POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostně právní

Katedra kriminální policie

Zpravodajství z otevřených zdrojů (OSINT) v oblasti národní bezpečnosti – zdroje, metody, postupy a nástroje

Diplomová práce

Open Source Intelligence (OSINT) in National Security – Sources, Methods, Procedures and Tools

Master thesis

VEDOUCÍ PRÁCE
Ing. Bc. Michálek Luděk Ph.D.

AUTOR PRÁCE
Bc. Radek Pařil

PRAHA
2022

Čestné prohlášení

Prohlašuji, že předložená práce je mým původním autorským dílem, které jsem vypracoval samostatně. Veškerou literaturu a další zdroje, z nichž jsem čerpal v práci, řádně cituji a zdroje jsou uvedeny v seznamu použité literatury.

V Prostějově, dne 20. 8. 2022 _____

Poděkování

Děkuji panu Ing. Bc. Luďku Michálkovi, Ph. D. za odborné vedení, podnětné připomínky a cenné rady při zpracování mé diplomové práce.

ANOTACE

Tato diplomová práce se zabývá zpravodajstvím z otevřených zdrojů (OSINT) v oblasti národní bezpečnosti a zdrojích, metodách, nástrojích a postupech souvisejících se zpravodajstvím z otevřených zdrojů. Pozornost byla při vypracování zaměřena na zpravodajství z otevřených zdrojů ve virtuálním internetovém prostředí a možnosti využití používaných nástrojů pro shromažďování dat a analýzu informací. Hlavní částí práce je případová studie současného konfliktu na Ukrajině z hlediska zpravodajství z otevřených zdrojů. Ta analyzuje aspekty a specifika zpravodajství na ruské a ukrajinské straně a možnosti využití rozličných zdrojů, nástrojů a metod z hlediska národní bezpečnosti.

KLÍČOVÁ SLOVA

diplomová práce * zpravodajství z otevřených zdrojů * národní bezpečnost * OSINT nástroje a metody * sociální sítě * rusko-ukrajinský konflikt *

ANNOTATION

This master’s thesis is focused on Open Source Intelligence (OSINT) and its sources, methods, tools, and procedures in the context of national security. The focus is dedicated towards OSINT in the virtual Internet environment, social media, and the capabilities of certain tools for data collection and information analysis. The main chapter of the thesis is a case study of the current conflict in Ukraine from the OSINT point of view. This chapter analyzes the aspects and specifics of intelligence collection on the Russian and Ukrainian side and the possibilities of using various sources, tools, and methods from the national security point of view.

KEYWORDS

master thesis * open-source intelligence * national security * zpravodajské nástroje * OSINT tools and methods * social media * Russo-Ukrainian conflict *

Obsah

Úvod

Tato práce se zabývá jedním z druhů zpravodajských metod, který je v současné době zásadní pro činnost mnoha organizací a státních institucí po celém světě. Tématika a problematika diplomové práce je zaměřena zpravodajství z otevřených zdrojů (OSINT) v oblasti národní bezpečnosti. Přesněji je zaměřena na její zdroje, nástroje a metody, které se pro zpravodajství z otevřených zdrojů využívá. Zdroje, jakožto místa, ať už virtuální nebo hmotné, ze kterých je možno informace čerpat. Poté nástroje, které jsou v dnešní době ve zpravodajství z otevřených zdrojů charakteristické v elektronické podobě a mohou zrychlit zpravodajský proces a rozšířit sféru znalostí o hrozbách proti národní bezpečnosti. A metody zpravodajství z otevřených zdrojů, které je možné použít univerzálně v obdobných analýzách.

Téma je to důležité a aktuální, protože hrozby proti národní bezpečnosti státu mohou být, díky zpravodajství z otevřených zdrojů, lépe předvídatelné. Mohou být sledovány a může se na základě zpravodajství predikovat další vývoj zkoumané problematiky. Problematikou je na mysli jakákoliv činnost nebo událost způsobená osobou, organizací nebo státem, která svými aktivitami ohrožuje jinou osobu, organizaci nebo stát. Proto je, nejen pro státní orgány, nezbytné se zpravodajstvím z otevřených zdrojů zabývat.

Motivací pro výběr tohoto tématu práce je moje vůle se v budoucnu podílet na boji s trestnou činností a dalším hrozbám proti zájmům České republiky. Také můj zájem prohloubit své znalosti o nástrojích zpravodajské analýzy. Současně se v praktické části zabývám aspekty informační války, mezinárodních vztahů a konfliktů, což jsou témata, o které se aktivně zajímám.

V jednotlivých kapitolách diplomové práce je rozpracován systém zpravodajství z otevřených zdrojů, primárně zaměřený na získávání dat z elektronických zdrojů a jejich zpracování. V první části se práce zabývá základními pojmy týkající se zpravodajství a národní bezpečnosti. Jednotlivě se jedná o pojmy jako data, informace, znalost, zpravodajský cyklus, zpravodajství

a národní bezpečnost. V pojmu zpravodajství jsou stručně zmíněny i další druhy zpravodajských metod. Dále se práce bude zabývat samotným zpravodajstvím z otevřených zdrojů; výhodami a výzvami spojenými s touto metodou zpravodajství. Poté je práce zaměřena na vyhledávání dat a informací na sociálních sítích, Deep Webu a Dark Webu a na jejich zdroje a nástroje, které lze na těchto platformách použít. Použití nástrojů a jejich možnosti jsou následně doplněny návrhy a doporučeními, které mohou přispět k úspěšnému průběhu analýzy. Poslední praktická část je zaměřena na kvalitativní analýzu zdrojů, metod a nástrojů zpravodajství z otevřených zdrojů týkající se aktuální situace stále probíhajícího konfliktu na Ukrajině.

1 Vymezení základních pojmů

Tato kapitola se zaměří na vymezení základních pojmů týkající se tématiky dat, informací, zpravodajství a národní bezpečnosti.

1.1 Data

Data se ve své nejjednodušší podobě sestávají z nezpracovaných alfanumerických hodnot. Jedná se o čísla, text, symboly, obrázky, zvukové nahrávky atp. Tyto nezpracované alfanumerické hodnoty mohou být získány mnohými rozličnými metodami. Jsou získávány z měření nebo z dolování dat z textu, obrázků, zvukových nahrávek, výsledků průzkumů či simulací. Data jsou kvantitativní nebo kvalitativní hodnoty proměnných, jež lze obvykle sestavit do tabulek a zobrazit v grafech či obrazcích.

V podstatě se data skládají ze záznamů transakcí nebo událostí, které se vytváří, aby zprostředkovali jistou výměnu mezi lidmi, nebo například počítačovými nebo jinak automatizovanými systémy. Data jako taková nemají význam, pokud člověk nerozumí kontextu, ve kterém byla data shromážděna. Jako taková, jsou data nezpracovaná, jsou objektivní a dají se kvantifikovat. V některých případech se může stát, že je dat velké množství, a tak může být složitější relevantní data nalézt a identifikovat.

Pro primární nezpracovaná data se pro přesnější definování užívá termín "*raw data*" (*surová data*). S tím že termín "*data*" se užívá pro data, která již byla vyfiltrována, strukturována nebo vizualizována, stále však nebyla zpracována natolik, aby mohla být nazývána informací.

Při zpracovávání dat se lze setkat s termínem "*metadata*", což jsou data o datech. Metadata obsahují informace, znaky, kterými se jednotlivá data vyznačují, a tak usnadňuje jejich vyhledávání a správu. Jednoduchý příklad metadat pro dokument může zahrnovat informace, jako je autor, velikost souboru, datum vytvoření dokumentu a klíčová slova popisující dokument. „*Metadata představují informace o datech, které se používají všude, v každém*

odvětví. Jsou všudypřítomné v informačních systémech, na sociálních sítích, webových stránkách, softwarech, hudebních službách a e-shopech. Metadata lze manuálně vyhledat a vybrat si určitá data, která potřebujeme, avšak lze je generovat a také vyhledávat automaticky.“[1]

1.2 Informace

Informace jsou produkovány, když jsou data zpracovávána, organizována nebo strukturována tak, aby poskytovala kontext, význam a vhled na analyzované téma. Informace mohou být chápany jako údaj o reálném prostředí, o jeho stavu a procesech v něm probíhajících. Informace jsou ve své podstatě zpracovaná data. Informace, stejně jako data, bývají přenášeny prostřednictvím symbolů; čísel, textu, obrázků, zvukových a audiovizuálních nahrávek atp. Informace proto přicházejí v různých formách, jako jsou spisy, články, prohlášení, statistiky, diagramy nebo tabulky. Informace mohou být subjektivní či objektivní. Měli by být relevantní k analýze, vypovídající o kontextu problematiky.

1.3 Zpravodajský cyklus

Zpravodajský cyklus je základním procesem při vypracovávání zpravodajské analýzy. Vzhledem k tomu, že je zpravodajská analýza systematický proces, tak je zpravodajský cyklus rozdělen do několika částí. Na základě dat ze kterých zpravodajství čerpá je nutné stanovit určitý model či metodu zpravodajského cyklu, díky kterému bude zpravodajská analýza co nejpřesnější a nejefektivnější.[2]

Existují čtyři hlavní fáze tradičního zpravodajského cyklu. První fází je určení zaměření analýzy a plánování jakým způsobem by mohla být uskutečněna. Což je určeno dle požadavků státních institucí, ale i vlastní činností v souladu s prioritami národní bezpečnosti. V druhé fázi poté zpravodajci

---

[1] CHAPPLE, Mike. *What Is Metadata?* [online]. [cit. 2022-04-16]. Dostupné z: https://www.thoughtco.com/metadata-definition-and-examples-1019177

[2] MCDOWELL, Don. *Strategic Intelligence: A Handbook for Practitioners, Managers, and Users* [online]. Revised. Scarecrow Press, 2009, s.17-21.

shromažďují data a informace ze skrytých i otevřených zdrojů pomocí různých zpravodajských metod.

Ve třetí fázi jsou tato informace zpracovány a transformovány analýzou relevantních informací, které se poté stávají zpravodajskou informací. V poslední fázi je tato zpravodajská informace zapracována do zpravodajského výstupu a zahrnuje zveřejňování výstupů oprávněným adresátům. V této poslední fázi mohou adresáti zhodnotit výstup a určit nové požadavky pro další postup. Tímhle způsobem se zpravodajský cyklus opakuje stále dokola. Podle různých teorií má postup zpravodajského cyklu více kroků s podrobnějším rozdělením, ale principiálně je shodný se zmíněnou základní verzi zpravodajského cyklu.

1.3.1 Zpravodajská informace

Zpravodajská informace je znalost, která slouží pro účely zpravodajské činnosti. Tato zpravodajská informace by měla být relevantní a odpovídat realitě, jelikož se podle ní mohou modifikovat budoucí kroky zpravodajské činnosti v určité problematice a predikovat další vývoj. To je hlavní rozdíl mezi obecnou informací a zpravodajskou informací.

Pokud je určitá stěžejní zpravodajská informace z nějakého důvodu zkreslená či neodpovídá reálnému stavu věci, tak to zcela negativně ovlivní další zpravodajskou činnost, což může mít negativní vliv také na důležitá rozhodnutí zpravodajské služby a dalších státních institucí.

1.3.2 Znalost

Znalosti jsou jedinečné pro každého jednotlivce a jsou výsledek všeho zkušeností a učení, pomocí kterých interpretujeme informace a přiřazujeme jim význam. Aby znalosti měli svůj význam, tak je jedinec musí využít a poté na základě něj realizovat svá rozhodnutí. K vytvoření použitelných zpravodajských informací, které mohou mít dopad na naše rozhodování, jsou zapotřebí relevantní informace, které bývají zpracovány z dat. Znalost se dá také

chápat z hlediska organizace a jejich nashromážděných zpracovaných informací a další evidence.

Informace se stávají individuální znalostí, když je osoba přijímá a uchovává v paměti jako formu pochopení informací, které ovlivňuje jeho osobní interpretaci reality. Velmi důležitou částí zpravodajského cyklu je následné porozumění nabyté znalosti a její následné vhodné využívání například v rámci dalších zpravodajských analýz.

Se znalostí je přímo spojen pojem *moudrost*, což je spojení informací a znalostí, jimiž je rozhodnutí podloženo. A také minulých zkušeností, které umožnily plné chápání situace a probíhajících dějů, na nichž může být rozhodnutí učiněno.[3]

1.4 Zpravodajství

Pojem zpravodajství má sám o sobě má různé významy, záleží na kontextu se kterým je tento pojem spojen. Význam, který je relevantní pro tuto práci, je zpravodajství jako činnost, kterou vykonávají zpravodajské služby a další bezpečnostní složky v jednotlivých státech na celém světě. Jejich úkolem je získávat, shromažďovat a vyhodnocovat informace důležité pro konkrétní bezpečnostní složky a zájmy států, jakožto hlavnímu subjektu, kterému jsou odpovědné. Zpravodajství je nenahraditelné pro vnitřní i vnější bezpečnost států, což zahrnuje kontrarozvědnou a rozvědnou činnost zpravodajských služeb.

V češtině je tento pojem spojen taktéž s činností médií a novinářskou prací. Zpravodajství je v tomto smyslu sdruženo s oblastí žurnalistiky a je uskutečňováno prostřednictvím novinových, rozhlasových, internetových nebo televizních zpráv.

[3] MCDOWELL, Don. *Strategic Intelligence: A Handbook for Practitioners, Managers, and Users* [online]. Revised. Scarecrow Press, 2009, s.11-13.

Avšak zpravodajství jako takové může být plnohodnotně uskutečněno i osobami, které nejsou nijak zaměstnány v rámci bezpečnostních složek. To platí pro mnoho druhů zpravodajské činnosti a pro zpravodajství z otevřených zdrojů to platí dvojnásob. Proto je z tohoto pohledu univerzálnější definice tohoto pojmu, která hovoří o zpravodajství jako „*záměrné lidské činnosti, která spočívá v utajovaném získávání a zpracovávání cizích utajených informací.“*[4] Pojem tedy odkazuje na celý proces zpravodajské analýzy od získání surových, nezpracovaných dat až po finální produkt analytického procesu.

Tento význam je přímo spojen s anglickým pojmem “**intelligence**“. Pojem “intelligence“ se kterým je možné se nezřídka setkat v zahraniční literatuře má krom zmíněného významu, další kontextuální nuanci. Odkazuje na celkový výsledek nebo výstup analýzy, jež je vytvořena osobami, kteří na ní pracují. Jinými slovy znamená, že všechny informace obsažené v těchto zprávách byly přezkoumány a vyhodnoceny a jsou přesné a kredibilní. Pro tyto závěrečné výstupy se využívá i zkrácený výraz “intel“, a to zejména z důvodu diferenciace výrazu vůči jiným významům slova “intelligence“ v rámci konkrétní verbální či písemné komunikace.

Zpravodajství zahrnuje použití specializovaných metod a procesů pro shromažďování informací a jejich následné zpracování. U zpracovávání informace poté záleží případ od případu, kdy je nutné informaci nějak dále standardizovat do zamýšlené podoby; informaci komprimovat nebo ji například přeložit, aby byla dále použitelná pro další kroky analýzy.

Po vypracování závěrečných výstupů, zpravodajské služby dále předkládají výsledky svojí práce vládám jednotlivých zemí a dalším státním orgánům, politickým i apolitickým. Ty působí v oblastech relevantních pro určitý zpravodajský výstup, mohou s ním dále pracovat a řídit se jeho doporučeními a predikcemi. Mohou například podniknout konkrétní opatření vůči ohrožení zájmů státu, která by měla být ve výstupu dostatečně odůvodněna. Také mohou

[4] ZEMAN, Petr. *Co je zpravodajství* [online]. [cit. 2022-05-02]. Dostupné z: https://www.absd.sk/co_je_zpravodajstvi#_ftn3

poskytnout zpravodajcům zpětnou vazbu, informovat je o dalším vývoji, o překážkách, praktické nemožnosti určitých kroků atp. [5]

Některé orgány mohou dávat požadavky na další zpravodajské informace a analýzy v určitých otázkách. Všeobecně však u zpravodajských služeb platí pravidlo embarga na poskytování tajných informací, které by mohlo mít za následek ohrožení činnosti zpravodajských služeb a vyzrazení citlivých informací nepovolaným osobám, a to i v případě státních orgánů s privilegiem na obdržení zjištěných informací zpravodajskou službou.

V České republice je toto pravidlo zasazeno v podobě zákona i do právního řádu. *„Zpravodajské služby předávají státním orgánům a policejním orgánům informace o zjištěních, která náleží do oboru jejich působnosti; to neplatí, jestliže by poskytnutí ohrozilo důležitý zájem sledovaný příslušnou zpravodajskou službou.“*[6] Státní orgány, jakožto adresáti zpravodajských informací spoléhají na zpravodajské informace, tyto informace dokáží ujasnit v té době relevantní problematiku a pochopení komplexnějších mezinárodních otázek.

Přitom je třeba brát na vědomí, že bezpečnostní složky nebývají jediným zdrojem informací pro státní orgány a jejich závěry nemusí nutně rozhodovat o tom, jakým způsobem musí tyto orgány postupovat. Zpravodajci nejsou přímou součástí politických rozhodnutí a změn, ale mnohdy musí poskytovat informace a analýzy, které komplikují nebo rozdmýchávají otázky o rozhodnutích nebo krocích administrativy. Což vždy nemusí přinést pořádek do řízení státních záležitostí.

Vztahy mezi zpravodajskými službami a státními orgány či různými politickými subjekty jsou v mnohých zemích často dlouhodobě nekonzistentní. Jsou ovlivněny nedůvěrou z obou stran, částečně kvůli špatnému pochopení předaných informací. Také kvůli různým zásadám jejich povolání, na kterých

[5] DNI. WHAT IS INTELLIGENCE? Office of the Director of National Intelligence [online]. [cit. 2021-12-01]. https://www.dni.gov/index.php/what-we-do/what-is-intelligence
[6] §8 odst.3 zákona 153/1994 Sb., o zpravodajských službách České republiky

jsou založeny. Nebo na vztahy působí osobní animozity mezi jednotlivými osobami z minulosti, které mohou být racionálně vysvětlitelné nebo ne.

Ochota dohody, pochopení vzájemných rolích a odpovědnosti vůči prosperitě státu a služba občanům země, musí být v rámci tohoto vztahu rozhodující a nadřazená jiným osobním nevraživostem. Přičemž ke vztahu, který je co nejbližší určité symbióze mezi těmito subjekty vede dlouhodobá komunikace, která se může stát předmětem, ale i řešením mnoha sporů.

I přes různé konflikty a malichernosti však nesmí být tento vztah patologický pro činnost a funkčnost státu. Tím je na mysli například ignorace upozornění zpravodajských služeb na hrozby, které by mohly ohrozit zájmy státu, pokud vztahy nejsou na dobré úrovni nebo se zpravodajský výstup a jeho predikce neshoduje s politickými idejemi osob ve státních orgánech a jejich plánem státní politiky. [7]

1.4.1 Druhy zpravodajství

Mezi nejvyužívanější druhy zpravodajství patří SIGINT, HUMINT a OSINT. V případě SIGINT jsou data shromažďována technickými systémy zahrnujícími pozemní elektronické systémy a letecké platformy nebo satelity na oběžné dráze Země, které shromažďují elektronické signály a snímky pomocí rozličných technologií. Tyto systémy dokáží získat velké množství relevantních informací, které mohou být následně využity k další analýze.

SIGINT je dále rozdělen do dalších specifičtějších kategorií. Tzv. COMINT zahrnuje všechny signály produkované telekomunikačními systémy, jako jsou telefony, internetové datové toky nebo rádia. COMINT je zvláště užitečný pro sledování a záznam komunikace mezi určitými subjekty, jejichž činnost poutá zájem státních orgánů. Mohou to být osoby páchající trestnou činnost,

[7] GEORGE, Roger Z. *Intelligence in the National Security Enterprise: An Introduction*. USA: Georgetown University Press, 2020, s. 7-8.

nebezpečné osoby, zločinecké a teroristické skupiny či cizí agenti a jiné zahraniční subjekty.[8]

Dále se v podmnožině SIGINT nachází ELINT, kterými se zpravodajské služby zaměřují například na signály vycházejícími z radarů a dalších elektronických vojenských systémů. Pokud je sběr informací pomocí ELINT úspěšný, tak může zvláště pomoci při předvídání konkrétních vojenských operací nebo expanzi dosavadních znalostí o nepřátelské technice a jejich možnostech a potenciálu.

