcem R = P x N x H, kdy součinem pravděpodobnosti **P**, následků **N** a názoru hodnotitelů **H** určíme míru rizika **R**. Ve výsledné tabulce uvedeme rovnou i zvolená opatření vztahující se ke konkrétnímu riziku. Poté můžeme vyhodnotit předpokládanou úroveň rizika po aplikaci opatření. (Váchal a Vochozka, 2013)

Základem metody jsou tabulky, které nám vyjadřují:

- Pravděpodobnost vzniku rizika, značíme P.
- Pravděpodobnost následků, značíme N.
- Názor hodnotitelů zahrnující např. závažnost, dobu působení, velikost skupiny osob, možnosti ochrany a jiné okolnosti ovlivňující míru rizika, značíme H. (Rizika a jejich analýza, 2006)

Pro objektivizaci je vhodné použít tým více hodnotitelů a do výsledné analýzy použít vážený průměr.

V první fázi je potřeba vytvořit tabulky pro hodnocení pravděpodobnosti vzniku rizika a závažnosti následků rizika. (Rizika a jejich analýza, 2006)

Tabulka 1: Pravděpodobnost vzniku a existence nebezpečí (Rizika a jejich analýza, 2006)

P – pravděpodobnost vzniku a existence nebezpečí

Nahodilá	1
Nepravděpodobná	2
Pravděpodobná	3
Velmi pravděpodobná	4
Trvalá	5

Tabulka 2: Možné následky ohrožení (Rizika a jejich analýza, 2006)

N – možné následky ohrožení

Poškození zdraví bez pracovní neschopnosti	1
Absenční úraz (s pracovní neschopností)	2
Vážnější úraz vyžadující hospitalizaci	3
Těžký úraz a úraz s trvalými následky	4
Smrtelný úraz	5

Tabulka 3: Názor hodnotitelů (Rizika a jejich analýza, 2006)

H – názor hodnotitelů

Zanedbatelný vliv na míru nebezpečí a ohrožení	1
Malý vliv na míru nebezpečí a ohrožení	2
Větší, nezanedbatelný vliv na míru ohrožení a nebezpečí	3
Velký a významný vliv na míru ohrožení a nebezpečí	4
Více významných a nepříznivých vlivů na závažnost a následky ohrožení a nebezpečí	5

Následně můžeme přejít k dalšímu kroku, kde vytvoříme tabulku pro výslednou míru rizika. Ta je součinem právě pravděpodobnosti vzniku rizika a závažnosti následků. (Rizika a jejich analýza, 2006)

Tabulka 4: Míra rizika (Rizika a jejich analýza, 2006)

Rizikový stupeň	R	Míra rizika
I.	> 100	Nepřijatelné riziko
II.	51 ÷ 100	Nežádoucí riziko
III.	11 ÷ 50	Mírné riziko
IV.	3 ÷ 10	Akceptovatelné riziko
V.	< 3	Bezvýznamné riziko

Jakmile známe míru rizika, přejdeme k poslední fázi. Tou je přijatelnost rizika. Ta musí obsahovat minimálně dvě kategorie, například přijatelné a nepřijatelné riziko, může být ale i více kategorií. Čím vetší počet kategorií, tím jemněji budou rizika odstupňována. (Rizika a jejich analýza, 2006)

Takhle máme veškeré podklady pro hodnocení identifikovaných rizik, které můžeme zapsat do tabulky rizik.

3 HYBRIDNÍ VÁLKA

I když prostředky hybridního boje jsou staré jako válčení samo, tak pojem, a hlavně užívání pojmu hybridní války, je vlastně novou záležitostí. Od expertů do médií se ve větší míře dostal teprve v souvislosti s novodobým konfliktem na Ukrajině někdy od roku 2014. O vzestupu hybridních válek psal teprve v roce 2007 americký důstojník Frank Hoffman, který je často považován za autora konceptu. Shoda na obecně akceptované definici hybridní války dnes vlastně neexistuje. Dalo by se však říct, že v základu jde o vedení boje konvenčním způsobem za podpory či přímého doprovodu nekonvenčního a asymetrického vedení boje (Kurfürst a Paďourek, 2021). Případně může jít o vedení boje bez použití konvenční síly, například za účelem oslabení, rozdělení, politického či jiného ovlivnění cílového státu. Dnes masivně vedené v kyberprostoru, tudíž bez smrtící či kinetické síly. Může jít právě o manipulaci s informacemi a informačním prostorem, útocích na kritickou infrastrukturu, ovlivňovaní politického složení aj. Výhodou je anonymita a defacto beztrestnost aktérů, nejasná hranice mezi mírem a válečným stavem, mnohem nižší cena za dosažené cíle a v neposlední řadě i mnohem nižší riziko pro vlastní zemi. Útočníkům se těžko připisuje odpovědnost, útoky jsou vedeny s velkou vágností, odezva na různé kampaně je velmi komplikovaná, případně často není útok ani identifikován či připsán alespoň nějakému státu. (Bilal, 2021)

3.1 Historie hybridní války

Při ohlédnutí do historie zjistíme, že hybridní válka není vlastně žádný nový fenomén. I když se dnes uvažuje o vedení boje převážně v prostoru ICT, tak kyberprostor je ve své základní podstatě prostředí šíření informací. A informační útoky jsou jedním z nástrojů kybernetických útoků. Když tedy pomineme dnešní technologické možnosti, prostor sítí kde se drtivá většina kybernetických útoků v dnešní době odehrává a útoky na IT (Informační technologie) systémy kritické infrastruktury, zůstává nám v historii minimálně otisk informačních útoků. A to jak získávání a využívání informací k plánování a útokům po zemi, vodě nebo vzduchu, tak použití dezinformací jako lstí, nebo úpravu myšlení obyvatelstva, vojáků a velení. Následují chybná rozhodnutí velení, koncentrace sil na místech, kam útok nepřijde, plýtvání munice na klamné cíle, pokles morálky, otočení obyvatel proti vládě, rozdělení společnosti, občanské nepokoje, dezerce, deprese anebo vyhoření vojáků. (Kurfürst a Paďourek, 2021)

Samotný pojem „hybridní válka“ vznikl přívlastkem slova, který určuje druh boje jiným způsobem. Websterův slovník uvádí u slova *„hybridní“* následující:

„cokoli, co je odvozeno či vytvořeno z různorodých zdrojů nebo složeno z prvků rozdílné nebo nesouměřitelné podstaty.“ (Kurfürst a Paďourek, 2021, s. 27)

Dalo by se tedy říct, že z historického pohledu hybridní válka označuje zakomponování jiných, než běžných a konvenčních prostředků boje k dosažení cílů a vítězství a historicky bylo vedení hybridní války běžnou součástí válečných strategií, jen chyběl onen pojem „*hybridní*“. „*Historie jevů je totiž odlišná od historie pojmů.“* (Kurfürst a Paďourek, 2021)

Nelze tedy spojit hybridní válku pevně s kybernetickým prostorem, ale jde spíše o soubor různých operací jako jsou PSYOPS (psychologické operace), lsti, špionáž apod. Kybernetický prostor v dnešním pojetí je tedy jen jedním z bojišť hybridní války.

„Vrcholem není svést spoustu bitev a vyhrát je, vrcholem je zlomit odpor nepřítele bez boje“ (Sun-c´)

4 DEFINICE PROSTŘEDKŮ BOJE A CÍLŮ ÚTOKŮ

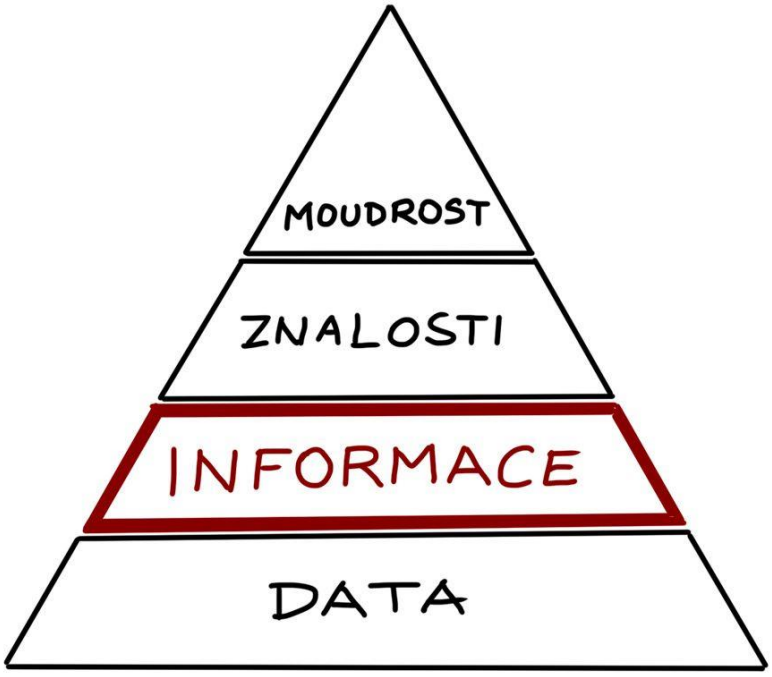
4.1 Data a informace

Informace se skládají z dat, ale data samotná nejsou informacemi. Takhle se dají shrnout definice o datech a informacích. *„Informace jsou údaje, které byly zpracovány do podoby užitečné pro příjemce. Každá informace je tedy údajem, datem, ale jakákoli uložená data se nemusejí nutně stát informací.“* (Kolouch a Bašta, 2019, s. 47)

Pokud tedy získáme nějaký údaj bez kontextu, získáme data. Například číslo 50, nebo údaj 120/80. Pokud k němu dáme kontext, či další data, která nám řeknou více, dostaneme informaci. Například když číslo 50 doplníme o km/h, dostaneme informaci o rychlosti, případně o kontext o maximální povolené rychlosti v obci na území ČR. Nebo když k hodnotě 120/80 doplníme, že se jedná o krevní tlak, dostáváme opět informaci. (Černý, 2017)

Informacemi se zabývá i norma ISO (Mezinárodní organizace pro normalizaci) 19650:

„Informace je opakovaně interpretovatelná formalizovaná reprezentace dat vhodná pro komunikaci, interpretaci nebo zpracování.“ (ČSN EN ISO 19650-1, 2019)



Obrázek 2: Informační pyramida (Ardit, 2022)

Jak ilustruje obrázek, data tvoří nejširší část. Jsou to údaje, které pro nás nemají užitek. Jakmile data obohatíme, získáváme informace. A ty už nám k užitku jsou. (Ardit, 2022)

4.2 Nevědomé odesílání informací

Uživatel může nevědomky, nebo jen vlastní neopatrností, zveřejňovat či zpřístupnit data a informace o sobě, jednotce, nebo poloze. Činit tak může například přes sociální sítě, kdy „připne“ svoji polohu ke statusu, nebo prostřednictvím cookies při prohlížení webového obsahu.

4.3 Dezinformace, misinformace a malinformace

Základem je slovo informace, před které se dále používají různé předpony, jako jsou dez-, mis– a mal-. V případě dezinformace se poté jedná o jakýsi průnik misinformací a malinformací. (BezFaulu, 2019)

4.3.1 Misinformace

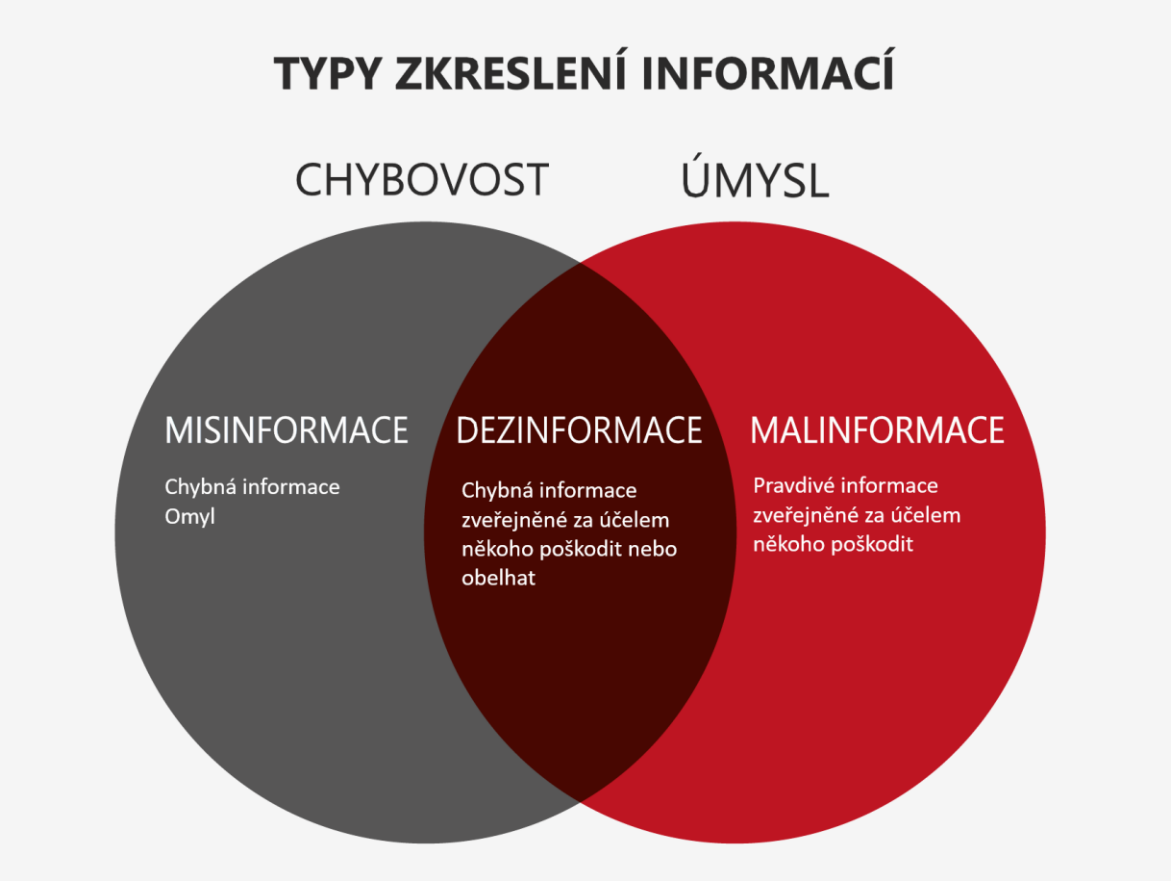
Jedná se o chybnou informaci, nikoli však záměrně. Autor udělá překlep, zamění nedopatřením fotku, zmýlí se v údaji, posune desetinou čárku apod. Tím vytvoří misinformaci. Po zjištění chyby se autor zpravidla omluví a vše uvede na pravou míru. Omluva a oprava je zřejmě nejlepším identifikátorem misinformací. (Burýšek, 2019)

