

Využití nástrojů zpravodajství z otevřených zdrojů v oblasti bezpečnosti

Tomáš Holub



Univerzita Tomáše Bati ve Zlíně

Fakulta logistiky a krizového řízení

Ústav ochrany obyvatelstva

Akademický rok: 2024/2025

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	Tomáš Holub
Osobní číslo:	L21381
Studijní program:	B1032A020002 Ochrana obyvatelstva
Forma studia:	Kombinovaná
Téma práce:	Využití nástrojů zpravodajství z otevřených zdrojů v oblasti bezpečnosti

Zásady pro vypracování

- Podle odborné literatury stanovte teoretický rámec problematiky informací z veřejně dostupných zdrojů a jejich získávání.
- U vybraných nástrojů pro získávání informací z veřejně dostupných zdrojů posudte hrozby a rizika spojená s problematikou z hlediska bezpečnosti.
- Navrhněte vhodná opatření ke snížení zjištěných rizik.

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

Seznam doporučené literatury:

1. BAŠTA, Pavel a KOLOUCH, Jan. *CyberSecurity*. Praha. CZ.NIC, 2019. ISBN 978-80-88168-31-7.
2. BAZZEL, Michael. *OSINT Techniques Resources for Uncovering Online Information*. Chicago. Independently Published, 2023. ISBN 979-83-6636-040-1.
3. BOTWRIGHT, Rob. *OSINT 101 Handbook*. Pastor Publishing Ltd, 2023. ISBN 1839385464.
4. HAYES, Darren Richard a CAPP, Francesco. Open-source intelligence for risk assessment. Online. *Business Horizons*. 2018, vol. 61, no. 5, s. 689-697. Dostupné z: <https://doi.org/10.1016/j.bushor.2018.02.001>.
5. LARSEN, Ole Halvar; NGO, Quoc-Hung a LE-KHAC, Nhien-An. A quantitative study of the law enforcement in using open source intelligence techniques through undergraduate practical training. Online. *Forensic Science International: Digital Investigation*. 2023, vol. 47. Dostupné z: <https://doi.org/10.1016/j.fsidi.2023.301622>.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

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

Datum zadání bakalářské práce: **2. prosince 2024**

Termín odevzdání bakalářské práce: **2. května 2025**

L.S.

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

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

V Uherském Hradišti dne 2. prosince 2024

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že

- odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., v platném znění bez ohledu na výsledek obhajoby;
- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a bude dostupná k nahlédnutí;
- jedno vyhotovení bakalářské práce v listinné podobě bude ponecháno Univerzitě Tomáše Bati ve Zlíně k uložení;
- 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 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 řádně citoval; v případě publikace výsledků budu uveden jako spoluautor;
- odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne: 2.5. 2025

.....
podpis autora

ABSTRAKT

Bakalářská práce se zaměřuje na problematiku využití nástrojů zpravodajství z otevřených zdrojů v oblasti bezpečnosti. Nejprve je zde vysvětlena úloha zpravodajství z otevřených zdrojů z hlediska bezpečnosti v různých sektorech lidské činnosti. Poté jsou popsány některé ze známých nástrojů pro získávání informací z veřejně dostupných zdrojů, včetně jejich základního rozdělení a funkčních atributů. Následně je proveden rozbor dvou skutečných případů zneužití veřejně dostupných informací a získané poznatky jsou aplikovány do analýzy rizik. Nakonec je na základě získaných informací navrženo odpovídající školení ohledně informační, kybernetické a osobní bezpečnosti.

Klíčová slova: Otevřené zdroje, zpravodajství, bezpečnost, sociální média, doxxing.

ABSTRACT

The bachelor thesis deals with the issue of the use of open-source intelligence utilities in the security sector. Firstly, it explains the role of open-source intelligence in the field of security across many areas of human pursuit. Secondly, there are described some well-known utilities for gaining information from publicly available sources including their basic sorting and functional attributes. Subsequently, there are explained characterizations of two real cases in connection with the misuse of publicly available information, and derived facts are applied to risk analysis. Lastly, there is introduced suggestion of relevant training based on gained information and facts and concluding possible improvements in information security, cyber security, and personal security.

Keywords: Open source, intelligence, security, social media, doxxing.

V první řadě bych rád poděkoval vedoucímu mé práce, panu Ing. Pavlu Valáškoví za jeho odborné vedení, věcné a užitečné rady, ochotu a přístup. Dále chci poděkovat své rodině a přátelům za podporu, trpělivost a inspiraci.

„Investice do vědění nesou nejvyšší úrok.“

Benjamin Franklin

OBSAH

ÚVOD.....	11
I TEORETICKÁ ČÁST	12
1 DEFINICE, PODSTATA, HISTORIE, PRÁVNÍ RÁMEC A SOUČASNÉ VYUŽITÍ ZPRAVODAJSTVÍ Z OTEVŘENÝCH ZDROJŮ	13
1.1 DEFINICE, PODSTATA A HISTORIE ZPRAVODAJSTVÍ Z OTEVŘENÝCH ZDROJŮ.....	14
1.2 PRÁVNÍ RÁMEC ZPRAVODAJSTVÍ Z OTEVŘENÝCH ZDROJŮ V PODMÍNKÁCH ČESKÉ REPUBLIKY	15
1.3 SOUČASNÉ VYUŽITÍ ZPRAVODAJSTVÍ Z OTEVŘENÝCH ZDROJŮ PRO ÚČELY POLICEJNÍHO VYŠETŘOVÁNÍ A VÝCVIKU	17
1.4 ZPRAVODAJSTVÍ Z OTEVŘENÝCH ZDROJŮ V SOUČASNÝCH VÁLEČNÝCH KONFLIKTECH.....	18
1.5 SOUČASNÁ ÚLOHA ZPRAVODAJSTVÍ Z OTEVŘENÝCH ZDROJŮ V GEOPOLITICKÉM DĚNÍ A INVESTIGATIVNÍ ŽURNALISTICE.....	21
1.6 AKTUÁLNÍ VYUŽITÍ ZPRAVODAJSTVÍ Z OTEVŘENÝCH ZDROJŮ PRO ÚČELY MAPOVÁNÍ A HODNOCENÍ RIZIK	23
1.7 ZPRAVODAJSTVÍ Z OTEVŘENÝCH ZDROJŮ PRO ZÍSKÁVÁNÍ INFORMACÍ ZE SOCIÁLNÍCH MÉDIÍ.....	26
1.8 MOŽNOSTI ZNEUŽITÍ INFORMACÍ Z OTEVŘENÝCH ZDROJŮ – DOXXING.....	28
2 NÁSTROJE PRO ANONYMIZACI A BEZPEČNÉ PROHLÍŽENÍ WEBU.....	32
2.1 NÁSTROJE PRO ANONYMIZACI UŽIVATELE.....	32
2.2 NÁSTROJE PRO BEZPEČNÉ PROHLÍŽENÍ WEBU	34
3 NÁSTROJE PRO ZÍSKÁVÁNÍ INFORMACÍ Z OTEVŘENÝCH ZDROJŮ.....	35
3.1 NÁSTROJE PRO OBECNÉ VYHLEDÁVÁNÍ	35
3.2 NÁSTROJE PRO VYHLEDÁVÁNÍ INTERNETOVÉ AKTIVITY A IDENTITY, EMAILOVÝCH ADRES, TELEFONNÍCH ČÍSEL A PRŮZKUM SOCIÁLNÍCH MÉDIÍ	37
3.3 NÁSTROJE PRO VYHODNOCOVÁNÍ METADAT	39
3.4 NÁSTROJE VYUŽITELNÉ PRO PRÁCI S MAPOVÝMI PODKLADY	40
3.5 VYUŽITÍ NÁSTROJŮ PRO ZÍSKÁVÁNÍ INFORMACÍ Z OTEVŘENÝCH ZDROJŮ V PREVENCI A OCHRANĚ PROTI DOXXINGU	42
II PRAKTICKÁ ČÁST	45
4 PŘEDSTAVENÍ VYBRANÝCH RIZIKOVÝCH UDÁLOSTÍ SOUVISEJÍCÍCH S MOŽNÝM ZNEUŽITÍM NÁSTROJŮ PRO ZÍSKÁVÁNÍ INFORMACÍ Z OTEVŘENÝCH ZDROJŮ.....	46
4.1 PRVNÍ UDÁLOST – INICIATIVA „HE WILL NOT DIVIDE US“	46
4.2 DRUHÁ UDÁLOST – STRAVALEAKS	48

4.3	SUMARIZACE POZNATKŮ	50
5	ANALÝZA PŘÍČIN A NÁSLEDKŮ EXPOZICE OSOBNÍCH ÚDAJŮ A DOPADŮ DOXXINGU	52
5.1	PARAMETRY ANALÝZY	52
5.2	ANALÝZA	53
5.3	VYHODNOCENÍ ANALÝZY	56
6	NÁVRH ŠKOLENÍ V OBLASTI INFORMAČNÍ, KYBERNETICKÉ A OSOBNÍ BEZPEČNOSTI	57
6.1	ZVÝŠENÍ POVĚDOMÍ O VLASTNÍ AKTIVITĚ NA SOCIÁLNÍCH MÉDIÍCH A NA INTERNETU OBECNĚ	57
6.2	DOPORUČENÍ KE ZŘIZOVÁNÍ PROFILŮ A ÚČTŮ.....	58
6.3	NEBEZPEČÍ VYPLÝVAJÍCÍ Z DOXXINGU, PHISHINGU A SOCIÁLNÍHO INŽENÝRSTVÍ	58
6.5	MOŽNÁ BUDOUCÍ NEBEZPEČÍ V SOUVISLOSTI S DOXXINGEM	60
6.6	SHRNUTÍ.....	60
6.7	OSNOVA NAVRHOVANÉHO ŠKOLENÍ	61
	ZÁVĚR.....	65
	SEZNAM POUŽITÉ LITERATURY	67
	SEZNAM OBRÁZKŮ	72
	SEZNAM TABULEK.....	73
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	74
	SEZNAM PŘÍLOH.....	75

ÚVOD

Informace z otevřených zdrojů se stávají čím dál více významným fenoménem, který se prolíná všemi oblastmi lidské činnosti. Ačkoli hlavní těžiště pro získávání informací z veřejně dostupných zdrojů leží v současné době v internetovém prostoru a moderních technologiích, tak samotný princip pro práci s nimi se neomezuje pouze na tyto oblasti. Prapůvodní princip práce s tímto druhem informací se formoval spolu s ranným zpravodajstvím z lidských zdrojů od doby vzniku prvních civilizací a spočívá především v umění hledat souvislosti mezi fakty, co, proč, kdy a jak lidé dělají, nařizují nebo říkají. Otevřené zdroje ve své podstatě zahrnují vše, co je možné pozorovat, dedukovat nebo jinak interpretovat bez nutnosti překonat něčí zákonem podložené zabezpečení informací nebo porušit příslušné právní normy upravující k takovým informacím přístup. Zároveň v současné době, vzhledem k uživatelské dostupnosti a jednoduchosti některých nástrojů pro získávání informací z otevřených zdrojů, není již bezpodmínečně nutné, že člověk vykonávající průzkum veřejných zdrojů musí mít rozsáhlé IT pozadí. Pro vysoce profesionální a anonymní práci s otevřenými zdroji je nicméně velmi dobrá znalost principů funkce internetových domén, virtualizace, vyhledávacích skriptů, či síťových protokolů nezbytná. Vyhledávání v otevřených zdrojích je také určitou vstupní branou a výchozí technikou pro hackery, a to jak pro ty etické, kteří testují odolnost a zabezpečení informačních systémů, tak i pro ty klasické využívající svých znalostí k nekalým účelům. Lze říci, že ačkoli vytěžování veřejných zdrojů má v současnosti silné technické pozadí, tak jejich vznik, obsah a podstata leží často také v psychologii a sociologii. Jak již bylo zmíněno, informace z otevřených zdrojů mají přesah do mnoha specifických oblastí lidské činnosti, nevylučují oblast bezpečnosti o čemž dále pojednává tato práce.

Cíle práce spočívají v prvotním stanovení teoretického rámce problematiky informací z veřejně dostupných zdrojů podle zahraniční i české odborné literatury, následně v posouzení, jaké hrozby a rizika jsou z hlediska bezpečnosti spojena s vybranými nástroji pro získávání informací z veřejně dostupných zdrojů, a nakonec navržení vhodných opatření ke snížení zjištěných rizik. Samotné zjištění a posouzení rizik je pak provedeno prostřednictvím rozboru dvou významných případů ohrožení bezpečnosti z minulosti a následnou analýzou, která využívá jak poznatků ze zmiňovaného rozboru, tak informací zmiňovaných v teoretické části této práce. Na základě informací zjištěných v teoretické části práce i zmiňovaném rozboru je nakonec navrženo školení se zaměřením na základní ochranu osobních údajů a informací z pohledu uživatele.

I TEORETICKÁ ČÁST

1 DEFINICE, PODSTATA, HISTORIE, PRÁVNÍ RÁMEC A SOUČASNÉ VYUŽITÍ ZPRAVODAJSTVÍ Z OTEVŘENÝCH ZDROJŮ

Informace z veřejně dostupných zdrojů a svobodný přístup k nim jsou jedním ze základních atributů moderní svobodné společnosti. Podle Botwright (2023) je proces získávání informací z otevřených zdrojů uměním extrakce smysluplných a relevantních náhledů a myšlenek z mnoha různých veřejně dostupných médií. Význam zpravodajství z otevřených zdrojů, anglicky Open Source Intelligence (dále OSINT), leží především v jeho podstatě, kdy může poskytnout přístup k validním informacím a hodnotné náhledy do mnoha situací a dění v podstatě každému. Na rozdíl od přístupu k utajovaným informacím, který je často omezen velmi striktními předpisy a pro neoprávněné osoby v podstatě zapovězen, OSINT spoléhá na otevřená data z webových stránek, sociálních médií, veřejných záznamů, novinových článků a dalších podobných zdrojů. Otevřenost tohoto typu zpravodajství umožňuje shromažďování velkého množství informací o jednotlivcích, organizacích, událostech a podobně, bez potřeby zvláštního povolení nebo prověrky. Jedním z kritických aspektů tohoto druhu zpravodajství je ovšem důraz na etické a právní rámce. Protože i když jsou získané informace veřejně dostupné, tak je stále žádoucí, aby byla respektována práva na ochranu soukromí a také přihlíženo k etickým doporučením. Dále co se týče širšího rámce zařazení OSINT, tak podle (Yu 2023) lze v současné době jednotlivé formy zpravodajství rozdělit do několika podkategorií, přičemž se některé kategorie mohou prolínat:

- **OSINT (Open Source Intelligence) – Zpravodajství z otevřených zdrojů**
- **SOCMINT (Social Media Intelligence) – Zpravodajství ze sociálních médií**
- **HUMINT (Human Intelligence) – Zpravodajství z lidských zdrojů**
- **IMINT (Imagery Intelligence) – Obrazové zpravodajství**
- **SIGINT (Signals Intelligence) – Signálové zpravodajství**
- **FININT (Financial Intelligence) – Zpravodajství z pohybu finančních prostředků**
- **MASINT (Measurement and Signature Intelligence) – Zpravodajství z měření a příznaků**

1.1 Definice, podstata a historie zpravodajství z otevřených zdrojů

Zpravodajství z otevřených zdrojů, je uměním sběru a analýzy veřejně dostupných informací, které pracuje se skutečností, že právě v otevřených doménách existují opravdu bohaté, rozsáhlé a aktuální zdroje dat. Obzvláště v dnešní digitální době, kdy je obrovské množství informací dostupné velmi jednoduše on-line, se zpravodajství z otevřených zdrojů stalo nenahraditelným nástrojem pro celou řadu úkonů, jako jsou akademické výzkumy, privátní i policejní vyšetřování, vyhledávání možných hrozeb v oblasti kybernetické bezpečnosti a nebo vytváření různých analýz a následných hodnocení rizik. Zpracování informací z veřejně dostupných zdrojů tudíž zastává velmi důležitou roli v oblasti získávání a shromažďování dat k různým účelům a nabízí unikátní, dostupný a hodnotný přístup. Důležitá je, ale také odpovídající práce se získanými daty. Což zahrnuje procesy třídění a prioritizace dat, založené na jejich relevantnosti a spolehlivosti. Z důvodu obrovské rozsáhlosti otevřených informačních kanálů jsou analytici věnující se této oblasti často zaplaveni velkým množstvím informací a musejí se naučit rozlišovat, jaké zdroje a data jsou pro ně skutečně hodnotné a aktuální vzhledem k povaze analýz, které v daném období tito analytici tvoří. Typický proces sběru informací z otevřených zdrojů zahrnuje identifikaci, sběr, zpracování, analýzu a report zájmových dat získaných ze zdrojů jako jsou veřejná média, sociální média, fóra, blogy, webové stránky, veřejná vládní data a publikace nebo komerční data. (Pastor-Galindo et al. 2020; Botwright 2023)

Podle Monterubio et al. (2021) existuje ucelený proces sběru a vyhodnocování veřejně dostupných informací již několik desítek let. Například v USA vznikla státní monitorovací agentura věnující se mimo jiné i vyhodnocování veřejně dostupných informací již v roce 1941. Tato agentura byla známa jako Foreign Broadcasting Monitoring Service zkráceně FBIS a během 2. světové války pokračovala ve sběru a vyhodnocování veřejných informací, které byly nějakým způsobem hodnotné pro válečné úsilí. Jedním případem takového sběru bylo například sledování vývoje cen pomerančů v Paříži a využití této informace jako podpůrného ukazatele efektivity spojeneckého bombardování mostů na území okupované Francie a přilehlých oblastí, neboť čím více v krátkém časovém období narůstala cena pomerančů, tím vyšší byla i pravděpodobnost, že došlo ke zničení významných mostů v zájmových lokalitách.

V průběhu následujících let docházelo ke zdokonalování technologií i postupů v oblasti sběru a vyhodnocování veřejně dostupných informací až do dnešní velmi sofistikované a široce zaměřené podoby. Kdy Botwright (2023) uvádí, že tvůrci

akademických a marketingových výzkumů mohou použít OSINT nástroje pro získávání a shromažďování potřebných dat, novináři mají možnost pomoci těchto nástrojů odhalovat skryté souvislosti nebo ověřovat validitu informací pro své články. Právní a detektivní agentury zase mohou pracovat s OSINT nástroji za účelem informační podpory vyšetřování a vyhledávání aktivity podezřelých. Specialisté v oblasti kybernetické bezpečnosti zase spoléhají na tyto nástroje při hledání potenciálních hrozeb a slabých míst IT infrastruktury. Nakonec OSINT nástroje a analýza získaných informací zastávají nezastupitelnou roli i v oblasti národní bezpečnosti a obrany, kde pomáhají vládám monitorovat a hodnotit vývoj situace jak na poli mezinárodního dění, tak i vznik nebo rozvoj potenciálních hrozeb pro bezpečnost státu.

1.2 Právní rámec zpravodajství z otevřených zdrojů v podmínkách České republiky

Ačkoli využití OSINT jako takové není v českých podmínkách právními normami přímo upravováno, což by bylo rovněž velmi složitě proveditelné vzhledem k rozsáhlosti a komplexnosti této problematiky, tak lze říci, že za určitých podmínek do této oblasti zasahují právní normy vztahující se ke kybernetické bezpečnosti (zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů) či svobodnému přístupu k informacím (zákon č. 106/1999 Sb. o svobodném přístupu k informacím) a další právní normy odvíjející se od sektoru, ve kterém zrovna k získávání veřejně dostupných informací dochází, kdy velmi specifický může být např. vojenský sektor. Ačkoli získávání informací z otevřených zdrojů není nějakým způsobem právně závadné, neboť pracuje s informacemi, které o osobě uživatelé sdílí vědomě (vědomost nicméně může být poměrně individuální, vzhledem k přístupu a technickým i informačním možnostem uživatele) a dobrovolně, tak mohou být uživatelská data získaná pomocí OSINT nástrojů zneužita pro útoky jako je sociální inženýrství či doxxing.