V poslední řadě pod SIGINT patří FISINT neboli signálové zpravodajství týkající se přístrojové komunikace. Je to zpravodajství, které pracuje s elektronickými signály, které vysílají objekty při vojenských či vědeckých testech. Jde například o telemetrická data z raketových a leteckých testů, ale i dalších povrchových a podpovrchových systémů.[9]

Co se týče metod HUMINT, jsou informace shromažďovány prostřednictvím skrytých nebo zjevných metod, primárně spojených se záměrnou operativní lidskou činností. Prostředkem využívaným v rámci HUMINT jsou například agenti, informátoři či osoby v rámci velvyslanectví a jiných diplomatických misí. Zde je cílem porozumět aktivitám, ale také předvídat záměry např. organizovaných zločineckých skupin, extremistických organizací, zahraničních vládních úředníků nebo jiných nestátních aktérů, a to uvnitř i vně území vlastního státu. Tato metoda je také velmi účinná například při shromažďování informací z nepřístupných a izolovaných oblastí, které jsou v rukou protivníka. Od zdrojů jako jsou emigranti, uprchlíci či váleční zajatci.[10]

---

[8] GEORGE, Roger Z. *Intelligence in the National Security Enterprise: An Introduction*. USA: Georgetown University Press, 2020, s. 12.
[9] GEORGE, Roger Z. *Intelligence in the National Security Enterprise: An Introduction*. USA: Georgetown University Press, 2020, s. 12-13.
[10] GOLDSTEIN, Frank L. *Psychological Operations: Principles and Case Studies.* Maxwell Airforce Base, Alabama: Air University, Press, 1996, s. 203-205.

Další, pro tuto práci zásadní formou shromažďování zpravodajských informací je zpravodajství z otevřených zdrojů (OSINT). Tato metoda je, jakožto hlavní téma této práce společně se SOCMINT, podrobněji popsána v následujících kapitolách.

Existují i další druhy zpravodajství specializovaného zaměření. Například IMINT, který je získáván z pozemních, leteckých a vesmírných snímacích systémů využívající fotografii, elektrooptiku, radary nebo infračervené senzory. Jde například o obrázky mapující protivzdušnou obranu protivníka, obrázky příprav na bojové a jiné vojenské operace nebo fotodokumentace korupčního jednání nebo distribuce nelegálních drog a jejich analýza.[11]

GEOINT je odvozena ze snímků a dalších geoprostorových informací, které využívají fyzickou geografii, vlastnosti a dynamiku povrchu Země. Může se jednat například o určování geolokace skrytých obranných zařízení, údaje potřebné k přesnému zaměření cíle pro bezpilotní letecké prostředky nebo fyzicko-geografické a environmentální změny po přírodních katastrofách.[12]

1.5 Národní bezpečnost

Národní bezpečnost může být definována jako souhrn schopností země nebo národa, předvídat a překonávat různorodé hrozby, které by mohly ohrozit zájmy země. S tím souvisí v prvé řadě zabezpečení samotného přežití národního státu, vyvážená a cílevědomá aktivita vlády země a využívání všech nástrojů státní politiky proti rozličným hrozbám, které mohou pozitivně ovlivnit další vývoj a relativní stabilitu a bezpečnost země, a to vše v co největší prospěch a obecnou spokojenost svého lidu. Maximalizace národní bezpečnosti je považován za cíl národní správy.

---

[11] GEORGE, Roger Z. *Intelligence in the National Security Enterprise: An Introduction*. USA: Georgetown University Press, 2020, s. 12-13.
[12] GEOINT – Geospatial Intelligence. Heavy.ai [online]. [cit. 2022-05-05]. Dostupné z: https://www.heavy.ai/technical-glossary/geoint

„Úkolem států je v příslušném rozsahu zajišťovat bezpečnost obyvatel, obranu svrchovanosti a územní celistvosti země a zachování náležitostí právního státu. Institucionálním nástrojem pro dosažení těchto cílů je komplexní a funkční bezpečnostní systém, který se průběžně přizpůsobuje aktuální bezpečnostní situaci.“[13]

Každý stát má svá specifická silná a slabá místa v různých oblastech v závislosti na mnoha a mnoha faktorech, kterými může být národní bezpečnost ovlivňována. Tyto faktory jsou zmíněny konkrétněji níže v této kapitole. Obecně se dá říct, že ochrana stavu národní bezpečnosti ve vztahu ke každému tomto faktoru může být, zaprvé, nedostatečná nebo nízká.

To znamená, že je třeba udělat kroky, které minimálně zmírní přímé ohrožení národní bezpečnosti, jež by mohla negativně ovlivnit chod státu. Pokud nutné kroky nemohou být z různých důvodů uskutečněny nebo se hrozby ignorují, může být národní bezpečnost ohrožena.

Zadruhé, lze hovořit o dostatečném či vyváženém stavu ochrany národní bezpečnosti v určité oblasti. A to, pokud jsou učiněna jistá opatření, která minimalizují možnou hrozbu a její následky a ve stejnou chvíli se tato hrozba může jevit jako méně pravděpodobná. Avšak pokud by k ohrožení došlo, existují krizové plány a další opatření, které mohou na ohrožení reagovat a alespoň minimalizovat možné negativní důsledky vůči stavu národní bezpečnosti.

Zatřetí, lze hovořit o velmi dobré nebo vysoké úrovni ochrany. Ta je zapříčiněna buďto nízkým stupněm hrozby ve srovnání s komplexnějšími opatřeními konkrétního státu, ale také prioritizací a předimenzování systému opatření vůči určité reálnější hrozbě, jejíž riziko ohrožení je tím limitováno na minimum a bylo by velmi složité či nákladné tyto opatření obejít nebo jinak překonat.

---

[13] *Bezpečnostní strategie ČR*. Praha: Ministerstvo zahraničních věcí České republiky, 2015. [cit. 2022-05-06].Dostupné z: https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf

Podobně se dají naopak hodnotit i samotné hrozby. Hrozba může být obecně zhodnocena ke každému státnímu či národnímu subjektu jako vysoká, střední nebo nízká, jako je tomu například v českém Auditu národní bezpečnosti. Taková zhodnocení rizik vypracovává každá země, jejichž existence, integrita či životy občanů země mohou být reálně ohroženy vnějšími, nebo vnitřními vlivy.[14]

Na základě toho bývají vypracovávána konkrétní opatření, krizové plány a bezpečnostní strategie. Tyto preventivní metody mohou, ve velké míře eliminovat hrozby vůči národní bezpečnosti. Každý stát by měl, v závislosti na svém postavení ve světě, zanalyzovat prostředí z hlediska národní bezpečnosti, aby vytvořil konkrétní bezpečností strategie a plány. Za tímto účelem musí zvážit všechny různé faktory, aby odhadl, jakým způsobem se může situace nadále vyvíjet, a jaký systém a politiku bude muset nastavit, aby mohl překonat hrozby vůči národní bezpečnosti.

Proces tvorby strategie je velmi podobný jakémukoliv jinému procesu, který má za cíl implementovat určitý koncept a zjistit zda může být funkční a efektivní. V prvé řadě je nutné posoudit a odhadnout další vývoj uvnitř státu a ve světě. Poté následuje celkové začlenění posouzení do strategií s ohledem na všechny relevantní prvky národní bezpečnosti. [15]

Tento krok následuje implementace konkrétních opatření. Všechna opatření musí být následně v průběhu času opakovaně revidována, zda jsou stále účinná, finanční náklady odpovídají nebezpečí hrozeb nebo, jestli hrozba pozbyla významnosti a opatření nemusí být nutně dále ponechávána v pohotovosti.

---

[14] *Audit národní bezpečnosti* [online]. Praha: Ministerstvo vnitra ČR, 2016 [cit. 2022-05-05]. Dostupné z: https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf

[15] PALERI, Prabhakaran. Revisiting National Security: Prospecting Governance for Human Well-Being. Singapur: Springer, 2022, s. 54-57.

Národní bezpečnost a její strategie se musí zaměřit na zabezpečení mnoha různých faktorů důležitých pro chod státu. Níže jsou ty nejdůležitější faktory obecně popsány a je uvedeno čeho činnost státu v těchto oblastech zhruba týká.

1. *Ekonomická bezpečnost* – zajištění zvyšování ekonomické síly a prosperity státu s dlouhodobě udržitelným rozpočtem odpovídajícím ekonomickým možnostem státu, hradící své závazky a udržující v chodu veškerou správu věcí veřejných; to vše aniž by byl stát co nejméně ekonomicky ovládán jinými státy a subjekty
2. *Vojenská bezpečnost* – zajištění schopnosti státu bránit se a chránit svoji suverenitu vůči agresorovi s pomocí vojenských a jiných ozbrojených složek; bojeschopnost armádních sil v případě ohrožení zájmů státu, v případě válečného konfliktu
3. *Státní hranice* – stanovení státních hranic a jejich fyzická obrana a ochrana před vnějšími nevyžádanými a škodlivými vlivy; kontrola osob vstupujících a opouštějících území státu, zamezení pašování zboží a osob
4. *Suroviny a další klíčové zdroje* – zajištění udržitelného příjmu surovin klíčových pro stát a jeho průmysl, také pro uspokojení základních potřeb občanů a dalších obyvatel na území státu; vše, co se týče povrchu území státu i jeho podzemí; vzduchu a jeho kvality, vody, jídla a jejich zdrojů a kvality; kovy a nerosty; suroviny nutné k výrobě elektrické energie
5. *Demografie* – starat se o obyvatelstvo státu, uzpůsobovat jejich schopnosti tomu, co stát potřebuje; investovat do obyvatelstva s maximální návratností v budoucnu; efektivně korigovat migraci lidí, příchozí i odchozí; nepřímo ovlivňovat přírůstek obyvatelstva
6. *Přírodní a jiné katastrofy* – schopnost státu co nejlépe předcházet katastrofám (přírodní, způsobené člověkem, hybridní) a zmírňovat škody na životech, majetku a životním prostředí z nich plynoucí; pomoc postiženým s vyrovnáním se se škodami, systémy a výzkum pro lepší předvídání přírodních katastrof, pravidla pro nakládání s nebezpečnými látkami, aktivní uklidňování vztahů mezi etniky s napjatými vztahy
7. *Energetika* – využívání a udržitelné zacházení s energetickými zdroji pro maximalizaci uspokojení obyvatelstva a prospěchu dalších státních zájmů; investice do výroby energie z obnovitelných či neobnovitelných zdrojů,

zabezpečení systémů před výpadky výroby a nemožnosti generování a následného dodání energie

8. *Geostrategie* – optimální zvážení veškerých geostrategických otázek státu v kontextu celého světa a regionu ve kterém se stát nachází; budování vztahů a diplomacie s ostatními státy, aktivní účast v mezinárodních organizacích, ucházení se o členství v organizacích

9. *Kybernetika* – schopnost státu plně kontrolovat svůj kybernetickým prostorem, správa státních záležitostí a věcí veřejných elektronicky; ochrana dat, informací a vnitřních strategických systémů, které by potenciálně mohly ohrozit státní bezpečnost

10. *Informace* – schopnost státu získávat, shromažďovat data a zpracovávat informace o relevantních otázkách ve věcech národní bezpečnosti a dalších státních aktivit; ochrana informací stěžejních pro fungování státu, ochrana veřejnosti před záměrně šířenými dezinformacemi, informační/psychologická válka s jinou zemí z důvodu státního zájmu

11. *Zdraví* – ochrana a udržování zdravého fyzického a psychického zdraví obyvatelstva, zmírňování dopadů nezdravého životního stylu; iniciace kroků a podpora projektů vedoucích k normalizaci návyků zdravého životního stylu u veřejnosti, psychologická pomoc na školách, psychiatrická pomoc pro osoby s psychickými poruchami, cílené dodávky potřebných léků do chudých oblastí.

12. *Životní prostředí* – udržovat životní prostředí na svém území pod ochranou, předcházet omezovat znečištění životního prostředí na minimum; snižování emisí skleníkových plynů, recyklace a nakládání s odpady, opatření proti znečišťování vod oceánů a řek[16]

Důsledky politiky národní bezpečnosti závisí na vytvořeném vnímání konceptu, na němž je tato politika založena, a na směru, kterým se stát či národ ubírá. Aplikace opatření na ochranu národní bezpečnosti bývá založena na národních potřebách a zájmech, které stát a jeho vláda vnímá jako důležité. Tím pádem hodně záleží na současné politické situaci v zemi a celkovém státním zřízení.

[16] PALERI, Prabhakaran. Revisiting National Security: Prospecting Governance for Human Well-Being. Singapur: Springer, 2022.

V závislosti na akcích vlád se opatření mohou soustředit na mnoho otázek. Na maximalizaci vlastní politické moci, otázky nástupnictví, opatření směřující k udržení vlastní moci, ovlivnění existence politického prostředí, anexi nebo faktickou kontrolu jiných území, posílení vojenské moci a jakýkoli další cíl, o kterém rozhoduje ten, kdo má moc. Což vždy nemusí být příznivé pro obyvatelstvo samotné, ale z pohledu vlády se může jednat o potřebný krok, nebo krok, který je v souladu s povahou státního zřízení.[17]

[17] PALERI, Prabhakaran. Revisiting National Security: Prospecting Governance for Human Well-Being. Singapur: Springer, 2022, s.353-355.

2 Zpravodajství z otevřených zdrojů

Zpravodajství z otevřených zdrojů (Open Source Intelligence) je oblast zpravodajství zabývající se shromažďováním, zpracováním a analyzováním údajů a informací z volně dostupných zdrojů. Zpravodajství z otevřených zdrojů je, při užití efektivních metod, relativně levná a rychlá forma zisku informací, která přímo neohrožuje život zpravodajců a přidává na hodnotě celému zpravodajskému cyklu. Vysoká důležitost zpravodajství z otevřených zdrojů pro činnost zpravodajských služeb na celém světě je v dnešní době již nevyvratitelná.

V minulosti se získávání informací z otevřených zdrojů týkalo pouze tzv. *klasických zdrojů* – novin, časopisů, knih, brožur, studií. Později přibyl netištěný druh klasických otevřených zdrojů, a to rozhlasové a televizního vysílání. Dále je možno využít tzv. šedé literatury – oficiálních zpráv a dokumentů státních institucí a mezinárodních organizací, vědecké a akademické práce atp. Zpravodajství z těchto zdrojů je nadále velmi důležité.

V rámci zpravodajství z otevřených zdrojů jsou v posledních dekádách běžně vytěžovány informační zdroje jako jsou například sociální sítě, blogy a diskusní fóra. Tyto tzv. *nová média* mohou poskytnout velmi aktuální a cenné údaje a informace. V posledních dekádách v rámci tohoto modernějšího druhu zpravodajství z otevřených zdrojů přibývá obrovské množství informací na internetu (Surface web, Deep web, Dark web), a tak je tomuto typu zpravodajství věnována čím dál větší pozornost.[18]

Zpravodajství z otevřených zdrojů však nezahrnuje pouze obvyklé komerčně dostupné tištěné a elektronické sdělovací prostředky, ale i mnoho různých metod a méně známých postupů. Z nich lze snazší cestou nalézt data, která potřebujeme a mohou objevit i taková data, o nichž často předem ani netušíme a nebylo by ani možné je bez jejich pomoci nalézt. Velký pokrok

[18] GIBSON, Stevyn D. , *Open Source Intelligence a contemporary intelligence lifeline,* PhD Thesis, Cranfield University, Defence College of Management and Technology, 2007, s.33.

v informačních technologiích způsobuje, že jsou otevřené zdroje čím dál více přístupné a diverzifikované, takže má veškerá zpravodajská činnost tendenci být stále více založená na analýze informací získaných z otevřených zdrojů a na využití akademických nebo soukromých specialistů. Zpravodajství je tak stále více základem činnosti při analýze informací získaných z otevřených zdrojů a na využití společenských akademických/soukromých specialistů. Odhaduje se, že data z otevřeného zdroje mohou představovat až 80–90 % veškerého zpravodajství týkající se obecně zpravodajské analýzy. [19]

Rozvoj nových otevřených zdrojů – internetu, konkrétně sociálních médií, napomohl ke komunikaci mezi různými kulturami a národy. Toto virtuální sbližování a sdílení dat každým člověkem využívajícím internet otevřelo nové příležitosti pro získávání zpravodajských informací. Zkoumání těchto dat napomáhá bojovat s mezinárodními bezpečnostními výzvami na národní bezpečnost jednotlivých států ve velmi proměnlivém mezinárodním prostředí.

Otevřené zdroje prokázaly svou užitečnost zvláště během posledních desetiletí, zejména proto, že poskytují zpravodajcům lepší přehled a celkový kontext toho, co se přesně děje na území jakéhokoliv státu na Zemi. A to i v dobách míru, nejen při široce diskutovaných konfliktech velkého rozsahu a obdobných událostech s možným vlivem na cizí státy. Vývoj toho, co je v dnešní době nazýváno bezpečnostním prostředím, je tak znatelně ovlivněno posunem od tajného či skrytého zpravodajství k primárnímu využívání otevřených zdrojů. Touto cestou vše dospělo k dnes již všeobecně užívanému zpravodajství z otevřených zdrojů, ať je předmět zájmů jakýkoliv.[20]

Zpravodajství z otevřených zdrojů je v dnešní době základním pilířem institucionálního a strategického plánování bezpečnostních služeb a jejich boje proti různým negativním vlivům působícím proti národní bezpečnosti státu.

---

[19] DAVYDOFF, Daniil. The cult of the search in open-source intelligence. *Security Magazine* [online]. 24.11.2020 [cit. 2022-05-10]. Dostupné z: https://www.securitymagazine.com/authors/2380-daniil-davydoff

[20] GIBSON, Stevyn D. *Secret Intelligence: Exploring the role and value of open source intelligence*. Second Edition. New York, USA: Routledge, 2020, s. 100-103.

Shromažďování informací o kriminálních aktivitách na území státu, možném ohrožení vně státní území, odhalování plánů a cílů subjektů (státy, nestátní aktéři, osoby atp.) jsou výzvou, kterou lze překonat aplikací zpravodajství z otevřených zdrojů a jeho integrací jako jedné z formy zpravodajství.

2.1 Výhody zpravodajství z otevřených zdrojů

Výhod, kterých má zpravodajství z otevřených zdrojů je hned několik. Zpravodajství z otevřených zdrojů může být samo o sobě praktikováno kýmkoliv, ať už laikem, zkušeným programátorem či příslušníkem zpravodajské služby. V podstatě vše, co člověk v dnešní době potřebuje, je internetové připojení a zařízení s webovým prohlížečem. Liší se pochopitelně zejména šíře možností využití zpravodajství z otevřených zdrojů na základě schopností člověka samotného. Existují nástroje pro vyhledávání, které jsou přístupné veřejnosti a jsou bez poplatků. Pro kvalitnější zpravodajskou analýzu se však využívají placené a profesionální verze těchto nástrojů, které zajistí širší a mnohdy efektivnější analýzu.

Otevřené zdroje mohou poskytovat informace v reálném čase, ve většině případů ihned potom, co se konkrétní událost stane. Informace tak mohou být analyzovány téměř okamžitě po jejich zveřejnění. Poskytují také indicie a důkazy o situaci ještě před proběhnutím událostí, a tak lze předpovídat možný budoucí vývoj a podniknout kroky, které se přizpůsobí nastalé situaci. Správně analyzované informace s opatřeními aplikovanými ve správný čas mohou pomoci bezpečnostním složkám a dalším státním institucím z hlediska národní bezpečnosti. Stejně tak mohou být užitečné i pro jednotlivce při jejich vlastní soukromé analýze.

Další výhodou, která napomáhá využívání zpravodajství z otevřených zdrojů ve větší míře, jsou současné technické možnosti z hlediska kvality počítačů a obdobných přístrojů. Jejich velmi rychlé a výkonné procesory a potenciál úložiště paměťové jednotky umožňuje provádět operace, které jsou

kapacitně náročné a při shromažďování, zpracování a analýze dat. Čím je přístroj výkonnější, tím více operací dokáže provést. [21]

Proto je stále účinnější, s ohledem na velké množství dat, využívat automatickou analýzu a komparaci velkého množství dat z různých zdrojů najednou. V současné době totiž existují nástroje a programy, které dokáží pomocí algoritmů z různých typů otevřených zdrojů vydolovat a analyzovat pouze relevantní data, a to ve velkých datových objemech. Při jejich využití lze vyhledat výsledky, které by bez těchto algoritmů byly jinak jen velmi složitě vyhledatelné. Některé z nich jsou zmíněny v následujících kapitolách.[22]

Tato dostupnost elektronických informací umožňuje jistou možnost kooperace bezpečnostních složek a veřejnosti na sběru a analýze informací, sdílení informací a znalostí s veřejností. Jedná se samozřejmě o informace, které nemohou ohrozit práci bezpečnostních složek, mohou být sdíleny a veřejnost tak může být obeznámena s problematickými tématy, o něž se bezpečnostní složky zajímají. Což je činěno například pomocí výročních zpráv. To může pomoci zabránit šíření hoaxů, dezinformací a spekulacím o činnosti bezpečnostních složek.