4.3.2 Malinformace

Nejedná se o informaci chybnou, ale pravdivou, avšak vypuštěnou za účelem poškodit nějakou osobu, organizaci, stát apod. Může být použito například informací o nějakém osobním nebo finančním problému, citlivé informace z osobního života či zákulisí kampaní, vedení podniků, apod. Někdy se používá i tzv. revenge porn, čili zveřejnění sexuálního obsahu někoho, kdo si to nepřeje. (Burýšek, 2019)

4.3.3 Dezinformace

Jedná se o cíleně chybnou informaci vypuštěnou záměrně (Burýšek, 2019). Z historického pohledu se nejedná o nějaký nový fenomén. Dříve se nazývala lest, klam apod. Byla součástí strategie špiónů, agentů a vyzvědačů. Je nedílnou součástí vedení asymetrického boje a hybridní války po staletí. (Gregor a Mlejnková, 2018)

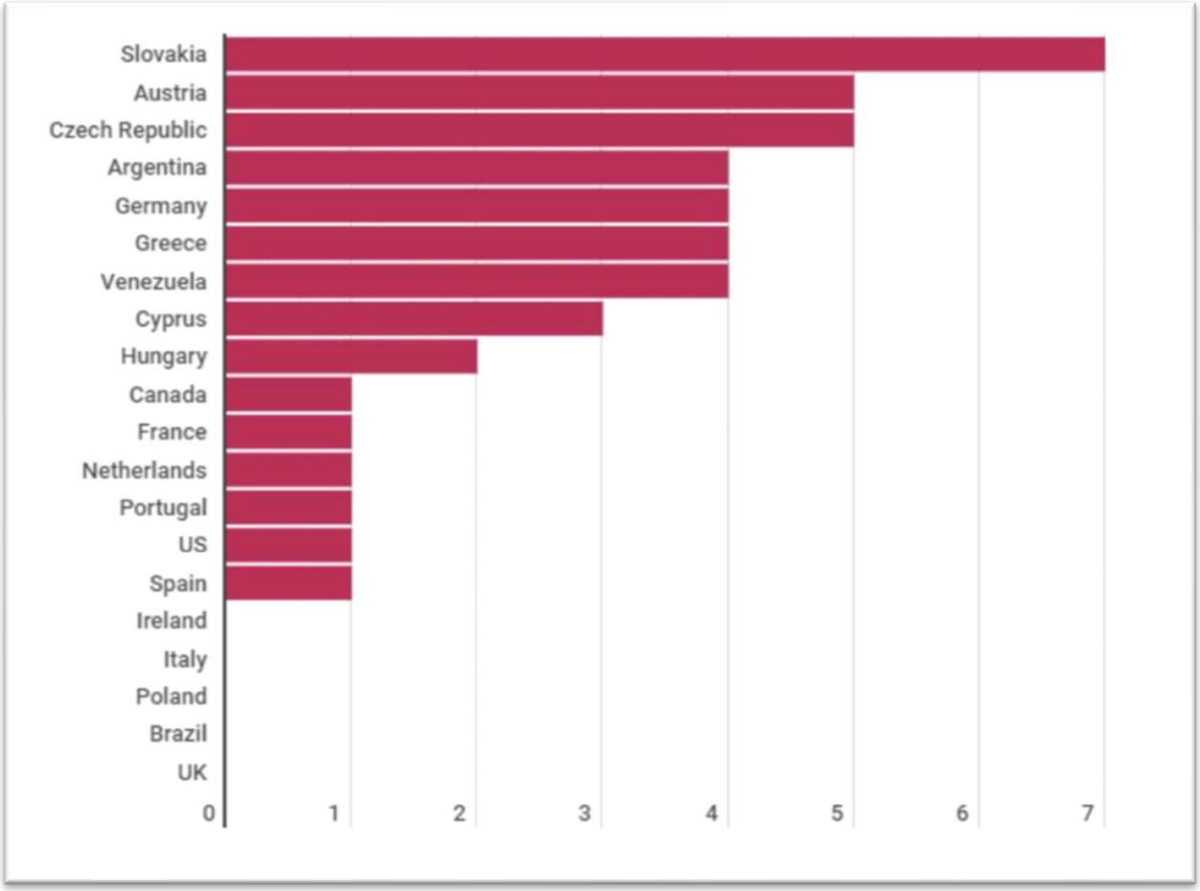


Obrázek 3: Typy zkreslení informací (BezFaulu, 2019)

Účelem dezinformací je cíleně ovlivnit náš úsudek a vnímání určitých skutečností v populaci, nebo alespoň její části. Dezinformace se tváří důvěryhodně, často se snaží jejich autoři dokládat jejich pravdivost různými důkazy, či tvrzením o zdroji informace od nějaké autority. Například jméno vědce pracujícího pro prestižní univerzitu. Není však výjimkou, že uvedené jméno zdroje buď ani neexistuje, nebo reálně s informací nemá nic společného. Zpravidla čtenář nedohledává spojitost a uvěří, že uvedený člověk toto opravdu řekl (Kopecký, 2008). Důvěryhodnost dezinformace je důležitá k zasažení co největší časti populace. Musí být takzvaně uvěřitelná. Například tvrzení, že část populace jsou ještěři nebude mít takový dosah a uvěřitelnost jako například přízemnější tvrzení o peněžních tocích v prezidentské kampani, byť také bez důkazu. (Gregor a Mlejnková, 2018)

Šíření dezinformací je v dnešní době sociálních sítí až 6x rychlejší než šíření faktů a ověřených informací. Podle studie časopisu Science je pravděpodobnost sdílení dezinformace až 70% (Dotyk, 2018). Tento trend potvrzuje i studie od organizace Institute for Strategic Dialogue, která uvádí, že v případě masakru civilního obyvatelstva ve městě Buča na Ukrajině byla polovina nejsdílenějších příspěvků právě z dezinformačních

a prokremelských webů. Na Slovensku byl dokonce počet sdílení z webů propagujících Kremelskou verzi 70%. (Zive.cz, 2022)



Obrázek 4: Počet sdílení z dezinformačních webů o masakru v Buči (Zive.cz, 2022)

4.4 Propaganda

Oxfordský slovník definuje propagandu následovně:

„Ideas or statements that may be false or present only one side of an argument that are used in order to gain support for a political leader, party, etc.“ (Oxford Learner's Dictionaries, 2023)

V překladu zní výklad takto:

„Myšlenky nebo prohlášení, které mohou být nepravdivé nebo mohou představovat pouze jednu stranu argumentu, které se používají k získání podpory politického vůdce, strany atd.“ (Oxford Learner's Dictionaries, 2023)

Propaganda působí na obyvatelstvo, nebo vojska a cíleně formuje názory, myšlenky, chování, pohled na situaci a chování a směřuje je k uplatnění cíle propagandisty. V různých

formách působí jak na nepřátele a nepřátelské obyvatelstvo, tak na vlastní vojska a vlastní obyvatelstvo. Součástí propagandy bývají často dezinformace. Rozdělit ji můžeme na následující tři směry:

4.4.1 Bílá propaganda

Je vlastně něco jako public relations na úrovni státu a využívá pravdivé informace. Místo zboží či služby ovlivňuje veřejné mínění vlastního obyvatelstva zejména ve věcech jako jsou například postoje a aktivity státu, mobilizace, diplomatické vztahy, podpora válečného úsilí, podpora kroků k ochraně obyvatelstva, bojové úspěchy apod. Tím působí i na nepřátele, kteří různými cestami dostávají informace o úspěších protivníka. (Gregor a Mlejnková, 2018)

4.4.2 Černá propaganda

Ta jako nástroje využívá polopravdy, věrohodné a tematicky vhodné dezinformace a skandály. Používá se k oslabení a pošpinění protivníka a působí na nepřátelské obyvatelstvo a vojska. Zdroje jsou zpravidla falešné, nebo úmyslně zavádějící. (Gregor a Mlejnková, 2018)

4.4.3 Šedá propaganda

Zpravidla propaguje pravdivé informace nepřátelské straně. K nepříteli se snaží dostat různými prostředky spousty informací o špatných rozhodnutích, prohraných bitvách a nezdarech ve válečném úsilí, problémech ve velení, logistice apod. (Gregor a Mlejnková, 2018)

Účinnost a dosah propagandy roste zároveň s vývojem ICT. Jak šel vývoj, tak se měnil i způsob oslovení. V novodobé historii šlo o noviny, poté rádia, televize a dnes již internet. Šíření propagandy v kybernetickém prostoru umožňuje oslovit obrovské publikum s opravdu nízkými náklady. Napsat článek na sociální síť je podstatně levnější než tisk novin, přeprava letadlem a shoz na nepřátelské území. (Táborský, 2020)

5 PROSTŘEDKY OBRANY

Prostředky obrany v kyberprostoru jsou jak technické, tak v masivním měřítku zejména uživatelské. Chování jednotlivců, přístup velení a vedení a zajištění obrany z vyšších stupňů je jedním ze základních kamenů kvalitní obranné linie.

5.1 Bezpečnost začíná u uživatele

Bezpečnost ve vztahu ke společnosti, státu, nebo dalším subjektům, ať už fyzickým, nebo právnickým je dnes aktuální téma, do kterého kybernetická bezpečnost zasahuje na většině úrovní. I když by se mohlo zdát, že se vše týká jen věcí v kyberprostoru, tak sociální inženýrství nám ukazuje opak. Dezinformace, hoaxy, hybridní vedení války, polarizace společnosti a další podobné disciplíny narušují bezpečnost společnosti skrze kybernetický prostor, ale přenosovým médiem může být dále i člověk, list papíru a podobně. To nám ukazuje, že bezpečnost v dnešní době není jen v odpovědnosti státu, i když stále na této úrovni hraje primární roli, ale že jde o veškeré subjekty na daném území, které se otázkou bezpečnosti zabývat musí jak na úrovni vlastní osoby, tak třeba na úrovni podniků.

Na základě rozšíření okruhu bezpečnosti je potřebně položit si čtyři základní otázky a zabývat se jimi:

- O čí bezpečnost se jedná?
- Jaké hodnoty jsou chráněny?
- Před čím jsou tyto hodnoty chráněny?
- Jaké zdroje nás ochrana těchto hodnot bude stát? (Kolouch, Bašta: CyberSecurity, 2019)

Vytvoření stavu absolutního bezpečí by bylo ideální, avšak jedná se o utopii. Aktuálně není možné tohoto stavu dosáhnout, jelikož vždy bude buď existovat riziko či hrozba, které není v bezpečnostním konceptu zahrnuto, nebo si útočník najde cestu, se kterou bezpečnostní opatření nepočítá, nebo na ni není připraveno.

5.2 Kybernetická bezpečnost

I u pojmu kybernetická bezpečnost nalezneme spousty různých definic, podobně jako u pojmu bezpečnost. A i zde není žádná jednotná. Platí to stejné – výklad je různý podle autorů a hloubky, do které se autor na tento problém dívá. Některé definice vymezují jen

ICT, jiné se zase zaměřují na omezený počet typů, nebo jen na konkrétní jeden typ kybernetických útoků, další se zaměřuje jen na data, nebo pouze na on-line kyberprostor i když již víme, že existuje i off-line kyberprostor. Jiné definice zase vymezují pouze právní rámec dané země, nebo společenství.

Pokud se podíváme na kybernetickou bezpečnost z pohledu zákona o kybernetické bezpečnosti zjistíme, že se jedná o bezpečnost v prostředí, které tvoří počítačové sítě, jejich prvky a všechna zařízení mající nějakou IP adresu. (Smejkal, Sokol a Kodl, 2019)

5.3 Základní principy kybernetické bezpečnosti

Pro uplatnění kybernetické bezpečnosti se užívají takzvané triády. Jedná se vždy o trojici nějakých zásad, postupů či metod. A když triády, tak ideálně alespoň tři. (Kolouch a Bašta, 2019)

5.3.1 Triáda CIA

Jedná se o nejpoužívanější a nejznámější triádu v kybernetické bezpečnosti. Písmena CIA značí dané zásady.