Podle Kolouch et al. (2019) se právě v případě sociálního inženýrství vedeného úmyslně pouze za účelem získání citlivých informací již může jednat o kybernetický útok o jehož znacích, důkazech a následné trestní sankci pojednává výše zmíněný zákon o kybernetické bezpečnosti. Samotný kybernetický útok lze charakterizovat jako „*jakékoli úmyslné jednání útočníka v kyberprostoru, které směřuje proti zájmům jiné osoby*“ (Kolouch et al. 2019, s. 82). Postihnutelnost takových skutků i jiných zločinů v kyberprostoru, tzv. kyberkriminality je nicméně o něco komplikovanější.

„Při vymezení obsahu pojmu kyberkriminalita je třeba si uvědomit, že spolu s růstem možností využívání informačních a komunikačních prostředků roste i možnost jejich užívání (zneužívání) k páčání trestné činnosti. Proto v podstatě neexistuje jakási univerzální, obecně přijímaná definice, která by rozsah a hloubku tohoto pojmu plně postihla.“ (Kolouch et al. 2019, s. 83)

„Kyberkriminalita, resp. kybernetická trestná činnost, představuje jakousi nejširší množinu pro veškerou trestnou činnost, ke které dochází v prostředí informačních a komunikačních technologií. Velmi často je přenášena >>klasická trestná činnost<< do kyberprostoru, neboť je zde tuto trestnou činnost možné páchat rychleji a efektivněji (např. podvody, šíření materiálů zobrazujících zneužívání dětí aj.). Vedle této transpozice známé kriminality pak dochází ke vzniku nových, mnohdy dosud právem neřešených útoků.“ (Kolouch et al. 2019, s. 83)

„Řadu kybernetických útoků je, i díky absenci trestněprávní normy, možné subsumovat pod jednání, které bude mít povahu správněprávního, či občanskoprávního deliktu, případně se nemusí jednat o jednání, které je postižitelné jakoukoli právní normou (může jít např. pouze o nemorální či netolerované jednání).“ (Kolouch et al. 2019, s. 83)

Vedle kybernetického útoku existuje také tzv. kybernetický incident, jenž je definován v § 7 odst. 2 zákona č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů: *„Kybernetickým bezpečnostním incidentem je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události.“ (Zákon č. 181/2014 Sb.)*

Přičemž tzv. bezpečnostní událostí se podle § 7 odst. 1 zákona č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů, rozumí: *„Kybernetickou bezpečnostní událostí je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací.“ (Zákon č. 181/2014 Sb.)*

„Z dikce zákona tedy vyplývá, že incident může být způsoben jak úmyslným, tak nedbalostním jednáním člověka, ale i vyšší mocí. Podstatné je, že dojde k narušení bezpečnosti informací nebo služeb a informačních a komunikačních systémů s nimi spojených.“ (Kolouch et al. 2019, s. 81)

1.3 Současné využití zpravodajství z otevřených zdrojů pro účely policejního vyšetřování a výcviku

Současný rozmach sociálních médií, internetových fór i veřejných databází v kombinaci s rozvojem OSINT postupů a technik umožnil rovněž vznik nových metod získávání informací za účelem policejního vyšetřování, což se týká jak zločinů v reálném světě, tak i v kyberprostoru. Podle Larsen (2023) je výuka bezpečného získávání informací z otevřených zdrojů pro účely digitálních forenzních věd jedním z klíčových předmětů osnov na mnoha policejních akademiích a souvisejících vzdělávacích institucích. Neboť použití OSINT pro účely digitálního vyšetřování vyžaduje od odpovědných vyšetřovatelů jak pečlivou přípravu používaného hardware a software, tak i určité zkušenosti. Klíčové otázky, které by měly být brány v úvahu jsou:

- Jaké informace jsou hledány.
- Kde by mělo být možné tyto informace najít.
- Zda je nutné sbírat tyto informace v anonymním režimu (každá metodologická prezentace technik zpravodajství z otevřených by měla zahrnovat diskusi ohledně odpovídajícího nastavení počítačového vybavení).

Dále García (2021) uvádí, že pro co nejefektivnější využití technik anonymizace, k zajištění bezpečnosti vyšetřovatele i vyšetřování samotného, je nezbytné, aby odpovědné policejní orgány zajistily na policejních stanicích dostupnost přednastavených vyhledávacích a analytických počítačů. Nicméně podle Larsen (2023) mohou vyšetřovatelé z důvodu větší kompaktnosti a efektivity používat pro účely šetření také prověřené hotspoty a předplacené SIM karty pro připojení k internetu pomocí mobilních telefonů, které jsou určeny k účelům vyšetřování. Larsen (2023) rovněž pojednává o bezpečnosti takového druhu vyšetřování, neboť sběr informací z veřejně dostupných zdrojů podle doporučené policejní metodologie vyžaduje, aby policie disponovala znalostmi potřebnými k zajištění operační bezpečnosti a anonymity.

Bez takových znalostí může být policie kompromitována a vyšetřovaná osoba může podniknout protiopatření nebo rovněž začít sbírat informace o profilu vyšetřovatele, což může nevratně poškodit samotné vyšetřování a, nebo jej významně ztížit. Znamá protiopatření podezřelých osob mohou zahrnovat například vymazání příspěvků ze sociálních médií, uzamčení nebo vymazání účtů, odstranění blogů nebo zveřejnění nových

příspěvků s nesprávnými či přímo falešnými informacemi za účelem zmást vyšetřovatele. V horším případě může také dojít k identifikaci vyšetřovatele a jeho napadení výhrůžkami či různými ultimáty. Dále co se týče vlastního provedení sběru dat, tak vyhledávací techniky používající pokročilejší funkce internetových vyhledávačů jsou jedněmi z nejdůležitějších dovedností při získávání informací z otevřených zdrojů pro účely vyšetřování. (Larsen 2023)

Další technika získávání veřejně dostupných informací pracuje s využitím účelově založených profilů na sociálních médiích. Pomocí těchto profilů je poté možné sledovaná sociální média poměrně anonymně procházet. Například v případě Facebooku, ale vznikají další komplikace, neboť Facebook vyžaduje ověření uživatele telefonním číslem. To je ovšem nežádoucí, protože policejní metodologie bezpečného vyhledávání veřejně dostupných dat vyžaduje velkou míru anonymizace. V minulosti bylo možné facebookový profil ověřit i pomocí potvrzeného emailové účtu, nicméně to se vzhledem ke stále přísnější bezpečnostní politice Facebooku změnilo. Co je ovšem nejdůležitější, případné telefonní číslo použité pro ověření takového účelového profilu, by nemělo být nijak spojené s osobou vyšetřovatele nebo policií celkově. Založení účtu na sociálních médiích jako Instagram nebo LinkedIn vyžaduje stejné kroky pro ověření uživatele jako tvorba facebookového účtu. Méně komplikované zůstává založení twitterového profilu, neboť na Twitteru (dnes síť X) je možné provést ověření uživatele pouze pomocí emailové adresy. (Larsen 2023)

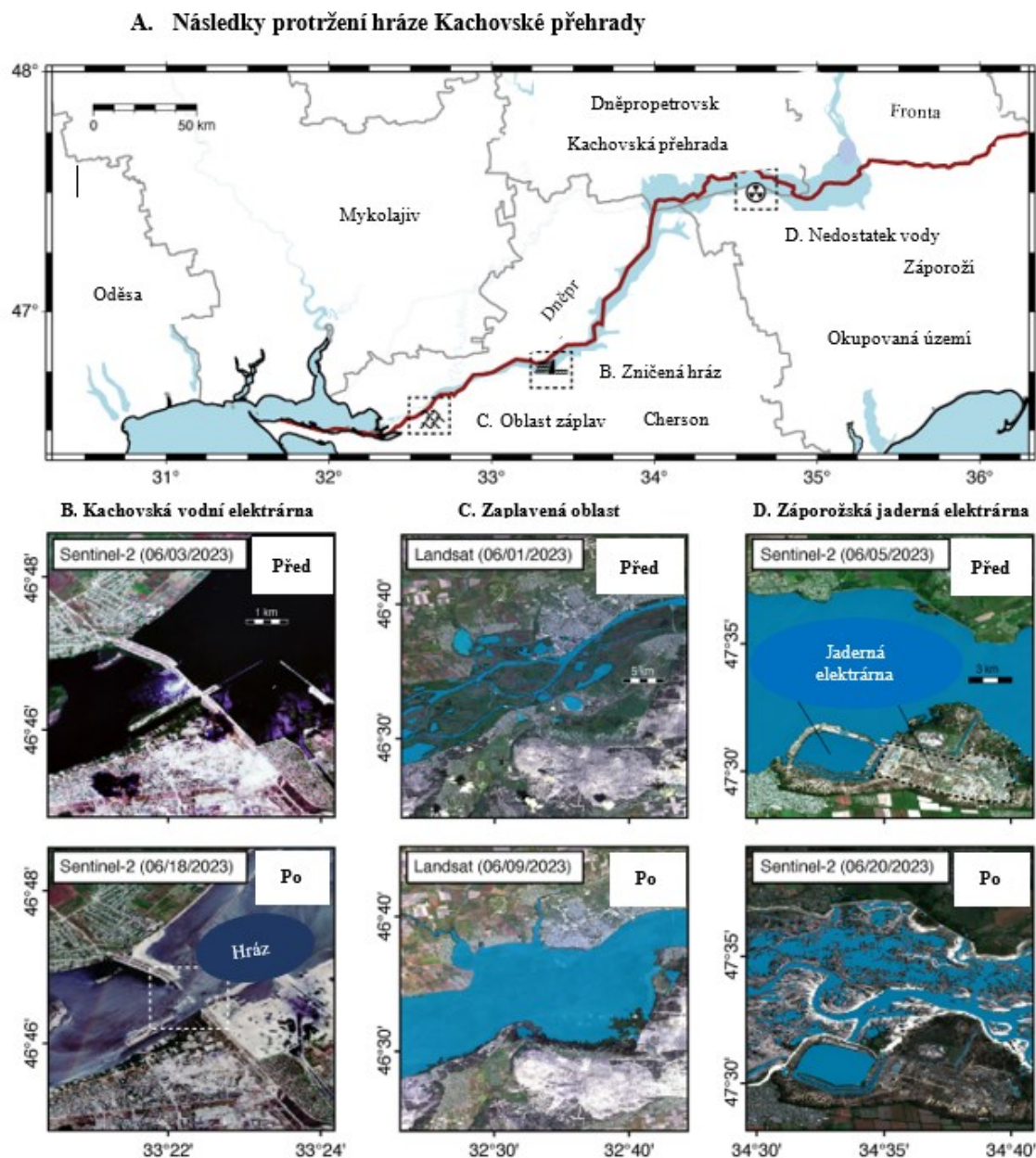
1.4 Zpravodajství z otevřených zdrojů v současných válečných konfliktech

S masivním technologickým rozvojem v oblasti mobilních telefonů, tabletů i počítačů a rozmachem sociálních médií a podobných informačních kanálů si metody práce s veřejně dostupnými informacemi a daty našly svou cestu i do sektoru analýzy a zpravodajské činnosti ve válečných konfliktech. Analýza informací z otevřených zdrojů má nezastupitelnou úlohu také v kontextu konfliktu na Ukrajině, kde komunita profesionálních i amatérských analytiků často pracujících v anonymním režimu pomáhá Ukrajině a v podstatě i celému světu v udržení povědomí o aktuálním dění. Zvláště patrný a klíčový byl potenciál OSINT analýz právě v počátcích ruské invaze, neboť většina novinářů a oficiálních pozorovatelů ze zřejmých bezpečnostních důvodů opustila ohrožené oblasti. Tudiž právě díky práci anonymních OSINT analytiků bylo možné udržet veřejné mapy frontových linií a povědomí o souvisejícím dění aktuální. Digitální otisky generované velkým množstvím záznamových zařízení jako jsou chytré telefony a počítače, produkují svými výstupy na

internetu drobné střípky konfliktu, přičemž jejich četnost a přesnost postupně narůstá. (Limonier 2022; Hauter 2023; Xu et al. 2024)

Informace z otevřených zdrojů tak umožňují zcela nové možnosti pozorování konfliktu, v historickém kontextu možná právě tak přelomové, jako bylo např. televizní zpravodajství stanice CNN během operace Pouštní bouře v roce 1991 (Limonier 2022). Hauter (2023) zmiňuje rusko – ukrajinskou válku jako první vojenský konflikt vysoké intenzity, který se odehrává v 21. století, věku sociálních médií. Poprvé v historii se aktuální, živé informace z frontové linie staly lehce dostupnými na platformách jako je Facebook, síť X (dříve Twitter) a TikTok. Různé výstupy jsou skrze sociální média sdíleny účastníky obou stran konfliktu. Velká rozsáhlost veřejně dostupných informací přímo z frontové linie vytvořila ze zpravodajství z otevřených zdrojů novou vojenskou strategickou doménu a zároveň další nástroj pro vedení informační války. Ve zmíněném konfliktu jsou také široce uplatňovány drony, nová vojenská technologie na poli válečného úsilí, jejichž schopnost poskytovat aktuální snímky vojenských operací, pomáhá zajistit operační působení pěších a mechanizovaných jednotek a snížit ztráty. Dále Xu et al. (2024) uvádí, že rusko – ukrajinský konflikt přerostl ve válku vysoké intenzity, což zcela roztříštilo několik desetiletí míru v Evropě a používání dronů a sociálních médií pasuje zpravodajství z otevřených zdrojů do role klíčové strategické domény.

Nicméně informace z těchto zdrojů mohou být sporadické, těžko ověřitelné a náchylné k manipulaci. Co se týče konkrétního využití dat, tak například veřejně dostupné satelitní snímky je možné použít hned k několika účelům, snímky terénního reliéfu lze využít ke zjištění rozsahu destrukce budov a infrastruktury, a to jak na frontové linii, tak i v zázemí. Mapové snímky zobrazující množství umělého světla vyzařovaného městy v noci je zase možné použít ke zjištění jaké konkrétní a jak velké oblasti byly zasaženy buď výpadky elektrického proudu nebo přímo destrukcí energetické infrastruktury, či zprostředkovaně děním na frontě, kdy některá města a vesnice drží světelnou kázeň z důvodu bezpečnosti záměrně. Dále třeba snímky terénu vystihující barevný kontrast sledovaného prostoru bylo možné použít pro zdokumentování rozsahu záplav podél řeky Dněpr, k nimž došlo z důvodu exploze a následného protržení hráze přehrady Kachovka viz. Obrázek 1. Správná interpretace vhodných dat z otevřených zdrojů může nabídnout objektivní informace o povaze a rozsahu destrukce během vojenských konfliktů. (Xu et al. 2024)



Obrázek 1 Následky protržení hráze přehrady Kachovka

(zdroj: přeloženo z Xu et al. 2024)

Zmíněné pozorování výkyvů intenzity umělého nočního osvětlení měst a vesnic indikuje různými způsoby vynucené změny lidské aktivity napříč celou Ukrajinou. Zatímco intenzita osvětlení měst a vesnic v sousedním Moldavsku, Rumunsku a Polsku byla stabilní, neboť v těchto oblastech nedocházelo k nějakému mimořádnému dění, tak velká část území Ukrajiny byla zahalena do tmy, což indikovalo masivní změnu zdejších podmínek. Napříč neokupovaným územím Ukrajiny se mnohá města a vesnice stala v noci neviditelnými. Pouze okolo tuctu velkých měst v oblasti západní, centrální a východní Ukrajiny byly díky světelné aktivitě rozpoznatelné. Naopak zase i jiné velké aglomerace v oblasti východní Ukrajiny, zůstaly z větší části potměšilé. Tyto pozorované jevy lze považovat jak za důsledek nařízení o světelné kázni vydaných za účelem omezení přesnosti častého bombardování a ostřelování, nebo za důsledek omezení pohybu osob a vozidel v nočních hodinách platící pro některé oblasti, tak i za důsledek masivního exodu velké části populace do spřátelených zemí. Za povšimnutí také stojí fakt, že města v Ruskem okupovaných ukrajinských oblastech sledovaly v inkriminované době rozdílný trend a vykazovaly normální nepřerušovanou světelnou aktivitu. (Xu et al. 2024)

Někdy se ale světelná aktivita měnila rovněž v souvislosti s činnostmi vojenských jednotek obou stran konfliktu, kdy například město Cherson na jižní Ukrajině bylo zasaženo první velkou vlnou výpadku elektřiny způsobenou především bojovými aktivitami již na počátku konfliktu při vpádu ruských jednotek, druhá velká vlna výpadku elektrického proudu v tomto městě pak korespondovala s protiútokem ukrajinských jednotek a osvobozením města na podzim roku 2022. Nicméně například město Lvov na západní Ukrajině v průběhu konfliktu redukovalo svou světelnou aktivitu záměrně, kvůli častým ruským bombardováním zdejší energetické soustavy (Xu et al. 2024). Dále Stone et al. (2024) uvádí, že metody a nástroje pro získávání informací z otevřených zdrojů byly na Ukrajině použity také za účelem vyšetřování válečných zločinů a sledování pohybu a aktivity vojenských jednotek.

1.5 Současná úloha zpravodajství z otevřených zdrojů v geopolitickém dění a investigativní žurnalistice

Ačkoli o vlivu získávání a zpracování informací z otevřených zdrojů na mezinárodní vztahy již začíná vznikat první odborná literatura, tak je v současné době stále poměrně obtížné najít validní zdroje zabývající se otázkou, jaký význam má OSINT v oblasti pozorování a analýzy geopolitického dění. Nicméně nově vznikající krize napříč celým

světem generují čím dál větší množství otevřených dat a pokud jsou tato data přehlížena, nebo považována za nespolehlivý zdroj a jednoduše ignorována, pak může tento přístup činit vlastní analýzy současných konfliktů a širokého geopolitického dění více a více nekompletní a nepřesné. Je zřejmé, že potřeba spojení funkčního monitoringu geopolitických záležitostí a OSINT metod a technik je více než urgentní. Skupiny specialistů, které se věnují analýzám otevřených dat se zaměřují na odkrývání skrytých souvislostí pomocí shromažďování a rozsáhlého ověřování vzájemných vztahů mezi informacemi z různých veřejně dostupných zdrojů. Tyto techniky nemají svůj původ v současných konfliktech, ale vyvíjejí se na pozadí veřejného dění již více než deset let a byly zpopularizovány mimo jiné i investigativními novináři a jejich informačními kanály jako je např. Bellingcat, jenž je známý mimo jiné svým vyšetřováním podílu ruské zodpovědnosti na sestřelení letu MH17, k němuž došlo nad Ukrajinou v roce 2014. Samotný Bellingcat bývá někdy také nadneseně přezíván „lidová zpravodajská agentura“. (Limonier 2022)

O aktivitách organizace Bellingcat se zmiňuje také Zegart (2023), přičemž uvádí, že amatérským investigativním novinářům této organizace se podařilo také identifikovat útočníky, kteří se ve Spojeném království pokoušeli odstranit bývalého ruského zpravodajského důstojníka Sergeje Skripala a dále se zmiňovaným investigativním novinářům povedlo lokalizovat v Evropě žijící podporovatele teroristické organizace Islámský stát. Bellingcat nicméně není jedinou existující civilní zpravodajskou iniciativou, za zmínku stojí také dvojice amerických badatelů (David Albright a Fabian Hinz), kteří se věnovali vyhledávání a ověřování informací souvisejících s íránským jaderným výzkumem či skupina detektivních výzkumníků z kalifornského James Martin Center for Nonproliferation Studies, která zase dokumentovala vznik více než dvou set nových raketových sil pro mezikontinentální balistické rakety na čínském území, což může naznačovat nebývale velký rozmach čínského jaderného arsenálu.

Dále Limonier (2022) uvádí, že při investigativní práci s OSINT technikami je velkou výhodou i určitý odstup a anonymita. To bylo patrné např. v případě skupiny novinářů, kteří se snažili zdokumentovat šíření ruského vlivu ve frankofonních afrických státech. Snahy novinářů sledovat působení skupin bývalých ruských zpravodajských důstojníků, žoldáků a kriminálních v Africe, byly pro samotné novináře značně nebezpečné a došlo i k vraždám několika novinářů, neboť žoldácké skupiny vystupovaly proti publicitě svých činností velmi tvrdě a bezohledně. Zapojení novináři nakonec našli bezpečnější zdroje informací o působení těchto jak polostátních, tak i soukromých žoldáckých skupin, a to právě díky

pokročilým technikám vyhledávání informací v otevřených zdrojích. Digitální otisky zoldáků zanechané emailovými účty, IP adresami apod., v konečném důsledku umožnily jak poměrně detailní zmapování těchto vlivových skupin, tak i hlubší pochopení jejich logiky, strategií a náhledu na business.