Zpravodajství z otevřených zdrojů jako takové nemusí sloužit pouze bezpečnostních složkám státu, na druhou stranu mají zrovna ony v podstatě největší možnosti z hlediska šíře informací, které by měly být schopny z kyberprostoru získat na základě svojí autority. Zejména v oblasti kriminality a kybernetické bezpečnosti je možné pomocí zpravodajství z otevřených zdrojů monitorovat podezřelé osoby nebo nebezpečné skupiny, sledovat profily radikalizovaných osob, identifikovat původ kybernetických útoků, studovat

[21] GANDOMI, Amir a Murtaza HAIDER. Beyond the hype: Big data concepts, methods, and analytics. International Journal of Information Management [online]. 3.12.2014, s. 137-144 [cit. 2022-05-12]. Dostupné z: https://doi.org/10.1016/j.ijinfomgt.2014.10.007
[22] Tamtéž

znepokojivé trendy společnosti nebo charakteristiku zločinů z kriminologického pohledu.[23]

2.2 Výzvy zpravodajství z otevřených zdrojů

Shromažďování informací z otevřených zdrojů není nic jednoduchého, zdrojů a informací je na internetu nepřeberné množství, kvalita informací a legitimita jejích zdrojů dokáže být proměnlivá a je nutné mít informace podložené, buďto z jiných druhů zpravodajství nebo si informace ověřit přes další zdroje informací, což může vést ke složité a časově náročné činnosti.

Je velmi obtížné sledovat a držet krok s negativními jevy působícími proti národní bezpečnosti, což samo o sobě vytváří další problémy s tříděním informací a s identifikací toho, co je relevantní a co je jen klamem, který má svést zpravodajskou analýzu špatným směrem. Dokonce i při cíleném zaměření se na daný subjekt, například na konkrétní jednotlivce nebo jejich kanály, je nutné se držet správných vodítek vzhledem k rozmanitosti metod v rámci informační války. Ty jsou právě využívány k úmyslnému šíření informací zavádějících analýzu na slepou stopu.

V předchozí kapitole zmíněné sdílení informací s veřejností, poskytuje, na druhou stranu, různým subjektům – státům, nestátním aktérům, zločineckým skupinám, lepší vhled do probíhajících činností v bezpečnostních složkách. Ty mohou naznačit jakým směrem se státní instituce ubírá a co činnosti škodícího subjektu ví a to pak využít ve svůj prospěch. Bezpečnostní složky musí, jak jsem již zmínil, vybrat veřejně dostupné údaje pečlivě, aby nedošlo k ohrožení vyšetřování, ani k ohrožení bezpečnosti osob.

Všeobecná dostupnost nástrojů zpravodajství z otevřených zdrojů logicky umožnila využívání i zmíněnými subjekty. Ti tak mohou využívat sociální sítě ke sběru informací o osobách, veřejné rejstříky k informacím o soukromých firmách

[23] TABATABAEI, Fahimeh a Douglas WELLS. OSINT in the Context of Cyber-Security. In: AKHGAR, Babak, P. Saskia BAYERL a Fraser SAMPSON. *Open Source Intelligence Investigation: From Strategy to Implementation*: Springer, 2016, s. 213-231.

nebo služby internetových map, kde je možné získat informace o situovanosti lokací po celém světě.

Analytici se často zabývají aktivitami, o kterých mají jen velmi málo spolehlivých údajů z otevřených zdrojů. Na základě těchto mohou jen velmi složitě vyvodit spolehlivé závěry. A to zejména v případech neznámých nebo nově vznikající subjektů, nebo z izolovaných a málo rozvinutých regionů. To může být částečně eliminováno tříděním zdrojů na základě důvěryhodnosti, nebo si připuštění pravděpodobné neověřitelnosti informace. [24]

Jak dokáže být dostatek dat výhodou zpravodajství z otevřených zdrojů, absolutní přebytek a nejasnost u množství dat lze považovat naopak za nevýhodu či výzvu, která se poté musí při analýze překonávat. V těchto případech je důležité využití automatizovaných systému vyhledávání a třídění dat podle určitých kritérií, aby byla přebytečná data odfiltrována a homogenizována.[25] K tomu je nutné mít dostatečné znalosti využívaných programů a metodologii, která dokáže zajistit co nejvyšší kvalitu shromažďovaných dat a následného zpracování a analýzy do konkrétních závěrů.

Sociální sítě a další internetová média jsou krom pravdivých a podložených informací plná také nepravdivých informací, subjektivních názorů, hoaxů a často ne příliš spolehlivých fact-checků dezinformací. Ve zpravodajství z otevřených zdrojů je třeba brát v úvahu riziko existence těchto neúplných informací a dezinformací.

---

[24] KLEČKOVÁ, Adéla. OPEN SOURCE INTELLIGENCE AND TERRORISM. PSSI ALUMNI BRIEF [online]. Praha: Prague Security Studies Institute, 2021. Dostupné z: https://www.pssi.cz/download//docs/8539_pssi-alumni-brief-01-osint-4.pdf

[25] FLEISHER, Craig S. Using open source data indeveloping competitive andmarketing intelligence. In: *European Journal of Marketing* [online]: Emerald Group Publishing Limite , s. 852-586 [cit. 2022-05-18]. 2008. Dostupné z: https://www.researchgate.net/publication/273745484_Using_Open_Source_Data_in_Developing_Competitive_and_Market_Intelligence

V ideálním případě by shromážděná data měla pocházet od všeobecně uznávaných a důvěryhodných zdrojů. Mezi ty se obecně dají zařadit oficiální dokumenty, vědecké zprávy apod., ale i u nich může dojít k faktickým chybám nebo úmyslně vydaným nepravdivým informacím, což práci analytika informací čerpaných z otevřených zdrojů může značně komplikovat. Tato nejednoznačnost však bývá u zpravodajství z otevřených zdrojů relativně obvyklá a je nutné ji doplnit například znalostmi z jiných zpravodajských disciplín.

Samotné výsledky by měly, avšak záleží na konkrétním případu, respektovat soukromí osob a neměly by odhalovat jejich intimní a osobní problémy a ve stejnou chvíli musí zohledňovat aktuální související předpisy, např. v Evropské Unii účinné GDPR. Jde například o případy, kdy lze z otevřených zdrojů logicky odvodit citlivé informace jako je sexuální orientace, náboženské přesvědčení nebo politický názor.

Jejich odhalení a zveřejnění by mohlo mít pro dotyčného v určitých zemích následky související s porušením zákona nebo ohrožením na životě ze strany určitých skupin. V poslední řadě se ve spojení se zpravodajstvím z otevřených zdrojů objevují obavy o narušování soukromí a osobní integrity. I když jsou otevřené zdroje veřejně přístupné, mohou odhalit citlivé informace, které na internetu nebyly v daném kontextu výslovně zveřejněny. [26]

Pro zpravodajství z otevřených zdrojů je tedy velmi důležité systematické a průběžné shromažďování a analýza dat, které nabízí cenný prostředek k poznání důležitých znaků o uskutečněných operacích proti vlastní národní bezpečnosti. To je základní předpoklad pro předpovídání hrozeb, bez informací z otevřených zdrojů by bylo obtížné proti hrozbám efektivněji bojovat.

[26] CASANOVAS, Pompeu. Cyber Warfare and Organised Crime. A Regulatory Model and Meta-Model for Open Source Intelligence (OSINT). In: *Philosophical Studies Series* [online]. [cit. 2022-05-20]. 2017, s. 155-156.

2.3 Otevřené zdroje informací

Tato podkapitola se zabývá otevřenými zdroji informací na internetu. Zaměřuje se na oblast sociálních sítí, Deep Webu a Dark Webu, o co se jedná, šíři jejich možností a schopností důležitých pro zpravodajství z otevřených zdrojů. Jsou zde zmíněny také některé jejich nástroje pro vyhledávání informací.

2.3.1 Sociální sítě

Sociální média jsou nyní velmi významným zdrojem informací o lidech, celkové společnosti a veškerého dění ve světě. SOCMINT neboli zpravodajství z prostředí sociálních sítí je jedním z druhů zpravodajství z otevřených zdrojů. Data produkovaná uživateli a informace, které uživatelé zveřejní na sociálních sítích, jsou využívána pro zpravodajskou analýzu informací. Využití SOCMINT je rozšířené v soukromém sektoru pro účely marketingu, v politice při plánování volebních kampaní, zároveň je ve velké míře využívána bezpečnostními složkami po celém světě.

Každým okamžikem je na internet sdíleno extrémně velké množství dat v bezprecedentním měřítku. Každým dnem velká část obyvatel na planetě užívá internetové stránky, aplikace, blogy, sociální sítě a fóra ke zveřejňování, sdílení a prohlížení obsahu a věcí, které je zajímají. Všechny jejich interakce zanechávají digitální stopu, podle kterých lze odvodit mnoho fenoménů a trendů, které mohou být nápomocny při zpravodajské analýze.

Mnohé nástroje a techniky, které se používají k analýzám sociálních sítí a informací z otevřených zdroj, jsou relativně nové a většinou jsou vytvořené samotnou komunitou zabývající se zpravodajstvím z otevřených zdrojů. Digitální sociální prostory jsou poměrně novým místem se stále větší sociální aktivitou. Lidé se tu mohou střetnout lidmi s jinými společenskými normami, hovořící jinými jazyky, lze sledovat politické, psychologické a sociální vlivy v jiných částech světa, které jsou aktuální a reálné v zemích doslova tisíce kilometrů daleko. [27]

[27] CHRISTOPHER, Andrew, Richard J. ALDRICH a Wesley K. WARK, ed. Secret Intelligence: A Reader. Second Edition. New York, USA: Routledge, 2020, s. 78-82.

Sociální sítě mohou mít i patologický vliv. Na dálku mohou extremisticky založené organizace oslovovat a verbovat osoby; lze tu vyzývat k násilí vůči osobě či osobám, nebo sociální síť může zprostředkovávat komunikaci, která může plynout v kriminální a jinou státu škodlivou činnost. Bezpečnostní složky na celém světě vědí o potenciálu pro zneužití sociálních sítí pro tyto účely. Informace ze sociálních sítí jsou dnes takřka nezbytné pro jejich činnost.

Sociální sítě na žádost bezpečnostních složek vydávají zejména záznamy korespondence uživatelů a metadata jako IP adresy, registrační údaje účtu a jeho užívané služby.[28] Ve velké míře je však získávání informací bezpečnostními složkami ze sociálních sítí značně neprůhledné.

Na nespočtu sociálních sítí jsou samotní uživatelé zprostředkovateli při "výrobě" informací, jelikož mohou různé události sami dokumentovat a sdílet své příspěvky do online prostředí přímo z první ruky. Mohou si také recipročně, pokud se o nějakých událostech dozvědí, sami vyžádat informace od osob nacházejících se v místě události. A to od osob ze stejného státu, města, městské části, ne-li ze stejné ulice, kde určitá pro ně důležitá událost proběhla.

Zároveň mohou na sociálních sítích informace ověřovat, přidávat další informace z jiných zdrojů. Přitom mohou při šíření různých informací nadhodnocovat nebo zkreslovat následky událostí, nebo jinak posuzovat reálnou situaci, čímž mohou ovlivnit postoje dalších osob, které sledují jejich sdílený obsah.

V této části budou popsány ty nejvíce využívané sociální sítě ze kterých lze čerpat nespočet různých informací. Zaměří se zejména na celkový charakter těchto sociálních sítí a typ informací, který na nich lze nejčastěji naleznout při

[28] SCHWIMMER, David. Žádosti o poskytnutí informací o uživatelích Facebooku, Googlu, Microsoftu a Seznamu. *Policie.cz* [online]. 20. 4. 2020 [cit. 2022-05-25]. Dostupné z: https://www.policie.cz/clanek/zadosti-o-poskytnuti-informaci-o-uzivatelich-facebooku-googlu-microsoftu-a-seznamu.aspx

zpravodajské analýze. Obecně platí, že na každé z níže zmíněných sociálních sítích lze najít informace pomocí vyhledávacích nástrojů jako Google, Bing, DuckDuckGo, Yandex, Baidu a dalších. Samotné sociální sítě mají své vlastní vyhledávací nástroje, s různou šíří možnosti filtrování, podle nichž lze také rozšířit potenciál celkového množství nalezených dat a informací. Pro vyhledávání uživatelů podle shodného jména účtu, nejen k níže zmíněným sociálním sítím, je vhodný nástroj NameCheckup (namecheckup.com), který všechny účty se stejným jménem dokáže zobrazit.

2.3.1.1 Facebook

Na Facebooku lze podle samotných informací na profilu a příspěvků na webové stránce profilu, neboli timeline, rozpoznat zaměstnání, vzdělání, věk, členy rodiny, přátelé, rodinný stav, polohu, navštívená místa, zájmy nebo oblíbené hudební skupiny. Fotografie a příspěvky účtů nám také mohou pomoci uvést do kontextu společnost nebo osobu, kterou zkoumáme, oblasti zájmu, které navštěvuje, nebo další aktivity z jejich života. Na sociální síti Facebook je měsíčně aktivních zhruba 2,9 miliard účtů. [29]

Na skupinách, ve kterých je členem lze explicitně vyhledat všechny příspěvky uživatele, podle jména účtu nebo podle použitých slov v příspěvku. U veřejných skupin lze tyto informace vyhledat bez nutnosti vlastního přijetí do skupiny, u soukromých a tajných skupin lze tyto informace získat až po přijetí. Na profilech a skupinách je možné vysílat živě pomocí samotného zařízení.

Po přihlášení se v horní části každé stránky na Facebooku zobrazí jednoduché vyhledávací pole. Facebook má svůj vyhledávácí nástroj, který vyhledá příspěvky, účty, fotky, videa, stránky, skupiny, události, které obsahují vložené slovo nebo frázi. Také lze pomocí tohoto nástroje nalézt předměty na Marketplace, což je služba, kde lidé mohou vystavovat věci určené k prodeji. Kromě toho je také možné vyhledávat například podle lokace, když skutečné

[29] DIXON, S. Most popular social networks worldwide as of January 2022: Ranked by number of monthly active users. Statista.com [online]. 26.7.2022 [cit. 2022-07-31]. Dostupné z: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

jméno účty určité osoby není známo a podle toho se pokusit najít konkrétní profil. Tak lze alternovat všechny způsoby dostupné vyhledávání.

2.3.1.2 Reddit, 4chan

Sociální síť *Reddit* a *4chan* spojuje webový obsah, zdroj zpráv, fórum a sociální síť do jedné univerzální platformy. Registrovaní členové mohou do jednotlivých tzv. subredditů respektive boardů sdílet příspěvky, obsahující obrázky, text, videa a odkazy.

U *Redditu* se každý subreddit týká jiného tématu a uživatel si může vytvořit svůj dle svého uvážení a zájmů. Každý příspěvek je možné ohodnotit a je pod ním možná další diskuze. Veškeré subreddity a příspěvky lze podle uživatele a klíčových slov vyhledat. Současně lze u jednotlivých uživatelů vidět jejich podrobnou aktivitu, což je při zpravodajství z otevřených zdrojů užitečné.

4chan je z hlediska struktury podobný, ale jeho uživatelské rozhraní je relativně nepřehledné a účty jsou v podstatě anonymní, samostatné profily uživatelů neexistují. To znamená, že účastníci mohou říkat a dělat prakticky cokoli, co chtějí, pouze s malou hrozbou odpovědnosti za své příspěvky. Znamená to také, že nelze ostatním uživatelům posílat zprávy nebo s nimi navázat jakýkoli sociální vztah, pokud sami uživatelé nějakým způsobem neprozradí svou identitu v rámci jednotlivých fór.

Tato sociální síť má velký potenciál, co se týče osob s extremistickými názory a poznání jejich myšlení, díky absolutní svobodě slova na této síti. Na druhou stranu takřka nelze trestnou nebo jinou společensky škodlivou činnost postihovat, jelikož je na této síti absolutní anonymita uživatelů.

2.3.1.3 Youtube, TikTok

YouTube a TikTok jsou sociální sítě založená na sdílení videí. Lze zde analyzovat obsah nahraný konkrétním uživatelem (témata, lokace, obrázky, místa a lidé objevující se ve videích), ale také názory a komentáře odběratelů, které lze nalézt pod každým videem. Každý komentář pod videem obsahuje

uživatelské jméno účtu, které komentář vytvořilo s odkazem na profil daného uživatele.[30]

„YouTube je měsíčně je využíván 2,5 miliardami uživatelů. Podle samotného YouTube, je každou minutu nahráno 500 hodin videí, což má je téměř 80 let nahraného videoobsahu každý týden.“[31]

Videa na těchto platformách užívají hashtagy, v TikToku jsou zobrazeny u videa. Na YouTube se veřejně zobrazují jen některé hashtagy, zbytek je skryt a slouží k přesnějšímu vyhledávání videí, pomocí vyhledávacího algoritmu. Při kontrole velkého množství dat může být obzvláště zajímavé zjistit, které hashtagy jsou pravidelně přidávány do TikToků, které již sdílejí jednu konkrétní značku. Mnoho TikToků obsahuje více hashtagů.

Analýzou vytvořených vzorců při společném užívání hashtagů lze například pomoci identifikovat videa s dezinformacemi nebo jinak zavádějící videa. V takových případech mohou být stejné hashtagy použity opakovaně v různých příspěvcích. Analýza většího počtu příspěvků může pomoci dozvědět se více o kontextu a dalších důvodech proč se konkrétní hashtag používá.[32]

2.3.1.4 Twitter

Twitter se využívá zejména pro sdílení informací, vlastních poznatků nebo pro rozpoutání diskuze na určitá témata. Na profilech, které bývají v drtivé většině veřejné, lze najít příspěvky uživatele a sdílené příspěvky jiných uživatelů uspořádané chronologicky na časové ose. Na Twitteru je uživatelsky přívětivé rozhraní, na kterém je možné vyhledávat na celé platformě podle klíčových slov, přesných frází, hashtagů, jazyka, data a tak dále. Můžeme tedy dokonce upřesnit vyhledávání prohledávání uživatelů a jejich účtů, jejich zmínek nebo

[30] BAZZELL, M. *Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information*. Ninth edition. 2022, s.353-358.
[31] Tamtéž, s. 353.
[32] This New Tool Lets You Analyse TikTok Hashtags. *Bellingcat.com* [online]. 11.5.2022 [cit. 2022-07-01]. Dostupné z: https://www.bellingcat.com/resources/how-tos/2022/05/11/this-new-tool-lets-you-analyse-tiktok-hashtags/

odpovědí. Více o této sociální síti je zmíněno v další části týkající se konfliktu na Ukrajině.

2.3.1.5 Instagram

Sociální sítě *Instagram, Snapchat a BeReal* jsou v dnešní době rozšířeně využívány jako platformy pro sdílení fotografií a vzájemnou soukromou komunikaci.

Na ***Instagramu*** existují účty veřejné přístupné všem přihlášeným uživatelům a účty soukromé, u kterých je nutné přijmutí žádosti o sledování, aby mohl být obsah účtu viditelný. Po zobrazení instagramového profilu uživatele je výchozím zobrazením timeline s fotkami, které je možné rozkliknout pro více informací. Místa, osoby a činnosti zobrazené a tagnuté na obrázcích mohou pomoci při celkovém profilování cíle.

V biu (popisku) účtu lidé sdílejí základní informace o sobě, jako je pohlaví, kde žijí, členy rodiny, s kým jsou ve vztahu, zájmy, informace o svém vzdělání a zaměstnání. Osoba si může také zobrazit všechny sledující účtu a účty, které tento účet sám sleduje.

Na Instagramu je dostupná také funkce *stories*, kam mohou uživatelé na 24 hodin sdílet obrázek, ke kterému lze, mimo jiné připojit konkrétní polohu, tím pádem je možno vidět, kde se osoba zrovna nachází. Za předpokladu, že tuto story osoba nesdílí s určitým zpožděním. Tato stránka bude také běžně obsahovat fotografii uživatele a všechny nedávné příspěvky na jejich stránce. Na Instagramu je poloha poměrně citlivým údajem, který je na této platformě velmi často sdílen.

Dalšími funkcemi k vyhledávání informací jsou hashtagy, které ve vyhledávacím nástroji Instagramu nebo samotným rozkliknutím hypertextového odkazu hashtagu, zobrazí příspěvky na veřejně přístupných profilech označených v popisku stejným hashtagem.

2.3.1.6 Snapchat

Sociální síť *Snapchat* je uzpůsobena zejména soukromou komunikaci a sdílení audiovizuálních příspěvků mezi uživateli, a to zasíláním zpráv mezi dvěma uživateli nebo ve skupinách osob. Přitom je důležitou částí, jako u Instagramu, možnost sdílení stories, které jsou primárně sdíleny mezi manuálně přidanými přáteli, lze však nastavit i veřejně dostupné story pro všechny uživatele Snapchatu. Ty je možné zobrazit v mapě, která umožňuje zaměřit se na konkrétní lokace na světě a všechny sdílené veřejné stories.

Lokace není přesná, dostupnost stories je vyobrazena tzv. heat zónami na mapě podle počtu sdílených veřejných stories. Veřejné stories mohou být užitečné při průzkumu konkrétní nastalé události, může na nich být zadokumentován záznam z události nebo na nich mohou místní lidé popisovat, co se v určitém městě, regionu či zemi zrovna děje. Při rozkliknutí se zobrazí v lokaci vytvořený tzv. snap, což bývá obrázek nebo video, doplněný popiskem a dalšími informacemi. Na mapě lze také vidět přesnou lokaci účtů v seznamu přátel, které mají na Snapchatu povolenu sdílenou polohu jejich zařízení.