C – Confidentiality (důvěrnost)

I – Integrity (celistvost)

A – Availability (dostupnost)

Obrázek 5: Triáda CIA (Clever and smart, 2010)

C jako důvěrnost

Výkladový slovník kybernetické bezpečnosti definuje důvěrnost jako *„vlastnost, že informace není dostupná nebo není odhalena neoprávněným jednotlivcům, entitám nebo procesům.“* Tento pojem definuje přístup k ICT, informacím, datům apod. pouze oprávněným osobám. (Kolouch a Bašta, 2019, s. 48)

I jako integrita

Výkladový slovník nazývá integritu jako *„vlastnost přesnosti a úplnosti.“* Jedná se tedy o maximální jistotu, že data nebyla změněna a nebylo jimi neoprávněně manipulováno. (Kolouch a Bašta, 2019, s. 52)

A jako dostupnost

Výkladový slovník uvádí pod dostupností *„vlastnost přístupnosti a použitelnosti na žádost oprávněné entity.“* Jedná se o přístup k informacím, či datům oprávněným osobám v okamžiku potřeby. (Kolouch a Bašta, 2019, s. 54)

5.3.2 Parkerian hexad

Odborná literatura poukazuje na fakt, že v dnešní době prosté využití této základní triády není v kybernetické bezpečnosti dostačující. Z toho důvodu se uplatňuje tzv. **Parkerian hexad**, což je CIA triáda doplněná o tři rozšiřující prvky.

P/C – Possession/control (držení nebo kontrola)

A – Authenticity (autentičnost)

U – Utility (užitečnost)

CIA triáda, ať už v základní, nebo v rozšířené podobě, je často vztahována spíše k informacím, potažmo informační bezpečnosti. (Kolouch a Bašta, 2019)

Obrázek 6: Parkerian hexad (Clever and smart, 2010)

5.3.3 Prvky kybernetické bezpečnosti

Tato triáda se opírá o trojici prvků, které umožní do jisté míry kybernetickou bezpečnost nastolit. Velmi výstižně jednotlivé prvky triády popisuje bezpečnostní expert Bruce Schneier. Bude tedy k věci každou část zahájit citací jeho slov k danému prvku, která přeložil jeden z autorů knihy CyberSecurity. (Kolouch a Bašta, 2019)

Lidé

„Lidé často představují nejslabší článek v bezpečnostním řetězci a jsou chronicky zodpovědní za selhání bezpečnostních systémů. (Bruce Schneier)“ (Kolouch a Bašta, 2019, s. 57)

V interakci s kybernetickou bezpečností se lidé dají rozdělit následovně:

- Tvůrce bezpečnosti.
- Příjemce bezpečnosti.
- Subjekty chráněné před kybernetickými útoky.
- Subjekty, které je důležité informovat o pravidlech a principech kybernetické bezpečnosti.
- Rizika a hrozby při vytváření a udržování kybernetické bezpečnosti.

Důvodů, proč jsou lidé nejslabším článkem je hned několik. Za prvé velmi krátká doba využívání počítačových systémů. Většina lidí začala využívat počítače a systémy po roce 1990. Masové připojení k internetu začalo probíhat kolem roku 1995. Chytré telefony se masového rozšíření kolem roku 2007. Sociální sítě, které dnes považujeme za běžnou součást našich životů s námi jsou jen něco kolem deseti let. K tomu je potřeba sledovat hardware a software, který prochází rychlým a dynamickým vývojem. Dále naše potřeba a dnes už i závislost na ICT tvoří lákavé cíle útoků v kyberprostoru. (Kolouch a Bašta, 2019)

„Amatéři hackují systémy, profesionálové ´hackují´ lidi. (Bruce Schneier)“ (Kolouch a Bašta, 2019, s. 59)

Technologie

„Pokud se domníváte, že technologie dokáže vyřešit vaše bezpečnostní problémy, nerozumíte problémům a nerozumíte technologii. (Bruce Schneier)“ (Kolouch a Bašta, 2019, s. 59)

Technologie jsou prostředkem jak interakce v kyberprostoru, tak jeho zabezpečení. Pro běžného uživatele jsou to zpravidla koncové technologie jako počítač, mobilní telefon nebo třeba tablet. Pro organizace se odkrývají další vrstvy jako infrastruktura sítí, služby anebo zabezpečení. Jedná se například o LAN (Lokální počítačová síť), Wi-Fi (Bezdrátová síť), servery, aplikace, firewall apod. Zpravidla se na technologiích nešetří a jedná se o nejméně rizikovou část. Opět největší riziko přináší interakce s uživatelem, který například neudržuje systém aktualizovaný, provádí platby v nezabezpečené síti, nebo například povolí přístup k rizikovému souboru aj. (Kolouch a Bašta, 2019)

Procesy

„Mantrou dobrého bezpečnostního inženýra je: ***Bezpečnost není produkt, ale proces.*** *Je to víc než navrhnout silnou kryptografii do systému. Je to o tom navrhnout celý systém tak, aby všechna bezpečnostní opatření, včetně kryptografie, spolupracovala. (Bruce Schneier)“* (Kolouch a Bašta, 2019, s. 61)

Jedná se o souhrn činností, které je potřeba provádět pro bezpečné využívání technologií a služeb lidmi. Mezi procesy se dá pro ilustraci uvést například řízení aktiv a rizik, správa uživatelů a rolí, aktualizace systémů a služeb, testování zabezpečení, audit kybernetické bezpečnosti, reakce na útoky, školení atd.

Procesy jsou na budování nejnáročnější částí kybernetické bezpečnosti. Kladou největší důraz na jednotlivé správce systémů. Doporučuje se provádět i reálné simulace incidentů.

5.3.4 Životní cyklus kybernetické bezpečnosti

Jedná se o triádu, která řeší kybernetickou bezpečnost z pohledu plynutí času. Je aplikovatelná jak na triádu CIA, tak na dílčí prvky kybernetické bezpečnosti. U této triády se jedná o prevenci, detekci a reakci. (Kolouch a Bašta, 2019)

Prevence

Předcházení útokům, tvorba zabezpečení, školení personálu, analýzy systému apod. (Kolouch a Bašta, 2019)

Detekce

Schopnost odhalit útok ať už v reálném čase, nebo zpětně odhalit útok, který již proběhl. Například aktivní kybernetickou obranou, sledováním chování sítě a vyhodnocováním anomálií, detekcí manipulace s daty nebo systémem apod. (Kolouch a Bašta, 2019)

Reakce

Může provádět buď CSIRT (Skupina pro reakce na počítačové bezpečnostní incidenty), případně správce sítě a systému, sám uživatel, nebo software k tomu určený aj. Jedná se reakci na útok. Cílem je buď odvrácení útoku, nebo alespoň minimalizace škod. (Kolouch a Bašta, 2019)

II. PRAKTICKÁ ČÁST

6 PROSTŘEDKY BOJE A JEJICH RIZIKA

V případě hybridní války na kybernetickém bojišti je kladen důraz na informace a ovlivnění protivníka. V oblasti kybernetické bezpečnosti je tudíž důležité chránit informace a bojovat proti technikám, které polarizují společnost a pokouší se obrátit jednu její část na svoji stranu.

Prakticky lze problematiku rozdělit na dvě hlavní části:

- Informační bezpečnost.
- Ovlivnění obyvatelstva a vojáků v boji – jak vlastních, tak nepřátelských.

6.1 Příklad provedení útoku

V případě provedení by útok mohl vypadat, mimo jiné varianty, například následovně:

K dispozici máte velké množství finančních zdrojů, diplomatických nástrojů, podřízený bezpečnostní aparát. Máte možnost ovládat média a vytvářet mediální zprávy a další prostředky, které stát může využít. Utočíte na stát, u kterého vytipujete slabá místa jako jsou vlivné osoby a skupiny osob, kteří vám jsou přirozeně nakloněni, případně další nespokojené osoby, vnitřní neshody, společnosti a obchodníky, kteří jsou na obchodu s vámi přímo existenčně závislí, případně obchodem s námi vydělají. Vysledujete strategické závislosti nejen na vás, ale i na jiných státech. Provedete pečlivou analýzu, vytvoříte časovou osu, která obsahuje budoucí známé důležité události jako jsou například volby, tendry kritické infrastruktury apod. Určíte cíl, kterého chcete dosáhnout a zahájíte operace v kontextu aktuální situace, či tématu. Oslabíte pozici i u okolních států a strategických spojenců.

Poté lze zahájit útok vybranými prostředky s důrazem na vybrané cíle. Celá kampaň vedená proti nepříteli je živoucí. Je důležité vyhodnocovat účinky a upravovat systém útoků a cíle. Při nejlepším možném výsledku lze očekávat úspěch i bez použití hrubé vojenské síly, a to díky převratu, občanské válce, nebo dosazením loutkové vlády apod. A to vše za mnohem menších finančních výdajů a bez dopadu na oslabení vlastní ekonomiky a pozice ve světě.

6.2 Informační bezpečnost

Jedna zpravodajská legenda říká, že v době války v Pacifiku byla japonská armáda na jednom z ostrovů tak dobře maskovaná, že se americkým zpravodajským službám ani za pomoci mnoha přeletů průzkumných letadel a pořízení nespočtu fotografií nedařilo odhadnout počet vojáků pro důkladné naplánování útoku. Jeden ze zpravodajců se zaměřil

na jediné nemaskované místo. Byly to latríny. Obstaral si jeden z ukořistěných předpisů japonské armády a vyčetl údaj o tom kolik vojáků je maximum pro jednu latrínu. Tento údaj poté jednoduše vynásobil počtem latrín. Po bitvě a vyhodnocení bylo zjištěno, že jeho odhad byl velice přesný.

Ať už je tato legenda pravdivá nebo ne, minimálně slouží jako perfektní ilustrace práce s informacemi. Ukazuje mimo jiné, že i informace o latrínách dokáže pomoci, či uškodit. To je důvod, proč při vedení hybridní války musíme informace v kybernetickém prostoru chránit, nejlépe vůbec neuvádět, nesdílet a neposkytovat.

Dnes je kybernetický prostor plný informací využitelných protivníkem. Pověstné slovní spojení „tak si to vygoogluj“ dostává v době informační války významu i na kybernetickém bojišti. Na internetu lze nalézt spousty taktických postupů, fotografií základen a techniky, polohy lidí i objektů a nespočet dalších taktických a strategických informací.

Informace se dají poté využít ke zjištění pozic protiletecké obrany, míst velení, logistických skladů, dislokací jednotek apod.

6.2.1 Získávání informací

V dnešní době chytré elektroniky je sdílení osobních informací běžnou součástí dne u obrovského množství uživatelů. Lze nalézt fotografie ze základen, kdy zpravodajci podle okolního terénu, markantů, znaků na uniformách a technice, rozložení budov, nebo i počasí v daný moment dokáží velice přesně určit polohu jednotky.

V roce 2018 proběhlo cvičení NATO, kde se tým programátorky Nory Bitenieceové pokusil pouze skrze kybernetický prostor získat detailní informace o cvičení a ovlivnit vojáky tak, aby buď opustili pozice, nebo vyzradili nějaká tajemství či aktuální průběh cvičení.

„V zásadě jsme si kladli jen tři otázky: Co se vlastně mohu dozvědět o probíhajícím vojenském cvičení z volně dostupných informací na internetu? Mohu se ze stejně snadno dostupných zdrojů dozvědět něco konkrétního o jednotlivých účastnících cvičení? A za třetí, mohu tato data nějak využít, abych dokázala ovlivnit chování nasazených vojáků tak, aby neuposlechli pokynů a rozkazů nadřízených?“ (Facebookové flirtování vs. NATO: kontrole se povedlo ovlivnit cvičení, 2019, s. 1)

V případě tohoto cvičení bylo zjištěno, že jako hlavní platforma byl užitečný Facebook. Znepokojujícím zjištěním je, že byla rozkryta sestava, pozice, datumy jednotlivých fází cvičení i kde budou nasazeny síly hlavního útoku.

Jiná situace, která se opakovala na více místech bylo zobrazení základen v mobilní sport trackové aplikaci Strava. Vojáci a zaměstnanci základny sdíleli veřejně své záznamy o aktivitách a tím volně zpřístupnili i polohu základny. I když poloha základny v rozměru, který umožňuje běhat delší trasy uvnitř, není zpravidla utajena, tak nepřítel může lehce využít informace o kumulaci osob v určitý čas na určitém místě a provést útok například nepřímou střelbou. Osoby v tomto prostoru jsou zpravidla nekryté, bez balistické ochrany. (Fitness tracking app Strava gives away location of secret US army bases, 2018)

Obrázek 7: Vojenská základna v provincii Helmand v Afghánistánu z aplikace Strava (Fitness tracking app Strava gives away location of secret US army bases, 2018)

Stejná situace se odehrála například i na anexovaném Krymu, konkrétně na základně Belbek, kde data sdíleli ruští vojáci. (Aktuálně.cz, 2018)

Obrázek 8: Vojenská základna na Krymu, Belbek z aplikace Strava (Aktuálně.cz, 2018)

6.2.2 Identifikace rizik

Kybernetický prostor obsahuje obrovskou škálu možných rizik, která jsou dobře využitelná při vedení hybridní války. Informace, ať už v době míru, nebo konfliktu nízké a vysoké intenzity, jsou a budou vždy žádaným artiklem. Stejně tak využití metod k ovlivnění jak vojáků, tak populace. Jelikož na bezpečnost těchto fenoménů má největší vliv jedinec, stejně jako útok přes různé kampaně je veden masivně na jednotlivce, jedná se o soubor rizik s vysokým nebezpečím. V dnešní době informačních technologií a sociálních sítí můžeme pozorovat tato rizika v nejrozšířenějších sociálních a informačních platformách. Identifikace rizik v této kategorii musí tedy zahrnovat tyto základní kanály:

- sociální sítě,
- zpravodajské weby,

- elektronickou poštu,
- aplikace s možností sdílení informací,
- zařízení s připojením do sítě.