1.6 Aktuální využití zpravodajství z otevřených zdrojů pro účely mapování a hodnocení rizik

Úloha OSINT v oblasti analýzy a hodnocení rizik je poměrně širokou problematikou, nicméně lze ji rozdělit do dvou hlavních vývojových proudů, kdy v prvním proudu mohou být informace z otevřených zdrojů použity převážně soukromými organizacemi za účelem zajištění bezpečnosti dané organizace, jejích zaměstnanců a konkrétních tržních a ekonomických zájmů. Naopak v druhém proudu jsou informace a data získaná pomocí OSINT technik a metod využívána státními, soukromými i dobrovolnickými institucemi především k zajištění bezpečnosti široké veřejnosti.

Vzhledem k prvnímu proudu Hayes a Cappa (2018) uvádí, že použití OSINT nástrojů jako je například Maltego pro trasování internetové aktivity a hledání možných bezpečnostních slabin jednotlivců i celých organizací, může zvýšit povědomí vedení i řadových zaměstnanců mnoha firem o těchto problémech. Následně, v reakci na zjištěné skutečnosti a hrozby může být odpovídajícím způsobem zvýšena kybernetická bezpečnost v prostředí dané organizace a vytvořeny podmínky pro potřebná školení a trénink zaměstnanců. Právě výše zmíněné Maltego je nástroj umožňující jak bezpečnostním analytikům, tak hackerům, vyhledání klíčových spojení, souvislostí a aktivit sledovaných uživatelů. Vyhledávání pomocí tohoto nástroje je možné provést na základě vložení jedné základní internetové identity sledovaného uživatele (např. emailu) a Maltego následně vyhledá všechny ostatní internetové identity a aktivity spojené s tou základní. To může zahrnovat i účty na sociálních médiích a zdejší „propojení“ sledovaného uživatele s ostatními uživateli či zájmovými objekty a organizacemi. Což mohou být velmi podstatné informace pro strůjce útoků známých jako „sociální inženýrství“. Kdy podstata tohoto druhu útoků spočívá v tom, že útočník předstírá, že je přítel oběti, popř. jiná osoba či internetová entita u níž je zřejmá důvěryhodnost pro oběť a láká z ní citlivé informace nebo žádá o spojení na sociálních médiích. Díky těmto informacím získaným buď přímo od napadené osoby, tak i nepřímo z jejích sociálních medií a ostatních účtů, se může být útočník následně schopen dostat i do neveřejných interních systémů zaměstnavatele oběti a zde způsobit úniky

dat a další škody. Pro sociální inženýrství mohou být zneužity i informace o partnerech a rodinných příslušnících obětí, získané právě z analýzy sociálních médií. Při ohrožení organizací kybernetickými útoky a úniky informací hraje významnou roli vedle možných pochybení zaměstnanců, také funkčnost vnitřního hardware a aktuálnost software. Včasné použití vhodných OSINT nástrojů za účelem zmapování a analýzy těchto aspektů následně umožňuje efektivní a rychlé odstranění vad technického rázu a také naplánování a aplikování vhodných školení pro zranitelné zaměstnance. Organizace by tudíž měly klást velký důraz na monitorování internetu za účelem snížení bezpečnostních rizik a odpovídajícím způsobem reagovat na nalezené úniky informací. Organizace větší velikosti by v souvislosti s úniky vnitřních informací měly kromě monitorování indexovaných „www – (World Wide Web)“ domén provádět také monitoring deep a dark webu. Proces analýzy by rovněž neměl vynechávat ani zaměstnance pracující na IT odděleních, popř. se vzděláním v oblasti informatiky apod. Někdy bývá zažitým předpokladem, že tito zaměstnanci znají přece možné hrozby nejlépe a není důvod u nich očekávat nějaké chyby, nicméně pravdou je, že určitá slabá místa může mít v podstatě každý. (Hayes a Cappa 2018)

Samotný výstup analýzy rizik by neměl být použit pro omezení přístupu zaměstnancům k interním systémům nebo zavedení jiných restriktivních opatření. Tento výstup by měl sloužit především jako indikátor pro vedení organizace upozorňující na rizikové technické nedostatky a zaměstnance, kteří by mohli potřebovat zvýšenou pozornost nebo školení ohledně bezpečného chování v kyberprostoru. Nakonec je vhodné zmínit, že vzhledem k povaze otevřených zdrojů, které jsou přístupné každému, je většina OSINT nástrojů zdarma, jako například výše zmíněné Maltego a podobné nástroje. Nicméně existují také zpoplatněné nástroje, které reprezentuje třeba LinkedIn Premium, umožňující mnohem detailnější vyhledávání informací než jeho neplacené verze. Ať už se ale daná organizace rozhodne pro kteroukoli variantu, finance vynaložené pro účely analýzy otevřených zdrojů by měly být považovány za přidanou hodnotu účelnou k celkovému zlepšení bezpečnosti organizace. (Hayes a Cappa 2018)

Co se týče druhého proudu využití OSINT nástrojů k analýze rizik hrozících široké veřejnosti, tak podle Stone et al. (2021) překotný rozvoj metod sběru informací z otevřených zdrojů poskytl v oblasti ochrany obyvatelstva zcela nové možnosti. Kdy jsou OSINT nástroje používány např. za účelem včasného varování před epidemiemi různých nemocí. Systémy brzkého varování vycházející ze zpravodajství z otevřených zdrojů, mohou doplnit a zlepšit výkon mechanismů veřejného dohledu, a to především zajištěním včasné detekce rizikových

událostí a vyplněním informační mezery při vyhodnocování dat z geografických oblastí, kde oficiální systémy zdravotního dohledu buď selhávají nebo zcela chybí. Rovněž oficiální systémy zdravotního dohledu vyžadují, aby kliničtí lékaři přiřadili specifické rysy jednotlivých onemocnění ke klíčovým historickým, geografickým a sociologickým datům za účelem rozeznání potencionálního rozvoje onemocnění, a to jak u jednotlivců, tak i u celých populací. Nicméně tento proces může být negativně ovlivněn nedostatkem klinických zkušeností posuzujícího zdravotnického personálu, biologickou variabilitou daného onemocnění v populaci, a především zpožděním v rozpoznání potencionálního onemocnění z důvodu inkubační doby nemoci. V kontrastu s tím, nástroje pro získávání dat z otevřených zdrojů mohou poskytnout dřívější varování před danou nemocí, a to především díky podrobné analýze velkých objemů nestrukturovaných dat a další internetové komunikace. Takové informace nevyžadují od svých zpracovatelů klinické zkušenosti, oficiální zdravotní reporty nebo výsledky laboratorních testování. Díky použití vhodných algoritmů pro sběr dat z otevřených zdrojů, tak mohou být podklady pro včasná varování při šíření různých onemocnění, získány z neoficiálních zdrojů jako jsou lokální novinové články a sociální média. I když by takto získané informace postrádaly lékařské ověření, pro účely okamžitého varování před šířením dané nemoci by byly dostačující. Zároveň by ihned následovalo běžné lékařské posouzení vážnosti situace, které by ověřilo nutnost a vhodnost vydaného prvotního varování. (Stone et al. 2021)

Stone et al. (2024) také pojednává i o nových možnostech využití OSINT nástrojů při ohrožení obyvatelstva radiací při haváriích či jiných poškozeních jaderných zařízení, a to v souvislosti s konfliktem na Ukrajině. Vydání včasného varování obyvatelstvu při ohrožení radiací může být z hlediska reakční doby a dostupných informací poměrně obtížné, a přitom vystavení takovému druhu látek může vyústit hned v několik život ohrožujících stavů a zároveň mají tyto látky zpravidla potenciál zasáhnout velké lidské populace. Např. po vystavení radiaci hrozí lidskému organismu akutní radiační syndrom, jehož příznaky mohou být patrné klidně až po několika hodinách, nicméně vhodné léčebné terapie často vyžadují podání ihned po zasažení organismu radiací. Během konfliktu na Ukrajině byl v některých oblastech výrazně omezen veřejný zdravotní dohled a další programy a mechanismy související s radiační ochranou. Tudíž v kontextu pokračujícího konfliktu a upadajících systémů ochrany obyvatelstva, je použití informací z otevřených zdrojů za účelem rychlé identifikace lokalit, kde mohlo dojít k mimořádným radiačním událostem velmi důležité a umožňuje včasné a efektivní nasazení početně limitovaných záchranných sil. Klíčovým

rozdílem ukrajinského konfliktu oproti jiným je především velmi široký a neustále pokračující přísun informací z otevřených zdrojů jako jsou sociální média nebo regionální zpravodajské deníky. Tím pádem mohou být i zdánlivě nesouvisející data z tohoto typu zdrojů, a to jak z ukrajinské, tak ruské strany, použita k detekci důležitých, zdraví ohrožujících událostí. (Stone et al. 2024)

Jmenovitě se této činnosti věnuje např. systém EPIWATCH, který funguje na principu umělé inteligence (anglicky Artificial Intelligence, dále AI) a používá jak oficiální data z úředních reportů, tak i informace a zmínky o projevech nemocí mezi lidmi, zveřejněné na sociálních médiích a internetových stránkách. Na základě těchto dat poté systém generuje epidemická varování. Dalším podobným systémem je EpiTweeter, jenž funguje na podobném principu jako EPIWATCH, avšak jeho hlavním účelem je sběr informací (především ze sociálních médií) naznačujících výskyt symptomů akutního respiračního syndromu. Nicméně při použití těchto systémů je nutné získané informace, pokud možno co nejvíce ověřovat, neboť sociální média mohou být náchylná k účelové manipulaci. (Stone et al. 2024)

1.7 Zpravodajství z otevřených zdrojů pro získávání informací ze sociálních médií

Zpravodajství ze sociálních médií (SOCMINT) obvykle zahrnuje dva typy zdrojů, otevřené zdroje (veřejně přístupné informace) a neveřejná data k nimž je umožněn přístup pouze uživatelům s nějakým privilegiem. Zpravodajství z otevřených zdrojů si jako takové získává čím dál více pozornosti, neboť lidé zjistili, jak jednoduché v současné době může být použití OSINT nástrojů a programů k vyhledání osobních informací. Jedná se např. o případy, kdy lidé pomocí analýzy fotek domů veřejně sdílených na sociálních médiích zjišťují, kde nějaká celebrita bydlí. Díky skutečnosti, že při sběru veřejně sdílených informací nedochází k narušování autorských práv a patentů nebo práv na ochranu soukromí, a především zásluhou faktu, že velké množství lidí otevřeně sdílí své osobní informace na sociálních médiích, se stal OSINT převládající částí SOCMINT, ačkoli SOCMINT jako takový může zcela legitimně zahrnovat i informace nepocházející z otevřených zdrojů. Zpravodajství ze sociálních médií zastává rovněž velmi důležitou úlohu v současném politickém klimatu. Analyzování politické a názorové orientace osob ve vztahu k extremismu se zdá být nikoli pouze vhodné a relevantní, ale rovněž také velmi důležité v případech masových střelců, terorismu a ohrožení národní bezpečnosti. Chování uživatelů

v internetovém prostředí se obvykle zjišťuje analýzou jejich digitálních stop. Digitální stopy jsou útržky dat zanechané internetovou aktivitou uživatele, a to jak vědomě, tak nevědomě. Mohou zahrnovat jednotlivé digitální výstupy jako jsou fotografie, komentáře či videa a, nebo systematicky produkována data jako jsou přihlašovací údaje, historie vyhledávání a metadata. Je zřejmé, že ne všechny digitální stopy jsou veřejně dostupné informace, jako například historie vyhledávání nebo fotografie z účtů s nastaveným vyšším stupněm ochrany soukromí. (Yu 2023; Rozo et al. 2024)

Lepší porozumění politickému a ideologickému přesvědčení rizikových osob může pomoci k přesnější analýze jejich digitálních otisků a dalších stop, což může učinit kybernetické forenzní vědy ještě více efektivní a spolehlivé. Neboť se jedná o poměrně široké a komplexní odvětví s mnoha proměnnými, např. i když nějaký uživatel zveřejňuje velké množství fotografií a dalších informačních sdělení spojených s určitým politikem, tak to nemusí vždy znamenat, že je jeho fanouškem. Obecně se má za to, že politická orientace osob je ovlivněna mnoha faktory jako je osobnost, prostředí, kde daný člověk vyrůstal, morální důvody nebo genetika. Současný trend v oblasti získávání dat pro SOCMINT a dostupná odborná literatura poukazují na čím dál častější spoléhání na AI a automatizovaný sběr velkých objemů dat. Všechny odborné diskuse zohledňující spolehlivost a uplatnitelnost tohoto typu sběru dat, vycházejí z předpokladu, že podklady pro SOCMINT jsou sbírány ve velkých objemech, aby mohly být konvertovány v čísla a podrobeny statistickým analýzám. K využití AI dochází i při tvorbě klasifikačních nástrojů určených ke konstantní a rychlé detekci urážlivého a obtěžujícího vyjadřování na internetu, dále ke sledování vývoje různých hanlivých či výhružných termínů, sloganů a kódovaných frází nebo na jejím principu fungují také nástroje určené k posouzení emoční intenzity textu výhružných zpráv a následná prioritizace těch emočně nejintenzivnějších. Ačkoli je zcela legitimní provádět analýzu sociálních médií pomocí AI algoritmů, je také nutné si přiznat, že v některých oblastech může být SOCMINT značně limitován s ohledem na množství dostupných dat, což může činit AI neefektivní. Např. vyšetřování kriminality v internetovém prostředí se mnohem více zaměřuje na aktivity určitých jednotlivců než na masivní agregaci dat o výskytu nějakých názorových vzorců. Je zřejmé, že i neautomatizovaný SOCMINT může být stále velmi žádoucí v případě absence velkého množství dat nutného pro vyhodnocování pomocí AI. (Yu 2023; Rozo et al. 2024)

Pro kvantitativní SOCMINT pomocí AI není také jednoduché analyzovat politické přesvědčení a názory vyjádřené pouze jemným nebo naopak velmi zmateným způsobem, např. sdílením tzv. „meme“ (často i vytvořeným někým jiným než sdílející osobou) nebo pomocí komentáře sestávajícího pouze z jedné nebo dvou chatrně napsaných vět. A tak, ačkoli jsou kvantitativní metody sběru dat pohodlné z hlediska svojí systematickosti a rozsahu, může kvalitní analýza sociálních médií a profilování možných hrozeb vyžadovat i provedení kvalitativního výzkumu. Dále je také důležité mít na paměti, že některé věci na sociálních médiích nemusejí vůbec korespondovat s realitou, lidé zde mohou falšovat jak svou identitu, tak i životní styl. Za tímto chováním může být buď obyčejná snaha udělat dojem na ostatní uživatele a, nebo může být takové jednání součástí rozsáhlejšího záměru. Ať jsou důvody jakékoli, výstupy SOCMINT analýz by měly brát v úvahu skutečnost, že některé aktivity na sociálních médiích mohou být více orientované na získávání pozornosti a vlivu nad ostatními uživateli než na snahu o pravdivé sebevyjádření. Stejně tak politické názory a orientace lidí nemusí být vždy neměnné. Tudíž prováděný průzkum sociálních médií může od vyhodnocujících vyžadovat určitý cit na možnou nekonzistenci a změny v přístupu k okolnímu dění ze strany zkoumaných objektů. Což je téměř nemožné zajistit, když jsou tyto analýzy zpracovávány automatizovaně z velkých datových objemů. (Yu 2023; Rozo et al. 2024)

1.8 Možnosti zneužití informací z otevřených zdrojů – doxxing

Doxxing je pojem odvozený od anglického slova „documents“ a jeho podstata spočívá ve sběru informací o určité organizaci nebo jednotlivci, a to jak ze sociálních médií, tak i z ostatních internetových stránek a zdrojů. Přičemž jsou k tomuto účelu někdy použity i programy k prolamování hesel, sociální inženýrství a podobné praktiky. Hlavní myšlenkou doxxingu je hrozit, zostuzovat a očeřňovat jak celé organizace či skupiny osob, tak i jednotlivce (Khanu et al. 2016). Tuto tezi podporuje i Foster a Cross (2024), jenž považuje doxxing za nový druh online obtěžování zahrnující záměrné zveřejňování citlivých osobních údajů na veřejných webech a fórech s úmyslem poškodit oběť a zprostředkovaně v ní vzbudit strach. Podobně doxxing charakterizuje i Wilson (2024), který uvádí, že se jedná o úmyslné zveřejňování osobních informací s úmyslem veřejně zostudit, ohrozit nebo potrestat vybranou oběť. Pachatelé doxxingu prohledávají internet a hledají informace, o kterých si oběť myslí, že jsou v bezpečí od cizího zájmu a následně tyto informace zveřejňují, často s negativní konotací či hanlivým komentářem. Zneužitelnými informacemi mohou být adresa bydliště, telefonní číslo, celé jméno, osobní fotografie a podobně. Pachatelé doxxingu

často zveřejňují tyto informace tak, aby byly co nejlépe dostupné pro široké množství jiných uživatelů a mohou, ale také nemusejí, vyzvat k nějaké akci vůči oběti. Dopady doxxingu na oběti zahrnují strach z fyzického napadení buď oběti samotné a, nebo její nejbližší rodiny či přátel a různá další psychická traumata. Odstranění takto zveřejněných informací může stát velké množství financí a trvat roky.

Podle Snyder et al. (2017) lze za hlavní motivy doxxingu považovat „špinavou“ soutěž, kdy jedna strana potřebuje ukázat převahu nad tou druhou, dále snahu o dosažení domnělé spravedlnosti, kdy se útočník snaží ukázat ostatním uživatelům, jak a čím se oběť doxxingu provinila a posledním motivem mohou být politické nebo rasové důvody. Také Zhou et al. (2024) uvádí, že doxxing je druhem kyberšikany, který je uskutečněn formou neschváleného zveřejnění citlivých osobních informací. Takovými informacemi mohou být např. adresa bydliště nebo pracoviště, telefonní čísla, či jiné osobní informace zneužitelné ke ztotožnění uživatele a následnému obtěžování nebo hanobení oběti, a to buď přímo pachatelem a, nebo i jinými osobami.

Doxxing může být také některými lidmi vnímán jako určitá forma „spravedlivého nátlaku“ a způsob, jak udržet ostatní zodpovědné za nějaký druh chování či názoru. Některé názory také uvádějí, že určité případy doxxingu musely být učiněny z důvodu ztotožnění provinilců a umožnění jejich obětem tyto viníky potrestat. A to i v případě, že jednání viníků třeba nebylo zcela nelegální, ale stále morálně špatné a společensky škodlivé. V tomto kontextu je doxxing někdy považován za formou určité samozvané „lidové spravedlnosti“. Nicméně tento fenomén u „lidovou spravedlností“ odsouzených jedinců často vede různým neblahým následkům jako je ztráta zaměstnání, poškození reputace a sociální vyloučení. Zamýšlené restrikce se tak mohou rozšířit daleko za úroveň svých cílů a ovlivnit osobní i pracovní životy zasažených osob, a to někdy i zcela nevratným způsobem. Např. když v USA došlo k záměrnému zveřejnění citlivých osobních údajů u lékařů vykonávajících umělé přerušování těhotenství, tak se mnozí z těchto lékařů cítili zranitelně a izolovaně a byli také nuceni buď omezit vykonávané činnosti a, nebo zcela přestěhovat své ordinace. (Zhou et al. 2024)

Tento trend potvrzuje také Rosen (2021) podle nějž jsou lékaři vykonávající interrupce již poměrně dlouho cílem vyhrožování a nátlaku, který vyvíjejí určité skupiny osob za účelem odradit lékaře od poskytování úkonů spojených s umělým přerušováním těhotenství. Tito lékaři jsou rovněž cílem záměrného shazování jejich odborných kompetencí v očích veřejnosti, a právě online platformy v kombinaci se svobodným přístupem k téměř

neomezeným veřejným záznamům, jsou vstupní branou k šíření nátlaku, pomlouvání i doxxingu.