Obrázek 1 – Ukázka mapy z aplikace Snapchat s heat zónami
Zdroj: www.snapchat.com

2.3.1.7 BeReal

Novou sociální sítí s velkým potenciálem pro zpravodajství z otevřených zdrojů do budoucnosti je sociální síť BeReal. BeReal zasílá uživatelům každý den v náhodnou dobu notifikace, která je vyzývá, aby zveřejnili co právě dělají,

tím, že se vyfotí. Na odpověď na notifikaci jsou vyhrazeny dvě minuty, kdy by uživatel měl vytvořit fotku z přední a zadní kamery. Následně je koláž těchto dvou snímků zveřejněna. Tato koláž je pak sdílena na zdi příspěvků všech přátel, koláže přátel lze vidět jen při vlastním zveřejněním denního příspěvku. Znovu je možná volba zveřejnit tuto koláž veřejně všem uživatelům BeReal.

Veřejně sdílené koláže se mohou ukázat všem lidem, kteří si načtou v aplikaci záložku Discovery. Koláže nelze konkrétně vyhledat a ukazují se náhodně. Při každém obnovení záložky Discovery se načtou další veřejné koláže z náhodných účtů. U těchto koláží lze zapnout možnost přesné lokalizace, která je poté přiložena ke koláži. Což v praxi znamená, že je možné pomocí koláží zjistit v kolik hodin a kde se přesně osoba nacházela.

Tím, že lze konkrétně hledat jen účty přidané do seznamu přátel a ostatní koláže se ukazují náhodně, je možnost zpravodajství z této sociální sítě alespoň prozatím relativně omezena. Efektivní je pouze pro zpravodajství z účtů, které jsou přidány do seznamu přátel.

2.3.2 Deep Web

Deep Web je součástí World Wide Web, jehož obsah není možné vyhledat standardními webovými vyhledávači. Opačným termínem je Surface Web který zahrnuje obsah, který je dostupný široké veřejnosti a lze jej vyhledávat pomocí standardních webových vyhledávačů.

V Deep Webu jsou zahrnuty například databáze, jež schraňují soubory jak veřejných, tak soukromých subjektů, které nejsou propojeny s jinými oblastmi webu. Jsou k dispozici pouze pro vyhledávání v rámci samotné databáze.

Dalším příkladem je intranet, což je interní síť využívaná podniky, státními institucemi, vzdělávacími institucemi a dalšími skupinami jednotlivců. Intranet je používán k soukromé komunikaci a interní kontrole různých oblastí v rámci jejich organizací. Intranet zpravidla vyžaduje, aby uživatel zadal heslo, které bývá

vytvořeno během registrace nebo jej musí obdržet přímo od vlastníka nebo admina webu.[33]

2.3.3 Dark Web

Na rozdíl od internetu a většiny Deep Webu nabízí Dark Web uživatelům, kteří jej využívají, anonymitu a soukromí. Tato vlastnost umožňuje zločincům využívat tuto síť k surfování, vyhledávání a publikování s nezákonnými účely a zároveň skrývá svou identitu.

Dark Web je proto ideálním zdrojem pro aplikaci zpravodajství z otevřených zdrojů a boj proti kyberzločinu, organizovanému zločinu nebo jiným kybernetickým hrozbám. Na druhou stranu, vysledování a deanonymizace těchto subjektů je v současné době nesnadný úkol.

Dark web označuje weby, které nejsou vyhledatelné v běžně využívaných internetových prohlížečích a lze k nim přistupovat pouze prostřednictvím specializovaných programů jako je například Tor, Freenet nebo I2P. Specializovaný program zprostředkovává uživateli relativně skrytý přístup na nedostupný web tím, že zamaskuje jeho IP adresu, čímž zajistí anonymitu jeho vyhledávání. Dark web zahrnuje výrazně menší počet stránek než Surface web a bývá považován za součást Deep webu. Typickým znakem darkwebových stránek je doména .onion využívaná na prohlížeči Tor.[34]

Anonymita dark webu znesnadňuje mapování tamějšího kriminálního prostředí, zejména stopování pachatele. Specializované programy umožňují komukoliv se, bez větších překážek, připojit k Dark webu anonymně surfovat po internetu a nezanechávat za sebou téměř žádné virtuální stopy. K využívání programů stačí pouze základní uživatelská znalost, počítač a přístup k internetu.

---

[33] KALPAKIS, George a Theodora TSIKRIKA a spol. OSINT and the Dark Web. In: AKHGAR, Babak a spol. *Open Source Intelligence Investigation: From Strategy to Implementation*. Springer, 2016, s. 111-112.
[34] Tamtéž, s. 118-121.

Uživatel poté může dodávat nebo nakupovat nelegální zboží a využívat nelegálních služeb na Dark Webu.[35]

Zároveň však Dark web vytváří svobodný prostor pro novináře, blogery, různé opoziční skupiny nebo stoupence extremistických ideologií. Ti využívají Dark Web jako platformu pro výměnu informací, diskutují o různých problémech a mohou zde svobodně vyjadřovat své názory. Což je vhodné zejména pokud žijí na území státu, který by je jinak za jejich vyjádření na internetu mohl perzekvovat. Stejně tak jsou uživatelům webu k dispozici bezplatné e-knihovny a zakázaná literatura. Dark Web však aktivně využívají jednotlivci, kteří jsou zapojeni do trestné činnosti, která je všeobecně brána jako společensky nebezpečná, ať už je stát totalitní nebo ne.[36]

Bezpečnostní složky po celém světě se aktivně podílejí na monitorovacím procesu Dark Webu, aby identifikovaly osoby zapojené do trestné činnosti; odhalily únik utajovaných či osobních informací; identifikovaly osoby pracující pro jiné státy a na základě toho mohly stanovit konkrétní opatření. Přestože se detekce nelegálních aktivit na Dark webu může zdát komplikovaná, bezpečnostním složky jsou schopny v mnoha případech úspěšně potírat nelegální aktivity využíváním dalších metod zpravodajství jako např. HUMINT nebo SIGINT.

Uživatelé Dark webu mohou narazit na utajované dokumenty soukromých společností a vlád, které byly získány v důsledku kybernetických útoků provedených hackery. V nedávné historii došlo k mnoha případům úniku utajovaných informací, které negativně ovlivnily reputaci některých států, firem a osob, odůvodněně či neodůvodněně.

---

[35] What is the Deep and Dark Web? *Kaspersky.com* [online]. 2022 [cit. 2022-07-04]. Dostupné z: https://www.kaspersky.com/resource-center/threats/deep-web

[36] KALPAKIS, George a Theodora TSIKRIKA a spol. OSINT and the Dark Web. In: AKHGAR, Babak a spol. *Open Source Intelligence Investigation: From Strategy to Implementation*. Springer, 2016, s. 120-124.

I vyhledávání a čerpání z uniklých dokumentů je považováno za jednu z metod zpravodajství z otevřených zdrojů. Mnohé ze získaných dokumentů jsou svým obsahem velmi cenné a odkrývají informace, které v původním záměru nebyly určeny pro veřejnost. Na druhou stranu mají na Dark Webu své tzv. mirrory i média jako např. BBC, The New York Times nebo Deutsche Welle, čímž zpřístupňují obsah svých stránek i pro osoby, které se nachází na území státu, který zakazuje jejich zobrazení.

K informacím a webovým stránkám na Dark webu lze přistupovat prostřednictvím vyhledávačů navržených speciálně pro web, ačkoli většina webových stránek vyžaduje znalost jejich přímých odkazů. Existuje mnoho webových stránek, které obsahují seznamy různých stránek z Dark webu. V mnohých případech mohou být odkazy zastaralé, protože webové stránky zejména na Dark webu nebývají zrovna stálé a neměnné. Často stránky mohou být smazány samotnými adminy stránky nebo bezpečnostními složkami, a to pokud se na nich nachází podle jejich legislativy nelegální obsah.

Níže jsou zmíněny některé zdroje a nástroje umožňující a usnadňující zpravodajství z otevřených zdrojů na Dark Webu.

The Hub (thehub7xbw4dc5r2.onion)

Největší diskusní fórum na dark webu zaměřené na recenze produktů a služeb na Dark webu, diskuzi o kryptoměnách a kybernetické bezpečnosti. Fórum poskytuje svým uživatelům přístup k různým zájmovým skupinám dle jejich výběru.

Sci-Hub (sci-hub.se)

Rozsáhlá databáze vědeckých prací a publikací z celého světa, které byly získány hackery a nahrány na Sci-Hub. Každý si zde může po vložení konkrétního linku volně stahovat a číst vědecké publikace, které bývají mimo

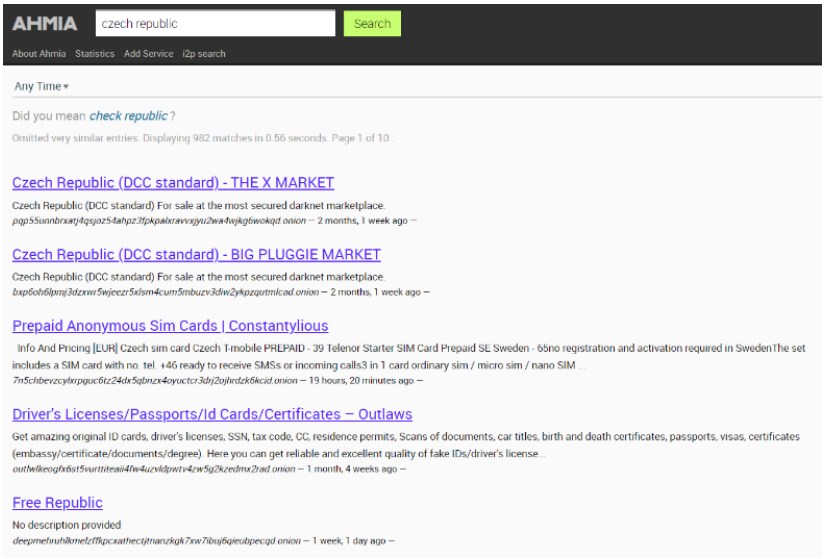
SciHub zdarma nepřístupné. V současné době se zde nachází zhruba 88 milionů vědeckých publikací ze všech oblastí vědy.[37]

Tor Facebook (facebookcorewwwi.onion)

Sociální síť Facebook vytvořila darkwebovou adresu pro uživatele, kteří chtějí navštěvovat jeho webovou stránku bezpečně, díky využití end-to-end šifrování. To znamená, že uživatelé programu Tor, kteří jej používají k obcházení vládní cenzury nebo omezení internetu na územích států, jako je Čína nebo Írán, budou moci používat Facebook bez obav z úniku svých osobních údajů. Uvádí se, že Tor Facebook používá více než 1 milion lidí měsíčně.

Ahmia (ahmia.fi)

Ahmia je původem finský Tor projekt, který zprostředkovává funkci vyhledávacího nástroje na Deep Webu. Ahmia eviduje adresy URL .onion ze sítě Tor a poté tyto stránky vkládá do jejich svého seznamu, který je jeden z nejrozsáhlejších na Deep Webu. Ahmia také poskytuje správcům stránek s doménou .onion zaregistrovat své stránky, což pak logicky umožňuje jejich nalezení na tomto vyhledávacím nástroji.[38]



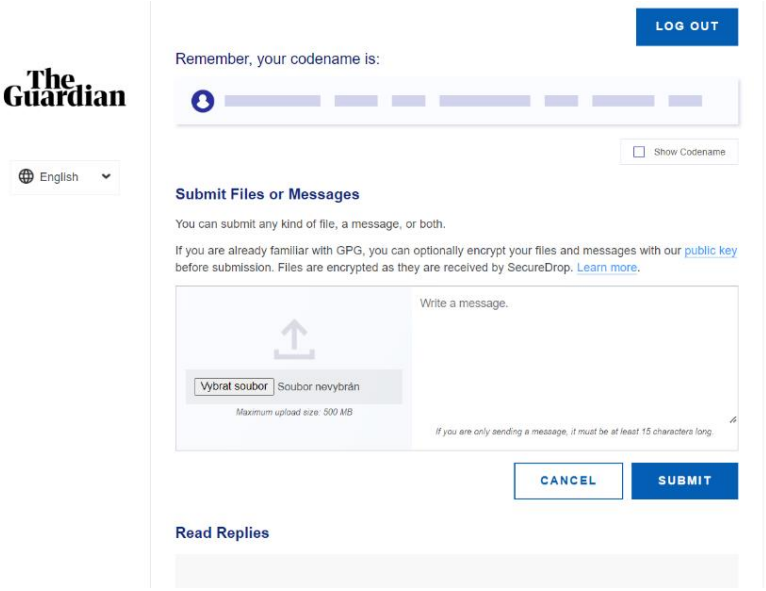
Obrázek 2 - Příklad výsledků vyhledávání na Toru v nástroji Ahmia
Zdroj: http://juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibsot4csyd.onion/

[37] Sci-Hub. Sci-hub.com [online]. 26.7.2022 [cit. 2022-07-04]. Dostupné z: https://sci-hub.se/about

[38] Tor at the Heart: The Ahmia project. *Tor Blog* [online]. 5.12.2016 [cit. 2022-07-04]. Dostupné z: https://blog.torproject.org/tor-heart-ahmia-project/

SecureDrop (securedrop.org)

SecureDrop na Dark Webu je místem, kam mohou whistleblowеři žurnalistům a jejich redakcím sdílet své informace. Zároveň mají na Dark Webu jistotu, že nemohou být vystopováni, pokud to sami nechtějí. Přispěvatelé informací na této stránce mívají často informace o kriminálních aktivitách probíhajících ve státní správě nebo ve firmách. Díky SecureDropu je mohou sdílet s významným snížením ohrožení své bezpečnosti. Mnoho významných světových redakcí (Bloomberg, Al Jazeera, Washington Post a mnoho dalších) využívá služeb těchto anonymních informátorů, a mají proto zřízenou vlastní stránku na SecureDropu.[39]



Obrázek 3 - Náhled Tor stránky deníku Guardian, kam mohou whistleblowеři vkládat své poznatky a soubory.
Zdroj: https://xp44cagis447k3lpb4wwhcqukix6cqqokbuys24vmxmbzmaq2qjvc2yd.onion/

2.4 Nástroje využívající otevřené zdroje

Začleněním automatizovaných technik do procesu zpravodajského cyklu může její závěry značně rozšířit, to vede k přesnějším analýzám a predikcím dalšího vývoje. Státní bezpečnostní složky, tak díky nim mohou být efektivnější při boji proti hrozbám v oblasti jejich národní bezpečnosti. Profesionální a vysoce pokročilé nástroje nebo placené verze nástrojů mohou být využívány zejména

[39] Securedrop Overview. Securedrop [online]. [cit. 2022-07-04]. Dostupné z: https://securedrop.org/overview/

státními institucemi, organizacemi a osobami, které disponují velkými peněžními prostředky pro jejich nákup. Jedná se například o americký systém XKeyScore a Prism nebo britskou Tempora.

V této části se zaměřím na charakter a využití veřejně dostupných nástrojů. Těchto nástrojů je velké množství zaměřené na dolování dat z různých zdrojů. Tato část se zaměřuje spíše na nástroje univerzálnější a snadněji použitelné, které jsou využívány velkým množstvím uživatelů a jsou efektivní pro zpravodajství z otevřených zdrojů.

2.4.1 Maltego CE

Aplikace Maltego je nástroj, který na základě příkazů dokáže provést dolování dat, přehledné shromažďování informací a vizuální zobrazení těchto informací ve schématech a síťových diagramech na základě spojitostí mezi vyhledanými výsledky. Maltego je výkonný vizuální nástroj pro zpravodajství z otevřených zdrojů, který lze upravovat podle vašich vlastních potřeb. Jelikož generuje grafy a schémata, poskytuje tak mnohem lepší přehled na rozdíl od nástrojů obsahující čistě jen příkazové řádky.

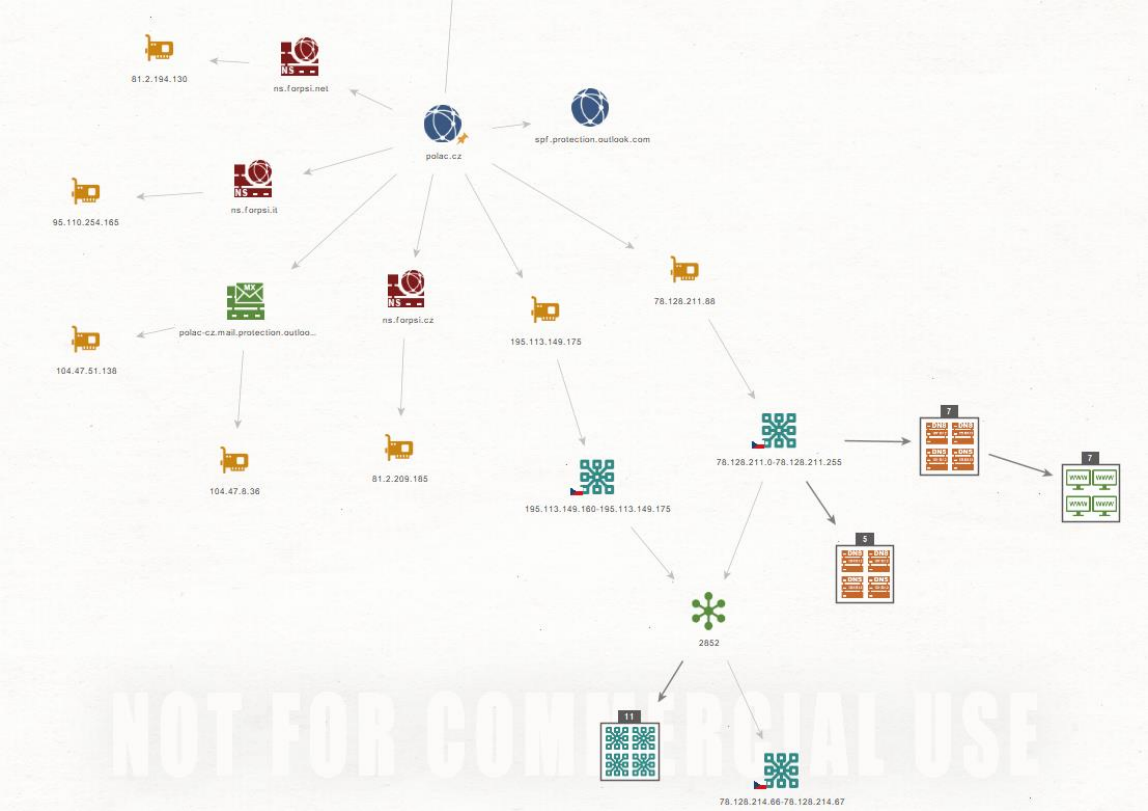
Maltego CE je komunitní verze Maltego, která je k dispozici zdarma po online registraci. K dispozici jsou ještě další verze Maltego; Maltego Pro a dva typy Maltego Business pro firmy a další subjekty. Maltego CE je limitovanější, avšak dostačující pro mnoho vlastních analýz.

Verze Maltego Pro je placená, analýza na této verzi může mít větší množství vyhledaných výsledků, jedno zadání příkazu neboli “Transform“ je schopno vyhledat až 64 tisíc výsledků a dohromady až 1 milionů jednotlivých entit[40] v celém schématu. Narozdíl od 12 výsledků a 10 tisíci entitám v jedné analýze na Maltego CE. Zároveň má dotyčný přístup i k návodům pro vlastní výzkumy a analýzy. Potenciál těchto výsledků je do jisté míry omezen i výkonem přístroje, na kterém je analýza prováděna. Nároky na paměť a výkon procesoru

[40] Abstraktivní reprezentace jakékoliv reálné nalezené informace

přístroje při analýze nejsou nepatrné. Ke každému výsledku lze navíc doplnit do poznámek více doplňujících informací podle vlastního uvážení.

Maltego se může prohledávat internetovou infrastrukturu, tzv. foot-printing, (např. domény, jména systému domén, IP adresy), vyhledávání informací o lidech (např. přihlašovací jména, e-mailové adresy, složky, dokumenty) a organizacích. Maltego tyto informace doluje prostřednictvím záznamů databáze Whois, vyhledávacích nástrojů, sociálních sítí, online API (rozhraní aplikací) a z dalších metadat. Následně nástroj dokáže na základě vztahů mezi daty, spojit mezi s sebou.[41]



Obrázek 4 - Vzhled schématu v aplikaci Maltego, s příkladem zobrazující footprinting webové stránky polac.cz. Vlastní zpracování.