Pozorovaná rizika na těchto kanálech můžeme identifikovat a klasifikovat následovně:

- Informace o
    - poloze,
    - jednotce,
    - technice a výbavě,
    - osobních údajích.
- Ovlivnění uživatele.

6.2.3 Bodování rizik

K bodování rizik byl sestaven tříčlenný tým, který měl letité zkušenosti s vedením lidí a zahraničními operacemi, aby pohled na problematiku mohl stavět na reálných základech a ne domněnkách. Důležitá byla znalost platforem a povědomí o problematice.

Každý z členů dostal vlastní formulář uvedený v příloze, z něhož se zpracoval průměr zaokrouhlený na celá čísla.

Zadání pro vyhodnocení bylo následující:

- Jak a zda může jednotku ohrozit, či ovlivnit daný problém a daná platforma.
- Hodnocená problematika vztažena na vojska v prostoru nasazení při dotyku s nepřítelem.
- Jaký je předpokládaný reálný dopad na úkol, vlastní a okolní jednotky.
- Jak velké zasažení lze očekávat, v jakém časovém horizontu lze řešit a zda je situace řešitelná na místě.

Zatímco o závažnosti následků rizika panovala spíše shoda, u pravděpodobnosti vzniku probíhala debata o aktuálnosti, míře používání a vlastně i dostupnosti zkoumaných platforem.

Při zjištění pravděpodobnosti rizika použijeme čtyři kategorie, které vychází z vypozorovaného používání jednotlivých platforem. Jako nejnižší pravděpodobnost vzniku rizika budeme zvažovat i možnost zanesení aktualizace, nových možností, nebo nové podobné platformy a s tím i nutnost kalkulovat s rizikem jako potenciálním.

Tabulka 5: Pravděpodobnost vzniku rizika (vlastní zpracování)

Pravděpodobnost vzniku – P	**Komentář**	**Hodnota**
Aktuálně nemožný výskyt	Na dané platformě aktuálně nepodporována možnost	1
Nepravděpodobný výskyt	Ojedinělý výskyt, případně na dané platformě aktuálně nepodporovaný	2
Občasný výskyt	Incidenty vznikají občas, nepravidelně	3
Častý výskyt	Časté opakování incidentů	4

Závažnost následků se bude dělit do čtyř kategorií, kdy při hodnocení bylo bráno v potaz i protnutí informací o jednotce a její polohy. V bodování se tedy může u rizika prozrazení polohy i informací hodnotit číslem dva v případech, kdy platforma umožňuje vyzrazení i pozice, ale hodnotící tým došel ke shodě, že vojáci zpravidla tyto možnosti nevyužívají. Riziko je tedy dále uvažované v tabulce závažnosti následků, ale v samotném hodnocení akceptovatelné.

Tabulka 6: Závažnost následků (vlastní zpracování)

Závažnost následků – N	**Komentář**	**Hodnota**
Bez následků	Bez vyzrazení pozice a informací o jednotce	1
Narušení operačních schopností	Vyzrazení informací o jednotce	2
Ohrožení života a zdraví	Vyzrazení pozice jednotky	3
Ztráta bojeschopnosti	Vyzrazení pozice a informací o jednotce	4

Poté se přidá názor hodnotitele. Vychází ze zkušeností týmu při práci s lidmi a pozorováním jejich návyků, chování, četnosti používání zkoumaných platforem, vlastního názoru na rizikovost platformy a předpokládaných možností při nasazení.

Tabulka 7: Názor hodnotitelů (vlastní zpracování)

Názor hodnotitelů – H	Komentář	Hodnota
Zanedbatelný vliv na operační schopnosti	Ohrožení jednotlivců, lze řešit v krátkém časovém horizontu a v místě nasazení	1
Vliv na operační schopnosti dané jednotky	Ohrožení jednotky, lze řešit v krátkém časovém horizontu a v místě nasazení	2
Vliv na operační schopnosti nadřazené jednotky	Ohrožení jednotky, nelze řešit v krátkém časovém horizontu a v místě nasazení	3
Vliv na operační schopnosti všech jednotek v prostoru nasazení	Ohrožení okolních jednotek, nelze řešit v krátkém časovém horizontu a v místě nasazení	4

Z předchozích dvou tabulek můžeme podle vzorce R = P x N x H vypočítat hodnoty, které nám znázorní míru rizika.

Tabulka 8: Rizikový stupeň (vlastní zpracování)

Rizikový stupeň	R	Míra rizika
1.	48-64	Nepřijatelné riziko
2.	32-47	Nežádoucí riziko
3.	16-31	Akceptovatelné riziko
4.	0-15	Bezvýznamné riziko

Díky míře rizika vytvoříme kategorie, dle nichž můžeme určit jak naléhavost, tak základní kroky.

Tabulka 9: Skupiny rizika (vlastní zpracování)

Skupina	Komentář	Hodnota
Nepřijatelné riziko	Nutnost odstranit riziko před zahájením operační činnosti, nebo okamžité ukončení operací	32-64
Nežádoucí riziko	Zahájit kroky k okamžitému odstranění rizika a zjistit rozsah škod a vliv na další plnění úkolů	11-31
Akceptovatelné riziko	Není potřeba zvláštních opatření. Monitorování daných platforem, zda nedošlo k aktualizaci či rozšíření	6-10
Bezvýznamné riziko	Není potřeba zvláštních opatření. Monitorování daných platforem, zda nedošlo k aktualizaci či rozšíření	0-5

Jak bylo zmíněno, samotné bodování bylo provedeno v týmu, kde se debatovalo o možnostech. Poté každý ze členů týmu zapsal hodnotu do formuláře a průměrem na celá čísla vznikla následující tabulka, která ukazuje různé rizikové stupně, barevně se shodující s celkovým hodnocením rizik. Zároveň jsou zaneseny základní kroky k ošetření rizika.

Tabulka 10: Bodování rizik metodou PNH (vlastní zpracování)

Platforma	Obsah	Identifikace nebezpečí	Vyhodnocení závažnosti rizika				Opatření k omezení rizika
			P	N	H	R	
Facebook	Multimédia	Informace o jednotce, poloze a uživateli	4	4	3	48	Nesdílet fotografie, zamezit přístup k zařízeni, anebo k síti
	Komentáře a příspěvky	Informace o jednotce, poloze a uživateli	3	4	4	48	Nepsat příspěvky, zamezit přístup k zařízeni, anebo k síti
	Malware	Informace o jednotce, poloze a uživateli	3	2	1	6	Neklikat na neznámé odkazy
	Sledování obsahu	Ovlivnění uživatele	4	2	2	16	Používat kritické myšlení a zásady pro identifikaci dezinformací a propagandy
	Ztráta účtu	Informace o jednotce, poloze a uživateli	3	4	3	36	Heslo používat unikátní, nikde ho nesdílet
Instagram	Multimédia	Informace o jednotce, poloze a uživateli	3	4	3	36	Nesdílet fotografie, zamezit přístup k zařízeni, anebo k síti
	Komentáře a příspěvky	Informace o jednotce, poloze a uživateli	2	3	3	18	Nepsat příspěvky, zamezit přístup k zařízeni, anebo k síti
	Malware	Informace o jednotce, poloze a uživateli	3	2	1	6	Neklikat na neznámé odkazy
	Sledování obsahu	Ovlivnění uživatele	2	1	1	2	Používat kritické myšlení a zásady pro identifikaci dezinformací a propagandy
	Ztráta účtu	Informace o jednotce, poloze a uživateli	3	3	3	27	Heslo používat unikátní, nikde ho nesdílet
Tik-Tok	Multimédia	Informace o jednotce, poloze a uživateli	4	3	3	36	Nesdílet fotografie, zamezit přístup k zařízeni, anebo k síti
	Komentáře a příspěvky	Informace o jednotce, poloze a uživateli	2	3	3	18	Nepsat příspěvky, zamezit přístup k zařízeni, anebo k síti
	Malware	Informace o jednotce, poloze a uživateli	2	3	2	12	Neklikat na neznámé odkazy
	Sledování obsahu	Ovlivnění uživatele	3	1	1	3	Používat kritické myšlení a zásady pro identifikaci dezinformací a propagandy
	Ztráta účtu	Informace o jednotce, poloze a uživateli	2	2	2	8	Heslo používat unikátní, nikde ho nesdílet

Platforma	Obsah	Identifikace nebezpečí	Vyhodnocení závažnosti rizika				Opatření k omezení rizika
			P	N	H	R	
Telegram	Multimédia	Informace o jednotce, poloze a uživateli	3	4	2	24	Nesdílet fotografie, zamezit přístup k zařízeni, anebo k síti
	Komentáře a příspěvky	Informace o jednotce, poloze a uživateli	3	3	2	18	Nepsat příspěvky, zamezit přístup k zařízeni, anebo k síti
	Malware	Informace o jednotce, poloze a uživateli	1	2	1	2	Neklikat na neznámé odkazy
	Sledování obsahu	Ovlivnění uživatele	2	1	1	2	Používat kritické myšlení a zásady pro identifikaci dezinformací a propagandy
	Ztráta účtu	Informace o jednotce, poloze a uživateli	3	3	2	18	Heslo používat unikátní, nikde ho nesdílet
E-mail	Odesílaná multimédia	Informace o jednotce, poloze a uživateli	3	4	2	24	Neposílat multimédia
	Odchozí e-mailová zpráva	Informace o jednotce, poloze a uživateli	2	2	1	4	V e-mailu nezmiňovat žádné informace o místě nasazení a vlastní jednotce
	Malware	Informace o jednotce, poloze a uživateli	3	2	2	12	Neklikat na neznámé odkazy
	Řetězové e-maily	Ovlivnění uživatele	2	2	1	4	Používat kritické myšlení a zásady pro identifikaci dezinformací a propagandy
	Ztráta účtu	Přístup k platformám nepoužívajícím dvoufázové ověření	3	4	2	24	Heslo používat unikátní, nikde ho nesdílet
Mobilní app	Multimédia	Informace o jednotce, poloze a uživateli	3	3	2	18	Nesdílet fotografie, zamezit přístup k zařízeni, anebo k síti
	Komentáře a příspěvky	Informace o jednotce, poloze a uživateli	1	2	1	2	Nepsat příspěvky, zamezit přístup k zařízeni, anebo k síti
	Malware	Informace o jednotce, poloze a uživateli	2	1	1	2	Neklikat na neznámé odkazy
	Ztráta účtu	Informace o jednotce, poloze a uživateli	3	3	2	18	Heslo používat unikátní, nikde ho nesdílet

7 OVLIVŇOVÁNÍ OBYVATEL A VOJSK

Účinná a levná zbraň. Z pohledu nepřátelského působení extrémně pozitivní výsledek může vyústit v ovládnutí území bez boje, či alespoň dosazení vedení země v podobě loutkové vlády. V běžném režimu více či méně ovlivňuje morálku a chuť vojáků k boji, snižuje podporu obyvatelstva a zvyšuje dezerci vojáků. Z pohledu vlastních nástrojů působí opačně na morálku a podporu. Také působí jako obranný systém proti nepřátelskému působení.

7.1 Dezinformace a dezinformační kampaně

Jedním z často zmiňovaných nástrojů při vedení hybridní války jsou dezinformační kampaně vedené proti napadenému státu. Obrana proti nim je dnes velkým tématem. Na úrovni státu zatím dochází pouze ke kontroverzním krokům jako například vypnutí webů, které dezinformace prokazatelně šíří. Existují však i neziskové organizace, nebo investigativní redakce, jako jsou například manipulátoři.cz, čeští elfové, hlidacipes.org, Bellingcat, neleţ a jím podobné, které se snaží dokládat fakty, že se jedná o dezinformaci. Nicméně ze statistik víme, že šíření dezinformací je rychlejší než šíření podložených a faktických informací, které jsou doloženy relevantními zdroji. U vyvracení dezinformací můžeme kalkulovat ještě s pomalejším šířením, a to zpravidla jen u určité skupiny lidí, která se o fakta zajímá. Dezinformace tedy i po odhalení a podloženém vyvrácení páchá nevratné škody.

Cílem dezinformační kampaně je klamat vojáky a civilisty například dezinformací o prolomení frontové linie v blízkosti jejich postavení a obydlí, o obklíčení jejich pozic a měst, o zničení logistických tras a skladů zásob, o zničení kritické infrastruktury a o dalších problémech ovlivňujících náhled na celkovou situaci u vlastních vojsk a civilního obyvatelstva.

Je důležité chápat je jako sofistikovaný a velmi účinný nástroj, který nepřítel používá promyšleně, a právě z důvodu složité obrany při jeho velmi nízkých nákladech. V případě vojáků může oslabit morálku a voják postupně přestává věřit ve smysl boje. V případě civilistů zase může způsobovat nedůvěru ve vlastní vojska a například v zájmu vlastní bezpečnosti kolaborovat a poskytovat informace nepříteli.