Dále je také zřejmé, že sociální média se v posledních letech staly hlavním centrem pro sdílení a šíření informací. Jejich role a vliv byly rovněž značně zesíleny během pandemie Covid – 19, neboť toto období bylo charakteristické intenzivními veřejnými debatami vzhledem ke zdravotní politice, kdy byla často přijímána různá opatření, počínaje nařízeními o nošení roušek a respirátorů, až po očkovací programy. Diskuze na výše zmíněná témata byly často velmi obsáhlé, značně polarizované a do značné míry reflektující hluboké názorové rozdělení ve společnosti. V takové situaci se některé skupiny hluboce polarizovaných osob ztotožňovaly s doxxingem jako s taktikou, jak ohrožit, umlčet nebo potrestat jak odborníky a lékaře, tak i ty členy společnosti, kteří stáli na některé z názorových stran a vyslovili se s nějakou obhajobou svého stanoviska. Zejména v oblasti zdravotnictví je čím dál častější, že pacienti přicházející do nemocnic se uchylují k hrozbám nemocničnímu personálu, a to jak verbálně, tak skrze sociální média, zatímco tento personál pouze vykonává svou práci a poskytuje pacientům potřebnou péči. V důsledku takového chování se zdravotnický personál často cítí obtěžován a vzniká nezdravé komunikační prostředí, kdy zdravotníci přestávají věřit nemocnicím jako institucím, neboť ty své zaměstnance často nedovedou podpořit a ochránit. Vzniklé situace dále vedou ke konfliktům na pracovišti a nízké morálce zdravotníků. Řešení situace poté dopadá na vedoucí zdravotnické pracovníky, což ještě více prohlubuje jejich pracovní vytížení. Pacienti také čím dál častěji vypouštějí svou frustraci v souvislosti s poskytovateli zdravotnické péče na veřejných komunikačních kanálech jako jsou sociální média. (Wilson 2024; Zhou et al. 2024)

Doxxing se tak stává v dnešním digitálním věku novou formou násilí na pracovišti, přičemž hranice pracoviště často překračuje. Zároveň je nepředvídatelný a má potenciál zanechávat trvalé negativní dopady jak z hlediska pracovního, tak z hlediska osobního i dlouhé poté, co daná expozice doxxingu skončí. Jak již bylo zmíněno, množství případů obtěžování a šikany ve zdravotnickém prostředí se konstantně zvyšuje. Je tudíž nezbytné, aby si byl vedoucí zdravotnický personál vědom potenciální zranitelnosti svých podřízených a věděl, jak tuto zranitelnost, pokud možno snížit a tím posílit společné úsilí, vedoucí k zajištění zdravého pracovního prostředí. Doxxing může napáchat rozsáhlé škody narušením přístupnosti a kontinuity léčby např. v případech, kdy byli napadení lékaři nuceni přestěhovat své kliniky a ordinace. V konečném důsledku tak může doxxing ještě více zatížit

již teď přetížený zdravotnický personál, urychlit jeho pracovní vyhoření a zvýšit riziko omylů a chyb ze strany zdravotníků a lékařů. (Wilson 2024; Zhou et al. 2024)

Doxxing a internetová šikana, ale nehrozí pouze osobám pracujícím v rizikových sektorech jako je např. zdravotnictví, ale rovněž i akademikům a dalším odborníkům, kteří se snaží tento negativní trend lidského chování a psychiky prozkoumat a zdokumentovat. Vystavení takové hrozbě může mít rovněž za následek přerušení nebo zastavení daného výzkumu s ohledem na bezpečnost jak výzkumného pracovníka, tak i ostatních zainteresovaných osob (Gelms 2021). Existuje také spojení mezi tzv. „temnou triádou“ vlastností lidské psychiky (machiavelismus, narcismus, psychopatie) a pravděpodobností, že se držitel minimálně jedné z těchto vlastností stane pachatelem doxxingu (Foster a Cross 2024). Rovněž může doxxing zanechat následky i na psychickém zdraví osob, kdy zejména mezi adolescenty, kteří byli jeho oběťmi, byl patrný úpadek v oblasti mentálního zdraví (Chen et al. 2018). Dalším jasným příkladem možných závažných dopadů doxxingu je fyzický útok na manžela členky amerického kongresu, k němuž došlo právě na základě zveřejnění osobních informací při doxxingovém útoku. Pachatelé fyzického útoku takto zveřejněných informací využili k nalezení rodinných příslušníků členky kongresu a zranili jejího manžela natolik, že musel být ošetřen v nemocnici (Foster a Cross 2024). Doxxing je neprofesionální a neetický, ohrožuje bezpečnost obětí a nevybíravě zasahuje do soukromí. Dále umožňuje šikanu a vyzívá širokou veřejnost k potrestání jednotlivců, což vede ke ztrátě nezávislé spravedlnosti. Obavy o osobní bezpečnost také mohou odradit mnohé profesionály a odborníky v různých oblastech, od prezentování jejich názorů, výsledků výzkumů i dalších odborných stanovisek a vedení otevřených dialogů s veřejností (Zhou et al. 2021).

2 NÁSTROJE PRO ANONYMIZACI A BEZPEČNÉ PROHLÍŽENÍ WEBU

Při sběru informací z veřejně dostupných zdrojů je velmi důležité brát v úvahu vlastní bezpečnost a soukromí, což často začíná vhodným výběrem operačního systému a způsobu jeho použití a pokračuje osvojením dalších technologií důležitých pro anonymizaci a potencionálně i bezpečnost. Co se týče operačního systému tak v OSINT komunitě a kyberbezpečnosti celkově je pro vlastní výkon hledání, testování apod. často upřednostňován Linux před Windows a macOS. A to jednak z důvodu bezpečnosti, kdy pro Linux existuje mnohem méně škodlivých programů a virů než pro Windows, tak i z důvodu praktičnosti a ceny. Linux je otevřený a nezaplatněný systém (krom několika málo zaplatněných distribucí), který si může stáhnout a nainstalovat každý. Jeho prostředí je také vhodnější ke zmiňovaným účelům, neboť pomocí příkazové řádky Linuxu je možné komunikovat přímo s webovými kanály a je možné zde rychle a efektivně instalovat různé OSINT nástroje, bez limitace mnoha bezpečnostními opatřeními a blokadami jako je tomu u Windows. Existují také distribuce Linuxu, jako je mimo jiné třeba Kali Linux, již vytvořené pro konkrétní účel v oblasti kybernetické bezpečnosti, což může být např. etický hacking. (Bazzel 2023)

2.1 Nástroje pro anonymizaci uživatele

V současné době je dostupných hned několik technik anonymizace, mezi které patří použití tzv. Virtual Private Network (dále VPN), česky známé jako virtuální privátní síť a The Onion Router (dále Tor), česky známého pod pojmem cibulové směřování. Prohlížeč Tor anonymizuje webovou aktivitu a identitu uživatele podobně jako VPN pomocí sítě serverů. Dále internetové prohlížeče jako Mozilla Firefox, Google Chrome, Safari a Internet Explorer již dnes také disponují možností nastavení či instalace přídatných funkcí, umožňujících větší anonymitu uživatele. Pro zajištění anonymity uživatele je důležitou a často používanou technologií také virtualizace. (García 2021)

VPN – Je jedním z klíčových bezpečnostních prvků jak pro OSINT účely, tak i celkově pro bezpečné procházení internetu. Pokud dochází k prohlížení internetu bez VPN, tak webové monitorovací nástroje, správci navštívených webových stránek či někdo další používající k tomuto účelu vhodné nástroje, mohou vidět přibližnou lokalitu, totožnost poskytovatele internetových služeb a druh internetového připojení uživatele. Poskytovatelé VPN služeb mají zpravidla k dispozici řadu serverů v různých státech či světadílech, ke

kterým se uživatel může připojit a maskovat tak svou polohu a další údaje, neboť to, co se zobrazí návštěvními robotům, webovým správcům apod. budou údaje vybraného vzdáleného serveru. Důležité je dbát na kvalitu poskytovatele VPN služeb, neboť u služeb poskytovaných zdarma hrozí, že VPN společnost využije identitu počítače uživatele jako server pro připojení někoho dalšího nebo bude necitlivě zacházet s údaji svých odběratelů. Známi placení poskytovatelé VPN služeb mají filozofii nakládání s údaji uživatelů většinou mnohem kompetentnější a připojení k jejich serverům bývá často rychlejší a spolehlivější. Pro zachování co největší míry anonymity, nabízí většina velkých poskytovatelů VPN služeb také možnost platby pomocí krypto peněženky. V porovnání s Tor při použití kvalitní VPN rovněž nedochází k odmítání přihlášení do různých internetových služeb a není výrazně zpomalena ani rychlost připojení. (Bazzel 2023)

Virtualizace – Z hlediska anonymity, bezpečnosti i praktičnosti se virtualizace stala velmi důležitou součástí OSINT problematiky. Podstata virtualizace spočívá ve vytvoření dalšího (virtuálního) počítače na mateřském počítači pomocí speciálních programů jako je např. VirtualBox, tento virtuální počítač po svém vytvoření sice využívá technických možností mateřského zařízení, nicméně funkčně je od toho mateřského oddělen a chrání tak skutečnou identitu uživatele. V ovládacím prostředí VirtualBoxu je možné jednotlivé virtuální počítače také jednoduše klonovat či mazat, což může být užitečné v případě zasažení virtuálního počítače škodlivými programy či jeho kompromitací vzhledem ke skutečností hledaným na webu. Je také výhodné připojit mateřský systém k VPN a tím zakrýt i ten virtualizovaný. Častým modelem bývá použití Windows jako operačního systému v mateřském počítači a následné nahrání Linuxu do virtuálního prostředí a jeho úprava k OSINT účelům. Velmi funkční a bezpečná je ale také varianta použití Linuxu jako mateřského systému a provedení virtualizace dalšího Linuxu s odpovídajícím programovým vybavením pro OSINT účely. Naopak počítače s macOS jsou na tom s podporou virtualizace o něco hůře. (Bazzel 2023)

Tor – Tor je zažitým názvem původem z anglického „The Onion Router“. Tento systém anonymizuje internetovou aktivitu připojených uživatelů pomocí sítě dobrovolníků spravovaných serverů a zároveň šifruje data uživatelů během prohlížení. Tor jako takový nemaskuje vstupní IP (Internet Protocol address) adresu počítače uživatele, tudíž je výhodné používat Tor v kombinaci s VPN, která zamaskuje vstupní IP adresu počítače. Ovládací prostředí Tor je pro správnou funkci nutné stáhnout do počítače, tudíž je důležité dbát na stažení instalačního souboru z oficiálního webu, neboť mohou existovat různé podvodné

weby, kde hrozí stažení škodlivých programů. Systém Tor je díky svým pokročilým funkcím anonymizace velmi často používán pro přístup k dark webu. (Botwright 2023)

2.2 Nástroje pro bezpečné prohlížení webu

Pro zvýšení vlastní bezpečnosti i efektivity vyhledávání při prohlížení internetu lze použít mimo jiné i tyto nástroje.

Mozilla Firefox – Je jedním z nejznámějších internetových prohlížečů. Jeho velkou výhodou oproti jiným prohlížečům jsou rozšířené možnosti nastavení bezpečnosti a soukromí a rovněž přítomnost dalších funkcí (karta Add-ons či Extensions) umožňujících efektivnější vyhledávání. Firefox také bývá často doporučován jako výchozí prohlížeč, neboť již v základním nastavení je poskytována úroveň ochrany soukromí a bezpečnosti uživatele vyšší než u dalších prohlížečů. Z hlediska získávání informací z otevřených zdrojů patří k jeho největším výhodám především určitá anonymita, kdy lze nastavit, zda a jaká data (cookies apod.), prohlížeč poskytne navštíveným webovým stránkám. (Bazzel 2023)

Google Chrome (Chromium) – Jde o velmi stabilní rychlý a bezpečný webový prohlížeč se značně přesným a efektivním výchozím internetovým vyhledávačem (Google). Pro Chrome je také dostupná celá řada rozšíření k zajištění větší bezpečnosti uživatele (např. rozšíření uBlock k blokování vyskakovacích oken). Nicméně ze své podstaty není Chrome při používání tak anonymní jako právě např. Firefox, neboť má rozdílně nastavenou celkovou filosofii ohledně monitorování internetové aktivity uživatele. (Bazzel 2023)

3 NÁSTROJE PRO ZÍSKÁVÁNÍ INFORMACÍ Z OTEVŘENÝCH ZDROJŮ

Souprava nástrojů pro sběr informací z otevřených zdrojů se může skládat ze softwarových programů i internetových aplikací, které technicky umožňují pokrytí různých fází sběru dat. Vedle níže zmíněných nástrojů, může k větší efektivnosti při sběru veřejně dostupných dat přispět také členství v komunitách zabývajících se OSINT tematikou a celkově komunikace s ostatními odborníky i laiky v dané oblasti, a to prostřednictvím různých fór, blogů a skupin na sociálních médiích. Tyto komunity mohou nabídnout zajímavý vhled do různých situací a událostí a jejich členové spolu sdílejí různé tipy a techniky. Vedle ryze praktického hlediska tyto komunity mohou poskytnout také přátelské prostředí, založené na základě sdíleného entusiasmu pro práci s informacemi. (Botwright 2023)

3.1 Nástroje pro obecné vyhledávání

Google – Jedná se velkou nadnárodní společnost zabývající se vývojem výpočetních technologií a produktů. Asi nejznámější produkt této společnosti, vyhledávač Google je v současné době jedním z nejmohutnějších a nejvíce rozvinutých internetových vyhledávačů s celou řadou různých nástrojů a funkcí, jako je elektronická pošta (Gmail), funkce sdílení dokumentů (Google Docs), mapy (Google Maps) nebo celá řada dalších organizačních a analytických nástrojů. Produktem společnosti Google je také například internetový prohlížeč Chrome. (Google 2025)

Google dorking – Botwright (2023) uvádí, že internetové vyhledávače jako je například Google ale i další, často umožňují přesnější definování vyhledávacích algoritmů a následné zobrazení relevantnějších výsledků. K upřesnění algoritmů dochází pomocí tzv. vyhledávacích operátorů, kdy operátory jako „site:“, „filetype:“ nebo „intitle:“ mohou významně zvýšit efektivitu vyhledávání v otevřených zdrojích. Botwright (2023) rovněž popisuje základní vyhledávací operátory:

- **„site:“** – Konkretizuje hledání na jednu určitou internetovou stránku, tudíž zobrazí výsledky hledání dostupné pouze na dané stránce např. „site: wikipedia.org“ zobrazí pouze výsledky dostupné na stránce Wikipedia.

- **„filetype:“** – Tento operátor filtruje hledání pouze na výsledky v požadovaném formátu např. „filetype:pdf kvantové počítače“ zobrazí výsledky ve formátu pdf, pojednávající o kvantové výpočetní technice.
- **„~“** – Jedná se operátor umožňující hledání synonym. Např. „~zdravé recepty“, zobrazí všechny výsledky jak pro spojení „zdravé recepty“, tak i pro jeho alternativy jako „nutriční recepty“ či „dietní recepty“.
- **„daterange:“** – Zobrazí všechny výsledky vztahující se k nějakému specifickému časovému rámci. Např. po použití „daterange:20220101-20220630 kryptoměna“, dojde k zobrazení výsledků vztahujících se ke kryptoměnám z období od 1. ledna 2022 do 30. června 2022.
- **„intitle:“** – Tento operátor umožní vyhledání výsledků, kde se klíčové slovo vztahuje přímo k názvu článku nebo souboru. Při použití „intitle:OSINT“ budou tudíž zobrazeny všechny články, kde se termín OSINT vyskytuje v jejich titulu.
- **„link:“** – Slouží k odkázání na konkrétní webovou stránku, např. „link:nytimes.com“ zobrazí odkaz vedoucí přímo na webovou stránku The New York Times.
- **„location:“** – Vyhledá výsledky vztahující se pouze k určité lokalitě. Tudíž při použití „location:Paříž cestovatelské tipy“ budou zobrazeny výsledky vztahující se k cestovatelským tipům při pobytu v Paříži.
- **„related:“** – Tento operátor umožňuje objevení webových stránek, které jsou nějakým způsobem spojeny s předmětem hledání, např. při použití „related:github.com“ budou zobrazeny stránky související s webem GitHub.
- **„inurl:“** – Vyhledá klíčová slova vyskytující se přímo v URL adrese.
- **„()“ a „(?)“** – Slouží k vyhledávání různých variant klíčových slov na základě stejného kořene.
- **Booleovské operátory** – Umožňují vytváření různých kombinací výše zmíněných operátorů, nejpoužívanější jsou především „AND“, „OR“ a „NOT“.

3.2 Nástroje pro vyhledávání internetové aktivity a identity, emailových adres, telefonních čísel a průzkum sociálních médií

Vhodná kontrola a ochrana vlastního digitálního otisku se v současné digitální době stává velmi důležitým aspektem úspěchu, soukromí a bezpečnosti. Význam digitálních otisků pro zpravodajství z otevřených zdrojů je čím dál větší, neboť množství otisků, které jednotlivci i celé organizace nevědomě zanechávají svými digitálními aktivitami je obrovské. Každá online interakce ať už se jedná o příspěvky na sociálních médiích, bankovní aktivity nebo jednoduše pouze brouzdání internetem, tak tvoří určité digitální otisky. (Botwright 2023)

OSINT Framework – Jedná se o soubor online nástrojů pro získávání informací z otevřených zdrojů, přičemž tento soubor zahrnuje široké spektrum různých druhů nástrojů určených pro průzkum sociálních médií, trasování webových domén a IP adres a mnoho dalších činností. Výhodou OSINT Framework je především jeho organizovanost, dobrá přístupnost a uživatelská přívětivost. (Botwright 2023)

Maltego – Jde o veřejně dostupný nástroj určený pro vyhledávání informací z otevřených zdrojů. Pracuje s tzv. „dotazy“ (vyhledávací dotazy) a „objekty“, což mohou být různé profily na webech a sociálních médiích či jiné internetové identity. Tyto „dotazy“ jsou různými úryvky programovacích kódů, často napsané v programovacím jazyce Python, s možností modifikace konkrétního kódu podle potřeb uživatele. Např. základní přednastavené vyhledávací dotazy Maltega jsou často navrženy ke skenování populárních sociálních médií, zatímco pro jiný účel napsané dotazy mohou být nově integrovány pomocí funkčního rámce Maltega a sloužit k identifikaci zájmových informací dostupných na dalších méně častých sociálních médiích a webech (Botwright 2023). Podobný popis funkce a určení uvádí také Monterrubio et al. (2021), podle nějž je Maltego nástroj navržený pro účely zpravodajství z otevřených zdrojů a forenzní software k analýze vztahů profilů sledovaných uživatelů mezi jednotlivými sociálními médii a dalšími webovými stránkami.

Shodan – Je nástrojem pro vyhledávání všech zařízení připojených k internetu (Monterrubio et al. 2021). To potvrzuje rovněž Bazzel (2023), jenž uvádí, že Shodan díky sledování provozu metadat odesílaných od zařízení k mateřským serverům, dokáže vyhledat např. servery, routery, cloudy, dohledové kamery, webkamery a různá další zařízení. Bezpečnostní specialisté používají tento nástroj k vyhledávání slabín v systémech, za něž

jsou odpovědní a kybernetičtí zločinci jej zase používají k nelegálním přístupům k nezabezpečeným zařízením.