Maltego poskytuje také úložiště zdrojů dat, kam dodavatelé vkládají již extrahovaná data. Je sem možné přidat také vlastní zdroje dat, ale integraci vytvoří interní vývojářský tým Maltega. Maltego je vytvořeno v Javě a funguje na

[41]*Maltego* [online]. [cit. 2022-07-06]. Dostupné z: https://www.maltego.com/product-features/?utm_source=paterva.com&utm_medium=referral&utm_campaign=301

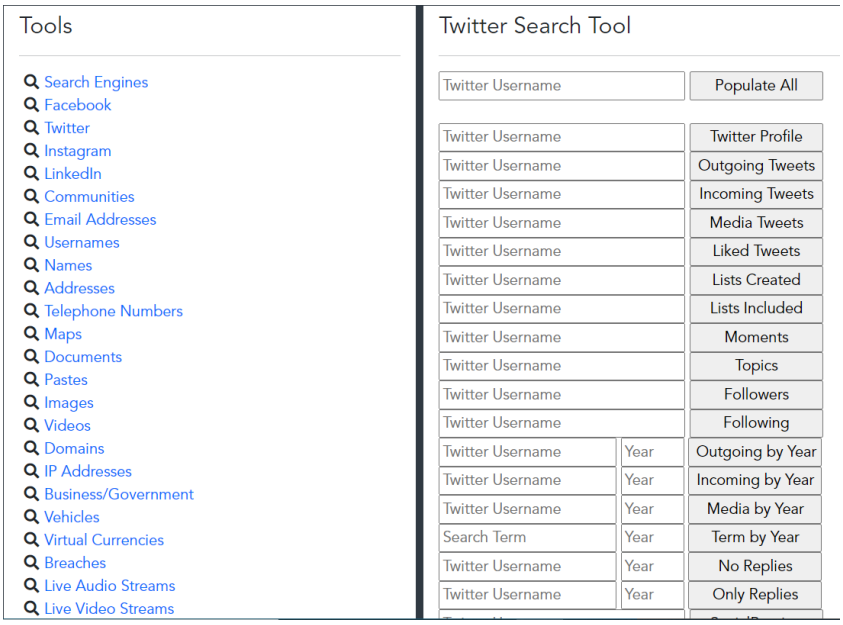
softwarech Windows, Mac a Linux. Uživatelské rozhraní Maltego je přehledné, intuitivní a snadno použitelné.

2.4.2 Inteltechniques

Inteltechniques je užitečný nástroj vytvořený propagátora zpravodajství z otevřených zdrojů a autora populárních publikací s návody pro výzkum z otevřených zdrojů Michaela Bazzella a jeho týmem. Jeho využívání může značně usnadnit vyhledávání informací z otevřených zdrojů. Tento bezplatný nástroj byl od června roku 2019 nedostupný, jelikož byl pod konstantními DDoS útoky a zatěžoval servery, na kterých tento web fungoval. Proto byl od té doby dostupný pouze v placené verzi. To se změnilo v červenci 2022, kdy byl tento nástroj znovuspuštěn v bezplatné verzi a je tak dostupný pro veřejnost takřka po celém světě.

Tento přehledný nástroj slouží jako zkratka pro vyhledávání na velkém množství internetových zdrojů, který zahrnuje ke každému z těchto zdrojů velkou škálu doplňujících informací, které mohou vyhledávání zpřesnit. Což je například u vyhledávání na sociálních sítích velmi užitečné, jelikož je díky tomu možné se zaměřit na konkrétní předmět zájmu výzkumu a eliminovat velké množství nerelevantních výsledků. Výsledky lze vyfiltrovat v těchto nástrojích uvnitř Inteltechniques pomocí vloženého jména účtu, data, lokace, reálného jména, slova, souřadnic, telefonních čísel, URL adresy, hashtagů a dalších specifických znaků.[42]

[42] IntelTechniques Search Tools [online]. [cit. 2022-07-07]. Dostupné z: https://inteltechniques.com/tools/index.html



Obrázek 5 - Možnosti výběru nástrojů vyhledávání na webu IntelTechniques na levé straně, s příkladem vyhledávání pro užší filtrování výsledků na sociální síti Twitter.
Zdroj : https://inteltechniques.com/tools/Twitter.html

Nástroj je rozdělen na několik kategorií, které jsou dále rozděleny do dalších konkrétních druhů vyhledávání. Jsou to zejména:

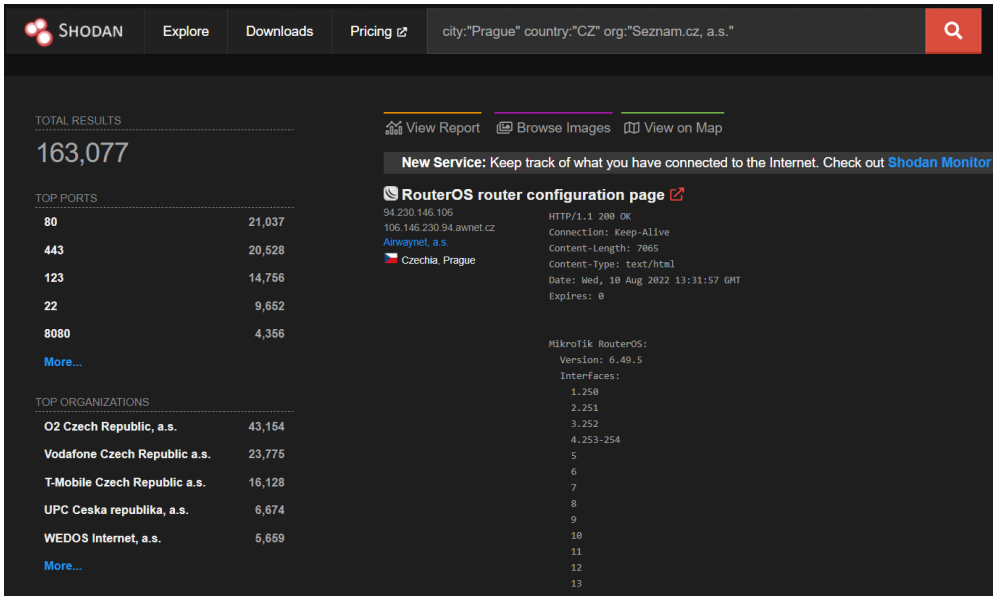
1. *Vyhledávací nástroje* (Google, Bing, Yahoo, Yandex, Baidu, DuckDuckGo, Brave, Wayback, Ahmia, Onionland…)
2. *Sociální sítě* (Facebook, Twitter, Instagram, LinkedIn)
3. *Komunitní sociální sítě* (Reddit, 4Chan, TikTok, Discord, Parler, Telegram…)
4. *Jména*, *emailové adresy*, *telefonní čísla*
5. *Domény*, *IP adresy*, *API*, *dokumenty*, *videa*, *obrázky*
6. *Lokalizace v mapách*
7. *Údaje o vozidlech*
8. *Údaje o kryptoměnových účtech a peněženkách*
9. *Živé audio a video přenosy* (televize, rádia, přenos z vysílacích kanálů)

2.4.3 Shodan

Shodan je vyhledávací nástroj internetových zařízení. Shodan dokáže zmapovat nemalé množství zařízení užívající internet. Shodan bere v potaz doslova každou IP adresu a její porty a shromažďuje informace o jejích

odpovědích a datových výměnách na konkrétním serveru. Pro efektivní užívání aplikace je nutné znát vyhledávací dotazy. Narozdíl Googlu a podobných vyhledávacích nástrojů, Shodan nevyhledává výsledky pouze v prostředí World Wide Webu, ale i v prostředí Deep Webu. [43]

Vyhledávání v Shodanu je velmi dobře navrženo a nabízí možnost používat pokročilé vyhledávací dorky[44] pro rychlé vyhledávání konkrétních cílů. Přístroje lze lokalizovat podle základních filtrů, které lze v aplikaci použít. Shodan je schopen nalézt konkrétní zařízení v konkrétním městě, státě, na určitých souřadnicích; zařízení se společným hostingem, podle IP adresy a portů, operačního systému; nebo například vyhledávat v určitém časovém období.



Obrázek 6 - Ilustrace výsledků programu Shodan, při filtrování všech zařízení v České republice, na území Prahy zaregistrované ve společností Seznam.cz, a.s.
Zdroj : https://www.shodan.io/

Pro více zobrazených výsledků vyhledávání a více možností filtrování je nutné pořídit si placenou verzi.

Informace získané pomocí Shodanu bývají využívány k několika účelům. Lze podle něj dohlížet na všechny zařízení, která se užívají v určitých lokacích

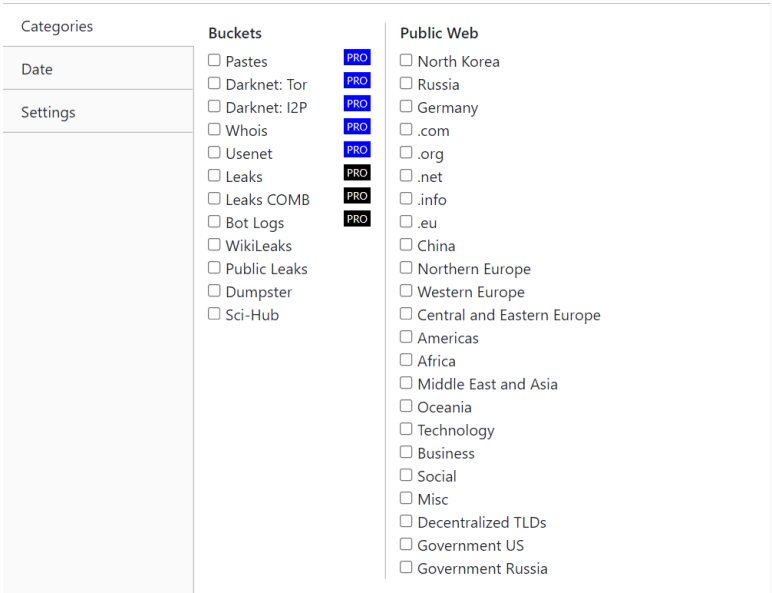
[43] Shodan. Shodan [online]. [cit. 2022-07-04]. Dostupné z: https://help.shodan.io/the-basics/what-is-shodan
[44] Vyhledávací řetězec, který používá pokročilé vyhledávací nástroje k nalezení informací, které nejsou na webu snadno dostupné

nebo konkrétních organizacích. Dále má využití pro výzkum trhu a různé statistické průzkumy, jelikož dokáže zobrazit kolik a která zařízení jsou využívána v určitých lokacích a regionech. Nebo v rámci vlastních zařízení zjistit, která jsou riziková a málo zabezpečená, kvůli možným útokům hackerů.

2.4.4 Dehashed, Leakcheck, IntelX

Nástroje Dehashed, Leakcheck a IntelX mají společně velmi podobný účel, za kterým se dají využít. Tyto stránky poskytují veškerá nalezená data uživatelům (jednotlivcům, firmám), kteří tak mohou být lépe informováni o tom, jaká data byla narušena. Na základě toho pak mohou podniknout další kroky, kterým zabrání zneužití dat a informací a jejím dalším možným únikům, například změnou hesla, změnou a smazáním účtu atp.

Jsou to nástroje pro zabezpečení a ochranu proti možným podvodům ze získaných dat z hackerských databází, které jsou veřejně dostupné, v různých částech internetu. Vyhledávání funguje pomocí konkrétních hledaných výrazů, jako jsou názvy e-mailové adresy, domény, URL adresy, IP adresy, CIDR, bitcoinové adresy atd. Hledá informace na místech jako je Dark Web, stránky pro sdílení dokumentů, záznamy úniků dat.



Obrázek 7 - Možnosti filtrování vyhledávání v programu IntelligenceX, výsledky s označením PRO mohou být použity při zaplacení plné verze nástroje.
Zdroj : https://intelx.io/

2.4.5 Spiderfoot

SpiderFoot je platforma určená pro zpravodajství z otevřených zdrojů, která je založena na konceptu řetězení získaných informací. To znamená, že každé ze shromážděných dat se používá k automatickému získání dalšího kusu dat v procesu plně využívající vlastní nalezené výsledky. Proces pak pokračuje v automatizovaném hledání dokud nejsou shromážděny všechny výsledky relevantní pro celkovou analýzu.

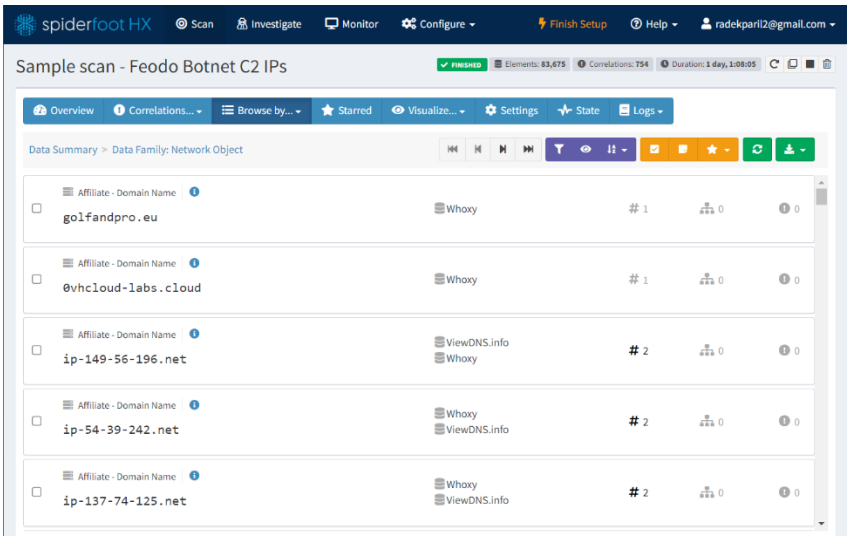
SpiderFoot řetězí a porovnává data pomocí více než 100 modulů. Shromažďuje informace o IP adresách, názvech domén, e-mailu, adresách, jménech a dalších. Používá také schémata pro znázornění vztahů mezi výsledky a jednotlivými entitami. Provádí skenování portů a dokonce prohledává i webové stránky. Díky tzv. automatizované rekurzivní analýze všech nových informací, získaných počátečním skenováním, všechny relevantní výsledky exponenciálně přibývají.[45]

Pokud je například nástrojem objevena e-mailová adresa, nástroje automaticky vyhledávají různá rozhraní, aby nalezly co nejvíce bodů připojení k této e-mailové adrese; zatímco u nástrojů s příkazovým řádkem je tento proces obvykle manuální. Tento nástroj automaticky zpracuje výsledky od prvního kroku a dále postupuje automaticky až do konce. V případě zkoumané e-mailové adresy Spiderfoot může detekovat, zda s ní bylo nějakým způsobem manipulováno, nebo zda jsou k dispozici informace o emailu ze zdrojů jako je Whois, SecurityTrails nebo Whoisology. V případě zjištěné IP adresy mohou nástroje automaticky vyhledat související názvy domén nebo se dotázat na zdroje informací o hrozbách vůči IP adrese. Spiderfoot pak také zkontroluje, zda je IP adresa zapsána v blacklistu, čímž se zablokuje proti škodlivým IP adresám, které by mohly mít přístup k této síti.[46]

---

[45] Spiderfoot. Spiderfoot [online]. [cit. 2022-07-06]. Dostupné z: https://www.spiderfoot.net/documentation/

[46] TROIA, Vinny. *Hunting Cyber Criminals: A Hacker's Guide to Online Intelligence Gathering Tools and Techniques*. Indianapolis, USA: John Wiley & Sons, 2020, s.84-85.



Obrázek 8 - Výsledky vyhledávání v programu Spiderfoot
Zdroj : https://sf-1ac1c26.hx.spiderfoot.net/

Spiderfoot má vylepšenou placenou verzi Spiderfoot HX, která je běží čistě na cloudu a obsahuje řadu dalších vylepšení a schopností. Vylepšenou rychlost skenování, souběžného skenování více procesů, přehlednější vizualizaci, možnost týmové spolupráce, identifikaci rizik a ještě lepší funkci automatické datové korelace.

Spiderfoot HX je schopen nalézt ještě větší množství výsledků, čímž může zvýšit celkovou kvalitu analýzy, jelikož se ve výsledcích, které jsou v placené verzi navíc může nacházet informace, která bude klíčová.

2.4.6 theHarvester

TheHarvester je open-source nástroj OSINT, který shromažďuje a analyzuje veřejně dostupné e-mailové adresy, subdomény, IP adresy a adresy URL z celé řady zdrojů dat, jako jsou Baidu, Bing, Censys.io, Crt.sh, Dogpile, Google, LinkedIn, NetCraft, PGP, ThreatCrowd, Twitter a VirusTotal. Hlavní výstup informací je zaměřený na firemní e-maily, domény a IP adresy.[47]

TheHarvester je nejspíše jeden z nejlepších dostupných nástrojů pro průzkum s využíváním příkazového řádku. Díky tomu pokrývá velmi širokou

[47] TheHarvester [online]. [cit. 2022-07-07]. Dostupné z: https://github.com/laramies/theHarvester

oblast vyhledávání. TheHarvester používá řadu technik k nalezení informací o svých cílech. Jsou to dorking vyhledávacích nástrojů, útoky DNS bruteforce[48], zpětného vyhledávání domén a hostitelů.

Harvester je nástroj vytvořený v programovacím jazyku Python a lze jej používat v prostředí operačního systému Linux.

Obrázek 9 - Vzhled programu theHarvester
Zdroj : https://www.kali.org/tools/theharvester/

2.4.7 Recon-ng

Recon-ng je jako theHarvester nástroj napsaný v programovacím jazyku Python, dostupný jen na Linuxu. Je to jeden z nejpoužívanějších nástrojů pro shromažďování zpravodajství z otevřených zdrojů. Kombinuje mnoho stejných funkcí jako theHarvester. V Recon-ng se však oproti theHarvesteru musí manuálně načíst a spustit každý modul, který se má použít. Nástroj Recon-ng je dodáván s mnoha vestavěnými moduly uspořádanými podle kategorií, z nichž každý má své vlastní vlastnosti. Recon-ng se užívá zejména pro průzkum a analýzu v širším měřítku. [49]

[48] Technika, kdy se ze seznamu jmen domén vybere subdoména a připojí se k ní její cílový odkaz a na základě odpovědi v novém odkazu určí, zda je odkaz validní nebo ne.
[49] Recon-ng [online]. GitHub. [cit. 2022-07-07]. Dostupné z: https://github.com/lanmaster53/recon-ng

Každý ze 76 modulů Recon-ng má svou vlastní sadu příkazů a možností. Protože je založen na příkazovém řádku, musíte Recon-ng v příkazových řádcích určit, co chcete, aby nástroj dělal, a manuálně vycházet z každé sady výsledků a alternovat vložené příkazy. V současné moduly umožňují v analýze uskutečnit různé typy vyhledávání konkrétních osob, společností, webových stránek, profilů sociálních sítí, domény, úložiště, IP adresy, kontaktní údaje atp.[50]

Recon-ng může používat Bing, Google, Facebook, Instagram, LinkedIn a další online aplikace, jakmile jsou API klíče vloženy do příkazů nástroje. Pomocí klíčů API nástroj umožňuje téměř neomezený přístup ke konkrétním aplikacím, sociálním sítím a vyhledávacím nástrojům. Recon-ng je považován za typický nástroj pro penetrační testery a hackery.

Obrázek 10 - Vzhled programu Recon-ng
Zdroj : https://www.kali.org/tools/recon-ng/

Výhodou použití manuálního přístupu Recon-ng ke shromažďování informací je naprostá kontrola nad přísunem informací, které se nástrojem vrací vyfiltrované zpět. Používání plně automatizovaných nástrojů může být skvělý

[50] Recon-ng [online]. GitHub. [cit. 2022-07-07]. Dostupné z: https://github.com/lanmaster53/recon-ng

způsob jak ušetřit čas. Automatizované nástroje ušetří značné množství času, tím že prohledají oblasti internetu, o kterých by v manuálně provedené analýze člověk ani neuvažoval a mohou tak přinést neočekávané pozitivní výsledky.

Odvrácenou stranou je, že po automatizovaném vyfiltrování relevantních dat může zůstat stále mnoho výsledků, které nejsou úplně relevantní pro určitou analýzu. Poté může být velmi zdlouhavým úkolem zkontrolovat stovky, nebo dokonce tisíce výsledků, jen pro zjištění, že se jedná o výsledky nerelevantní cíli analýzy.

2.4.8 Metagoofil

Metagoofil je nástroj pro shromažďování informací, který umožňuje extrahovat metadata z veřejně dostupných dokumentů na webu. Znovu se jedná o nástroj napsaný v programovacím jazyku Python, dostupný jen na operačním systému Linux. Metagoofil funguje tak, že na Googlu vyhledává dokumenty obsahující potenciálně užitečná metadata. Což je velmi užitečné pro shromažďování zpravodajství z otevřených zdrojů, penetrační bezpečnostní testy nebo určování, jaké data a informace unikají ze souborů organizace či státní instituce do vyhledávacího nástrojů, jako je Google.

Mezi jeho schopnosti patří schopnost ukládat dokumenty lokálně a extrahovat na dálku metadata z široce používaných typů souborů a formátů, zahrnující například, dokumenty Word, seznamy Excel, soubory PDF a mnoha dalších. Z metadat lze pomocí tohoto nástroje extrahovat z dokumentů např. jména, e-mailové adresy, sdílené zdroje a jména serverů.[51]

[51] Metagoofil. GitHub [online]. [cit. 2022-07-08]. Dostupné z: https://github.com/opsdisk/metagoofil

3 Návrhy a doporučení v metodologickém postupu

V případě čerpání informací a analýzy z otevřených zdrojů je samozřejmě v prvé řadě nutné určit cíl každé jednotlivé analýzy. Na základě něj můžeme určit, jakým způsobem bude analýza směřována. Každá analýza nebo vyšetřování má však pokaždé jiný cíl, proto je vždy přesný postup unikátní, zároveň je nutné se v průběhu přizpůsobovat nově nabytým informacím. A tak může analýza směřovat jiným směrem, než bylo podle prvního plánu původně zamýšleno a předpokládáno.