Jelikož sami vojáci často dezinformacím uvěří, je důležité v rámci obrany při bojových operacích sledovat chování jednotlivců a skupin z pozice nižších velitelů a v případě odhalení právě dokládat fakta nenásilným způsobem. Velitel musí být schopný vést diskusi nenásilným způsobem a s vojákem, nebo svým družstvem, potažmo četou správně

komunikovat. Důležité je nepředkládat pouze fakta, ale ptát se. Nechat vojáky zasažené dezinformací mluvit a vysvětlit, proč tomu věří. Často sami zjistí, že jejich přesvědčení stoji tzv. „na vodě“ a poté právě přichází čas, kdy je vhodné použít faktický protiargument. K tomu je důležité pracovat i s dezinformací, zjistit fakta, která může v ideálním případě poskytnout nadřízený stupeň či VeKySIO (Velitelství kybernetických sil a informačních operací). V tomto ohledu je také důležitá psychologická příprava velitelů se zaměřením na komunikaci.

Použít v tomto případě můžeme například příručku „Člověka v tísni“, která nám radí, jaké otázky si položit při čtení mediálního obsahu a pokládat je při debatě s vojáky. (Gregor a Mlejnková, 2018)

- *„KDO: Kdo je autorem nebo tvůrcem sdělení? Můžu si o něm něco dohledat? Kdo má kontrolu nad vznikem a šířením sdělení?“*
- *„CO: Co je obsahem sdělení? Jsou ve sdělení uvedeny zdroje? Jaké názory a hodnoty jsou ve sdělení přítomny? Jaké informace naopak ve sdělení chybí?“*
- *„KOMU: Které cílové skupině je sdělení určeno? Jakým způsobem se sdělení k příjemci dostává a jak se šíří? Jak může sdělení ovlivnit názory, postoje a chování příjemců?“*
- *„JAK: Jak se sdělení snaží upoutat pozornost? Jaký je jazyk a forma sdělení a proč? Jaké emoce se ve mně sdělení snaží vyvolat?“*
- *„PROČ: Proč bylo sdělení vytvořeno? Kdo má ze sdělení užitek?“* (Gregor a Mlejnková, 2018, s. 126)

Často stačí málo a lze doložit, že se jedná o dezinformaci. Při jednom článku stačilo zadat jméno doktora, který byl uveden jako autor studie pracující na konkrétní prestižní škole do vyhledávání a to prozradilo, že jmenovaný člověk vůbec nemá doktorát, nepracuje na zmíněné univerzitě a obor co studuje nemá s problematikou nic společného. Bylo tedy jen použito jeho jméno, aby dodalo informaci určitou uvěřitelnost.

„Reagujeme více na příběhy než na data.“ (Bruce Schneier: Přízrak bezpečnosti, 2010)

V krajních případech lze sáhnout i k fyzické bezpečnosti. Nicméně nejedná se o řešení příčiny a situaci to v konečném důsledku může zhoršit utužením přesvědčení o pravdivosti dezinformace. Nicméně například k odebrání komunikačních zařízení se v případě konfliktu vysoké intenzity přistupuje.

7.2 Propaganda

Obrana proti nepřátelské propagandě se může z části řídit obranou proti dezinformacím, které může používat. Jako další nástroj slouží použití **bílé propagandy** a tím udržování morálky na pozitivní úrovni. Případně využití prostředků, jak bílou propagandou působit na nepřátelské vojska a obyvatelstvo, jako jsou ICT, tiskoviny, nebo i ukázka a ovlivnění zajatců určených k výměně apod. Zejména tiskoviny v konfliktu vysoké intenzity mohou být klíčové pro ovlivnění obou stran konfliktu v předních liniích a v dotyku s protivníkem. V těchto místech velmi často nefunguje mobilní síť a jsou velké problémy se zdroji energie pro různá zařízení schopná zobrazovat jakýkoliv druh online zpráv. Stejné prostředky můžeme použít i pro šíření **černé propagandy** a působit na nepřátelská vojska a nepřátelské obyvatelstvo. Jako příklad lze uvést britskou operaci za druhé světové války. Jednalo se o vysílání zdánlivě německého rádia, kde vystupoval falešný moderátor pod přezdívkou *Der Chef*. Ten se vydával za nižšího německého důstojníka a otevřeně kritizoval německé poměry. Jelikož využíval informace a situace o kterých se obecně vědělo, ale nemluvilo, nebo se je vedení snažilo potlačit, bylo to pro běžného Němce snadno uvěřitelné a obyvatelé to vnímali jako upřímné vyjádření nespokojenosti s poměry ve válečném Německu. U **šedé propagandy** můžeme opět používat stejné prostředky dopravy na cíl a jako příklad uvést noviny s názvem *Zprávy pro vojáka*, které za druhé světové války spojenecká vojska shazovala z letadel. Noviny podávaly objektivní a pravdivé informace, ale zaměřovaly se na prohrané bitvy a problémy třetí říše. Jelikož se o těchto prohraných bitvách a problémech mezi vojáky mluví, byl to další z nástrojů pro snížení morálky vojsk. (Gregor a Mlejnková, 2018)

8 NÁVRH OPATŘENÍ

Problém se sdílením dat a informací je zpravidla dán samotnými jedinci. V tomto případě se využívají data a informace volně dostupné, již zveřejněné. Řešením je důkladné poučení a školení personálu, a to jak v operacích, tak na mírových základnách. V bezpečnostně náročnějších podmínkách, utajení a podobných situacích odebírat osobní komunikační zařízení a používat výhradně služební.

Každého příslušníka pravidelně školit o možnosti zneužití poskytovaných informací. Uvádět praktické příklady a již známé situace. S důrazem upozornit na důsledky sdílení. Přesah v informacích o bezpečnosti do soukromého života tak, aby bezpečné chování na internetu a sociálních sítích bylo běžnou součástí života každého uživatele, nejen pracovní povinností.

V místech dotyku s nepřítelem a místech velení a řízení boje v případě potřeby zavést i opatření odebráním mobilních telefonů a jiných komunikačních zařízení, nebo omezit přístup k veřejné síti například zarušením, vypnutím nebo zničením mobilní sítě.

Při provozu v rádiové síti se vojáci řídí poučkou: „Pozor! Nepřítel naslouchá!“. Což představuje určitý soubor pravidel a opatření, jak při vedení hovoru v rádiové síti komunikovat, aby nedocházelo k prozrazení citlivých informací v případě odposlechu. Přenést toto pravidlo do moderních systémů a vytvořit systém poučení, jak nakládat s informacemi ve veřejné síti.

8.1 Školení

V rámci školení o bezpečnosti a rizicích spojených s poskytováním informací v kybernetickém prostoru vojáky a vojákyněmi z povolání je důležitá pravidelnost a důslednost. V této dynamické době rychle vznikajících nových trendů a způsobů, které útočníci k získávání informací používají, je optimální školit kvartálně a pozornost posluchačů ověřit buď testem, nebo alespoň občasnou otázkou k posluchačům. Veškeré informace podávat v kontextu s praxí a civilním životem tak, aby každý co nejlépe pochopil účel a způsob daných protiopatření a jejich význam ve vztahu k bezpečnosti jak příslušníků samotných, tak i jejich rodin a jednotek.

V rámci školení mimo jiné obecně vysvětlit:

Síla hesla:

Rizika – Získání hesla a přístupu do účtu. Při používání stejného hesla dostává útočník automaticky přístup na všechny platformy užívající stejné heslo.

Opatření – Ukázat systém brute force attack a vysvětlit důvod a důležitost používat různá hesla. Nesdílet hesla. Používat dostatečně silná hesla a dvoufázová ověření. Ukázat doporučení tvorby silného hesla a jeho různých variant, například za pomoci silného kořenu hesla a „obalu“ vytaženého z názvu webu, platformy, nebo jiné související a dobře zapamatovatelné variace.

Cookies:

Rizika – Zaznamenání polohy zařízení, jako jsou počítače, smartphony, smartwatche a následné určení polohy jednotlivce. Z důvodu nutnosti odsouhlasit prakticky na všech webových stránkách může obsahovat skrytý odkaz na škodlivý software.

Opatření – Používat VPN a anonymní vyhledávače jako například DuckDuckGo.

Obecně k účtům:

Rizika – prolomení přístupu a získání veškerého obsahu. Možnost použití k ovlivnění jiných osob.

Opatření – používat silná a jedinečná hesla.

Zaměřit se primárně na rizika na nejrozšířenějších platformách jako jsou:

Facebook:

Rizika – napadení účtu a získání veškerého obsahu. Sdílení fotografií s možností vyčtení polohy podle okolního terénu a markantů, používané techniky a zbraní, druhu vojska a příslušníků jednotky. Možnost sdílení polohy. Vliv dezinformací a propagandy na jednotlivce.

Opatření – uživatelům ukázat v prezentaci nastavení soukromí a nástroj na ověření zobrazovaných informací na profilu. Vysvětlit proč si do přátel přidávat jen ověřené

uživatele, které známe osobně. Omezit sdílení informací na přátelům známá témata a informace. V případě potřeby mít vyčleněného člověka, který pomůže jednotlivcům s nastavením. Prezentaci a postup nastavení mít volně přístupný. Vysvětlit důležitost používání silného hesla. Řídit se opatřeními pro boj s dezinformacemi a nepřátelskou propagandou.

Instagram:

Rizika – sdílení fotografií s možností vyčtení polohy podle okolního terénu a markantů, používané techniky a zbraní, druhu vojska a příslušníků jednotky.

Opatření – Nesdílet fotografie z míst nasazení. Nastavit sledování profilu jen po potvrzení.

TikTok:

Rizika – sběr informací o uživateli, jeho zařízení a aplikacích v něm včetně Wi-Fi SSID, IMEI, sériového čísla SIM karty apod. Přístup Čínské vlády k uloženým datům. Pravidelné zjišťování polohy zařízení.

Opatření – varovat před výše zmíněnými riziky a nepoužívat aplikaci.

Telegram:

Rizika – cíleně vytvořené skupiny s dezinformacemi a propagandou.

Opatření – varovat před výše zmíněnými riziky a nepoužívat aplikaci.

E-mail:

Rizika – získáním přístupu k emailu lze často získat přistup k většině účtů, jelikož pro resetování hesla se zpravidla používá e-mail. Šíření dezinformací a nepřátelské propagandy.

Opatření – použití unikátního a velmi silného hesla. Řídit se opatřeními pro boj s dezinformacemi a nepřátelskou propagandou.

Aplikace požadující přístup ke kontaktům, poloze a úložišti telefonu:

Rizika – aplikace, které uživatel povolí přístup k datům a informacím v zařízení mohou být napojeny na server, který je může sbírat a zaznamenávat.

Opatření – poučit o aplikacích vyžadujících výše zmíněné přístupy. Instalovat jen známé aplikace a nepovolovat přístup, který aplikace zřejmě nepotřebuje.

8.2 Soubor opatření „nepřítel sleduje tvůj profil“

Vytvoření příručky nebo karty shrnující opatření obsažená ve školení obecně k poskytování informací na sociálních sítích.

Tabulka 11: Karta s doporučením chování na sociálních sítích (vlastní zpracování)

Nepřítel sleduje tvůj profil!
Při vojenské operaci nedávej statusy na sociální sítě!
Nikdy nikde nesdílej fotografie! I jeden dům v dálce jde najít na mapě!
Dbej na vypnutí GPS tak, aby nikde nebyla zaznamenána tvoje poloha!
Nekomentuj příspěvky! I neurčitá informace může být dílkem zpravodajské skládačky!
Nikdy si nepřidávej do přátel, nebo ke sledování někoho, koho neznáš osobně!
Vždy se chovej tak, jako bys měl nepřítele v přátelích!

Pro úpravu tabulky a její objektivizaci bylo použito metody brainwriting, která rovněž poukázala na orientaci v problematice u různých věkových skupin. Vybrána byla skupina pěti vojáků různých hodností a věku, kteří měli anonymně napsat minimálně tři krátké poučky o chování na sociálních sítích. Po zjištění, že starší vojáci zpravidla dokázali napsat jen jednu bylo upuštěno od systému předání lístků a skupině byla předložena původní navržená kartička viz. výše. Mladší vojáci se v problematice orientovali velmi dobře a dokázali vtipně aplikovat zásady na vojenský slang a tzv. „hlášky“, kdy některé z nich se začali po brainwritingu i šířit, což lze považovat za sice neplánovaný, ale velký úspěch. Zlidovění a zařazení nějaké takové věty do vojenského slangu znamená šíření poučky mezi vetší množství vojáků a větší pravděpodobnost na její udržení v paměti. Po brainwritingu by tabulka mohla vypadat následovně:

Tabulka 12: Upravená karta s doporučením chování na sociálních sítích (vlastní zpracování)

Nepřítel sleduje tvůj profil!
Při vojenské operaci nedávej statusy na sociální sítě!
Nikdy nikde nesdílej fotografie! I jeden dům v dálce jde najít na mapě!
Dbej na vypnutí GPS tak, aby nikde nebyla zaznamenána tvoje poloha!
Nekomentuj příspěvky! I neurčitá informace může být dílkem zpravodajské skládačky!
Nikdy si nepřidávej do přátel, nebo ke sledování někoho, koho neznáš osobně!
Vždy se chovej tak, jako bys měl nepřítele v přátelích!
Nesdílej fotografie! Místo lajku můžeš dostat dělostřeleckou palbu!
Fotografie rodiny ukazují nepříteli, co je ti drahé!
Nekomentuj! Jsi žrádlo pro kulomet, ne pro trolla!