EyeWitness – Tento nástroj je v podstatě skriptem napsaným v programovacím jazyce Python a automatizuje sběr informací o webových stránkách navštívených zájmovým počítačem (uživatelé) a také o souvisejících spojeních na sociálních médiích daného uživatele. Získané informace o webových stránkách jsou poměrně detailní a zahrnují screeny, IP adresy serverů, názvy, data jednotlivých úprav a zdrojové kódy webových stránek navštívených sledovaným uživatelem. (Bazzel 2023)

Sherlock, SocialScan, Holehe, WhatsMyName, Blackbird, Maigret, Email2Phone, GHunt – Tyto nástroje slouží k hledání různých spojení a zmínek o hledaném uživateli napříč internetem. Po vložení nejčastěji emailové adresy či jiné základní internetové identity zájmového uživatele, je možné pomocí nich najít telefonní čísla, profily na sociálních médiích či fórech a další internetové výstupy související s danou emailovou adresou. Mírně atypický je poté nástroj GHunt, který je při zjišťování výše zmíněných informací velmi efektivní, nicméně pro správnou funkci vyžaduje spojení s Google účtem. (Bazzel 2023)

Toutalis – Jedná se o nástroj pro získávání informací ze sociálního média Instagram. Nástroj se soustředí především na data a další přidružené účty nějakým způsobem související s řešeným instagramovým účtem. Jsou to např. celá emailová adresa a přidružené telefonní číslo. Pro používání tohoto nástroje je nutné disponovat instagramovým profilem, pomocí nějž proběhne přihlášení do média. (Bazzel 2023)

Osintgram – Nástroj určený rovněž k získávání informací o uživateli ze sociálního média Instagram, narozdíl od předchozího nástroje je možné pomocí něj získat kromě emailové adresy a telefonního čísla zájmového uživatele také jeho fotografie, příběhy, komentáře a celou síť sledujících a sledovaných včetně jejich emailových adres, telefonních čísel a dalších informací. Používání tohoto nástroje nicméně také vyžaduje přihlášení do Instagramu pomocí přihlašovacích údajů k nějakému profilu, skrze nějž může potom průzkum média probíhat. Dále je také čím dál častější, že Instagram detekuje aktivity vedoucí k hromadnému sběru informací o účtech a nastavuje nové bezpečnostní opatření k ověření identity průzkumného profilu. (Bazzel 2023)

3.3 Nástroje pro vyhodnocování metadat

Bazzel (2023) definuje metadata následovně: metadata jsou tzv. data o datech, u obrázků se jim také někdy říká „Exif data“ a mohou obsahovat informace o použitém fotoaparátu či kameře a lokaci nebo času pořízení snímku. Poté se Bazzel (2023) věnuje i popisu funkce a určení některých souvisejících nástrojů:

- **Exiftool** – Je nástrojem pracujícím nejčastěji v terminálovém prostředí Linuxu a slouží k hromadnému zjištění metadat u většího množství obrázků, vztahujících se k nějakému uživateli nebo lokalitě. Zjištěná metadata následně exportuje do CSV formátu.
- **mat2** – Zatímco předchozí nástroj sloužil ke zjišťování metadat, tento nástroj používaný především na linuxových distribucích naopak slouží k mazání metadat u vlastních obrázků, přičemž maže informace jako jsou datумы, časy, polohové údaje a podrobnosti o fotoaparátu.
- **Xeuledoc** – Jedná se aplikaci extrahující metadata skrytá v Dokumentech Google, a to včetně jména autora, emailové adresy a dalších identifikátorů. Jde o velmi dobrý způsob, jak zjistit, kdo je konkrétním autorem určitého Google dokumentu.
- **Sherloq** – Je nástrojem sloužícím k identifikaci nějakým způsobem pozměněných a upravených oblastí na fotografiích, k čemuž mohl být použit například Photoshop.
- **Metagoofil** – Tento nástroj je navržený primárně pro Linux a je možné pomocí něj najít a stáhnout dokumenty. Bývá ovšem vzhledem k principu svojí funkce poměrně často blokován vyhledávačem Google a pro obnovení jeho funkčnosti je nutné jej aktualizovat na verzi, která ještě není blokována.
- **HTTrack** – Jedná se o poměrně starou aplikaci, jejíž hlavní funkcí je vytvoření přesné kopie libovolných webových stránek a sítí sociálních médií malé i střední velikosti a následné uložení kopie na lokální disk. Velkou výhodou je, že takto vytvořené kopie internetových stránek lze poté prohlížet stejným způsobem, jako kdyby se jedlo o funkční, živé stránky. Aplikace rovněž funguje ve více rozhráních, lze ji používat jak v terminálovém rozhraní (většinou na Linuxu), tak i v rozhraní internetového prohlížeče.

- **MediaInfo** – Hlavním účelem tohoto nástroje je získávání metadat o digitálních výstupech získaných přímo z originálního zdroje. Může se jednat např. o videa zaslaná emailem přímo z telefonu, který je pořídil. Nástroj následně získá informace o formátu záznamu, místu a času jeho pořízení a také modelu a verzi operačního systému daného záznamového zařízení.

3.4 Nástroje využitelné pro práci s mapovými podklady

Geografická analýza pomocí OSINT nástrojů je v podstatě univerzální a může být aplikována při mnoha scénářích různých událostí, např. při sledování a zjišťování rozsahu přírodních katastrof, monitorování občanských nepokojů, posuzování rozvoje městské zástavby a, nebo při vyšetřování kriminálních aktivit. (Botwright 2023)

Google Earth Pro – Jde o aplikaci, která posouvá svou mateřskou stránku Google Maps na vyšší úroveň. Tato aplikace umožňuje výrazné rozšíření možných činností s mapovými podklady, neboť disponuje celou paletou různých nástrojů. Je zde např. možnost importování geografických dat přímo z tabulek, což může pomoci při potřebě jejich rychlé a efektivní vizualizace. Co se týče dalších funkcí, tak prvním krokem je při podrobné práci s touto aplikací vyhledání zájmové lokality (např. pomocí vepsání/vložení GPS souřadnic do vyhledávací kolonky), následně je možné nastavit potřebný stupeň přiblížení a poté je možné začít přidávat vrstvy. Ve výchozím nastavení se zobrazí pouze satelitní snímek sledované lokace, nicméně v menu na levé straně obrazovky lze zvolit různé možnosti (vrstvy) přidaného obsahu do aktuálního mapového snímku. Jednotlivé vrstvy zobrazí v mapě následující charakteristiky:

- **Fotografie** – Digitální fotografie, které uživatelé v dané oblasti nahráli skrze sociální média a další síť.
- **Ulice** – Textová vrstva s názvy ulic ve sledované oblasti.
- **3D Budovy** – Alternativní 3D modely budov v lokalitě.
- **Galerie** – Zobrazí další obsah sdílený lidmi v dané lokalitě, mohou to být i videa na YouTube apod.

Další důležitou funkcí v aplikaci Google Earth Pro je tzv. „historické prohlížení“, které se aktivuje pomocí ikony hodin v liště horního menu. Výběr této možnosti následně otevře časovou osu, při jejímž posouvání je možné sledovat jednu konkrétní oblast v různých časových obdobích. Obvykle ovšem se stářím obrazového podkladu klesá i jeho kvalita,

nicméně pro sledování majoritních změn ve vybrané lokaci je tato funkce velmi účelná. Těmito změnami mohou být např. různé přístavby a modifikace budov, nárůst množství vozidel parkujících v okolí budov či terénní změny. Co se týče konkrétního využití této funkce, tak ji pro monitorování podezřelých objektů často používají například i policejní vyšetřovatelé se zaměřením na odhalování výroby a distribuce drog. (Bazzel 2023)

Google Maps – Jsou jedním z mnoha produktů společnosti Google. Tyto mapy jsou velmi pokročilé a poskytují detailní přehled o rezidenčních i komerčních oblastech, institucích, veřejných komunikacích a mnoha dalších objektech v libovolných lokalitách po celém světě. Po vyhledání zájmové lokality v mapách Google je dále možné zobrazit tuto lokalitu detailněji pomocí funkce „Street view“. Tato funkce umožňuje uživatelům se vizuálně v podstatě „postavit“ na ulici či náměstí ve sledované lokalitě a také se virtuálně projít a získat tak dobrou představu o podobě zdejších staveb, parků a ulic včetně různých detailů jako jsou vstupní dveře nebo fasády domů. Měla by se, ale brát v úvahu také skutečnost, že obrazové podklady pro „Street view“ mohou být i několik let staré, tudíž ne vždy aktuální nebo nemusí být v některých oblastech podklady pro tuto funkci ani dostupné. (Larsen 2023)

Mapy.cz – Velmi povedenou stránkou a v dnešní době i aplikací s mapovými podklady jsou také Mapy.cz nabízené českým webovým portálem a vyhledávačem Seznam.cz. V podmínkách ČR nabízejí Mapy.cz stejný servis a funkce jako Google Maps, přičemž je jejich ovládání intuitivnější a jejich podklady v tuzemských případech i detailnější. Při hledání mapových podkladů a detailů v zahraničních státech, je nicméně znát, že širší pokrytí Google Maps je celosvětovém měřítku větší. Mezi hlavní funkce aplikace Mapy.cz patří například zaměření a sledování dané pozice, sdílení polohy, vyhledávání různých míst a bodů, plánování tras, foto tipy zajímavých míst v okolí a navigace, jak pro automobily, tak i pro cyklisty a pěší. Dalšími povedenými funkcemi jsou „Panorama“, což je určitou obdobou funkce „Google Street View“ umožňující detailní procházení snímků ulic a domů a funkce „3D Pohled“, která umožňuje zobrazení 3D modelů budov a dalších objektů. (Seznam.cz 2025)

3.5 Využití nástrojů pro získávání informací z otevřených zdrojů v prevenci a ochraně proti doxxingu

Podle Khanna et al. (2016) mohou být k doxxingu použity různé OSINT nástroje jako je například Maltego, jež umožňuje vyhledání webové architektury sledované organizace či internetových otisků osob, což může být vodítkem k nalezení slabin v kybernetické bezpečnosti. Stejně tak, ale Maltego může dobře posloužit i při prevenci proti doxxingu či jinému druhu kybernetických útoků, kdy je možné pomocí něj slabá místa uživatelů i organizací najít a daný stav napravit či jinak vhodně reagovat, dříve, než se někdo pokusí například právě o doxxing. Doxxingu lze předcházet pomocí následujících technik:

- **„Dox Yourself“** – Tato technika zahrnuje použití nástrojů jako je výše zmíněné Maltego k vyhledání co největšího množství informací o vlastní osobě a následně zajištění nezbytných opatření, pokud by některé z objevených informací neměly být veřejně dostupné. Takto posbírané informace by také měly být opatrně posouzeny z hlediska jejich potenciálu tvořit spojení a nebo odkazovat na další zdroje citlivých dat o osobě nebo organizaci. Důležitou částí prevence proti doxxingu je také minimalizace vystavování osobních údajů v chatovacích místnostech a zprávách obecně.
- **Dvoufázové ověření hesla** – Tento ochranný princip spadá do bezpečnostního konceptu víceúrovňového ověřování a bývá používán jak k ochraně interních systémů různých organizací, tak i k ochraně dat jednotlivců. Jeho výhoda spočívá v tom, že když útočící hacker úspěšně zjistí nebo uhádne heslo uživatele, tak mu samotné heslo nestačí, neboť druhá fáze ověření uživatele vyžaduje jednorázový bezpečnostní kód zasláný textovou zprávou na telefon uživatele. Tato koncepce je užitečná, neboť zvyšuje celkovou ochranu uživatelů a zároveň mohou být uživatelé také informováni ohledně možného napadení účtu v případě cizího neautorizovaného pokusu o přihlášení.
- **Použití Tor** – Tato technologie může být použita jako bezpečnostní prvek internetové komunikace, pokud chce uživatel zakrýt svou IP adresu a lokaci před někým, kdo by se pokoušel o skenování používané sítě. Hlavní výhodou použití routeru Tor je ochrana soukromí uživatelů a znemožnění monitoringu jejich aktivit.

- **Jiné možnosti** – Další možnou metodou, jak se chránit před doxxingem je vytvoření falešných účtů na sociálních médiích a jejich propojení s vícero emailovými adresami založenými pouze za tímto účelem. Taková kombinace zavádějících informací poté může potenciálního hackera zmást. Rovněž je výhodné znát identitu pachatele, tudíž připadá v úvahu především na větších webových serverech a v interních systémech zajistit a nastavit možnosti detekce a upozorňování na neoprávněné pokusy o přihlášení do sítě.

O dalších preventivních technikách pojednávají také Barnett (2020) a Wilson et al. (2024) přičemž doporučují následující opatření:

- Vyhledat skrze vyhledávače pomocí operátorů co je již veřejně dostupné o dané osobě.
- Najít důvěryhodné přátele či rodinné příslušníky, kteří budou nápomocni při nahlašování možného doxxing incidentu.
- Prostudovat si možnosti nastavení a bezpečnostní politiky používaných online účtů, což pomůže ve zlepšování povědomí o možnostech ochrany a způsobech oznamování podezřelých aktivit.
- Redukovat množství veřejně dostupných informací o vlastní osobě. Za tímto účelem je také možné využít služeb organizací, které zabývají stahováním a mazáním shromážděných osobních dat z internetu.
- Být pozorný k nastavení vlastních internetových prohlížečů, ujistit se, zda netrasují činnost uživatele a nevidují údaje o navštívených stránkách a dalších aktivitách.
- Zajistit silnou kontrolu přístupu k účtům na sociálních médiích a vhodně nastavit soukromí, dbát na to, aby zveřejněné příspěvky neobsahovaly osobní informace jako jsou telefonní čísla, adresy, informace o koníčcích a zájmech, nebo fotografie poskytující vodítka k aktuální poloze uživatele. Všechny příspěvky je také nutné zveřejňovat se soudností, opatrností a vědomím, že cokoli je otevřeně zveřejněno, si může stáhnout nebo vyfotit téměř každý. Dále se doporučuje vyhledat vlastní označené fotografie na sociálních médiích a odebrat označení uživatele a také vymazat ty účty, které již nejsou používány.

- Být vnímavý a pozorný vůči pokusům o sociální inženýrství nebo o phishing, žádající o identifikační, přihlašovací a další osobní údaje. Je také doporučeno provést revizi hesel a zajistit, aby tato hesla splňovala požadované parametry a nebyla na různých účtech stejná. Je také důležité monitorovat pohyby peněz na vlastním bankovním účtu.

II PRAKTICKÁ ČÁST

4 PŘEDSTAVENÍ VYBRANÝCH RIZIKOVÝCH UDÁLOSTÍ SOUVISEJÍCÍCH S MOŽNÝM ZNEUŽITÍM NÁSTROJŮ PRO ZÍSKÁVÁNÍ INFORMACÍ Z OTEVŘENÝCH ZDROJŮ

Následující události velmi dobře poukazují na rizika spojená se sdílením osobních informací na internetu, sociálních médiích i sportovních a trasovacích aplikacích. Takto sdílené informace mohou být zneužity k doxxingu i sociálnímu inženýrství a phishingu. Tyto útoky mohou vést ke krádežím identity a finančních prostředků, poškození dobrého jména organizací či jednotlivců, obtěžování, šikaně, fyzickým útokům, záměrnému rozvracení vztahů ve společnosti a v krajním případě omezení spolehlivosti a funkčnosti institucí státní správy.

4.1 První událost – iniciativa „HE WILL NOT DIVIDE US“

Iniciativa „HE WILL NOT DIVIDE US“ (On nás nerozdělí), byla určitým politickým a názorovým hnutím v USA, jehož počátek lze datovat do roku 2017. Hlavním motivem pro vznik a činnost tohoto názorového hnutí bylo zvolení Donalda Trumpa americkým prezidentem a iniciátory vzniku hnutí byli americký herec Shia LaBeouf a dále umělci Nastja Säde Rönkkö a Luke Turner. Prvotním cílem hnutí bylo sdružovat lidi s podobným politickým názorem (většina z nich podporovala protikandidátku Donalda Trumpa) a umožnit jim si vzájemně vyjádřit účast, celá iniciativa měla trvat 4 roky, což mělo být celé jedno funkční období nově zvoleného prezidenta Donalda Trumpa. (Internet Historian 2017; Marantz 2017)

Pro tento účel vzniklo u muzea filmového umění (Museum of the Moving Image) v newyorském Queensu místo s živě nahrávající kamerou, kde se zapojení lidé postupně scházeli a dokola opakovali mantru celého hnutí, slogan „HE WILL NOT DIVIDE US“, aby dali najevo svůj názor a vzájemně se podpořili, rovněž se mezi lidmi začaly objevovat i transparenty a vlajky se sloganem iniciativy. Takovýto výstup měl nicméně svá rizika, od expozice spojení tváří zúčastněných osob s daným politickým názorem a následné hrozby a slovní útoky skupiny amerických anarchicko-fašistických internetových trollů, až po přítomnost živých provokatérů na živých vysíláních. Jedna taková událost se poměrně vymstila i samotnému zakladateli iniciativy. Výše zmínění trollové se transformovali, v jakou internetovou entitu „Pepe the Frog“ a provokatéři s vazbami na tuto entitu se vypravili i před zmiňované muzeum, kde ve shromáždění příznivců „HE WILL NOT DIVIDE US“ začali vykřikovat různé nacistické slogany a obhajovat nacistické zločince. To

vedlo k dramatickým výměnám názorů a fyzickým konfrontacím přímo před živě vysílající kamerou. Herec Shia LaBeouf se buď vlivem provokace nebo nedorozuměním dopustil napadení jiné osoby a byl zadržen policií a přesto, že byl poté zase brzy propuštěn, zmiňované muzeum po těchto neblahých událostech s odvoláním na vyhlášky o veřejné bezpečnosti, ukončilo s iniciativou spolupráci. Další místo, které Shia LaBeouf použil pro svou iniciativu a živé nahrávání bylo skladiště pneumatik ve městě Albuquerque v Novém Mexiku, nicméně ani zde neměla iniciativa dlouhého trvání, po několika peprných prohlášeních ze strany herce k internetovým trollům, bylo jimi i toto místo objeveno a zvandalizováno sprejerstvem. (Internet Historian 2017; Marantz 2017)

Způsob vyjadřování hnutí se tedy musel změnit a posunul se více do online roviny, přičemž se bílá vlajka s černým písmem napsaným textem „HE WILL NOT DIVIDE US“ umístěná na neznámém místě stala jakýmsi symbolem hnutí. Tento prapor byl nepřetržitě živě nahráván na kameru, což se stalo jakýmsi vyjádřením, že hnutí je stále živé a nikdo nemá sílu ho zlomit. Z vyjádření politického názoru a snahy o spojení lidí se nicméně stala určitá „hra“, v komunitě kyberbezpečnosti a OSINT známá také jako „Capture the Flag“ a někteří nadšenci zabývající se především problematikou geografické lokalizace, se začali pokoušet odhalit lokalitu umístění praporu. Což se jim nakonec podařilo díky kombinaci analýzy času stmívání, dráhy letadel zachycených na pozadí (bílý prapor byl umístěn proti obloze) a analýze sociálních médií, neboť jedna uživatelka žijící nedaleko lokality umístění praporu, zveřejnila v nedávné minulosti snímek s hercem Shiou LaBeuf a někteří další uživatelé také potvrdili, že herce v dané lokalitě zahlédli rybařit. Bylo objeveno, že hledanou lokalitou je Greeneville ve státě Tennessee a přilehlé okolí. Po vyzrazení lokace praporu došlo jedné noci k jeho uloupení a na uvolněnou žerď byla navlečena červeno-bílá kšiltovka s mottem Donalda Trumpa „Make America Great Again“ a tričko s vyobrazením entity „Pepe the Frog“. Shia se sice pokusil o nápravu stavu a dané předměty z žerď sundal, nicméně nebylo to nic platné, neboť pomocí dronů byla na žerď opět umístěna kšiltovka s mottem „Make America Great Again“ a konfедераční vlajka. Toto mělo ještě více podtrhnout zbytečnost úsilí a myšlenek iniciativy „HE WILL NOT DIVIDE US“. (Internet Historian 2017; Marantz 2017)