Při používání jednotlivých nástrojů se předpokládá znalost jejich funkcí. V druhé kapitole zmíněné nástroje, jmenovitě Maltego, theHarvester nebo Recon-ng, mají velmi specifická rozhraní a je u nich užitečná komplexnější znalost jednotlivých příkazů k dolování dat. Dotyčný díky tomu může provést analýzu o poznání rychleji a šířeji. Nástroje theHarvester a Recon-ng, ale i nespočet dalších uživateli vytvořených nástrojů (např. na GitHubu), mají další specifikaci v tom, že správně fungují pouze v operačním systému Linux.

Linux je považován mezi lidmi zabývajícími se zpravodajstvím z otevřených zdrojů a programátory za stěžejní operační systém. Linux nabízí mnohem větší variabilitu, je možné jej upravovat podle vlastní potřeby, narozdíl od dalších operačních systémů. Linux je také mnohem bezpečnější a rychlejší, což je pro každého analytika velmi důležité. Linux je vybaven složitým šifrováním, proto je lépe zabezpečen a sám o sobě chrání proti narušení ze stran třetích stran. Stran větší rychlosti Linuxu, operační systém neobsazuje v zařízení tak velkou část paměti jako v operačním systému Windows.

V případech analýz, kdy hrozí riziko úniku osobních údajů, je vhodné využívat Linux. Ve spojení s využitím služeb VPN a tzv. Virtual Machine (virtuálně existující počítač) současně zůstane reálné zařízení, ze kterého je vyhledávání prováděno, v téměř stoprocentním bezpečí. VPN zabezpečí IP adresu, zabrání sledování zařízení a šifruje komunikaci zařízení s internetem. Virtual Machine je rozhraní počítače, které existuje pouze ve virtuálním prostředí

a zabezpečuje zařízení před možným nabouráním se do reálného zařízení. I přes tyto opatření je nutné být ostražitý v případě sdílených souborů mezi virtuálním a reálným zařízením a ve sdílení informací, které by mohly prozradit vlastní identitu nebo jiné osobní údaje.

Zpravodajstvím z otevřených zdrojů můžeme zjistit konkrétní informace o osobách, o jejich emailových adresách, uživatelských jménech, reálných jménech, telefonních číslech, kde se nachází. Současně lze, jak bylo ukázáno v předchozí kapitole, zmapovat určitou událost a zjistit široké množství poznatků o různých problematikách.

Při analýze informací o politické situaci v zemi nebo o válečném konfliktu je třeba použít jiné postupy než při analýze osoby nebo skupiny osob. Samozřejmě se analýzy těchto typů mohou v určitých částech svými metodami a použitím nástrojů překrývat. Princip by však měl být při každé analýze stejný, a to vyhledat a zpracovat informace tak, aby byla analýza odpovídající skutečnosti. U analýz týkající se politických a jinak kontroverzních záležitostí by měl analytik situaci posuzovat objektivně. Což znamená vědomě nezabarvovat analýzu podle osobních preferencí nebo preferencí nadřízených pro které analýzu vypracovává.

Na výběr nástrojů a metod vliv faktor času, který k analýze potřebujeme a který si můžeme dovolit nad analýzou strávit. V krátkém omezeném čase bude analýza probíhat přímým, nejjednodušším možným způsobem, za účelem zisku důležitých informací. Pokud bude třeba širší náhled na cíl analýzy se snahou zjistit více informací, je vhodné využít plný potenciál různých účinných nástrojů. Nelze nikdy nespoléhat na jediný nástroj, vždy je lepší použít nástrojů a metod více, aby se potvrdila, přesnost a úplnost výsledků.

Je také velmi důležité si všechny zjištěné poznatky při analýze informací průběžně zapisovat a ukládat si soubory a zdrojové odkazy, pro budoucí ověření anebo pro zisk dalších informací. Pokud je člověk zaneprázdněn jinými úkony má tendenci zapomínat, proto je vždy lepší si informace zapsat. Podle druhu

analýzy může být vhodné zapsání poznatků na papír, nebo využít aplikací podporující vkládání textových a jiných vizuálních médií. Například v aplikaci Maltego lze ke každé části schématu přidat svoje vlastní poznámky. Nakonec je třeba veškeré výsledky analýzy zkompilovat, uložit veškeré informace a podklady k nim a vyvodit z nich závěry.

4 Praktická část

Tato část diplomové práce je zaměřena na případovou studii týkající se zpravodajství z otevřených zdrojů ve spojitosti s národní bezpečností. Konkrétně je zaměřena na kvalitativní analýzu zdrojů, metod a nástrojů zpravodajství z otevřených zdrojů týkající se aktuální situace stále probíhající války na Ukrajině.

První část je zaměřena na politické projevy státníků a jejich roli, jakožto zdroje informací. Druhá část se zabývá hromadně sdělovacími prostředky a dalšími médii. Třetí část je o tamější roli sociálních sítí a téma poslední části se týká dalších nástrojů, metod a zdrojů informací, které se zabývají aktuálními událostmi a aktivitami konfliktu na Ukrajině. V každé části se analýza zabývá také celkovým kontextem, specifiky a hodnocením spolehlivosti informací; které je třeba brát v potaz v případě čerpání informací o probíhajícím válečném konfliktu.

V kapitolách je krom představení zmíněných zdrojů, metod a nástrojů také užita metoda kvalitativní historicko-komparativní metody. To znamená, že se v podkapitolách metody používané ve válce na Ukrajině snaží přirovnat ke zpravodajství z otevřených zdrojů válečných konfliktů z minulosti, případně zpravodajsky nahlíží na konflikty a jejich ekvivalenty a míru podobnosti.

Válečné konflikty, které mohou být brány v potaz ke komparaci k ukrajinsko-ruskému konfliktu mohou být z období posledních desetiletí. Ke srovnání poslouží zejména válečné konflikty, které probíhali po roce 1990. V některých z těchto konfliktů lze najít jisté ekvivalenty.

Tento časový úsek byl vybrán z důvodu tehdejšího počátku věku internetu, jeho šíření a všeobecnému přístupu k internetu, takřka na celé planetě v dalších dekádách. A tak se situace stala od počátku devadesátých let ve většině států z tohoto pohledu velmi podobnou, tudíž je zde místo k určité komparaci. Díky historickým podobnostem se do jisté míry dá předpovídat další průběh. Otázkou,

která by měla tato část odpovědět tedy je, zda se za tuto dobu obecně zvýšila možnost objektivního zhodnocení informací.

4.1 Historický kontext

Téma ukrajinské samostatnosti zůstalo sporné i po referendu o nezávislosti v prosinci 1991, a to zejména kvůli dlouhodobé a otevřené nelibosti ze strany Ruska. Po rozpadu socialistického východního bloku se většina bývalých východoevropských satelitů Sovětského svazu systematicky integrovaly do západních institucí, jako je EU a NATO.

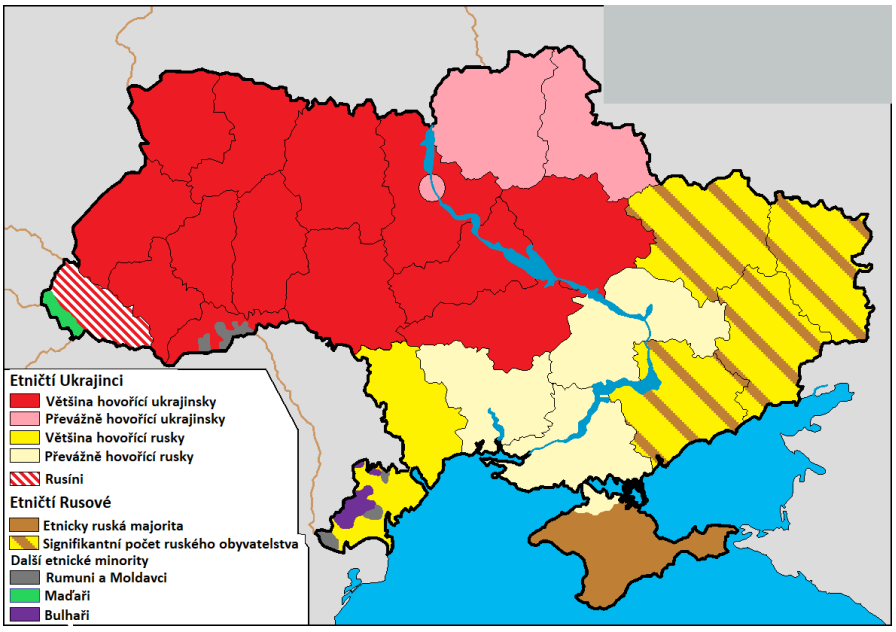
Po rozpadu celého Sovětského svazu bylo Rusko uvrženo do politické nestability s velkými ekonomickými problémy spojené s přechodem z plánované ekonomiky, navíc řešilo jiné územní problémy na některých pohraničních regionech, proto nebyla tolik aktivní na mezinárodní scéně při jiných probíhajících světových konfliktech.

Po nástupu Vladimira Putina na post prezidenta Ruska začala postupně získávat zpět svou ekonomickou stabilitu, s tím znovu započala ruská snaha o vliv na své ztracené území Sovětského svazu a na státy bývalého východního bloku. Což zahrnovalo i Ukrajinu. Rusko nepřijalo revoluční odstranění demokraticky zvoleného, k Rusku nakloněného, Viktora Janukovyče a zesílení prozápadní orientace na Ukrajině. Nestabilita a konflikt jsou typickou charakteristikou ukrajinsko-ruských vztahů od pádu Sovětského svazu.

Mezi několika dalšími problémy, které udržely ukrajinsko-ruské vztahy na špatné úrovni, hrály významnou roli formální likvidace aktiv a dluhů Sovětského svazu, energetický dluh Ukrajiny, strach možného rozšíření NATO na východ, vymezení hranic mezi oběma národy a situace ruské menšiny na Ukrajině. Ruské využívání násilného občanského konfliktu v zemích v relativní blízkosti Ruska je prostředek k růstu svého vlivu v postsovětských státech. Tímto způsobem pak dokáže Rusko snižovat vliv západních zemí.

Moskva preferuje stabilní a přátelské sousedství a snaží se zmenšovat počet méně servilních, a pro Rusko nežádoucích prozápadních sousedních států. Zranitelnost Ukrajiny spočívá v celkové rozpolcenosti. Ukrajina je ovlivňována z různých směrů – EU a NATO ze západu a Ruska z východu. Což spolu s vnitřními problémy Ukrajiny, jako je socioekonomická krize, korupce, neefektivní a slabé státní instituce a národnostní rozpolcenost obyvatelstva, vedlo zemi do těžkých dob.

Rozpolcenost obyvatelstva v Ukrajině je možné vidět i na demografické etnolingvistické mapě, která zobrazuje většinově ukrajinsky mluvící obyvatelstvo v západní a severozápadní části země. A většinově rusky mluvící obyvatelstvo na východě a jihovýchodě země. Což automaticky neznamená, že je obyvatelstvo nakloněno na jednu či druhou stranu konfliktu, spíše to jen zdůrazňuje nejednoduchost řešení konfliktu.



Obrázek 11 - Etnolingvistická mapa Ukrajiny s legendou
Zdroj : https://commons.wikimedia.org/wiki/File:Ethnolingusitic_map_of_ukraine.png

V roce 2010 se prezidentem stal Viktor Janukovyč, s čímž jeho odpůrci nesouhlasili a dožadovali se zneplatnění výsledků voleb. Koncem roku 2013 započala další vlna protestů na Ukrajině v důsledku toho, že její vláda odmítla

podepsat novou dohodu s EU. Krize na Ukrajině pak v roce 2014 vyústila ve parlamentním svržení prezidenta Viktora Janukovyče. Ten poté z Ukrajiny utekl.

Následný podpis obchodní dohody s EU jako prvním kroku k členství prozatímní vládou (prozápadní) v únoru přispělo k ruskému zahájení okupace Krymu a podporu separatistických hnutí ve východní části Ukrajiny jako nástroj pro ochranu etnicky ruské menšiny. V dubnu téhož roku byl Krym Ruskem dobyt a v letech 2015 byla podepsána Ruskem, Ukrajinou, Francií a Německem Minskou dohoda o příměří, která přímý vojenský konflikt na nějakou dobu oddálila.

V dubnu 2019 byl prezidentem Ukrajiny zvolen Volodymyr Zelensky. V lednu 2021 ukrajinský prezident Zelensky požádal o vstup do NATO, což vedlo k tomu, že Rusko nashromáždilo vojska na ukrajinských hranicích pod záminkou výcviku vojenských jednotek. Rostoucí napětí mezi západními zeměmi, Ruskem a Ukrajinou pomalým, ale stálým tempem vedlo nejprve k ruskému uznání nezávislé Luhanské a Doněcké lidové republiky 21. února 2022 a k ruské invazi Ukrajiny dne 24. února 2022. V reakci na tento útok západní spojenci Ukrajiny oznámili tvrdé finanční sankce vůči Rusku, jako jsou restrikce vůči ruské centrální bance, vyloučení velkých ruských bank z globálního platebního systému a zákaz vydávání víz ruským občanům“.

4.2 Politické projevy

Projevy a další politická vystoupení se dají využít jako zdroj informací a jejich analýza a výklad jako metoda zpravodajství z otevřených zdrojů. Analýzou těchto veřejných vystoupení, zejména analýzou jejich slovního obsahu, ale i povahou jejich prezentace, můžeme vyčíst záměry představitelů státu a dalších konkrétních osob a celkově predikovat další vývoj událostí. Na základě toho, ale hlavně ve spojení s dalšími druhy zpravodajství lze poté lépe ověřit či dále rozšířit plejádu predikativních scénářů dalšího vývoje a lépe tak chránit národní bezpečnost.

Politický projev je dlouhodobě využívaným politickým nástrojem po celém světě. Ač by se mohlo zdát, že jsou politické projevy jen plné prázdných slov, které kromě demonstrace moci nemají příliš význam, tak je tomu právě naopak. Alespoň tedy u válečných konfliktů mají tyto projevy významný vliv na průběh války, mohou vyjádřit jakým způsobem bude vláda postupovat, mohou zmást nepřítele a vyvolat moment překvapení, který může nepřítele ochromit.

Veřejný projev může mít nesmírný pozitivní i negativní vliv na obyvatelstvo v rámci psychologické války, jelikož charakteristickým rysem politického projevu je, že jsou nezřídka určeny pro širší veřejnost. Vliv na jejich postoje a morálku může být cílen nejen na vlastní obyvatelstvo, ale i na lidi po celém světě.

Proto musí každá země a její bezpečnostní složky analyzovat politické projevy představitelů států, které by mohly evokovat přímý nebo nepřímý vliv na jejich funkci a stabilitu. Ve stejnou chvíli není možné spoléhat pouze na politický projev jako zdroj informací, je nutné to, co bylo řečeno porovnat se skutečným stavem událostí a s dalšími zpravodajskými metodami. Není totiž výjimkou, že tyto projevy mohou obsahovat lživé a zavádějící informace, které mohou situaci v realitě eufemizovat nebo nadhodnocovat.

Funkce politického projevu z hlediska strategie při válečném konfliktu, tak mohou na cílové publikum působit psychologickým nátlakem, přetvářkou; legitimizací, bagatelizací nebo distancováním se od svých aktivit. Nebo naopak delegitimizací a zavržením aktivit svého nepřítele.[52]

V posledních desetiletích se na veřejných politických projevech podílí týmy osob, které předem tvoří texty tak, aby měli zamýšlený vliv na masy lidí a splnili svůj účel v co největším rozsahu. Celkově se musí přizpůsobit celý text tak, aby odpovídal metodologiím z rétorické, lingvistické, sémantické a psychologické stránky. Každý věta a slovní obrat musí přesně zacílit na určené vjemy. Všechny

[52] SCHÄFFNER, Christina a Paul CHILTON. *Discourse Studies: A Multidisciplinary Introduction*. Vol.2. Londýn, UK: Sage Publications, 1997 s. 206-210.

fráze musí být přesné a jasné, aby projevy neobsahovaly dvojité významy a nemohli být cílovým publikem pochopeny jiným způsobem než bylo zamýšleno. Samozřejmě za předpokladu, že určitý dvojsmysl není do projevu vložen plánovaně.

Pronesený politický projev a zmíněné faktory je možné analyzovat a dle toho dosadit poznatky z jiných zpravodajských analýz. A zda je možné indikovat další směřování a predikovat kroky, které měl projev předznamenávat. Lze ověřit celkovou validitu projevu, analýzou toho, zda projev má nebo nemá relevantní a podložené důkazy, jako je popis situace v projevu, ověření zmíněných statistik, uvedených příkladů proběhlých událostí. Celkově je však nejdůležitější zhodnotit cíl projevu, ať už obsahuje spíše faktické nebo zavádějící informace. Politický projev má informovat společnost, ale i přesvědčit o správnosti kroků, které budou nebo byly učiněny.

Řečníky jsou obvykle vládnoucí politici, ministři nebo jejich zmocnění zástupci. Cestou projevu mohou hovořit k členům a příznivcům stejných politických a ideologických stran a frakcí, což by bylo příkladem tzv. vnitřní politické komunikace. Dalším druhem projevu je sdělení, které oslovuje celý národ nebo se snaží šířit své slovo a poselství svého projevu ideálně po celém světě, aby o něm všichni věděli. Takový projev kombinuje prvky vnitřní a vnější politické komunikace. Mezi takový typ politického patří mezistátní politická komunikace, kdy například politický zástupce svým projevem působí na politiky a veřejnost během návštěvy v zahraničí.[53]

Lidé v současné době obecně očekávají, že řečník bude ve svém projevu věcný, měl by se spíše vyhnout příliš emocionálním výzvám a vyjadřováním čistě osobních názorů. Místo toho očekává jasnou artikulaci obecně přijímaných hodnot a norem a šíření postojů zaujímaných celou zemí jako takovou. Předpokládá se, že se dotyčný dokáže povznést nad svůj osobní politický názor a za všechny občany své země. Pouze mimo tyto oficiální politické projevy, se

[53] SCHÄFFNER, Christina. *Analysing Political Speeches*.. Londýn, UK: Multilingual Matters, 1997 s. 63-64.

osoba s reprezentačními povinnostmi může pokusit nastavit méně formální diskusi v určitých tématech, kde nehrozí žádná nedorozumění a může tak působit na publikum ve svém zájmu mnohem lidštěji.

4.2.1 Rusko

Vladimir Putin ve svém hodinu trvajícím projevu, který pronesl necelé tři dny před zahájením ruské invaze na Ukrajinu, hovořil o veškerých důvodech a záminkách, které Rusko nutí do již naplánovaných vojenských a dalších akcí vůči samostatnému ukrajinskému státu. Tomuto projevu předcházely, jak již bylo zmíněno, měsíce vojenských šarád na ruském území v blízkosti Ukrajiny. Projev zdůvodňoval pochyby Ruska o legitimitě podle něj agresivního a nacionalistického ukrajinského vedení země, hranicích území Ukrajiny, obchodech Ukrajiny a krádeži ruského plynu atp. [54]

Zdůraznil ohrožení, které ukrajinské vedení země znamená pro Rusko, o ukrajinské genocidě na ruské obyvatelstvo, vlivu tzv. Západu na Ukrajině a o stavbě vojenské infrastruktury na území Ukrajiny, která může Rusko ohrozit v řádů několika minut. Projev byl ukončen pronesením o uznání nezávislosti Luhanské a Doněcké lidové republiky, které v té době byli z velké části de facto a celkově de iure ukrajinské. Vzhledem k tomu, že se již před tímto projevem mluvilo o ruské invazi na Ukrajinu a plánu obklíčit hlavní město Kyjev a v samotném projevu Putin hovoří o nemožnosti řešení donbaského problému jinak než vojensky, tak tento projev posloužil jako takové stvrzení pro ostatní státy, že k invazi v blízké době dojde.[55] A opravdu k ní 24. února v ranních hodinách došlo. Vladimir Putin od té doby užívá projevy k ruskému národu, kterým zdůrazňuje hrdost a sílu Ruska a nutnost Ruska bojovat proti současnému ukrajinskému zřízení. K aktuálnímu vývoji se pak v průběhu doby

[54] Address by the President of the Russian Federation. Kremlin [online]. 21.2.2022 [cit. 2022-07-10]. Dostupné z: http://en.kremlin.ru/events/president/news/67828

[55] RYŠÁNEK, Adam. Rusko plánuje největší válku v Evropě od roku 1945, tvrdí Johnson. *Seznam Zprávy* [online]. 20.2.2022 [cit. 2022-07-10]. Dostupné z: https://www.seznamzpravy.cz/clanek/zahranicni-rusko-planuje-nejvetsi-valku-v-evrope-od-roku-1945-tvrdi-johnson-189307

z pozice Ruska veřejně vyjadřují zejména mluvčí prezidenta, ministři ruské vlády a jejich mluvčí.