8.3 Fyzická bezpečnost

V poli budeme těžko ve vztahu k úniku informací od jednotlivců řešit režimovou ochranu. Mnohem účinnější budou technické a organizační opatření.

Spousta vojáků může buď nevědomky formou statusu na sociální síti, nebo informováním rodinných příslušníků a přátel prozradit důležité informace, které poté nepřítel využije k jejich lokalizaci. Zvýšený provoz na mobilní síti někde uprostřed lesů ve válečné oblasti je jasným znakem pohybu jednotky. Obyčejná fotka se zprávou „nebojte se, je tady klídek“ může rozkrýt pozici a po „klídku“ přijde například dělostřelecký přepad. Jedná se o jedno z důležitých omezení, které má za účel eliminovat možnost vynášet jakékoliv informace.

Organizační opatření spočívá v odebrání a vypnutí mobilních telefonů, ideálně vytažení SIM karet, jelikož při používání mobilních telefonů operátor ukládá přibližné polohy zařízení, tudíž je možné zpětně dohledat pohyb osob se zapnutým telefonem, který je k síti přihlášen.

Technické opatření může spočívat například ve využití rušiček, nebo vypnutí či zničení mobilní sítě v prostoru nasazení. Avšak velká nevýhoda spočívá v nemožnosti využít mobilní síť pro vlastní účely. V případě zarušení eliminujeme možnost sdílet informace,

nicméně zarušení samo o sobě představuje velmi silný radiový signál, který je možno vysledovat a zaměřit.

8.4 Předpokládaná rizika po ošetření

Po provedení školení, zavedení nutných a potřebných částí opatření jak ve fyzické bezpečnosti, tak v přístupu a povinnostech nižších velitelů, můžeme předpokládat snížení rizika. Důsledky v boji jsou však nadále stejné. Prozrazení prostoru rozmístění v dosahu nepřátelské dělostřelecké palby, nebo v prostoru s možností raketového či leteckého úderu nepřítele bude mít stále fatální důsledky na operační úkol a životy a zdraví vojáků. Správným opatřením však můžeme pravděpodobnost vzniku rizika minimalizovat. Tabulka s bodováním rizika bude vypadat různě podle použitých opatření.

V případě školení se předpokládá snížení pravděpodobnosti vzniku rizika P minimálně o jeden bod. Závažnost následků N se nemění. Pokud riziko vznikne, následek zůstává.

V případě fyzické bezpečnosti by pravděpodobnost vzniku rizika P mohla být téměř nulová. Kalkulovat můžeme snad jen s nějakým ukrytým neodevzdaným zařízením, případně získáním jiného v týlovém prostoru při obnově bojeschopnosti mezi operačními úkoly. V případech vypnutí sítě se toto riziko u zkoumaných fenoménů a platforem limitně blíží nule. Je důležité vnímat fakt, že vypnutí sítě nám odhaluje prostor operace v případech lokálního vypínání a možnosti nepřítele aktivitu sítě sledovat.

ZÁVĚR

Z pohledu teorie není oblast kybernetické bezpečnosti a pojmů s ní spojených zcela jednotná. Literatura uvádí často i protichůdné definování pojmů.

Po popsání určitých prostředků a typů útoků a způsobů obrany byla rizika ošetřena a snížena. Nicméně dopady rizika jsou v boji stále velmi destruktivní a pro jednotku můžou být fatální. Snížená rizika a způsob jejich snížení formou školení je vhodný v době míru, avšak z důvodu následků je zřejmé, že i přes důkladnou přípravu bude vhodné při bojích přistoupit k fyzické bezpečnosti. V době míru by mělo být prioritou připravovat nižší velení, které je v přímém kontaktu s vojáky.

Hlavním cílem práce bylo definovat rizika, pojednat o fenoménu hybridního válčení a možnostech, které nabízí kybernetický prostor. Výstupem práce jsou návrhy určitých opatření, které mohou pomoci zvýšit bojeschopnost jednotek, podpořit spolupráci místního obyvatelstva a ochránit život a zdraví jednotek. Bylo pojednáno jak o způsobech úniku dat, tak rovnou i o konkrétních problémech, či přímo konkrétních platformách, kterými je potřeba se aktivně zabývat a připravovat se na jejich řešení. O vlivu propagandy a dezinformací směrem od nepřítele, ale také ukázka toho, jak takové operace využít ve vlastní prospěch.

Hybridní válka ve spojení s kyberprostorem skýtá obrovskou škálu možností útoků. Jako návaznost na tuto práci by bylo vhodné z kybernetické zbraně hromadného ničení, jakou informační boj je, přejít k cíleným útokům speciálních jednotek působících v kybernetickém prostoru, které mají vyšší požadavky na odbornost, ale jejich útoky zvládnou eliminovat moderní systémy nepřítele, nebo získat data cennější než jen obecné informace a pozice jednotek. Může se jednat o plány nadcházejících útoků, vypínání kritické infrastruktury, anebo působení ekonomických ztrát. Jako zajímavá součást válečného úsilí se jeví i kybernetický odboj. V dnešní podobě si říká Anonymous a nejedná se o nic menšího než odborníky v kybernetické problematice, kteří v dnešní Rusko-Ukrajinské válce provádí záškodnické operace a pomáhají obráncům. Opět se v jejich podání ukazuje síla hybridní války a využití kybernetického prostoru, kdy i s levným zařízením člověk z kteréhokoliv koutu světa dokáže provádět sofistikované útoky, které mají reálný dopad. A to jak psychologické operace, nebo přímo útoky na kritickou infrastrukturu.

SEZNAM POUŽITÉ LITERATURY

Aktuálně.cz, 2018. In: *Aktuálně.cz* [online]. Praha: Economia [cit. 2023-04-29]. Dostupné z: https://zpravy.aktualne.cz/

Ardit [online], 2022. Praha: Ardit [cit. 2023-04-29]. Dostupné z: https://www.ardit.cz/
BezFaulu [online], 2019. Česká republika: BezFaulu [cit. 2023-04-29]. Dostupné z: https://bezfaulu.net/

BILAL, Arsalan, 2021. Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote. In: *NATO* [online]. Norsko: NATO review [cit. 2023-03-07]. Dostupné z: https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html

Bruce Schneier: Přízrak bezpečnosti, 2010. In: *TED* [online]. Pennsylvania: TED [cit. 2023-04-29]. Dostupné z: www.ted.com

BURÝŠEK, Jiří, 2019. CO JE TO DEZINFORMACE?. In: *Bezfaulu.net* [online]. Bezfaulu.net [cit. 2023-02-26]. Dostupné z: https://bezfaulu.net/clanky/o-manipulaci/co-je-to-dezinformace/

Clever and smart [online], 2010. Dolní Břežany: Miroslav Čermák, 2008 [cit. 2023-04-09]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/duvernost-integrita-dostupnost/

Cyberspace Operations Concept Capability Plan 2016-2028 [online], 2010. USA: The United States Army's [cit. 2023-04-16]. Dostupné z: https://irp.fas.org/doddir/army/pam525-7-8.pdf

ČERNÝ, Jan, 2017. Data, informace a cesta ke znalostem. In: *Informační gramotnost* [online]. Hostivice: Information Factor [cit. 2023-02-26]. Dostupné z: https://www.informacnigramotnost.cz/data-informace-znalosti/

ČSN EN ISO 19650-1: Organizace a digitalizace informací o budovách a inženýrských stavbách včetně informačního modelování staveb (BIM) - Management informací s využitím informačního modelování staveb, 2019. Druhé. Praha: Česká agentura pro standardizaci.
DataReportal [online], 2023. Singapur: Kepios Pte. Ltd. [cit. 2023-04-29]. Dostupné z: https://datareportal.com/

DOLEŽAL, Jan, Pavel MÁCHAL a Branislav LACKO, 2012. *Projektový management podle IPMA*. 2., aktualiz. a dopl. vyd. Praha: Grada. Expert (Grada). ISBN 978-80-247-4275-5.

Dotyk: Falešné zprávy se šíří šestkrát rychleji než pravdivé, říká nová studie [online], 2018. Praha: VLTAVA LABE MEDIA a.s. [cit. 2023-04-29]. Dostupné z: https://www.dotyk.cz/publicistika/falesne-zpravy-se-siri-sestkrat-rychleji-nez-pravdive-rika-nova-studie.html

Facebookové flirtování vs. NATO: kontrole se povedlo ovlivnit cvičení [online], 2019. Praha: iDnes [cit. 2023-02-15]. Dostupné z: https://www.idnes.cz/xman/styl/nato-cviceni-facebook-flirt-stratcom-spion-diskreditace-sarts-biteniece.A190222_123656_xman-styl_fro

Fitness tracking app Strava gives away location of secret US army bases [online], 2018. United Kingdom of Great Britain and Northern Ireland: The Guardian [cit. 2023-02-22]. Dostupné z: https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases

GREGOR, Miloš a Petra MLEJNKOVÁ, 2018. *Nejlepší kniha o fake news, dezinformacích a manipulacích!!!*. 1. vydání. Brno: CPress. ISBN 978-80-264-1805-4.

JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR, 2022. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Páté doplněné a upravené vydání. Přeložil Karel VAVRUŠKA. Praha: Česká pobočka AFCEA. ISBN 978-80-908388-4-0.

KOLOUCH, Jan a Pavel BAŠTA, 2019. *CyberSecurity*. 1. vydání. Praha: CZ.NIC, z.s.p.o. CZ.NIC. ISBN 978-80-88168-31-7.

KOPECKÝ, Kamil, 2008. Co je to vlastně ten hoax, dezinformace, misinformace nebo třeba fake news? Čím se tyto termíny liší a co mají společného?. In: *E-bezpečí* [online]. Olomouc: Pedagogická fakulta Univerzity Palackého V Olomouci [cit. 2023-03-07]. 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

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

KRÁL, Mojmír, 2015. *Bezpečný internet: chraňte sebe i svůj počítač*. První. Praha: Grada Publishing. Průvodce (Grada). ISBN 978-80-247-5453-6.

KURFÜRST, Jaroslav a Jan PAĎOUREK, ed., 2021. *Za zrcadlem: hybridní válka jako staronový fenomén mezinárodních vztahů*. Vydání první. Praha: Academia. Společnost (Academia). ISBN 978-80-200-3237-9.

Oxford Learner's Dictionaries, 2023. In: *Oxford Learner's Dictionaries* [online]. Oxford: Oxford University Press [cit. 2023-04-29]. Dostupné z: https://www.oxfordlearnersdictionaries.com

PAČKA, Roman, 2019. *CSIRT: v přední linii boje proti kybernetickým hrozbám*. První. Brno: Centrum pro studium demokracie a kultury. Politologická řada. ISBN 978-80-7325-473-5.

PETROWSKI, Thorsten, 2014. *Bezpečí na internetu: pro všechny*. První. Liberec: Dialog. Tajemství (Dialog). ISBN 978-80-7424-066-9.

Rizika a jejich analýza [online], 2006. Ostrava: VŠB [cit. 2023-04-29]. Dostupné z: https://fei1.vsb.cz/kat420/vyuka/Magisterske%20nav/prednasky/web/RIZIKA.pdf

SMEJKAL, Vladimír a Karel RAIS, 2013. *Řízení rizik ve firmách a jiných organizacích*. 4., aktualiz. a rozš. vyd. Praha: Grada. Expert (Grada). ISBN 978-80-247-4644-9.

SMEJKAL, Vladimír, Tomáš SOKOL a Jindřich KODL, 2019. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. 1.vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o. ISBN 978-80-7380-765-8.

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

VÁCHAL, Jan a Marek VOCHOZKA, 2013. *Podnikové řízení*. 1. vyd. Praha: Grada. Finanční řízení. ISBN 978-80-247-4642-5.