Tato iniciativa ale ve své činnosti pokračovala, nicméně přesunula své působení a vlajku na evropský kontinent, konkrétně do Liverpoolu na střešku jednoho z místních muzeí (FACT Museum). Ani zde nicméně nemělo utajení dlouhého trvání a vlajka byla následující den ráno objevena. Příznivci entity „Pepe the Frog“ uvažovali, jak prapor opět sundat a padly

i návrhy na použití dronů, či infiltraci personálu muzea a použití falešných novinářských průkazů. Nicméně, než bylo cokoli ze zmiňovaného uskutečněno, tak došlo k neoprávněnému vniknutí (vyšplhání) tří maskovaných osob na střechu muzea a ti ačkoli nedokázali samotný prapor sundat, tak způsobili komplikace jak ochrance objektu, tak policii. Ačkoli nebyl nikdo zadržen, tak s ohledem na prevenci příštích pokusů, kdy by mohl někdo spadnout při šplhání na vysokou budovu nebo ublížit někomu dalšímu, se muzeum rozhodlo ukončit s iniciativou spolupráci. Prapor byl sundán a po jednom krátkém pokusu o umístění do dřevěného srubu uprostřed divočiny (jehož lokace byla rovněž rychle objevena) byl přemístěn do místnosti v neznámé budově s bílou stěnou na pozadí. Zde se povedlo dohledat pouze přibližnou lokaci díky sklonu denního světla z předpokládaného okna dané místnosti a dále díky času rozsvícení pouličních lamp patrných rovněž díky světlu z předpokládaného okna, to bylo ale vše. Následně tato aféra ztratila na mediálním významu a další pokusy o uloupení praporu se již neuskutečnily. Internetovým trollům se tak nakonec svým způsobem podařilo uzavřít živou iniciativu, plnou lidských emocí do jedné anonymní místnosti. (Internet Historian 2017; Marantz 2017)

4.2 Druhá událost – StravaLeaks

Tato událost se týká především zveřejňování sportovních aktivit pomocí fitness aplikace Strava, členy ochranky francouzského prezidenta Emanuela Macrona, dále členy ochranky amerických prezidentů Joe Bidena a Donalda Trumpa, a nakonec francouzskými námořníky a dalším personálem sloužícím na jaderných ponorkách a jejich domovských základnách. Za odhalení a zdokumentování případu stojí novináři francouzského deníku Le Monde, a kromě potencionálního zneužití osobních údajů samotných má tento případ přesah i do možného zneužití údajů o online aktivitě osob a jejich pohybu pro účely rozkrytí činnosti vojenský jednotek, jejichž činnost jinak probíhá ve veřejně nepřístupném či utajovaném režimu nebo má přesah do možných rizik vyplývajících z důsledků vyzrazení podrobností pracovních cest vysokých státních činitelů. (Le Monde in English 2024; France 24 English 2024; Lawrence 2025)

Ve všech případech byl princip potencionálního ohrožení bezpečnosti v podstatě stejný, členové ochranky prezidentů otevřeně sdíleli své běžecské výkony, a především trasy běhu s ostatními uživateli aplikace a tím pádem bylo poměrně snadné určit v jaké lokalitě se nacházejí. Členové ochranky prezidentů zároveň takto sdílené příspěvky často i doplňovali fotografiemi, kde byli dobře rozeznatelní, jak oni samotní, tak v některých případech i jejich rodinní příslušníci (především manželky a děti) a vzhledem k tomu, že tváře ochránců

vrcholných politiků je možné často vidět na fotografiích v médiích a zprávách a také v mnoha příspěvcích z různých politicky významných událostí na sociálních médiích, tak nebylo těžké identitu těchto strážců odhalit (obzvlášť když sdíleli své informace veřejně). Dále se také stávalo, že z těchto fotografií bylo možné získat další indicie o inkriminovaných lokalitách, například jeden člen ochranky francouzského prezidenta Emanuela Macrona se vyfotil tak, že za ním bylo možné dobře rozeznat letní sídlo prezidenta a vzhledem k tomu, že ochranka doprovází vysoce postavené státníky na všech jejich cestách, tak nebylo obtížné se dovědět, že v daný čas se prezident nachází zrovna ve svém letním sídle. Zvlášť když běžecké trasy z dané lokality sdíleli ještě i jiní členové ochranky. Stojí také za povšimnutí, že se tento problém netýkal pouze jednoho státu či jedné legislativy, ale došlo k němu v určitém časovém období hned v několika státech, ve Francii, USA i Rusku a možná i řadě dalších států. (Le Monde in English 2024; France 24 English 2024; Lawrence 2025)

Je zřejmé, že aktivní sdílení příspěvků v aplikacích a sociálních médiích je celospolečenský trend a povědomí o jeho možné nebezpečnosti nebylo v nedávné minulosti velké ani v úzkém okruhu tak důležitých a vysoce specializovaných pracovníků, jako jsou členové ochranky prezidentů a námořníci sloužící na jaderných ponorkách. Konkrétně v případě námořníků z francouzských jaderných ponorek byl průběh události značně podobný dříve zmiňovaným. Jak někteří námořníci, tak i další personál námořní základny, uveřejňovali své sportovní výkony spolu s běžeckými trasami, které se často vyskytovaly v blízkosti námořní základny ve francouzském Brestu, o níž je známo, že v ní kotví ponorky, vybavené jadernými střelami. Tyto ponorky spadají do důsledně utajovaného francouzského programu jaderného odstrašení, kdy vždy minimálně jedna ponorka operuje v neznámých lokalitách na moři do té doby, než je vystřídána jinou ponorkou, aby bylo zajištěno, že v případě cizího jaderného útoku bude existovat vlastní jaderná síla, o jejíž poloze nepřítel nemá představu a bude tak možné uskutečnit protiútok. Ze samotných tras běhu kolem základny ještě nebylo možné určit, kdo na ponorce skutečně slouží a kdo je pomocný personál základny (ačkoli do vnitřní lokality kolem doků, kde byly běžecké trasy pozorovány už mělo přístup znatelně menší množství lidí než do základny samotné), nicméně jeden námořník začal své příspěvky komentovat ve stylu „Je těžké se dostat zpátky do formy po více než dvou a půl měsících v krabici“ a ještě doprovodil tyto vyjádření obrázkovými emoji bublinek a potápěčské masky. Při důslednějším sledování vícero uživatelů běžajících kolem doků, byla v pravidelném přidávání běžeckých výkonů v aplikaci Strava najednou patrná několika měsíční odmlka. I to svědčilo o tom, že námořníci pravděpodobně vyrazili do

operačního nasazení. Takováto informace ve špatných rukou už může být poměrně velký problém, neboť je najednou známa identita námořníků, spojená se skutečností, že jsou členy posádky jaderné ponorky. Dále není vždy úplně možné utajit, která konkrétní ponorka se vrací z plavby, neboť kolem pobřeží musí v některých místech ponorky plout vynořeny, tudíž jsou viditelné pro náhodné pozorovatele. Díky tomu bylo možné přiřadit výše zmíněné námořníky ke konkrétní ponorce a také zjistit přibližnou operační dobu jedné ponorky. Prosáknutí podrobných informací o tak choulostivém odvětví bezpečnosti, jako jsou jaderné zbraně a personál podílející se na jejich obsluze, na veřejnost, může mít závažné důsledky, obzvláště v současném politickém napětí, kdy se k takovým informacím může snadno dostat cizí jaderná mocnost. (Le Monde in English 2024; France 24 English 2024; Lawrence 2025)

4.3 Sumarizace poznatků

Tato sumarizace poznatků z obou výše rozvedených událostí slouží jako výstupní bod k provedení analýzy v následující kapitole. Jak v případě iniciativy „HE WILL NOT DIVIDE US“, tak v případě aféry „StravaLeaks“ hrály významnou roli následující činnosti, data a postupy:

- Informace o totožnosti uživatelů získané ze sociálních médií a sportovních aplikací.
- Fotografie uveřejněné skrze sociální média a sportovní aplikace, díky kterým poté bylo možné odvodit v jakých lokalitách byly pořízeny a následně vydedukovat polohu uživatele.
- Veřejně dostupné mapové podklady, které umožnily zobrazení některých detailů francouzské námořní základny a polohy kamer a vlajek v případě iniciativy „HE WILL NOT DIVIDE US“.
- Spojení profilů na sociálních mediích i sportovních aplikacích s emailovými účty a další internetovou aktivitou.
- Zneužití zjištěných informací k provokacím, útokům a veřejné dehonestaci (některé fáze doxxingu). Při sledování iniciativy „HE WILL NOT DIVIDE US“, bylo zřejmé, že k těmto událostem docházelo na místech, kde zmiňovaná kamera nahrávala větší množství stejně názorově exponovaných lidí. Když se do davu vmísili provokatéři, tak se situace často obrátila spíše proti samotné iniciativě.

- Kooperace ve skupině při hledání souvislostí. Ať už to byli novináři francouzského deníku Le Monde nebo trollové internetové entity „Pepe the Frog“, práce ve skupině se ukázala jako velmi efektivní, neboť se kumulovaly různé znalosti a pozorovací schopnosti více osob.
- Souvislosti týkající se návštěv a cest prezidentů dostupné na internetových stránkách a sociálních médiích různých velkých světových mediálních agentur.

5 ANALÝZA PŘÍČIN A NÁSLEDKŮ EXPOZICE OSOBNÍCH ÚDAJŮ A DOPADŮ DOXXINGU

Cílem analýzy je posoudit možnost vzniku vážných a nebezpečných důsledků plynoucích z nechtěné expozice osobních údajů a doxxingu ve vztahu k uživatelům zaměstnaným ve státní správě i privátním sektoru. Státní správa je zde sledována především z důvodu návaznosti na bezpečnost jako celek a privátní sektor především v souvislosti možného ohrožení jednotlivců, jejich blízkých a dále také zaměstnavatelů. Pro účely analýzy bylo vycházeno z obecných předpokladů o prostředí, interakci a postavení zaměstnanců v dané kategorii, nicméně nebylo možné zohlednit všechny individuality a specifičnost jednotlivých složek a organizací.

5.1 Parametry analýzy

Možné dopady doxxingu a zneužití osobních informací vycházejí z části z odborných zdrojů a z části z minulých událostí rozebraných v předchozích kapitolách. Události v jednotlivých kategoriích jsou číselně i barevně odstupňovány, přičemž číslo 5 představuje střední míru rizika a čísla 8 a 10 vysokou míru rizika. Číselná hodnocení jsou rovněž, podloženy barevným rozlišením, kdy se žlutá barva vztahuje ke střední míře rizika a červená pak k vysoké míře rizika. Jako podklad pro stanovení číselných hodnot rizika je použita metodika pro informační bezpečnost z amerického Národního institutu standardů a technologií a to konkrétně tabulka *G-4: ASSESSMENT SCALE – LIKELIHOOD OF THREAT EVENT RESULTING IN ADVERSE IMPACTS* nacházející se v příloze dokumentu a udávající pravděpodobnost, s jakou riziková událost v případě svého vzniku povede k předpokládaným následkům (The National Institute of Standards and Technology 2012). Analyzovány jsou následující kategorie zaměstnanců:

- **Řadový personál bezpečnostních sborů a ozbrojených sil**
- **Vedoucí personál bezpečnostních sborů a ozbrojených sil**
- **Specialisté bezpečnostních sborů a ozbrojených sil**
- **Lékaři a zdravotnický personál**
- **Soudci, právníci a justiční úředníci**
- **Zaměstnanci společností v privátním sektoru**

5.2 Analýza

První část analýzy se v první sekci soustředí na řadový a v druhé sekci na vedoucí personál bezpečnostních sborů a ozbrojených sil.

Tabulka 1 První část analýzy

Objekt	Událost	Následek	Riziko	Navrhovaná řešení
Řadový personál bezpečnostních sborů a ozbrojených sil.	Otevřené sdílení osobních informací, fotografií a aktivit na sociálních médiích a fitness aplikacích, aktivní účast v internetových diskuzích a následné cizí zneužití těchto informací.	Možné ohrožení jak samotných osob a jejich nejbližšího okolí, tak i vyšších zájmů v rámci zastávané služební pozice a přiděleného úkolu např. únik citlivých detailů ohledně výjezdu do zahraniční operace.	8	Zvýšení povědomí a disciplíny uživatelů o rizicích sdílení osobních údajů a sdělování informací skrze sociální média a fitness aplikace vzhledem k zastávané pozici a přidružené služební činnosti.
Vedoucí personál bezpečnostních sborů a ozbrojených sil.	Otevřené sdílení osobních informací, fotografií a aktivit na sociálních médiích a fitness aplikacích, aktivní účast v internetových diskuzích a následné cizí zneužití těchto informací.	Možné ohrožení klíčových osob jako jsou vojenští a policejní důstojníci, nebezpečí jejich vydírání skrze informace o rodinných příslušnících apod. v krajním případě ohrožení státních zájmů.	10	Zvýšení povědomí a disciplíny uživatelů o rizicích sdílení údajů skrze sociální média a fitness aplikace vzhledem k zastávané pozici a přidělenému úkolu, v odůvodněných případech vlastní preventivní monitoring pomocí OSINT nástrojů.

(zdroj: vlastní 2025)

Druhá část analýzy řeší v první sekci specialisty bezpečnostních sborů a ozbrojených sil a v druhé sekci lékaře a zdravotnický personál.

Tabulka 2 Druhá část analýzy

Objekt	Událost	Následek	Riziko	Navrhovaná řešení
Specialisté bezpečnostních sborů a ozbrojených sil.	Neopatrné zveřejňování osobních a nepřímo i pracovních informací sdílením polohy, aktivit a fotografií na sociálních médiích a skrze fitness aplikace a následné cizí zneužití těchto informací (viz. případ StravaLeaks).	Možné ohrožení zájmů celého organizačního celku, možné ohrožení osob se zvláštním statusem, možné ohrožení některých aspektů státní bezpečnosti.	10	Zvýšení povědomí a disciplíny uživatelů o rizicích sdílení údajů skrze sociální média a fitness aplikace vzhledem k zastávané pozici, vlastní preventivní monitoring pomocí OSINT nástrojů.
Lékaři a zdravotnický personál.	Doxxing vedený vzhledem k poskytované službě (viz. doxxing personálu interrupčních klinik) a doxxing jako útok na zdravotníky obecně (viz. doxxing lékařů a sester v době opatření proti COVID-19).	Možné přerušení nebo ukončení poskytování specializovaných zdravotních služeb v dané oblasti (soukromé kliniky) nebo vyhoření, demotivace a odchodovost zdravotnického personálu (veřejné nemocnice a kliniky).	5	Zavedení funkčních mechanismů k zajištění větší ochrany soukromí zdravotníků, rychlejší potrestání pachatelů doxxingu a přidání vhodných doporučení ohledně ochrany soukromí pro zdravotnický personál.

(zdroj: vlastní 2025)

Třetí část analýzy se v první sekci věnuje zaměstnancům v oblasti justice a v druhé sekci pak zaměstnancům společností v privátním sektoru.

Tabulka 3 Třetí část analýzy

Objekt	Událost	Následek	Riziko	Navrhovaná řešení
Soudci, právníci a justiční úředníci.	Doxxingový útok spojený s kompromitací oběti na základě otevřeně sdílených osobních informací, fotografií a aktivit na sociálních médiích a veřejně dostupných dat dohledatelných v různých informačních médiích.	Ohrožení důvěry ve spravedlivost a nezájatost soudních procesů zejména ve významně mediálně sledovaných případech. Riziko eskalace situace k možným demonstracím a blokování soudních budov či fyzickému napadání obětí doxxingu.	8	Zvýšení povědomí uživatelů o rizicích sdílení údajů skrze sociální média vzhledem k významu jejich pracovního a společenského postavení. Využití OSINT nástrojů k monitoringu internetových profilů podílejících se na jednoznačném a účelovém šíření nenávisti.
Zaměstnanci společností v privátním sektoru.	Doxxingový či jiný útok na základě otevřeného sdílení osobních informací, fotografií a aktivit na sociálních médiích a fitness aplikacích, aktivní účast v internetových diskuzích.	Ohrožení soukromí a bezpečnosti jednotlivých fyzických osob a jejich rodin, dále možné ohrožení kolegů a nadřízených v práci. Může dojít také dojit ke zneužití získaných informací k rozsáhlejšímu kybernetickému útoku na společnost či skupinu osob s níž je osoba sdílející informace spojena.	5	Zvýšení povědomí uživatelů o rizicích sdílení údajů skrze sociální média a fitness aplikace s ohledem na bezpečnost jak jejich, tak i blízkých osob a firem (případných zaměstnavatelů).

(zdroj: vlastní 2025)

5.3 Vyhodnocení analýzy

Z provedené analýzy vyplývá, že riziko ohrožení bezpečnosti osob i institucí při zneužití informací z otevřených zdrojů a doxxingu se odvíjí podle konkrétního postavení a činnosti napadených osob, načasování i vnějšího prostředí a motivu pachatele. Nelze tvrdit, že při každém neuváženém zveřejnění údajů na sociálních médiích a fitness aplikacích musí dojít k ohrožení bezpečnosti, nicméně každá nepromyšleně sdílená informace může sloužit potencionálnímu pachateli jako vodítko a střípek skládačky k případné nekalé činnosti. Což může mít vážné důsledky, např. pokud napadení uživatelé pracují jako vedoucí personál nebo specialisté ve státních službách či bezpečnostních sborech a ozbrojených silách. Neboť v rámci své pracovní náplně mohou často nějakým způsobem přicházet do styku s citlivými informacemi a i když případný pachatel nemá k takovým informacím přímý přístup, tak z internetové aktivity inkriminovaných osob a dalších střípků jako jsou třeba zmínky o budoucích návštěvách státníků v médiích a na sociálních médiích nebo fotografie pohybu vojenských jednotek a techniky zveřejněné kolemjdoucími lidmi na sociálních médiích, lze poskládat určitou mozaiku toho, co se asi bude v nejbližších dnech a měsících dít. Kdo, kam, na jak dlouho a v jakém počtu pojede apod. Na základě takových informací už poté není pro nepřátelské nebo zločinné aktéry obtížné naplánovat a provést nějakou formu útoku nebo kombinace útoků (teroristický útok, sabotáž, kybernetický útok atd.) a to buď přímo na státní reprezentanty a zaměstnance nebo na některý z důležitých státních zájmů. Zároveň nelze z hlediska sdílených osobních informací podceňovat ani bezpečnost zaměstnanců v oblasti justice a zdravotnictví, neboť přestože nejsou tak lukrativními cíli jako výše zmiňované skupiny státních zaměstnanců, tak případný kybernetický či fyzický útok by mohl napáchat velké škody. Velmi problematický by v širším kontextu mohl být také rozsáhlý a cílený doxxingový útok, který by vedl k dehonestaci bezpečnostních složek, justičního a soudního i zdravotního systému a následné ztrátě důvěry v tyto instituce v očích určité části společnosti. Koncept takového útoku by mohl vycházet z postojů, názorů a míry vyhrocenosti či radikalizace dané části společnosti. Poznatky získané v analýze byly zapracovány do následujícího školení.

6 NÁVRH ŠKOLENÍ V OBLASTI INFORMAČNÍ, KYBERNETICKÉ A OSOBNÍ BEZPEČNOSTI

Na základě provedené analýzy lze navrhnout školení v oblasti informační, kybernetické a osobní bezpečnosti v následující podobě:

6.1 Zvýšení povědomí o vlastní aktivitě na sociálních médiích a na internetu obecně

Na základě zjištění získaných pomocí analýzy lze doporučit důsledné seznámení uživatele s možnostmi nastavení vlastního soukromí na všech provozovaných profilech. Vhodné nastavení soukromí profilů na sociálních médiích může zabránit mnoha případům nežádoucího sledování a různým formám doxxingu. Obecně je nejlepší, když má uživatel svůj profil zcela uzamčen a umožní k němu přístup pouze lidem, které dobře zná. Velmi důležité ale také je, aby si byl uživatel vědom, že v podstatě každá jeho aktivita a identita na internetu a sociálních médiích je z určité části dohledatelná, a to ať už pomocí metadat, sledování aktivit jiných uživatelů spojených s daným uživatelem, pomocí zapomenutých fotek a dalších vodítek zveřejněných v dávné minulosti nebo s využitím mnoha dalších technik sběru informací z veřejně dostupných zdrojů. Jako vhodnou bezpečnostní bariéru a možnost, jak případnému slídilovi ztížit jeho úsilí, lze doporučit používání VPN při každém procházení internetu, zde ale člověk musí buď počítat s tím, že poskytne své platební údaje poskytovatelské společnosti a, nebo se ponoří do světa kryptoplateb a rozšíří tak svou anonymitu o další vrstvu (většina poskytovatelů VPN již dnes umožňuje platbu kryptoměnou) i když ne zcela neprodyšnou. Dále je nutno mít na paměti, že pro některé autorizační procesy může být VPN někdy komplikací. Nedoporučuje se také používání nezaplatněných VPN, daný poskytovatel si svůj zisk může vybrat jinak např. využitím počítače uživatele jako serveru pro někoho jiného, prodejem údajů uživatele nebo zneužitím počítače uživatele k dalším hackerským praktikám.