Ekvivalentem situace těsně před začátkem konfliktu například ta z počátku devadesátých let před iráckou invazí 2. srpna 1990 do Kuvajtu. Irácký prezident Saddám Husajn ve svém projevu 17. července 1990 hrozil použitím síly vůči arabským zemím těžícím ropu, aby omezili objem těžby ropy, jelikož tím úmyslně snižují její cenu a škodí tak jejich ekonomice. Irák v té době nebyl nedlouho po válce s Íránem v dobré ekonomické situaci. Irák obvinil Kuvajt, že krade jejich ropu, protože s využitím šikmých vrtů těží ropu z iráckého území. Stejně jako Putin tak již s předstihem odůvodňoval či omlouval před světem svoji invazi do Kuvajtu, který byl a je stejně jako Ukrajina samostatným státem s územní suverenitou. Přitom již mohli ostatní státy, i na základě veřejného projevu Saddáma Husajna, řešit opatření z hlediska národní bezpečnosti, které by pro ně plynula z tehdy ještě teoretického válečného konfliktu.

Druhým obdobným příkladem je situace před válkou v Iráku, Taktéž světová velmoc a její spojenci užili velmi vratké záminky k agresivním útoku na menší nezávislý stát. Také 17. března 2003 došlo k projevu tehdejšího prezidenta George Bushe o nedodržení podmínek a zmínění důvodů pro útok na Irák. Tento projev předcházel invazi zahájené 20. března 2003.[56]

4.2.2 Ukrajina

Prezident Ukrajiny Volodymyr Zelensky využívá síly projevu ve více směrech. Již fakt, že hlavní představitelé zůstali na území Ukrajiny a neutekli do bezpečí exilu vyslalo signál ostatním zemím, že je Ukrajina schopna se bránit a má tak smysl je v rámci ochrany vlastní národní bezpečnosti podporovat. Svými projevy z hlavního města směrem k ukrajinským obyvatelům se podařilo udržet relativně vysokou morálku v rámci boje, která zdá se, že byla jedním z faktorů neúspěšného dobytí hlavního města Kyjev a donutila Rusko zaměřit se

[56] A transcript of George Bush's war ultimatum speech from the Cross Hall in the White House. Guardian [online]. 18.3.2003 [cit. 2022-07-12]. Dostupné z: https://www.theguardian.com/world/2003/mar/18/usa.iraq

hlavně na ovládnutí Luhanské a Doněcké oblasti a dalších regionů na východě Ukrajiny. Tyto projevy jsou sdíleny a sledovány zejména přes sociálních sítě a televizní vysílání.

Dále se svými projevy snaží apelovat na ostatní státy Evropy, USA a další mocnosti, aby jim byla poskytnuta pomoc v co největší míře. Zajímavým, předtím nevídaným způsobem jsou projevy představitelů Ukrajiny, přímo účastných nebo na dálku vysílaných v parlamentech různých zemí. V nich politici děkují jednotlivým parlamentům za materiální pomoc a podporu, apeluje na nutnost jejich kontinuální pomoci. Upozorňuje na nebezpečí rozšíření válečného konfliktu do Evropy v případě ukrajinské prohry a ujišťuje, že se Ukrajina nehodlá vzdát bez boje. Tyto politické projevy byly velmi důležité pro zvýšení celkové důvěry dalších států, a mají vliv i na její občany.[57] [58] [59]

Tím u spojeneckých zemí zvyšuje potenciál toho, co jim může být v blízkém budoucnu poskytnuto na obranu jejich země. Na základě toho se mohou tímto válečným konfliktem ovlivněné státy zařídit, měnit různá opatření a poskytnout přiměřenou pomoc jiné zemi, aby byl negativní dopad na jejich zemi a obyvatelstvo co nejmenší.

4.3 Hromadně sdělovací prostředky

Obecně je v kontextu všech válečných konfliktů problematické získávání stoprocentně pravdivých a objektivních informací z hromadně sdělovacích prostředků. U konfliktu na Ukrajině máme dvě hlavní strany konfliktu Rusko a Ukrajinu. Jako spojenci Ruska a Ukrajiny poté stojí další desítky zemí, které

---

[57] Speech by President of Ukraine Volodymyr Zelenskyy at the NATO Summit. *President of Ukraine* [online]. 24.2.2022 [cit. 2022-07-13]. Dostupné z: https://www.president.gov.ua/en/news/vistup-prezidenta-ukrayini-volodimira-zelenskogo-na-samiti-n-73785

[58] DOKUMENT: Přepis projevu Volodymyra Zelenského před oběma komorami českého parlamentu. *ČT 24* [online]. 15.6.2022 [cit. 2022-07-14]. Dostupné z: https://ct24.ceskatelevize.cz/domaci/3506574-dokument-prepis-projevu-volodymyra-zelenskeho-pred-obema-komorami-ceskeho-parlamentu

[59] SHAH, Hasit. Full text of Ukrainian president Volodymyr Zelenskyy's speech to the US Congress. Quartz [online]. 16.3.2022 [cit. 2022-07-14]. Dostupné z: https://qz.com/2142992/transcript-of-volodymyr-zelenskyys-speech-to-the-us-congress/

jejich aktivity podporují nebo odsuzují. Každý z těchto států má vlastní veřejnoprávní a komerční média, která čerpají své informace ze svých zdrojů různé kvality. Některá média mají mnohem větší sledovanost než jiná, to bohužel neznamená, že více sledovaná média mají přímou úměrou také důvěryhodnější informace.

Samotné hlavní dvě strany konfliktu a jejich státní média, obzvlášť v době války, mají tendence zkreslovat realitu, a tak přímo ovlivňují nejednoduchost analýzy informací z nich a také vnímání veřejnosti. Hromadně sdělovací prostředky tak mohou složit státu a být zapojeni v informační válce záměrně. Nebo mohou nevědomky šířit informace, většinou převzaté odjinud, které byly původně vytvořeny, aby působily klamně a médium tento klam neodhalilo. Selektivní výběr proběhlých událostí, zveličování škod způsobených protivníkem, nebo naopak neinformování o dílčích neúspěších a snižování čísel o vlastních ztrátách může být při válečném konfliktu velice obvyklou praxí.[60]

Když informace ze státních médií Ruska a Ukrajiny spojíme s informacemi šířenými z ostatních zemí, může vzniknout nepřehledná směs navzájem si odporujících informací. Ty je nutné vyfiltrovat pomocí vlastních znalostí, metod analýz informací na základě hodnocení jejich důvěryhodnosti a použitím dalších zpravodajských metod.

4.3.1 Rusko

Ruská svoboda tisku od nástupu Vladimira Putina k moci na začátku století pouze zhoršovala, a to jak z pohledu žebříčku mezinárodních organizací, tak z pohledu opatření, která byla implikována za období jeho vlády. Za příklad se dají uvést zákon z roku 2013, který kriminalizuje urážlivý veřejný postoj vůči

[60] BEDNÁŘ, Jaroslav. Vývoj mediálního obrazu válečných konfliktů a reflexe jeho utváření v českých internetových denících [online]. Olomouc, 2020 [cit. 2022-07-14]. Dostupné z: https://theses.cz/id/vr2zau/Bednar_Jaroslav_BP.pdf. Bakalářská. Univerzita Palackého v Olomouci. Vedoucí práce Mgr. Eva Lebedová, Ph.D.

náboženství, věřícím, patriarchům a kněžím pravoslavné církve.[61] Dále, současně hojně využívaný zákon vydaný v roce 2012, který opravňuje státní instituce vyžadovat registraci na ruském ministerstvu spravedlnosti a čtvrtletní hlášení o činnosti od nevládních organizací zabývajících se politickými záležitostmi. Což vedlo k tomu, že všechna opoziční ruská média, která nesouhlasila s vládní politikou, prezidentem a jejich kroky, byla ruské veřejnosti nuceně představena jako tzv. zahraniční agent.[62]

Od roku 2022 nutnost registrace do seznamu zahraničních agentů může zahrnovat i jiné formy aktivit, navázaných na činnost zahraničními médii. Jsou tak posuzovaný se zahraničními médii shodné organizační, metodické, vědecké, technické nebo jiné postupy, nejen příjem finančních prostředků nebo majetku. Znamená to taktéž, že i jednotlivci mohou být uvedeni jako zahraniční agenti, i když nejsou nikým ze zahraničí placeni. Zákon stanoví sankce pouze za šíření názorů, což posuzují příslušná rozhodnutí ruských úřadů.[63]

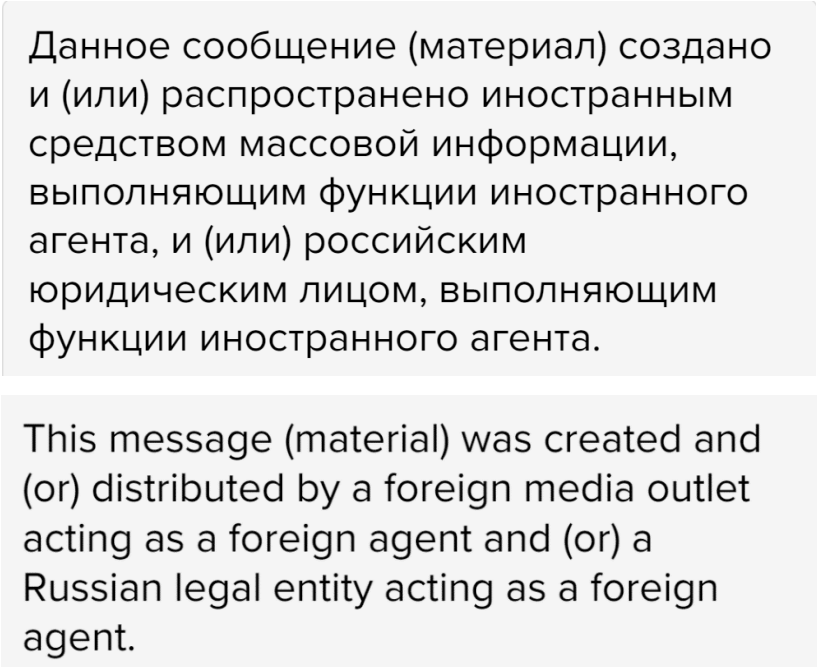
Tato média, pokud chtěla dále informovat své čtenáře, musela před každý článek na svých internetových platformách umístit do záhlaví upozornění, že se jedná o ‘článek vytvořený zahraničním médiem, distribuován zahraničním agentem jednající prostřednictvím ruské právnické osoby, která vykonává činnost zahraničního agenta‘. Zákon tím chtěl v ruském čtenáři evokovat, že práce určitého média může být škodlivá pro ruské zájmy a jedná tak ve prospěch cizí země. A to nehledě na to, že je informace pravdivá či ne, nebo se článek týká nepolitického tématu nerelevantní k situaci v Rusku.

---

[61] SCHRECK, Carl. Holy Slight: How Russia Prosecutes For 'Insulting Religious Feelings'. *Radio Free Europe* [online]. 2020 [cit. 2022-07-11]. Dostupné z: https://www.rferl.org/a/russia-prosecuting-insults-to-religious-feelings/28678284.html

[62] GALPEROVICH, Danila. Russia Using Foreign Agent Law to Attack Journalism, Media Say. Voice of America [online]. 10.7.2022 [cit. 2022-07-12]. Dostupné z: https://www.voanews.com/a/press-freedom_russia-using-foreign-agent-law-attack-journalism-media-say/6206858.html

[63] Russia tightens legislation on 'foreign agents'. Deutsche Welle [online]. 29.6.2022 [cit. 2022-07-12]. Dostupné z: https://www.dw.com/en/russia-tightens-legislation-on-foreign-agents/a-62307066



Obrázek 12 - Záhlaví nacházející se u článků od tzv. zahraničních agentů
Zdroj : https://meduza.io/

Počátkem války, kdy Rusko porušilo jednu z hlavních zásad mezinárodního práva, a to zákaz hrozby silou a použití síly, veškerá média samozřejmě informovala o tomto vpádu ruských vojsk na Ukrajinu. Ta média, která psala o této agresi ze strany Ruska jinak než státem řízená média byla perzekvována. Jejich internetové platformy, kam byly sdíleny jejich články, byly na území Ruska státní institucí *Roskomnadzor* zablokovány. Mezi hojně čtená ruská média, která byla zablokována v prvních týdnech války na Ukrajině patřila např. Meduza, Dozhd nebo Novaya Gazeta. Tato média se přesídlila mimo území Ruska, aby mohla dále vykonávat svoji činnost a dále o situaci v Rusku informují z exilu.

V podstatě jediná média dnes působící v Rusku bez cenzury jsou ta vlastněna státem, a to jak tištěná, tak digitální. Nebo soukromá média, která přistoupila na pravidla stanovená ruským zřízením.

Média, která chtějí na ruském území tvořit zpravodajství tak musí souznít s názorem sdíleným v ruských státem řízených médiích nebo pod silnou autocenzurou, jinak by byla zablokována. Autocenzura se týká konkrétních zakázaných témat a používaných slov.

To platí pro ruské i zahraniční firmy nebo sociální sítě informující o ruské politice a konfliktu na Ukrajině. Na počátku března byl vydán zákon, kdy za sdílení nepravdivých informací o ukrajinském konfliktu, kde hrozí odnětí svobody až do výše až 15 let.[64]

4.3.2 Ukrajina

Ukrajina se jako většina zemí Evropy, jejíž bezpečnost je díky ruskému vpádu na Ukrajinu pod přímým útokem, rozhodla pro absolutní zablokování všech stránek, které šířily informace vyprodukované Ruskem a ruskými státními médii.

Ukrajinská mediální scéna je různorodá, ale zůstávala z velké části ve vlastnictví oligarchů. To se ve vývoji posledních měsíců změnilo, jelikož se nejbohatší oligarcha Rinat Achmetov vzdal svých licencí televizních kanálů Media Group Ukraine ve prospěch ukrajinské vlády. Achmetov tak udělal z důvodu zákonu vydaného v roce 2021, který má za cíl omezit vliv oligarchů. A tak jsou nejsledovanější média v zemi v současné době spravována státem.[65]

„Na Ukrajině ani před válkou nevládla zrovna nejvyšší úroveň svobody projevu. Informační válka s Ruskem degradovala ukrajinské mediální prostředí už před ruskou invazí. Média považovaná za prokremelská byla prezidentským dekretem zakázána a přístup k ruským sociálním sítím byl omezen. Na začátku ruské invaze byla pak média s ruskou propagandou zablokována. Ruská armáda se totiž při invazi zaměřila i na novináře, média a telekomunikační infrastrukturu, aby zabránila ukrajinskému obyvatelstvu v přístupu ke zprávám a informacím.“[66]

---

[64] Putin Signs Law Introducing Jail Terms for 'Fake News' on Army. The Moscow Times [online]. 4.3.2022 [cit. 2022-07-13]. Dostupné z: https://www.themoscowtimes.com/2022/03/04/putin-signs-law-introducing-jail-terms-for-fake-news-on-army-a76768

[65] BALMFORTH, Tom. Ukraine's richest man announces his holding's exit from media business. The Moscow Times [online]. 11.7.2022 [cit. 2022-07-13]. Dostupné z: https://www.reuters.com/business/media-telecom/ukraines-richest-man-announces-his-holdings-exit-media-business-2022-07-11/

[66] Ukraine. Reporters Without Borders [online]. 2022 [cit. 2022-07-14]. Dostupné z: https://rsf.org/en/country/ukraine

Většina zemí Evropy, jejich populace i vlády má obecně kladnější postoj vůči Ukrajině, proto může hrozit, že informace, které nehovoří v prospěch Ukrajiny mohou být v médiích záměrně upravovány nebo se o nich v hromadně sdělovacích prostředcích nebude vůbec psát. Což neznamená, že se takový jev musí objevovat při jakékoliv informaci z probíhající války, proto je třeba si informace ověřovat.

Senzacechtivost některých hromadně sdělovacích prostředků na počátku války vytvořila několik zkreslených příběhů o incidentech, které proběhly nebo měly proběhnout při válečných střetech armád Ukrajiny a Ruska.

Příkladem se dají uvést dvě dezinformace, které byly po celém světě sdíleny na internetu a další masových médiích a uváděly se jako stoprocentně pravdivé. První je situace z Hadího ostrova, kde podle zpráv z druhého dne války hrdinsky zahynulo 13 ukrajinských vojáků, potom co se odmítlo vzdát Rusům po výzvě ruské válečné lodi. I prezident Ukrajiny Zelensky podle tehdejších informací padlé bojovníky in memoriam vyznamenal.[67] Ve skutečnosti však byli ukrajinští vojáci, bránící Hadí ostrov zajati, aby pak byli na konci března ve výměně zajatců vydáni zpět ze zajetí.[68]

Druhým příkladem je případ letce tzv. Ghost of Kiev (Kyjevský Duch). Mělo jít o velmi výjimečného stíhacího pilota. Údajně od začátku invaze sám sestřelil zhruba 40 ruských letadel. Ukrajinské vládní účty na sociálních sítích opakovaně šířily příběh o tomto letci. V médiích se poté spekulovalo o jakého letce se jedná a zda bylo pro letce vůbec možné takového čísla sestřelů dosáhnout. Později byla tato zpráva vyvrácena s tím, že v prvních týdnech války Ukrajina

[67] Snake Island: Ukraine says troops who swore at Russian warship are alive. BBC [online]. 28.2.2022 [cit. 2022-07-14]. Dostupné z: https://www.bbc.com/news/world-europe-60554959
[68] CHAPPELL, Bill. Snake Island sailors are freed as Ukraine and Russia conduct a prisoner exchange. National Public Radio [online]. 24.3.2022 [cit. 2022-07-14]. Dostupné z: https://www.npr.org/2022/03/24/1088593653/snake-island-sailors-freed-prisoner-swap

potřebovala příběh, který by zvýšil ukrajinskému lidu odvahu a morálku a v tom jsou tyto hrdinské příběhy o národních hrdinech účinné.[69]

To vše je samozřejmě racionálně pochopitelné, avšak hromadně sdělovací prostředky, které tuto zprávu sdíleli jako stoprocentně pravdivou, by měly ztratit část své kredibility. Pokud jsou schopny šířit nepravdivé informace při méně podstatných událostech, jaká jistota může být, že v budoucnu budou sdílet pouze pravdivé informace. Především v situacích, kde budou informovat o zásadních událostech, nebo o situacích, které ve velké míře mohou médium ovlivnit.

Proto je vhodné využívat metody hodnocení spolehlivosti zdrojů a jeho informací. Na základě toho se zvlášť posoudí spolehlivost média jako celku a poté jednotlivě důvěryhodnost každé relevantní zprávy. Na základě toho vznikne kombinace, díky které je možné systematicky ohodnotit jednotlivé informace podle známek. Na základě toho pak ve spojení s dalšími zjištěními lze posoudit, zda je informace použitelná pro zpravodajskou analýzu.

Spolehlivý	*Není pochyb o autenticitě, důvěryhodnosti nebo kompetentnosti zdroje; v minulosti naprosto spolehlivý.*
Obvykle spolehlivý	*Menší pochybnost o autenticitě, důvěryhodnosti nebo kompetentnosti zdroje; v minulosti poskytoval většinou validní informace.*
Docela spolehlivý	*Pochybnost o autenticitě, důvěryhodnosti nebo kompetentnosti zdroje, ale v minulosti zdroj poskytoval validní informace.*
Nepříliš spolehlivý	*Významné pochybnosti o autenticitě, důvěryhodnosti nebo kompetentnosti zdroje, v minulosti zdroj poskytoval validní informace.*
Nespolehlivý	*Zdroj bez autenticity, důvěryhodnosti a kompetence; historie nevalidních informací.*
Nelze posoudit	*Zdroj ještě nebyl ověřen. Neexistuje žádné hodnocení spolehlivosti zdroje.*

Tabulka 1 - Dělení hodnocení spolehlivosti zdroje

[69] LAURENCE, Peter. How Ukraine's 'Ghost of Kyiv' legendary pilot was born. BBC [online]. 1.5.2022 [cit. 2022-07-15]. Dostupné z: https://www.bbc.com/news/world-europe-61285833

Potvrzené	*Potvrzeno jinými nezávislými zdroji; sám o sobě logický; v souladu s dalšími informacemi ve stejné věci.*
Pravděpodobné	*Nepotvrzeno; logický sám o sobě; v souladu s dalšími informacemi ve stejné věci.*
Nejspíše pravdivé	*Nepotvrzeno; samo o sobě relativně logický; shoduje se s některými dalšími informacemi ve stejné věci.*
Spíše nepravdivé	*Nepotvrzeno; možné, ne však logické; žádné další informace ve stejné věci.*
Nepravděpodobné	*Nepotvrzeno; samo o sobě nelogické; v rozporu s jinými informacemi ve stejné věci.*
Dezinformace	*Neúmyslně nepravdivé; samo o sobě nelogické; v rozporu s jinými informacemi ve stejné věci; potvrzeno dalšími nezávislými zdroji.*
Klam	*Úmyslně nepravdivé; v rozporu s jinými informacemi ve stejné věci; potvrzeno dalšími nezávislými zdroji.*
Nelze posoudit	*Neexistuje žádný podklad pro hodnocení důvěryhodnosti informace.*[70]

Tabulka 2 - Dělení hodnocení důvěryhodnosti informace

Což podle výše uvedených tabulek v praxi znamená, že je vhodné si zdroj a samotnou informaci oznámkovat. Takže podle této metody hodnocení zdroje spolehlivého (známka 1) po neposouditelný (známka 6). A u informace potvrzené (známka 1) po neposouditelnou (známka 8). Pokud tedy máme více informací ke stejnému tématu, můžeme si systematicky informace rozdělit a oznámkovat, což může pomoci ke kvalitněji vypracované analýze. Stejná metoda lze použít u všech informací, ať pocházejících z hromadně sdělovacích prostředků nebo sociálních sítí.