Zive.cz, 2022. In: *Zive.cz* [online]. Praha: Czech News Center [cit. 2023-04-29]. Dostupné z: https://www.zive.cz/

Znalostní systém prevence rizik v BOZP, 2023. In: *Znalostní systém prevence rizik v BOZP* [online]. Praha: Výzkumný ústav bezpečnosti práce [cit. 2023-04-29]. Dostupné z: https://zsbozp.vubp.cz/

Znalostní systém prevence rizik v BOZP, 2023. In: *Znalostní systém prevence rizik v BOZP - Identifikace rizik* [online]. Praha: Výzkumný ústav bezpečnosti práce [cit. 2023-04-29]. Dostupné z: https://zsbozp.vubp.cz/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

CSIRT	Computer Security Incident Response Team – Skupina pro reakce na počítačové bezpečnostní incidenty
FMEA	Failure Mode and Effects Analysis – Analýza možného výskytu a vlivu vad
GPS	Global Position Systém – Globální poziční systém
ICT	Information and Communication Technologies – Informační a komunikační technologie
ISO	International Organization for Standardization - Mezinárodní organizace pro normalizaci
IT	Information Technology – Informační technologie
LAN	Local Area Network – Lokální počítačová síť
NATO	The North Atlantic Treaty Organization – Severoatlantická aliance
PSYOPS	Psychological Operations – Psychologická operace
VeKySIO	Velitelství kybernetických sil a informačních operací
Wi-Fi	Wireless Fidelity – Bezdrátová síť

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: TABULKA HODNOCENÍ OD JEDNOTLIVCŮ

Platforma	Obsah	Identifikace nebezpečí	Vyhodnocení závažnosti rizika				Opatření k omezení rizika
			P	N	H	R	
Facebook	Multimédia	Informace o jednotce, poloze a uživateli					Nesdílet fotografie, zamezit přístup k zařízeni, anebo k síti
	Komentáře a příspěvky	Informace o jednotce, poloze a uživateli					Nepsát příspěvky, zamezit přístup k zařízeni, anebo k síti
	Malware	Informace o jednotce, poloze a uživateli					Neklikat na neznámé odkazy
	Sledování obsahu	Ovlivnění uživatele					Používat kritické myšlení a zásady pro identifikaci dezinformací a propagandy
	Ztráta účtu	Informace o jednotce, poloze a uživateli					Heslo používat unikátní, nikde ho nesdílet
Instagram	Multimédia	Informace o jednotce, poloze a uživateli					Nesdílet fotografie, zamezit přístup k zařízeni, anebo k síti
	Komentáře a příspěvky	Informace o jednotce, poloze a uživateli					Nepsát příspěvky, zamezit přístup k zařízeni, anebo k síti
	Malware	Informace o jednotce, poloze a uživateli					Neklikat na neznámé odkazy
	Sledování obsahu	Ovlivnění uživatele					Používat kritické myšlení a zásady pro identifikaci dezinformací a propagandy
	Ztráta účtu	Informace o jednotce, poloze a uživateli					Heslo používat unikátní, nikde ho nesdílet
Tik-Tok	Multimédia	Informace o jednotce, poloze a uživateli					Nesdílet fotografie, zamezit přístup k zařízeni, anebo k síti
	Komentáře a příspěvky	Informace o jednotce, poloze a uživateli					Nepsát příspěvky, zamezit přístup k zařízeni, anebo k síti
	Malware	Informace o jednotce, poloze a uživateli					Neklikat na neznámé odkazy
	Sledování obsahu	Ovlivnění uživatele					Používat kritické myšlení a zásady pro identifikaci dezinformací a propagandy
	Ztráta účtu	Informace o jednotce, poloze a uživateli					Heslo používat unikátní, nikde ho nesdílet
Telegram	Multimédia	Informace o jednotce, poloze a uživateli					Nesdílet fotografie, zamezit přístup k zařízeni, anebo k síti
	Komentáře a příspěvky	Informace o jednotce, poloze a uživateli					Nepsát příspěvky, zamezit přístup k zařízeni, anebo k síti
	Malware	Informace o jednotce, poloze a uživateli					Neklikat na neznámé odkazy
	Sledování obsahu	Ovlivnění uživatele					Používat kritické myšlení a zásady pro identifikaci dezinformací a propagandy
	Ztráta účtu	Informace o jednotce, poloze a uživateli					Heslo používat unikátní, nikde ho nesdílet

Platforma	Obsah	Identifikace nebezpečí	Vyhodnocení závažnosti rizika				Opatření k omezení rizika
			P	N	H	R	
E-mail	Odesílaná multimédia	Informace o jednotce, poloze a uživateli					Neposílat multimédia
	Odchozí e-mailová zpráva	Informace o jednotce, poloze a uživateli					V e-mailu nezmiňovat žádné informace o místě nasazení a vlastní jednotce
	Malware	Informace o jednotce, poloze a uživateli					Neklikat na neznámé odkazy
	Řetězové e-maily	Ovlivnění uživatele					Používat kritické myšlení a zásady pro identifikaci dezinformací a propagandy
	Ztráta účtu	Přístup k platformám nepoužívajícím dvoufázové ověření					Heslo používat unikátní, nikde ho nesdílet
Mobilní app	Multimédia	Informace o jednotce, poloze a uživateli					Nesdílet fotografie, zamezit přístup k zařízeni, anebo k síti
	Komentáře a příspěvky	Informace o jednotce, poloze a uživateli					Nepsát příspěvky, zamezit přístup k zařízeni, anebo k síti
	Malware	Informace o jednotce, poloze a uživateli					Neklikat na neznámé odkazy
	Ztráta účtu	Informace o jednotce, poloze a uživateli					Heslo používat unikátní, nikde ho nesdílet

Pravděpodobnost vzniku rizika - P	Komentář	Hodnota
Aktuálně nemožný výskyt	Na dané platformě aktuálně nepodporována možnost	1
Nepravděpodobný výskyt	Ojedinělý výskyt, případně na dané platformě aktuálně nepodporovaný	2
Občasný výskyt	Incidenty vznikají občas, nepravidelně	3
Častý výskyt	Časté opakování incidentů	4

Závažnost následků rizika - N	Komentář	Hodnota
Bez následků	Žádné prozrazení pozice a informací o jednotce	1
Narušení operačních schopností	Vyzrazení informací o jednotce	2
Ohrožení života a zdraví	Vyzrazení pozice jednotky	3
Ztráta bojeschopnosti	Vyzrazení pozice a informací o jednotce	4

Názor hodnotitelů - H	Komentář	Hodnota
Zanedbatelný vliv na operační schopnosti	Ohrožení jednotlivců, lze řešit v krátkém časovém horizontu a v místě nasazení	1
Vliv na operační schopnosti dané jednotky	Ohrožení jednotky, lze řešit v krátkém časovém horizontu a v místě nasazení	2
Vliv na operační schopnosti nadřazené jednotky	Ohrožení jednotky, nelze řešit v krátkém časovém horizontu a v místě nasazení	3
Vliv na operační schopnosti všech jednotek v prostoru	Ohrožení okolních jednotek, nelze řešit v krátkém časovém horizontu a v místě	4

Hodnotitel: ……

PŘÍLOHA P II: NÁVRHY Z BRAINWRITINGU

Pamatuj, že svým chováním můžeš ohrozit nejenom sám sebe.

Soukromí a bezpečnost nejdou ruku v ruce s aktivitami na social. sítích.

I hloupá fotka dokáže způsobit velké nepříjemnosti.

Ti kdo opravdu umí nemají potřebu se zviditelňovat na sociálních sítích.

NEPŘÍTEL SLEDUJE TVŮJ PROFIL

CO NEDÁVAT NA SOCIÁLNÍ SÍTĚ A PROČ !!

NEJLÉPE NEDÁVAT VŮBEC NIC

- NEPŘÍTEL SE MŮŽE TVÁŘIT A CHOVAT JAKO PŘÍTEL.

- FOTKY A INFORMACE Z PRÁCE NEPATŘÍ DO SOUKROMÉHO ŽIVOTA = NEPATŘÍ ANI NA PROFIL.
- FOTKY RODINY, MAZLÍČKŮ, AUTA, DOMU, DRAHÝCH VĚCÍ
  - UKAZUJEŠ NEPŘÍTELI, CO JE TI DRAHÉ A ČÍM TI MŮŽE UBLÍŽIT
- FOTKY Z DOVOLENÉ S POPISEM „ČEKÁ NÁS 14 DNÍ V RÁJI"
  - NEPŘÍTEL VÍ, ŽE MÁ 14 DNÍ NA VYKRADENÍ DOMU
- PŘÍSPĚVEK „BUDU MĚSÍC PRACOVNĚ PRYČ, OD MILÁČKŮ"
  - MĚSÍC BUDE RODINA BEZ „OCHRANY"

1. Fotky si dělej na dovolené v plavkách, ne na vojenské operaci v fullgearu
2. Nesdílej informace víc než je třeba, ne každý potřebuje všechno vědět (ani tvoje mamka ne)
3. Stanovuj si důvěryhodné potenciální [illegible], [illegible] attention [illegible] o úspěchu na sebe neupozorňuj
4. A vůbec, zruš si ty sociální sítě, [illegible] čas
5. Nikde nic nekomentuj, [illegible]

NENECH SE VYPROVOKOVAT V DISKUZÍCH NA INTERNETU

JSEŠ ŽRÁDLO PRO KULOMET NE PRO TROLY

TVOJE PRÁCE NENÍ PC HRA

SVÉ KILLSHOTY NESDÍLEJ

HOLKU Z TINDRU NEZAUJMEŠ DOSTŘELEM TANKU

A NAVÍC…

JSEŠ SI JISTÝ ŽE SI PÍŠEŠ S HOLKOU Z FOTKY ?

- DRAHÉ VĚCI, DOVOLENÁ… VYVOLÁVAJÍ ZÁVIST
- FOTKA JÍDLA - PŘEHLÉDNETE ODRAZ EIFFELOVKY, JÍDELNÍ LÍSTEK S NÁZVEM RESTAURACE = NEPŘÍTEL VÍ, ŽE SE DNES NEVRÁTÍTE
- SDÍLENÝ AKTIVITY Z HODINEK - PROZRADÍTE VÁŠ DOMOV, PRÁCI, ČASTÝ MÍSTA, AKTUÁLNÍ MÍSTO DESTINACE…

Nehraj online hry.

Nesdílej aktivity (Strava, Garmin, …)

Po použití mobilu se přesuň.

Měj vypnutý mobil.

PŘÍLOHA P III: VÝSTUP HODNOTITELŮ PHN METODY

Platforma	Obsah	Identifikace nebezpečí	Vyhodnocení závažnosti rizika				Opatření k omezení rizika
			P	N	H	R	
Facebook	Fotografie	Informace o jednotce, poloze a uživateli	3	3	2		Nesdílet fotografie, zamezit přístup k zařízeni, anebo k síti
	Komentáře a příspěvky	Informace o jednotce, poloze a uživateli	2	2	2		Nepsát příspěvky, zamezit přístup k zařízeni, anebo k síti
	Malware	Informace o jednotce, poloze a uživateli	3	1	1		Neklikat na neznámé odkazy
	Sledování obsahu	Ovlivnění uživatele	3	3	2		Používat kritické myšlení a zásady pro identifikaci dezinformací a propagandy
	Ztráta účtu	Informace o jednotce, poloze a uživateli	3	3	2		Heslo používat unikátní, nikde ho nesdílet
Instagram	Fotografie	Informace o jednotce, poloze a uživateli	3	3	2		Nesdílet fotografie, zamezit přístup k zařízeni, anebo k síti
	Komentáře a příspěvky	Informace o jednotce, poloze a uživateli	2	2	2		Nepsát příspěvky, zamezit přístup k zařízeni, anebo k síti
	Malware	Informace o jednotce, poloze a uživateli	3	1	1		Neklikat na neznámé odkazy
	Sledování obsahu	Ovlivnění uživatele	3	3	2		Používat kritické myšlení a zásady pro identifikaci dezinformací a propagandy
	Ztráta účtu	Informace o jednotce, poloze a uživateli	3	3	2		Heslo používat unikátní, nikde ho nesdílet
Tik-Tok	Fotografie	Informace o jednotce, poloze a uživateli	3	3	3		Nesdílet fotografie, zamezit přístup k zařízeni, anebo k síti
	Komentáře a příspěvky	Informace o jednotce, poloze a uživateli	2	2	2		Nepsát příspěvky, zamezit přístup k zařízeni, anebo k síti
	Malware	Informace o jednotce, poloze a uživateli	1	1	1		Neklikat na neznámé odkazy
	Sledování obsahu	Ovlivnění uživatele	3	2	2		Používat kritické myšlení a zásady pro identifikaci dezinformací a propagandy
	Ztráta účtu	Informace o jednotce, poloze a uživateli	1	1	1		Heslo používat unikátní, nikde ho nesdílet
Telegram	Fotografie	Informace o jednotce, poloze a uživateli	2	2	3		Nesdílet fotografie, zamezit přístup k zařízeni, anebo k síti
	Komentáře a příspěvky	Informace o jednotce, poloze a uživateli	2	2	2		Nepsát příspěvky, zamezit přístup k zařízeni, anebo k síti
	Malware	Informace o jednotce, poloze a uživateli	1	2	2		Neklikat na neznámé odkazy
	Sledování obsahu	Ovlivnění uživatele	1	1	2		Používat kritické myšlení a zásady pro identifikaci dezinformací a propagandy
	Ztráta účtu	Informace o jednotce, poloze a uživateli	2	2	2		Heslo používat unikátní, nikde ho nesdílet

Platforma	Obsah	Identifikace nebezpečí	Vyhodnocení závažnosti rizika				Opatření k omezení rizika
			P	N	H	R	
E-mail	Odesílané fotografie	Informace o jednotce, poloze a uživateli	3	3	2		Neposílat fotografie
	Odchozí e-mailová zpráva	Informace o jednotce, poloze a uživateli	3	2	2		V e-mailu nezmiňovat žádné informace o místě nasazení a vlastní jednotce
	Malware	Informace o jednotce, poloze a uživateli	1	1	1		Neklikat na neznámé odkazy
	Řetězové e-maily	Ovlivnění uživatele	1	1	1		Používat kritické myšlení a zásady pro identifikaci dezinformací a propagandy
	Ztráta účtu	Přístup k platformám nepoužívajícím dvoufázové ověření	2	1	1		Heslo používat unikátní, nikde ho nesdílet
Mobilní app	Fotografie	Informace o jednotce, poloze a uživateli	4	3	2		Nesdílet fotografie, zamezit přístup k zařízení, anebo k síti
	Komentáře a příspěvky	Informace o jednotce, poloze a uživateli	3	1	1		Nepsát příspěvky, zamezit přístup k zařízení, anebo k síti
	Malware	Informace o jednotce, poloze a uživateli	4	2	2		Neklikat na neznámé odkazy
	Ztráta účtu	Informace o jednotce, poloze a uživateli	2	2	1		Heslo používat unikátní, nikde ho nesdílet