Známí zpoplatnění a kvalitní VPN poskytovatelé si většinou udržují určité renomé důvěryhodnosti a spolehlivosti. Nicméně celkově při dnešním trendu digitalizace a online služeb je stále těžší zůstat na internetu anonymní a při hledání odpovědi na otázku kolik informací je o nějakém konkrétním uživateli zjištěných, často záleží jak na promyšlenosti jednání a opatrnosti uživatele, tak i na tom jak velkou motivaci, čas, znalosti a finanční i technické prostředky má případný slídil k dispozici a také jak velkou bariérou pro něj jsou zákony. Při případném cizím zjištění a úmyslném uveřejnění osobních údajů, ať už

k takovému jednání došlo z důvodu finanční motivace a, nebo z důvodu osobních či názorových antipatií, je sice možné, že dojde k dopadení a potrestání pachatele, nicméně osobní informace postiženého uživatele, které už se za tu dobu velmi pravděpodobně dostaly k vícero lidem s podobným morálním nastavením jako má odsouzený útočník, je ze všech zákoutí internetu poměrně obtížné a drahé stáhnout zpátky. A to, jaké dopady na soukromí, kvalitu života a bezpečnost postiženého uživatele bude takový incident mít je poměrně individuální a záleží to na tom jak společensky a pracovně je daná oběť situována, na prostřední, kde k incidentu došlo a na mnoha dalších aspektech. Je ovšem vhodné tyto skutečnosti nepodceňovat a nevystavovat se zbytečnému nebezpečí. Nežádoucí zveřejnění osobních údajů se zároveň nemusí týkat jen postižené osoby samotné, ale i jejích rodinných příslušníků, známých, přátel a zaměstnavatele. Proto je také vhodné dbát na určitý stupeň kázně při označování osob na sociálních médiích, zveřejňování podrobných fotografií dětí apod.

6.2 Doporučení ke zřizování profilů a účtů

Vzhledem k dnešnímu rozmachu různých zákaznických účtů vázaných k emailu uživatele/zákazníka, je množství informací dohledatelných o uživateli opravdu velké, stejně tak propojenost sociálních médií značně ulehčuje hledání informací a pokud se někdo nabourá do toho jednoho jediného emailu, tak se skrze něj často dostane i ke všem ostatním souvisejícím účtům. Což může být obzvláště nebezpečné pokud, je s daným emailem spojena například i bankovní identita. Možným řešením, jak tento trend redukovat je používání vícero emailových adres, kdy např. ta, která je spojena s bankovní identitou není používána při získávání slevových karet v obchodech a neslouží ani jako přístupová adresa k sociálním médiím apod. Je důležité mít na paměti, že právě emailová adresa je jeden ze základních údajů, díky němuž lze pomocí odpovídajících OSINT nástrojů hledat přidružená telefonní čísla, profily na sociálních médiích a další internetové identity daného uživatele.

6.3 Nebezpečí vyplývající z doxxingu, phishingu a sociálního inženýrství

Všechny tyto tři činnosti lze zahrnout do škodlivých internetových praktik, které mohou být v určité právní a skutkové konstelaci i trestné a zároveň je k jejich uskutečnění možné použít stejný informační základ zjištěný pomocí nástrojů zpravodajství z otevřených zdrojů. V případě phishingu a sociálního inženýrství se zneužití veřejně dostupných informací obrací přímo proti oběti především za účelem dosažení zisku či získání dalších informací. Zatímco záludnost doxxingu spočívá především v tom, že se zneužitím veřejně dostupných

informací o oběti snaží útočník proti ní otočit určitou část společnosti, kolegů či přátel. Doxxing může být veden jako určitá forma manipulace a jakmile je někdo ztotožněn s nějakou negativní konotací či třeba i domnělým prohřeškem, tak smazat tyto skutečnosti z očí veřejnosti je většinou velmi obtížné až téměř nemožné. Společenská škodlivost doxxingu by neměla být brána na lehkou váhu. Z tohoto důvodu lze uživatelům doporučit, aby sledovali vývoj v oblasti OSINT nástrojů, neboť ten je někdy tak rychlý a samotných nástrojů je tak velké množství, že školení uskutečněné jednou za nějaké časové období (např. jeden rok), zpravidla nedokáže pokrýt všechny nově vzniklé eventuality v této oblasti. Rovněž je také někdy vhodné, jak již bylo doporučováno v teoretické části a jak také ukazuje experiment, občas zkusit vyhledat OSINT nástroji nebo pomocí vyhledávacích operátorů (ale i obyčejné vyhledávání bez nich je lepší než nic) informace o vlastní osobě a v rámci možností se poté pokusit objevené informace redukovat např. pomocí přísnějšího nastavení soukromí na sociálních médiích apod. V době současného politického napětí mohou vznikat velmi specifické situace také u příslušníků ozbrojených sil a dalších bezpečnostních sborů, kdy nelze vyloučit opakování obdobných doxxingových útoků, k jakým docházelo v zahraničí vůči některým lékařům v době zavádění opatření proti šíření nemoci COVID-19.

Dalším rozměrem možných zdrojů ohrožení v souvislosti s příslušníky ozbrojených sil a bezpečnostních sborů je čím dál častější propagace jednotlivých složek na sociálních médiích. Na té by samo o sobě nebylo nic zvláštního, zodpovědní lidé, kteří tvoří příspěvky na sociální média mají obvykle odpovídající školení o tom, co ještě mohou zveřejnit a co už ne a jejich texty pravděpodobně procházejí revizí z vícero organizačních úrovní. Co nicméně nedovede téměř žádná složka regulovat je kumulování identit uživatelů v reakcích na jednotlivé příspěvky, kdy zejména v případě profilů na sociálních médiích u menších organizačních celků je velmi pravděpodobné, že na příspěvky budou reagovat rodinní příslušníci a známí lidí sloužících v daném celku. Toto nabízí poměrně široké pole pro sběr informací o sloužících příslušnících i za předpokladu, že oni sami budou v internetovém prostředí velmi opatrní. Není možné s určitostí říct, že takováto kumulace uživatelů a informací musí vždy nutně znamenat riziko, nicméně i vzhledem k technologickému rozvoji vyhledávačů, OSINT nástrojů a AI, nelze takové zdroje informací přehlížet a je čím dál více patrné, že sociální média mohou být ve své podstatě „dvousečná zbraň“.

6.4 Možná budoucí nebezpečí v souvislosti s doxxingem

Celkový rozměr a nebezpečnost doxxingu může být v blízké budoucnosti ještě posílena technologiemi AI, což se může projevit v efektivitě vyhledávání veřejně dostupných informací, ale i v propracovanosti a nebezpečnosti internetových „důkazů“ a kompromitujících materiálů vůči napadené osobě. Lze si představit např. vytvoření velmi obtížně identifikovatelných „deepfakes“, které budou někoho usvědčovat z jednání, které nespáchal a na základě těch materiálů bude poté pomocí doxxingu usilováno o veřejné „potrestání“ tohoto uživatele. Může vzniknout mnoho kompromitujících materiálů a následných situací, které mají potenciál ohrozit pracovní i soukromý život mnoha osob. Rovněž nelze vyloučit, že se z doxxingu nestane nástroj hybridního boje, používaný s cílem rozvrátit vztahy ve společnosti. Je otázkou, zda zákonné regulace v oblasti kybernetické bezpečnosti dovedou zcela pokrýt rychlost technologického rozvoje. Jednou z mála možností, jak se možným výše zmíněným incidentům bránit tudíž zůstává především zvyšování povědomí uživatelů o možných rizicích.

6.5 Shrnutí

Následující body stručně shrnují výše popsaná doporučení:

- Udržovat si povědomí o vlastní aktivitě na sociálních médiích a fitness aplikacích.
- Přemýšlet o tom, co je zveřejňováno i vzhledem k lukrativnosti takových informací pro někoho dalšího.
- Zveřejňovat fotografie z navštívených lokalit až s časovým odstupem. Zmenší se tím riziko zjištění aktuální lokace uživatele z čerstvě zveřejněných fotografií.
- Používat technologie umožňující alespoň určitou úroveň anonymizace vlastní aktivity (VPN, vhodné nastavení prohlížeče či kombinace obojího).
- Občas zkontrolovat množství informací dostupných o vlastní osobě (s použitím vyhledávačů, vyhledávacích operátorů nebo i vhodných OSINT nástrojů) a minimalizovat dobře čitelné vazby s ostatními uživateli (např. označení na rodinných fotografiích zveřejněných na sociálních médiích). Posílí to bezpečnost a soukromí, jak vlastní, tak i ostatních spřízněných uživatelů.
- Přistupovat kriticky k informacím, fotografiím i videím, dokud nejsou ověřeny z vícero nezávislých zdrojů. V praxi může být toto doporučení hůře proveditelné,

nicméně lze ho považovat za jakousi malou brzdu při řetězovém šíření deepfakes a dezinformací. Je také vhodné minimálně nešířit nějakým způsobem „šokující“ druh obsahu, dokud není potvrzena jeho pravdivost.

- Používat k různým registracím a zřizování rozličných účtů vícero emailových adres.
- Dodržovat doporučení ohledně délky a vhodného formátu hesla a pravidelně svá hesla obměňovat.
- Hlásit podezřelé aktivity a internetové entity zodpovědným institucím, ať už se jedná o administrátory či kontrolní mechanismy sociálních médií a webových stránek nebo o policii v případě vážnějších událostí.
- Věnovat zvýšenou pozornost zprávám a telefonátům, které důsledně požadují okamžité poskytnutí přihlašovacích údajů (uživatelské jméno, heslo) k internetovému bankovníctví nebo kamkoli jinam. Může se jednat o podvod, banka nebo jiné instituce takto detailní informace zpravidla nemá proč vyžadovat.

6.6 Osnova navrhovaného školení

Tato kapitola pojednává o konkrétním rozsahu a podobě výše řešeného školení.

- **Úvod**

Informace z otevřených zdrojů se stávají čím dál více významným fenoménem, který se prolíná všemi oblastmi lidské činnosti. Ačkoli hlavní těžiště pro získávání informací z veřejně dostupných zdrojů leží v současné době v internetovém prostoru a moderních technologiích, tak samotný princip pro práci s nimi se neomezuje pouze na tyto oblasti a spočívá především v umění hledat souvislosti mezi fakty, co, proč, kdy a jak lidé dělají, nařizují nebo říkají.

- **Doporučení pro sociální média**

- Nastavit profil jako soukromý a udržovat si přehled o tom, kdo může sledovat mé příspěvky, aktivitu a okruh přátel.
- Při zveřejňování příspěvků brát v potaz, že cokoli je již jednou zveřejněno, tak v podstatě už nelze vzít zpět, neboť každý, kdo daný příspěvek uvidí si může udělat snímek obrazovky a uložit si informaci pro sebe, čímž autor ztrácí nad svým příspěvkem kontrolu. Dále také komplexní odstranění jednou

zveřejněného příspěvku ze všech internetových databází je velmi komplikovaný a zdlouhavý proces.

- Nezveřejňovat fotografie, ze kterých je přímo patrné místo bydliště nebo důležité detaily týkající se rodiny či práce. Z hlediska práce v soukromém sektoru se až na výjimky nejedná nutně o skutečnost, kde konkrétně člověk pracuje, což dnes v době rozmachu LinkedInu nebo při podnikání lze jen velmi těžko schovat, ale spíše o fotografie či jiné výstupy z nichž lze získat indicie o bezpečnostní architektuře společnosti nebo hesla k interním systémům apod.
- Státním zaměstnancům lze pak doporučit ještě větší míru obezřetnosti při zveřejňování příspěvků na sociálních médiích neboť např. informace o služební činnosti zveřejněné vojáky nebo policisty mohou být velmi lukrativním zbožím pro cizí aktéry a jejich zneužití může mít vážné důsledky.
- Pravidelně měnit svá hesla na sociálních médiích. Jedná se o jakousi pojistku, kdyby se někomu podařilo heslo naleznout, uhodnout či jinak získat. Pravidelnou změnou hesel lze snížit šanci, že možný útočník našel právě to aktuální, platné heslo. Vhodným posílením bezpečnosti může být také vícefázové ověření uživatele při přihlašování.
- Zveřejňovat fotografie či označení polohy až s časovým odstupem. Je důležité zmínit, že zveřejňování příspěvků v reálném čase má svá rizika, neboť každý může ihned vědět, kde se autor daného příspěvku v inkriminovaný okamžik nachází. Obecně lze tudíž doporučit zveřejňovat příspěvky z konkrétních míst až s určitým časovým odstupem. Délka časového odstupu se může odvíjet jak od povahy prostředí a době trávené v daném místě tak i od preferencí uživatelů.
- Při prohlížení sociálních médií je také potřeba přihlížet kriticky k informacím, fotografiím i videím, pokud nejsou tyto výstupy ověřeny z vícero nezávislých zdrojů a nešířit pochybné zprávy a informace, neboť je tak možné alespoň částečně zabránit řetězovému šíření deepfakes a dezinformací.

- **Doporučení při používání fitness aplikací**

- Používání fitness aplikací se v posledních letech stalo velmi aktuálním trendem, lidé spolu skrze fitness aplikace a sociální média sdílí své aktivity, porovnávají výkony a podporují se. Zároveň i samotní uživatelé si díky těmto aplikacím drží lepší přehled o svých výkonech. Z hlediska bezpečnosti je nicméně důležité vidět

i tu odvrácenou stránku, totiž že aplikace vedou detailní záznam o tom kde, kdy a s jakou pravidelností se uživatelé pohybují.

- V první řadě nastavit možnosti sdílení aktivit na soukromé a držet si kontrolu nad tím, kdo všechno může vidět sdílený obsah.
- Nepokládat nastavení soukromého profilu za zcela neprůstředné, může se vyskytnout bezpečnostní chyba v aktualizacích software dané aplikace a tím pádem mohou být údaje o aktivitě a poloze uživatelů vystaveny nechtěné pozornosti.
- Příslušníkům bezpečnostních složek lze doporučit ještě vyšší míru obezřetnosti než ostatním uživatelům. Neboť detailní informace o vojácích a policistech mohou mít z hlediska bezpečnosti velmi velký význam a jejich zneužití může mít dalekosáhlé následky.
- Při fyzických aktivitách zapínat trasovací funkce až v určité vzdálenosti od bydliště nebo práce.

- **Doporučení pro surfování na webu a emailovou komunikaci**

- Pro bezpečné a anonymní prohlížení internetu lze doporučit vhodné nastavení internetového prohlížeče, popř. instalaci jeho rozšíření za účelem zamezení webovým stránkám v některých monitorovacích aktivitách a omezení funkce vyskakovacích oken.
- Použití VPN (Virtual Private Network) pro zvýšení anonymity prohlížení a v konečném důsledku i zvýšení bezpečnosti. Zde je nicméně důležité upřednostnit kvalitu před cenou, neboť neplacené VPN si často mohou svou „platbu“ vybrat jinde a zneužít buď technické vybavení počítače nebo osobní údaje uživatele. Na trhu zavedení placení poskytovatelé VPN si obvykle drží určité renomé a respektují zákonné, bezpečnostní i etické normy. Platit za služby VPN poskytovatelů je dnes již zpravidla možné hned několika metodami od karetní transakce až po platbu kryptoměnou.

- Pro ochranu vlastních osobních informací se také doporučuje používat větší množství emailových adres a dbát na diversifikaci a třídění internetových identit spojených s danou emailovou adresou. Např. email, který je spojený s bankovní identitou nebude používán pro tvorbu členství v obchodech nebo na seznamkách apod.
- Občas se pro lepší představu o vlastní internetové aktivitě může také hodit vyhledat údaje dostupné o vlastní osobě. K tomuto účelu lze využít buď klasické vyhledávače (např. Google) nebo některou z vyhledávacích technik (např. dorking – vyhledávací operátory) či některý z vhodných OSINT nástrojů.
- V neposlední řadě je také důležité věnovat zvýšenou pozornost emailovým zprávám vyžadujícím poskytnutí přihlašovacích údajů (uživatelské jméno, heslo apod.) k internetovému bankovníctví, popř. jiné elektronické identitě. Často se může jednat o podvod, banky nebo jiné instituce zpravidla takové informace touto cestou nevyžadují.

• Závěr

Návrh tohoto školení v oblasti kybernetické bezpečnosti zaměřený především zvýšení povědomí uživatelů o vlastní bezpečnosti a možných důsledcích rizikového jednání při sdílení informací na sociálních médiích a internetu obecně, byl vypracován na základě bakalářské práce, kde byly zjištěny různé rizikové faktory z odborných pramenů i rozboru reálných případů z minulosti a následně provedena analýza, v níž byly zjištěné rizikové faktory konkretizovány a odstupňovány z hlediska míry rizikovosti. Informace z otevřených zdrojů mají přesah do mnoha specifických oblastí lidské činnosti, nevyjímaje oblast bezpečnosti, zároveň je pravděpodobné, že problematika veřejně dostupných informací ve vztahu k bezpečnosti se v budoucnu stane ještě více aktuální, než je tomu dnes. Tento trend je dán mimo jiné vývojem společnosti, větší poptávkou po informacích a významným rozvojem umělé inteligence.

ZÁVĚR

Práce sledovala dané cíle, kdy stanovení teoretického rámce problematiky informací z veřejně dostupných zdrojů a jejich získávání bylo provedeno prostřednictvím jak zahraniční, tak tuzemské odborné literatury. Poté posouzení, jaké hrozby a rizika jsou z hlediska bezpečnosti spojena s vybranými, v předešlých kapitolách popsány nástroji pro získávání informací z veřejně dostupných zdrojů proběhlo pomocí rozboru reálných případů z minulosti a následné analýzy rizik uskutečněné na základě informací získaných ze zmiňovaného rozboru a výše uvedené odborné literatury. Tato literatura byla zároveň vybrána tak, aby bylo pokryto co nejširší spektrum oblastí lidského úsilí, kde dochází k získávání a využívání informací z otevřených zdrojů a zároveň je zde patrný silný přesah vzhledem k bezpečnosti. A to jak k bezpečnosti samotných uživatelů, tak i k bezpečnosti obecně, v širším kontextu. Konečný návrh vhodných opatření ke snížení zjištěných rizik byl pak zpracován v podobě školení řešícího problematiku ochrany proti zneužití informací získaných z otevřených zdrojů. Celkově byla v této bakalářské práci řešena aktuální problematika získávání informací z otevřených zdrojů, přičemž v teoretické části byla zmíněna související legislativa v podmínkách ČR a následně popsány oblasti lidské činnosti, které jsou silně ovlivněny současným rozmachem technologií a nástrojů pro sběr, zpracování a využití veřejně dostupných informací. Pro získání co možná nejvíce detailního obrazu o roli, významu a současném vývoji technologií a nástrojů pro zpravodajství z otevřených zdrojů bylo využito především zahraniční odborné literatury a vědeckých článků, neboť samotná problematika je více globální než lokální a v rámci českých odborných pramenů se zatím jedná o nepříliš zdokumentované téma. V praktické části práce byly nejprve podrobně rozebrány dva mediálně známé a z hlediska bezpečnosti významné případy zneužití osobních informací zveřejněných na internetu. Poznatky a skutečnosti podnětné ve vztahu k bezpečnosti, získané z těchto dvou případů i odborné literatury byly v následné analýze zasazeny do kontextu různých osob působících napříč spektrem rozličných lidských činností za účelem zjištění možných dopadů v případě zneužití veřejně vystavených osobních informací. Parametry analýzy a její následné vyhodnocení byly koncipovány tak, aby byly pokryty jak rizika konkrétní, tak i ta obecná, komplexnější, vyplývající právě z těchto menších, konkrétních. Nakonec byl na základě možných rizik a hrozeb zjištěných z odborných pramenů i rozbořem reálných případů z minulosti, konkretizovaných a z hlediska míry rizikovosti odstupňovaných provedenou analýzou, vypracován návrh školení v oblasti informační, kybernetické a osobní bezpečnosti zaměřený především na

zvýšení povědomí uživatelů o vlastní bezpečnosti a možných důsledcích rizikového jednání při sdílení informací na sociálních médiích a internetu obecně. Je pravděpodobné, že problematika veřejně dostupných informací ve vztahu k bezpečnosti se v budoucnu stane ještě více aktuální, než je tomu dnes. Tento trend je dán mimo jiné vývojem společnosti, větší poptávkou po informacích a významným rozvojem umělé inteligence.

SEZNAM POUŽITÉ LITERATURY

- BARNETT, Daly. *Doxxing: Tips To Protect Yourself Online & How to Minimize Harm*. Online, blogový příspěvek. December 16, 2020. Dostupné z: Eff.org, <https://www.eff.org/deeplinks/2020/12/doxxing-tips-protect-yourself-online-how-minimize-harm>. [citováno 2025-03-29].
- BAŠTA, Pavel a KOLOUCH, Jan, 2019. *CyberSecurity*. Praha. CZ.NIC. ISBN 978-80-88168-31-7.
- BAZZEL, Michael, 2023. *OSINT Techniques Resources for Uncovering Online Information*. Chicago. Independently Published. ISBN 979-83-6636-040-1.
- BOTWRIGHT, Rob, 2023. *OSINT 101 Handbook*. Pastor Publishing Ltd. ISBN 1839385464.
- CHEN, Qiqi; CHAN, Ko Ling a CHEUNG, Anne Shann Yue, 2018. Doxing Victimization and Emotional Problems among Secondary School Students in Hong Kong. Online. *International Journal of Environmental Research and Public Health*. Vol. 15. Dostupné z: <https://doi.org/10.3390/ijerph15122665>. [citováno 2025-03-04].
- FOSTER, Stephen a CROSS, Jasmine, 2024. Dark doxxing: How Dark Triad traits impact support for doxxing behaviors. Online. *Personality and Individual Differences*. Vol. 217. Dostupné z: <https://doi.org/10.1016/j.paid.2023.112432>. [citováno 2025-03-10].
- FRANCE 24 ENGLISH [@France24_en]. *Dates of French nuclear submarine patrols revealed by crew members on Strava • FRANCE 24 English*. Online, video. 2025-01-14. Dostupné z: YouTube, <https://www.youtube.com/watch?v=MS9JqC8INwU>. [citováno 2025-03-10].
- GELMS, Bridget, 2021. Social Media Research and the Methodological Problem of Harassment: Foregrounding Researcher Safety. Online. *Computers and Composition*. Vol. 59. Dostupné z: <https://doi.org/10.1016/j.compcom.2021.102626>. [citováno 2025-03-05].
- GOOGLE. *Google Products*. Online. Dostupné z: <https://about.google/products/#all-products>. [citováno 2025-03-09].
- HAYES, Darren Richard a CAPPA, Francesco, 2018. Open-source intelligence for risk assessment. Online. *Business Horizons*. Vol. 61, no. 5, s. 689-697. Dostupné z: <https://doi.org/10.1016/j.bushor.2018.02.001>. [citováno 2025-03-02].

INTERNET HISTORIAN [@InternetHistorian]. *Capture the Flag | He Will Not Divide Us*. Online, video. 2017-03-16. Dostupné z: YouTube, <https://www.youtube.com/watch?v=vw9zyxm860Q>. [citováno 2025-03-11].

INTERNET HISTORIAN [@InternetHistorian]. *Liverpool's Closed | He Will Not Divide Us*. Online, video. 2017-03-31. Dostupné z: YouTube, https://www.youtube.com/watch?v=3aZuj_SDqDo. [citováno 2025-03-11].

INTERNET HISTORIAN [@InternetHistorian]. *The Triggering of Shia | He Will Not Divide Us*. Online, video. 2017-02-02. Dostupné z: YouTube, https://www.youtube.com/watch?v=_p4h3jwJob0. [citováno 2025-03-11].

INTERNET HISTORIAN [@InternetHistorian]. *The Walking Divided | He Will Not Divide Us*. Online, video. 2017-08-24. Dostupné z: YouTube, https://www.youtube.com/watch?v=O_ldHq3NzC0. [citováno 2025-03-11].

KHAN, Zafran; KHAN, Zeeshan; LEE, Byung-Geun; KIM, Hong Kook a JEON, Moongu, 2024. Graph neural networks based framework to analyze social media platforms for malicious user detection. Online. *Applied Soft Computing Journal*. Vol. 155. Dostupné z: <https://doi.org/10.1016/j.asoc.2024.111416>. [citováno 2025-03-04].

KHANNA, Parul; ZAVARSKY, Pavol a LINDSKOG, Dále, 2016. Experimental Analysis of Tools Used for Doxing and Proposed New Transforms to Help Organizations Protect against Doxing Attacks. Online. *Procedia Computer Science*. Vol. 94, s. 459–464. Dostupné z: <https://doi.org/10.1016/j.procs.2016.08.071>. [citováno 2025-03-05].

LARSEN, Ole Halvar; NGO, Quoc-Hung a LE-KHAC, Nhien-An, 2023. A quantitative study of the law enforcement in using open source intelligence techniques through undergraduate practical training. Online. *Forensic Science International: Digital Investigation*. Vol. 47. Dostupné z: <https://doi.org/10.1016/j.fsidi.2023.301622>. [citováno 2025-03-02].

LAWRENCE, Tom. *Crew of nuclear submarine gave away their position and patrol schedule 'to Russia' by using Strava fitness app*. Online. In: Daily Mail, 14.01.2025. Dostupné z: <https://www.dailymail.co.uk/news/article-14280163/Crew-nuclear-submarine-position-Russia-Strava.html>. [citováno 2025-03-13].

LE MONDE IN ENGLISH [@LeMondeInEnglish]. *Biden and Trump put in danger by Secret Service agents: #StravaLeaks 2/2*. Online, video. 2024-10-28. Dostupné z: YouTube, <https://www.youtube.com/watch?v=KX7f1PwXEWg>. [citováno 2025-03-12].

LE MONDE IN ENGLISH [@LeMondeInEnglish]. *How Emmanuel Macron can be tracked: #StravaLeaks 1/2*. Online, video. 2024-10-27. Dostupné z: YouTube, <https://www.youtube.com/watch?v=4eQKnV0zsMc>. [citováno 2025-03-11].

LIMONIER, Kevin, 2022. The war in Ukraine, open source investigation and the potential for “digital fieldwork” in geopolitics. Online. *Political Geography*. Vol. 99. Dostupné z: <https://doi.org/10.1016/j.polgeo.2022.102733>. [citováno 2025-03-02].

MARANTZ, Andrew. *Trolls Protest Shia LaBeouf's Anti-Trump Protest Art*. Online. In: The New Yorker, 27.03.2017. Dostupné z: <https://www.newyorker.com/magazine/2017/04/03/trolls-protest-shia-labeoufs-anti-trump-protest-art>. [citováno 2025-03-11].

MONTERRUBIO, Sergio Mauricio Martinez; NOAIN-SÁNCHEZ, Amaya; PERÉZ, Elena Verdú a CRESPO, Rubén González, 2021. Coronavirus fake news detection via MedOSINT check in health care official bulletins with CBR explanation: The way to find the real information source through OSINT, the verifier tool for official journals. Online. *Information Sciences*. Vol. 574, s. 210–237. Dostupné z: <https://doi.org/10.1016/j.ins.2021.05.074>. [citováno 2025-03-10].

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Guide for Conducting Risk Assessments, Information Security. Online. In: *National Institute of Standards and Technology, U.S. Department of Commerce*. 2012, NIST Special Publication 800-30, Appendix G s. G-2. Dostupné z: <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf>. [cit. 2025-04-06].

ROSEN, Joanne D. a RAMIREZ, Joel J., 2022. When doctors are “doxxed:” An analysis of information posted on an antiabortion website. Online. *Contraception*. Vol. 115, s. 1–5. Dostupné z: <https://doi.org/10.1016/j.contraception.2022.07.008>. [citováno 2025-03-04].

ROZO, Andrés Zapata; CAMPO-ARCHBOLD, Alejandra; DÍAZ-LOPÉZ, Daniel; GRAY, Ian; PASTOR-GALINDO, Javier; NESPOLI, Pantaleone; MÁRMOL, Félix Gómez a MCCOY, Damon, 2024. Cyber democracy in the digital age: Characterizing hate networks in the 2022 US midterm elections. Online. *Information Fusion*. Vol. 110. Dostupné z: <https://doi.org/10.1016/j.inffus.2024.102459>. [citováno 2025-03-01].

SEZNAM.CZ. *Mapy.cz pro mobilní zařízení Android a Ios*. Online. Dostupné z: <https://napoveda.seznam.cz/cz/mapy/mapy.cz-pro-mobilni-zarizeni-android-ios/vlastnosti-funkce-aplikace-mapy.cz/>. [citováno 2025-03-09].

SNYDER, Peter; DOERFLER, Periwinkle; KANICH, Chris a MCCOY, Damon, 2017. Fifteen Minutes of Unwanted Fame: Detecting and Characterizing Doxing. Online. *IMC '17: Proceedings of the 2017 Internet Measurement Conference*. s. 432–444. Dostupné z: <https://doi.org/10.1145/3131365.3131385>. [citováno 2025-03-01].

STONE, Haley; HESLOP, David; LIM, Samsung; SARMIENTO, Ines; KUNASEKARAN, Mohana a MACINTYR, Raina, 2023. Open-Source Intelligence for Detection of Radiological Events and Syndromes Following the Invasion of Ukraine in 2022: Observational Study. Online. *JMIR Infodemiology*. Vol. 3. Dostupné z: <https://doi.org/10.2196/39895>. [citováno 2025-03-02].

WILSON, R. Coleen a ZWANG, Kelsey, 2024. Call to Action: Supporting Teams when Cyberbullying and Doxing Occurs a New Form of Workplace Violence. Online. *Nurse Leader*. Vol. 22, no. 5, s. 520-525. Dostupné z: <https://doi.org/10.1016/j.mnl.2024.06.006>. [citováno 2025-03-12].

XU, Hang; BARBOT, Sylvain a WANG, Teng, 2024. Remote sensing through the fog of war: Infrastructure damage and environmental change during the Russian-Ukrainian conflict revealed by open-access data. Online. *Natural Hazards Research*. Vol. 4, s. 1–7. Dostupné z: <https://doi.org/10.1016/j.nhres.2024.01.006>. [citováno 2025-03-12].

YU, Szde, 2023. Cyber profiling: Predicting political orientation with SOCMINT. Online. *Telematics and Informatics Reports*. Vol. 10. Dostupné z: <https://doi.org/10.1016/j.teler.2023.100058>. [citováno 2025-03-09].

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: *Sbírka zákonů*. 23. 7. 2014. ISSN 1211-1244.

ZEGART, Amy, 2023. Open Secrets. New York. *Foreign Affairs*. Vol. 102, no. I, s. 54–70. ISSN 00157120.

ZHOU, Albert E.; RAO, Ishani H.; JAIN, Neelesh P.; GRONBECK, Christian; SLOAN, Brett; GRANT-KELS, Jane M. a FENG, Hao, 2024. Ethics of Doxxing and Cyberbullying in Dermatology. Online. *Clinics in Dermatology*. Vol. 42, s. 730–732. Dostupné z: <https://doi.org/10.1016/j.clindermatol.2024.06.003>. [citováno 2025-03-13].

SEZNAM OBRÁZKŮ

Obrázek 1 Následky protržení hráze přehrady Kachovka	20
---	-----------

SEZNAM TABULEK

Tabulka 1 První část analýzy	53
Tabulka 2 Druhá část analýzy	54
Tabulka 3 Třetí část analýzy.....	55

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AI	Artificial Intelligence	Umělá inteligence
FININT	Financial Intelligence	Zpravodajství z pohybu finančních prostředků
HUMINT	Human Intelligence	Zpravodajství z lidských zdrojů
IMINT	Imagery Intelligence	Obrazové zpravodajství
IP address	Internet Protocol address	IP adresa
MASINT	Measurement and Signature Intelligence	Zpravodajství z měření a příznaků
OSINT	Open Source Intelligence	Zpravodajství z otevřených zdrojů
SIGINT	Signals Intelligence	Signálové zpravodajství
SOCMINT	Social Media Intelligence	Zpravodajství ze sociálních médií
Tor	The Onion Router	Cibulové směrování
VPN	Virtual Private Network	Virtuální privátní síť

SEZNAM PŘÍLOH

Příloha P I: Prezentace – Školení v oblasti informační, kybernetické a osobní bezpečnosti

PŘÍLOHA P I: PREZENTACE – ŠKOLENÍ V OBLASTI INFORMAČNÍ, KYBERNETICKÉ A OSOBNÍ BEZPEČNOSTI

Školení v oblasti informační, kybernetické a osobní bezpečnosti

 Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Vypracoval: Tomáš Holub
Uherské Hradiště

Osnova školení

 Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

- **Úvod**
- **Doporučení pro sociální média**
- **Doporučení pro používání fitness aplikací**
- **Doporučení pro surfování na webu a emailovou komunikaci**
- **Závěr**

Informace z otevřených zdrojů se stávají čím dál více významným fenoménem, který se prolíná všemi oblastmi lidské činnosti. **Ačkoli hlavní těžiště pro získávání informací z veřejně dostupných zdrojů leží v současné době v internetovém prostoru a moderních technologiích, tak samotný princip pro práci s nimi se neomezuje pouze na tyto oblasti a spočívá především v umění hledat souvislosti mezi fakty, co, proč, kdy a jak lidé dělají, nařizují nebo říkají.**



- **Nastavit profil jako soukromý** a udržovat si přehled o tom, kdo může sledovat mé příspěvky, aktivitu a okruh přátel.
- **Při zveřejňování příspěvků brát v potaz, že cokoli je již jednou zveřejněno, tak v podstatě už nelze vzít zpět,** neboť každý, kdo daný příspěvek uvidí si může udělat snímek obrazovky a uložit si informaci pro sebe, čímž autor ztrácí nad svým příspěvkem kontrolu. Dále také komplexní odstranění jednou zveřejněného příspěvku ze všech internetových databází je velmi komplikovaný a zdlouhavý proces.
- **Nezveřejňovat fotografie, ze kterých je přímo patrné místo bydliště nebo důležité detaily týkající se rodiny či práce.** Z hlediska práce v soukromém sektoru se až na výjimky nejedná nutně o skutečnost, kde konkrétně člověk pracuje, což dnes v době rozmachu LinkedInu nebo při podnikání lze jen velmi těžko schovat, ale spíše o fotografie či jiné výstupy z nichž lze získat indicie o bezpečnostní architektuře společnosti nebo hesla k interním systémům apod.



- **Státním zaměstnancům** lze pak doporučit ještě větší míru obezřetnosti při zveřejňování příspěvků na sociálních médiích neboť např. informace o služební činnosti zveřejněné vojáky nebo policisty mohou být velmi lukrativním zbožím pro cizí aktéry a jejich zneužití může mít vážné důsledky.
- **Pravidelně měnit svá hesla na sociálních médiích.** Jedná se o jakousi pojistku, kdyby se někomu podařilo heslo naléznout, uhodnout či jinak získat. Pravidelnou změnou hesel lze snížit šanci, že možný útočník nalezl právě to aktuální, platné heslo. Vhodným posílením bezpečnosti může být také **vícefázové ověření** uživatele při přihlašování.



- **Zveřejňovat fotografie či označení polohy až s časovým odstupem.** Je důležité zmínit, že zveřejňování příspěvků v reálném čase má svá rizika, neboť každý může ihned vědět, kde se autor daného příspěvku v inkriminovaný okamžik nachází. Obecně lze tudíž doporučit zveřejňovat příspěvky z konkrétních míst až s určitým časovým odstupem. Délka časového odstupu se může odvíjet jak od povahy prostředí a době trávené v daném místě tak i od preferencí uživatelů.
- **Při prohlížení sociálních médií je také potřeba přihlížet kriticky k informacím,** fotografiím i videím, pokud nejsou tyto výstupy ověřeny z vícero nezávislých zdrojů a nešířit pochybné zprávy a informace, je tak možné alespoň částečně zabránit řetězovému šíření deepfakes a dezinformací.



- **Používání fitness aplikací se v posledních letech stalo velmi aktuálním trendem**, lidé spolu skrze fitness aplikace a sociální média sdílí své aktivity, porovnávají výkony a podporují se. Zároveň i samotní uživatelé si díky těmto aplikacím drží lepší přehled o svých výkonech. Z hlediska bezpečnosti je nicméně důležité vidět i tu odvrácenou stránku, totiž že **aplikace vedou detailní záznam o tom kde, kdy a s jakou pravidelností se uživatelé pohybují**.
- V první řadě nastavit **možnosti sdílení aktivit na soukromé** a **držet si kontrolu nad tím, kdo všechno může vidět sdílený obsah**.



- **Nepokládat nastavení soukromého profilu za zcela neprůstřelné**, může se vyskytnout **bezpečnostní chyba** v aktualizacích software dané aplikace a tím pádem mohou být údaje o aktivitě a poloze uživatelů **vystaveny nechtěné pozornosti**.
- **Příslušníkům bezpečnostních složek lze doporučit ještě vyšší míru obezřetnosti než ostatním uživatelům**. Neboť detailní informace o vojácích a policistech mohou mít z hlediska bezpečnosti velmi velký význam a jejich zneužití může mít dalekosáhlé následky.
- Při fyzických aktivitách **zapínat trasovací funkce až v určité vzdálenosti od** bydliště nebo práce.



- **Pro bezpečné a anonymní prohlížení** internetu lze doporučit **vhodné nastavení internetového prohlížeče**, popř. instalaci jeho rozšíření za účelem zamezení webovým stránkám v některých monitorovacích aktivitách a omezení funkce vyskakovacích oken.
- **Použití VPN (Virtual Private Network) pro zvýšení anonymity prohlížení** a v konečném důsledku i bezpečnosti. Zde je nicméně důležité upřednostnit kvalitu před cenou, neboť neplacené VPN si často mohou svou „platbu“ vybrat jinde a zneužít buď technické vybavení počítače nebo osobní údaje uživatele. Na trhu zavedení placení poskytovatelé VPN si obvykle drží určité renomé a respektují zákonné, bezpečnostní i etické normy. Platit za služby VPN poskytovatelů je dnes již zpravidla možné hned několika metodami od karetní transakce až po platbu kryptoměnou.



- **Pro ochranu vlastních osobních informací** se také doporučuje **používat větší množství emailových adres** a dbát na **diversifikaci a třídění internetových identit spojených** s danou emailovou adresou. Např. email, který je spojený s bankovní identitou nebude používán pro tvorbu členství v obchodech nebo na seznamkách apod.
- Občas se pro **lepší představu o vlastní internetové aktivitě** může také **hodit vyhledat údaje dostupné o vlastní osobě**. K tomuto účelu lze využít buď klasické vyhledávače (např. Google) nebo některou z vyhledávacích technik (např. dorking – vyhledávací operátory) či některý z vhodných OSINT nástrojů.
- V neposlední řadě je také důležité **věnovat zvýšenou pozornost emailovým zprávám vyžadujícím poskytnutí přihlašovacích údajů (uživatelské jméno, heslo apod.)** k internetovému bankovníctví, popř. jiné elektronické identitě. Často se může jednat o podvod, banky nebo jiné instituce zpravidla takové informace touto cestou nevyžadují.



Návrh tohoto školení v oblasti kybernetické bezpečnosti zaměřený **především zvýšení povědomí uživatelů o vlastní bezpečnosti a možných důsledcích rizikového jednání při sdílení informací na sociálních médiích a internetu obecně**, byl vypracován na základě bakalářské práce, kde byly zjištěny různé rizikové faktory z odborných pramenů i rozboru reálných případů z minulosti a následně provedena analýza, v níž byly zjištěné **rizikové faktory konkretizovány a odstupňovány z hlediska míry rizikovosti**. Informace z otevřených zdrojů mají přesah do mnoha specifických oblastí lidské činnosti, nevyjímaje oblast bezpečnosti, zároveň je pravděpodobné, že problematika veřejně dostupných informací ve vztahu k bezpečnosti se v budoucnu stane ještě více aktuální, než je tomu dnes. Tento trend je dán mimo jiné vývojem společnosti, větší poptávkou po informacích a významným rozvojem umělé inteligence.



Děkuji za pozornost

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Tomáš Holub

Fakulta logistiky a krizového řízení
Ústav ochrany obyvatelstva