Pravděpodobnost vzniku rizika - P	Komentář	Hodnota
Aktuálně nemožný výskyt	Na dané platformě aktuálně nepodporována možnost	1
Nepravděpodobný výskyt	Ojedinělý výskyt, případně na dané platformě aktuálně nepodporovaný	2
Občasný výskyt	Incidenty vznikají občas, nepravidelně	3
Častý výskyt	Časté opakování incidentů	4

Závažnost následků rizika - N	Komentář	Hodnota
Bez následků	Žádné prozrazení pozice a informací o jednotce	1
Narušení operačních schopností	Vyzrazení informací o jednotce	2
Ohrožení života a zdraví	Vyzrazení pozice jednotky	3
Ztráta bojeschopnosti	Vyzrazení pozice a informací o jednotce	4

Názor hodnotitelů - H	Komentář	Hodnota
Zanedbatelný vliv na operační schopnosti	Ohrožení jednotlivců, lze řešit v krátkém časovém horizontu a v místě nasazení	1
Vliv na operační schopnosti dané jednotky	Ohrožení jednotky, lze řešit v krátkém časovém horizontu a v místě nasazení	2
Vliv na operační schopnosti nadřazené jednotky	Ohrožení jednotky, nelze řešit v krátkém časovém horizontu a v místě nasazení	3
Vliv na operační schopnosti všech jednotek v prostoru nasazení	Ohrožení okolních jednotek, nelze řešit v krátkém časovém horizontu a v místě nasazení	4

Platforma	Obsah	Identifikace nebezpečí	Vyhodnocení závažnosti rizika				Opatření k omezení rizika
			P	N	H	R	
Facebook	Fotografie	Informace o jednotce, poloze a uživateli	4	4	3		Nesdílet fotografie, zamezit přístup k zařízeni, anebo k síti
	Komentáře a příspěvky	Informace o jednotce, poloze a uživateli	3	5	5		Nepsát příspěvky, zamezit přístup k zařízeni, anebo k síti
	Malware	Informace o jednotce, poloze a uživateli	5	2	1		Neklikat na neznámé odkazy
	Sledování obsahu	Ovlivnění uživatele	4	2	2		Používat kritické myšlení a zásady pro identifikaci dezinformací a propagandy
	Ztráta účtu	Informace o jednotce, poloze a uživateli	3	3	3		Heslo používat unikátní, nikde ho nesdílet
Instagram	Fotografie	Informace o jednotce, poloze a uživateli	3	4	3		Nesdílet fotografie, zamezit přístup k zařízeni, anebo k síti
	Komentáře a příspěvky	Informace o jednotce, poloze a uživateli	2	3	3		Nepsát příspěvky, zamezit přístup k zařízeni, anebo k síti
	Malware	Informace o jednotce, poloze a uživateli	2	2	1		Neklikat na neznámé odkazy
	Sledování obsahu	Ovlivnění uživatele	3	2	1		Používat kritické myšlení a zásady pro identifikaci dezinformací a propagandy
	Ztráta účtu	Informace o jednotce, poloze a uživateli	3	3	3		Heslo používat unikátní, nikde ho nesdílet
Tik-Tok	Fotografie	Informace o jednotce, poloze a uživateli	4	3	3		Nesdílet fotografie, zamezit přístup k zařízeni, anebo k síti
	Komentáře a příspěvky	Informace o jednotce, poloze a uživateli	2	3	3		Nepsát příspěvky, zamezit přístup k zařízeni, anebo k síti
	Malware	Informace o jednotce, poloze a uživateli	2	3	2		Neklikat na neznámé odkazy
	Sledování obsahu	Ovlivnění uživatele	3	1	1		Používat kritické myšlení a zásady pro identifikaci dezinformací a propagandy
	Ztráta účtu	Informace o jednotce, poloze a uživateli	2	2	2		Heslo používat unikátní, nikde ho nesdílet
Telegram	Fotografie	Informace o jednotce, poloze a uživateli	3	4	3		Nesdílet fotografie, zamezit přístup k zařízeni, anebo k síti
	Komentáře a příspěvky	Informace o jednotce, poloze a uživateli	2	3	3		Nepsát příspěvky, zamezit přístup k zařízeni, anebo k síti
	Malware	Informace o jednotce, poloze a uživateli	2	3	3		Neklikat na neznámé odkazy
	Sledování obsahu	Ovlivnění uživatele	4	2	4		Používat kritické myšlení a zásady pro identifikaci dezinformací a propagandy
	Ztráta účtu	Informace o jednotce, poloze a uživateli	3	3	3		Heslo používat unikátní, nikde ho nesdílet

Platforma	Obsah	Identifikace nebezpečí	Vyhodnocení závažnosti rizika				Opatření k omezení rizika
			P	N	H	R	
E-mail	Odesílané fotografie	Informace o jednotce, poloze a uživateli	3	4	3		Neposílat fotografie
	Odchozí e-mailová zpráva	Informace o jednotce, poloze a uživateli	3	3	2		V e-mailu nezmiňovat žádné informace o místě nasazení a vlastní jednotce
	Malware	Informace o jednotce, poloze a uživateli	1	2	1		Neklikat na neznámé odkazy
	Řetězové e-maily	Ovlivnění uživatele	2	1	1		Používat kritické myšlení a zásady pro identifikaci dezinformací a propagandy
	Ztráta účtu	Přístup k platformám nepoužívajícím dvoufázové ověření	3	3	2		Heslo používat unikátní, nikde ho nesdílet
Mobilní app	Fotografie	Informace o jednotce, poloze a uživateli	2	4	2		Nesdílet fotografie, zamezit přístup k zařízeni, anebo k síti
	Komentáře a příspěvky	Informace o jednotce, poloze a uživateli	2	2	1		Nepsát příspěvky, zamezit přístup k zařízeni, anebo k síti
	Malware	Informace o jednotce, poloze a uživateli	4	1	2		Neklikat na neznámé odkazy
	Ztráta účtu	Informace o jednotce, poloze a uživateli	3	1	1		Heslo používat unikátní, nikde ho nesdílet

Pravděpodobnost vzniku rizika - P	Komentář	Hodnota
Aktuálně nemožný výskyt	Na dané platformě aktuálně nepodporována možnost	1
Nepravděpodobný výskyt	Ojedinělý výskyt, případně na dané platformě aktuálně nepodporovaný	2
Občasný výskyt	Incidenty vznikají občas, nepravidelně	3
Častý výskyt	Časté opakování incidentů	4

Závažnost následků rizika - N	Komentář	Hodnota
Bez následků	Žádné prozrazení pozice a informací o jednotce	1
Narušení operačních schopností	Vyzrazení informací o jednotce	2
Ohrožení života a zdraví	Vyzrazení pozice jednotky	3
Ztráta bojeschopnosti	Vyzrazení pozice a informací o jednotce	4

Názor hodnotitelů - H	Komentář	Hodnota
Zanedbatelný vliv na operační schopnosti	Ohrožení jednotlivců, lze řešit v krátkém časovém horizontu a v místě nasazení	1
Vliv na operační schopnosti dané jednotky	Ohrožení jednotky, lze řešit v krátkém časovém horizontu a v místě nasazení	2
Vliv na operační schopnosti nadřazené jednotky	Ohrožení jednotky, nelze řešit v krátkém časovém horizontu a v místě nasazení	3
Vliv na operační schopnosti všech jednotek v prostoru nasazení	Ohrožení okolních jednotek, nelze řešit v krátkém časovém horizontu a v místě nasazení	4

Hodnotitel: .....

Platforma	Obsah	Identifikace nebezpečí	Vyhodnocení závažnosti rizika				Opatření k omezení rizika
			P	N	H	R	
Facebook	Fotografie	Informace o jednotce, poloze a uživateli	4	4	3		Nesdílet fotografie, zamezit přístup k zařízeni, anebo k síti
	Komentáře a příspěvky	Informace o jednotce, poloze a uživateli	3	~~4~~	4		Nepsát příspěvky, zamezit přístup k zařízeni, anebo k síti
	Malware	Informace o jednotce, poloze a uživateli	2	2	2		Neklikat na neznámé odkazy
	Sledování obsahu	Ovlivnění uživatele	4	1	1		Používat kritické myšlení a zásady pro identifikaci dezinformací a propagandy
	Ztráta účtu	Informace o jednotce, poloze a uživateli	3	4	~~3~~		Heslo používat unikátní, nikde ho nesdílet
Instagram	Fotografie	Informace o jednotce, poloze a uživateli	4	4	3		Nesdílet fotografie, zamezit přístup k zařízeni, anebo k síti
	Komentáře a příspěvky	Informace o jednotce, poloze a uživateli	2	4	~~3~~		Nepsát příspěvky, zamezit přístup k zařízeni, anebo k síti
	Malware	Informace o jednotce, poloze a uživateli	3	2	1		Neklikat na neznámé odkazy
	Sledování obsahu	Ovlivnění uživatele	2	1	1		Používat kritické myšlení a zásady pro identifikaci dezinformací a propagandy
	Ztráta účtu	Informace o jednotce, poloze a uživateli	3	4	3		Heslo používat unikátní, nikde ho nesdílet
Tik-Tok	Fotografie	Informace o jednotce, poloze a uživateli	4	4	3		Nesdílet fotografie, zamezit přístup k zařízeni, anebo k síti
	Komentáře a příspěvky	Informace o jednotce, poloze a uživateli	2	4	3		Nepsát příspěvky, zamezit přístup k zařízeni, anebo k síti
	Malware	Informace o jednotce, poloze a uživateli	2	4	2		Neklikat na neznámé odkazy
	Sledování obsahu	Ovlivnění uživatele	3	1	1		Používat kritické myšlení a zásady pro identifikaci dezinformací a propagandy
	Ztráta účtu	Informace o jednotce, poloze a uživateli	3	4	2		Heslo používat unikátní, nikde ho nesdílet
Telegram	Fotografie	Informace o jednotce, poloze a uživateli	3	4	3		Nesdílet fotografie, zamezit přístup k zařízeni, anebo k síti
	Komentáře a příspěvky	Informace o jednotce, poloze a uživateli	3	4	4		Nepsát příspěvky, zamezit přístup k zařízeni, anebo k síti
	Malware	Informace o jednotce, poloze a uživateli	3	~~3~~	3		Neklikat na neznámé odkazy
	Sledování obsahu	Ovlivnění uživatele	4	1	4		Používat kritické myšlení a zásady pro identifikaci dezinformací a propagandy
	Ztráta účtu	Informace o jednotce, poloze a uživateli	4	~~4~~	2		Heslo používat unikátní, nikde ho nesdílet

Platforma	Obsah	Identifikace nebezpečí	Vyhodnocení závažnosti rizika				Opatření k omezení rizika
			P	N	H	R	
E-mail	Odesílané fotografie	Informace o jednotce, poloze a uživateli	3	4	7		Neposílat fotografie
	Odchozí e-mailová zpráva	Informace o jednotce, poloze a uživateli	3	4	2		V e-mailu nezmiňovat žádné informace o místě nasazení a vlastní jednotce
	Malware	Informace o jednotce, poloze a uživateli	2	2	1		Neklikat na neznámé odkazy
	Řetězové e-maily	Ovlivnění uživatele	2	1	2		Používat kritické myšlení a zásady pro identifikaci dezinformací a propagandy
	Ztráta účtu	Přístup k platformám nepoužívajícím dvoufázové ověření	4	4	2		Heslo používat unikátní, nikde ho nesdílet
Mobilní app	Fotografie	Informace o jednotce, poloze a uživateli	2	4	2		Nesdílet fotografie, zamezit přístup k zařízeni, anebo k síti
	Komentáře a příspěvky	Informace o jednotce, poloze a uživateli	2	3	1		Nepsát příspěvky, zamezit přístup k zařízeni, anebo k síti
	Malware	Informace o jednotce, poloze a uživateli	2	1	1		Neklikat na neznámé odkazy
	Ztráta účtu	Informace o jednotce, poloze a uživateli	2	2	1		Heslo používat unikátní, nikde ho nesdílet

Pravděpodobnost vzniku rizika - P	Komentář	Hodnota
Aktuálně nemožný výskyt	Na dané platformě aktuálně nepodporována možnost	1
Nepravděpodobný výskyt	Ojedinělý výskyt, případně na dané platformě aktuálně nepodporovaný	2
Občasný výskyt	Incidenty vznikají občas, nepravidelně	3
Častý výskyt	Časté opakování incidentů	4

Závažnost následků rizika - N	Komentář	Hodnota
Bez následků	Žádné prozrazení pozice a informací o jednotce	1
Narušení operačních schopností	Vyzrazení informací o jednotce	2
Ohrožení života a zdraví	Vyzrazení pozice jednotky	3
Ztráta bojeschopnosti	Vyzrazení pozice a informací o jednotce	4

Názor hodnotitelů - H	Komentář	Hodnota
Zanedbatelný vliv na operační schopnosti	Ohrožení jednotlivců, lze řešit v krátkém časovém horizontu a v místě nasazení	1
Vliv na operační schopnosti dané jednotky	Ohrožení jednotky, lze řešit v krátkém časovém horizontu a v místě nasazení	2
Vliv na operační schopnosti nadřazené jednotky	Ohrožení jednotky, nelze řešit v krátkém časovém horizontu a v místě nasazení	3
Vliv na operační schopnosti všech jednotek v prostoru nasazení	Ohrožení okolních jednotek, nelze řešit v krátkém časovém horizontu a v místě nasazení	4