4.4 Sociální sítě

Sociální sítě jsou ve válce na Ukrajině naprosto stěžejní zdroj informací o jejím vývoji. Nejaktuálnější informace přímo od osob přítomných v místech střetů jsou sdíleny téměř okamžitě po tom co se udají. Tyto informace z terénu jsou poté dále sdíleny a později bývají se zpožděním použity jako součást zpravodajství hromadně sdělovacích prostředků. Touto cestou mohou i státy a jejich státní instituce sdílet informace a instrukce svým obyvatelům, ale i dalším lidem, kteří se zajímají o různé válečné a politické konflikty probíhající na planetě.

[70] US DEPARTMENT OF THE ARMY. Open-Source Intelligence [online]. Washington, DC: Army Techniques Publication, 2012 [cit. 2022-07-17]. S.8 Dostupné z: https://irp.fas.org/doddir/army/atp2-22-9.pdf

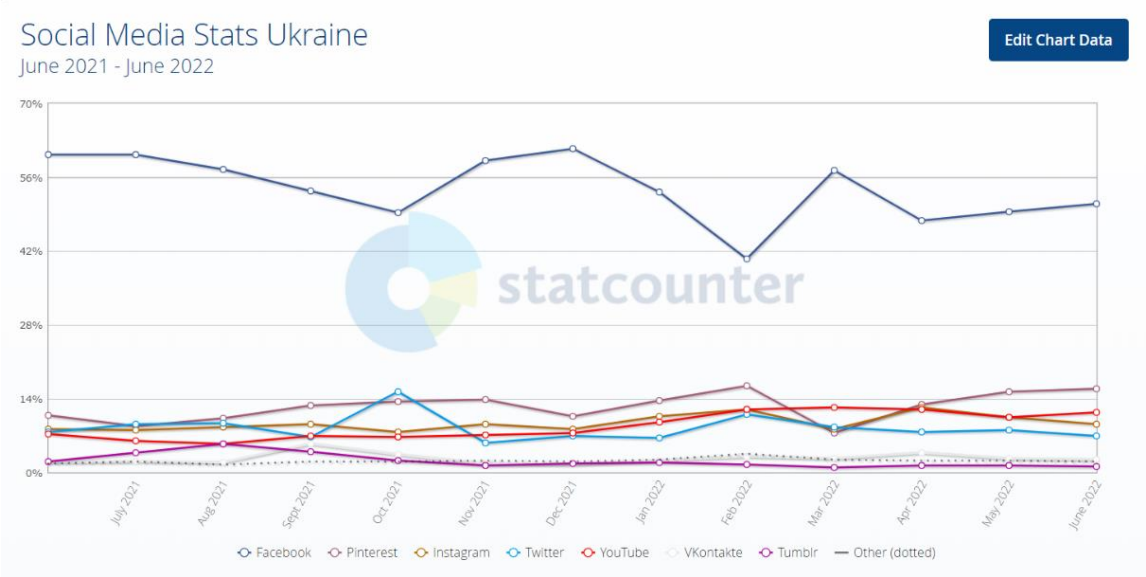
Vzhledem k tomu, že v současné době využívá služeb sociálních sítí více než 4,5 miliardy lidí, je možné najít informace o situaci v zemích na celé planetě.[71] I pro obyvatele z chudých oblastí planety jsou technologie a internet čím dál dostupnější a počty uživatelů sociálních sítí tak stále stoupají. Sdílením různých mimořádných situací na sociální sítě a možnosti jejich zobrazení tak poté mohou sloužit jako užitečný a mnohdy i důvěryhodnější zdroj než stále nejvíce využívané hromadně sdělovací prostředky. Stejně jako u hromadně sdělovacích prostředků je vhodné využívat metodiku důvěryhodnosti informací a spolehlivosti zdrojů.

A právě to je pro tento válečný konflikt charakterističtější než kdy v minulosti. O událostech neinformují z velké části pouze lidé s novinářskými licencemi nebo zaměstnaní v masmédiích, díky sociálním sítím může sdílet informace z místa konfliktu v podstatě kdokoliv s elektronickým zařízením a přístupem na internet. V historickém srovnání není mnoho mezistátních válečných konfliktů, které by měly takovou míru událostí zdokumentovaných na sociální sítě přímo z bojiště, které byly sdíleny primárně na sociální sítě. Srovnatelným způsobem se dostávali do povědomí společnosti informace z války v Karabachu v roce 2020. Informování v dřívějších válečných konfliktech a jejích následcích byly primárně sdíleny několika hromadně sdělovacími prostředky, až poté se informace šířily do prostředí sociálních sítí.

Co se týče války na Ukrajině, relevantních sociálních sítí, ze kterých lze čerpat je velké množství. Jak Ukrajinci, tak Rusové využívají sociální sítě velmi rozšířeně. Obyvatelé na Ukrajině využívají zejména globální sociální sítě, nejvíce Facebook, poté s velkým odstupem Pinterest, YouTube, Instagram a Twitter.[72] Okrajově je využívána i ruská sociální síť VKontakte, ta je však na území Ukrajiny oficiálně zablokována a je třeba využít přesměrování VPN, aby bylo možné sociální síť zobrazit. Pro Ukrajinu jsou sociální sítě důležité, jelikož dokáží

[71] KEMP, Simon. Digital 2022: Global Overview Report. Data Reportal [online]. 26.1.2022 [cit. 2022-07-18]. Dostupné z: https://datareportal.com/reports/digital-2022-global-overview-report
[72] Social Media Stats Ukraine. StatCounter [online]. [cit. 2022-07-18]. Dostupné z: https://gs.statcounter.com/social-media-stats/all/ukraine

informovat obyvatelstvo Ukrajiny o dění, pomáhá udržovat vnější podporu ze strany cizích států a pomáhá zachovat odhodlání vzdorovat Rusku a vyvracet možné dezinformace.



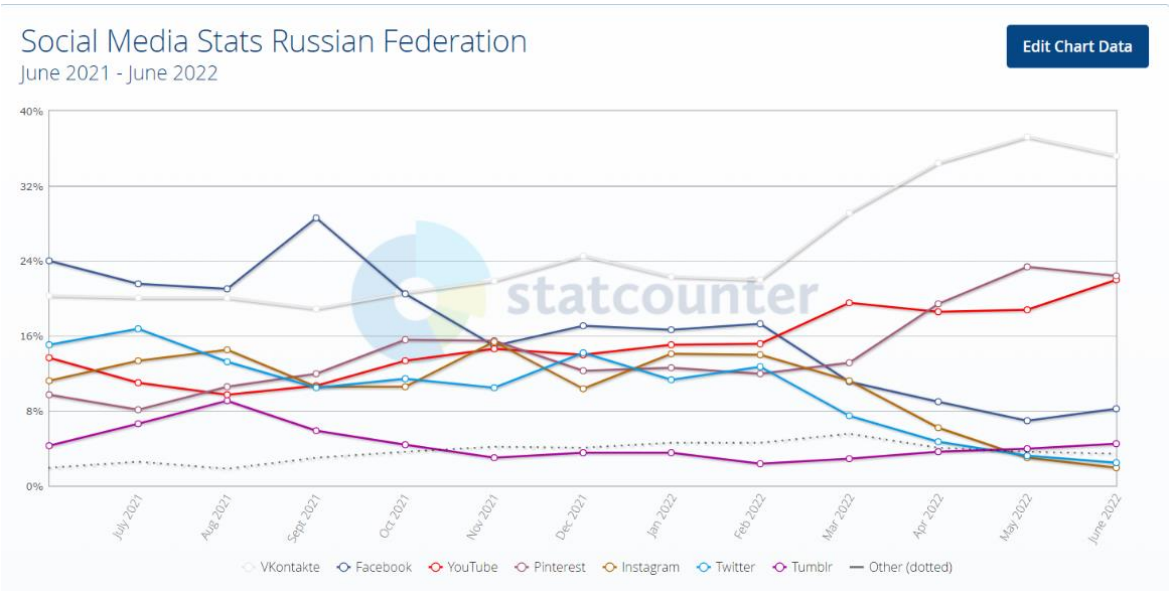
Obrázek 13 - Percentil obyvatel využívajících sociálních sítí na území Ukrajiny
Zdroj : https://gs.statcounter.com/social-media-stats/all/ukraine

Naopak Rusové používají po zablokování sociálních sítí vlastněných americkou firmou Meta (Facebook, Instagram), která byla ruskými úřady prohlášena za extremistickou organizaci, v drtivé většině ruské sociální sítě VKontakte a Odnoklassniki.[73] Znovu platí, že zablokované sociální sítě mohou být z ruského území zpřístupněny pouze pomocí VPN služeb. Tyto ruské sociální sítě propojují ruské obyvatele a další rusky hovořící osoby ze zemí bývalého Sovětského svazu.

VKontakte, známý také jako VK byl velmi populární i před zablokováním jiných sociálních sítí. Funkce a vzhled jsou dost podobné Facebooku, vyhledávací nástroje a informace uvedené na účtech se z velké části také shodují. Uživatelé mohou zůstat v kontaktu s přáteli, přispívat do skupin, zveřejňovat zprávy, fotografie a videa a další soubory na soukromých nebo veřejných profilech. Další ruskou sociální sítí, kterou je třeba zmínit, jsou

[73] Social Media Stats Russian Federation. StatCounter [online]. [cit. 2022-07-18]. Dostupné z: https://gs.statcounter.com/social-media-stats/all/russian-federation

Odnoklassniki, kterou používají hlavně dospělí Rusové. Jejím hlavním účelem je udržovat kontakt s přáteli a hledat bývalé kolegy nebo staré přátele.



Obrázek 14 - Percentil obyvatel využívajících sociálních sítí na území Ruska
Zdroj : https://gs.statcounter.com/social-media-stats/all/russian-federation

Analýzou těchto sociálních sítí lze například získat další informace o vojácích bojujících na Ukrajině, kteří mohli páchat válečné zločiny nebo zločiny proti lidskosti a přiřadit jim reálnou identitu. Díky několika hackerským útokům a dalším únikům tajných dat ruské armády a dalších ruských státních institucí jsou známa jména a další osobní informace desítek tisíc vojáků všech šarží.[74]

Jak již bylo v zmíněno, ruský veřejný prostor je pod dohledem cenzury a jakékoliv vyjádření a články, které svým obsahem odporují ruské vládě a jejím krokům mohou být důvodem k trestnímu stíhání.

Pro konflikt na Ukrajině se pro zpravodajství z otevřených zdrojů ukázaly jako stěžejní sociální sítě Telegram, Twitter, Reddit nebo audiovizuální sociální sítě TikTok a Youtube, zejména z důvodu snadného sdílení obsahu s krátkým

[74] CHIRINOS, Carmela. Anonymous takes revenge on Putin's brutal Ukraine invasion by leaking personal data of 120,000 Russian soldiers. Fortune [online]. 4.4.2022 [cit. 2022-07-18]. Dostupné z: https://fortune.com/2022/04/04/anonymous-leaks-russian-soldier-data-ukraine-invasion/

popisem a možností diskuze uživatelů pod každým z příspěvků. Některým z těchto sociálních sítí se budou šířeji věnovat následující podkapitoly.

4.4.1 Telegram

Na Telegramu je většina obsahu šifrovaná soukromá komunikace mezi jednotlivci. Byla zde však přidána služba kanálů a ty se staly uživatelsky populárními. Kanály mohou být veřejně viditelné a v mnohých případech zahrnují obsah sdílený z jiných sociálních sítí a webových stránek.

Telegram je jednou z nejpopulárnějších sociálních aplikací na Ukrajině a v Rusku. Je to bezplatná cloudová aplikace, která uživatelům umožňuje odesílat a přijímat zprávy, hovory, fotografie, videa, audio a další soubory. Zprostředkovává veřejné a soukromé skupiny až 200 000 uživatelů, kde mohou jednotlivci posílat zprávy a komunikovat. A také kanály, které umožňují jednosměrné vysílání odběratelům kanálu. Prostřednictvím těchto skupin a kanálů mohou organizace oslovit stovky tisíc lidí pomocí zpráv, živých vysílání a dalších audiovizuálních souborů.

Telegram však nabízí i další vrstvu zabezpečení prostřednictvím funkce „tajného chatu“. Když je toto povoleno, komunikace mezi dvěma uživateli bude šifrována end-to-end. Tato data nejsou uložena nikde kromě zařízení odesílatele a příjemce. Nemá k němu přístup ani Telegram. Uživatelé mohou také nastavit časované zprávy na tajných chatech. Jakmile čas uplyne, komunikace navždy zmizí.

Telegram je využíván jako nástroj protestu v dobách konfliktů a útlaku. Mnoho Rusů začalo používat tuto aplikaci pro příjem nezávislé informace po zásahu Kremlu proti svobodným médiím s tím, že tajný chat zabezpečuje svobodné šíření jejich názorů bez nucené autocenzury.

Ukrajinský prezident a další členové vlády Ukrajiny využívají Telegram k informování o aktuálním vývoji. Telegram je také cenný pro ukrajinskou

armádu, protože může pomoci něj obejít ruské sledování a provádět zpravodajské operace. Ruské pronikání do ukrajinských telekomunikačních sítí bylo během invaze všudypřítomné.

Ruská vláda provozuje kanály Telegram pro státní média, včetně zpráv Sputnik a RT, agentury TASS a vyzvala uživatele, aby sledovali na Telegramu jejich obsah.[75]

4.4.2 Twitter

Twitter je sociální síť určená pro sdílení krátkých příspěvků do 280 znaků. Každý den se na Twitter sdílí zhruba 867 miliónů příspěvků (tweetů), z čehož se nemalá část zabývá tak mediálně známým konfliktem na Ukrajině.[76] Například od počátku konfliktu 24. února 2022 do 8. března 2022 bylo podle automatického nástroje naprogramovaného k vyhledávání konkrétních klíčových slov (např. ukraine, russia, putin, zelensky, Україна, Київ atp.), sdíleno přes 63 milionů tweetů.[77]

Z nich lze vyčíst jak postoj konkrétních účtů a osob k tomuto konfliktu, lze z nich analyzovat informace týkající se aktivit ve válečných regionech. Z tweetů z nich lze analyzovat postoj a další postup vlád jednotlivých zemí, jelikož má mnoho politiků a státních institucí svoje twitterové účty. V případě válečných konfliktů je z politiků vhodné sledovat účty vlád zainteresovaných zemí, prezidentů a ministrů, zejména jejich ministerstva zahraničí a obrany. Také mnohé hromadně sdělovací prostředky sdílí zprávy a odkazy na své webové stránky prostřednictvím těchto tweetů.

---

[75] BERGENGRUEN, Vera. How Telegram Became the Digital Battlefield in the Russia-Ukraine War. The Time [online]. 21.3.2022 [cit. 2022-07-18]. Dostupné z: https://time.com/6158437/telegram-russia-ukraine-information-war/

[76] YAQUB, M. How Many Tweets per Day 2022 (New Data). The Time [online]. 8.7.2022 [cit. 2022-07-18]. Dostupné z: https://www.renolon.com/number-of-tweets-per-day/

[77] CHEN, Emily a Emilio FERRARA. Tweets in Time of Conflict: A Public Dataset Tracking the Twitter Discourse on the War Between Ukraine and Russia [online]. Marina del Rey, CA, USA: University of Southern California, Information Sciences Institute, 2022 [cit. 2022-07-18]. Dostupné z: https://arxiv.org/pdf/2203.07488.pdf

Při vyhledávání informací z Twitteru lze využít vyhledávacího nástroje, ten dokáže vyhledat jednotlivé účty a tweety, osoby podle jejich jména, klíčových slov, lokace, hashtagů a data sdílení. Twitter má také mnohé externí nástroje a postupy, které dokáží zjednodušit práci při získávání informací z Twitteru. Lze jimi například zobrazit již smazané a jiným způsobem nedostupné tweety; zobrazí tweety konkrétního uživatele na jedné webové stránce, zobrazí uživatelova oblíbená témata v jeho feedu, zobrazení společných sledujících a sledovaných dvou zvolených účtů atp.[78]

Ze zdrojů informací na Twitteru je za poslední měsíce obrovské kvantum tweetů zmiňující válku na Ukrajině nebo diskutující o celkové problematice dalších jevů, na které má konflikt celosvětově vliv. Ovšem je hned několik konkrétních účtů, které o válce na Ukrajině zprostředkovávají pravidelné příspěvky. Mezi příklady těchto twitterových účtů patří:

1. *Váleční zpravodajové* – účty, které sdílí tweety o válečném vývoji, postupu ruských a ukrajinských vojsk, video a fotodokumentaci vojenské techniky – *@IAPonomarenko*, *@ua_industrial*, *@RALee85*, *@Osinttechnical*, *@Blue_Sauron*, *@TheStudyOfWar*, *@jmvasquez*
2. *Ukrajinské mediální platformy – @UKRINFORM*, *@KyivIndependent*, *@KyivPost*
3. *Ruské mediální platformy* (*státem vlastněné*) – *@RT_com*, *@SputnikInt*, *@tassagency_en*
4. *Ruské mediální platformy* (*ostatní*) - *@meduza_en*, *@MoscowTimes*
5. *Účty se zvláštním zaměřením* - *@UAWeapons* – účet sledující a dokumentující využití vojenské techniky, jejím původem a přesným názvem; případy zničení nebo ukořistění ruské vojenské techniky ukrajinskou armádou; *@GeoConfirmed* – účet sdílející potvrzené přesné lokace z válečných událostí na Ukrajině, která byla zdokumentována na videích a obrázcích sdílených na internetu

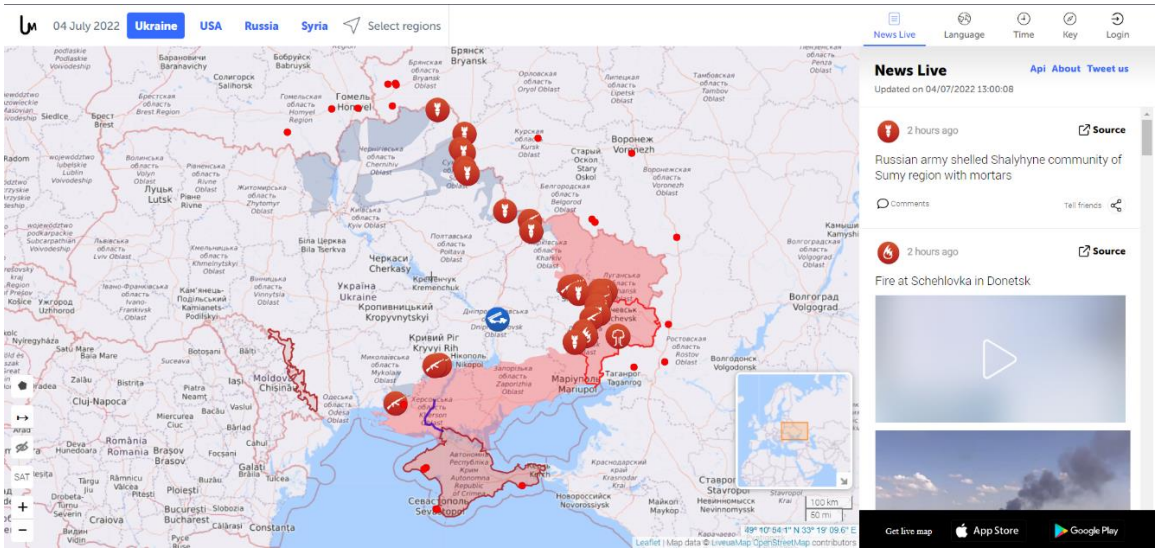
[78] BAZZELL, M. *Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information*. Ninth edition. 2022, s.185-201.

4.5 Nástroje a zdroje

4.5.1 Liveuamap

Liveuamap je velmi užitečný nástroj, kterým je možné chronologicky sledovat vývoj událostí na Ukrajině. Tento nástroj byl vytvořen v roce 2014 ukrajinskými žurnalisty a softwarovými vývojáři, kteří působí zejména mimo území Ukrajiny. Projekt jako takový má název Live Universal Awareness Map. K vyhledávání relevantních informací a analyzování dat jsou využívány automatizované webové nástroje, které jsou následně ověřeny a postoupeny fact checkingu, dle oficiálních stránek Liveuamap, odbornými analytiky. Zároveň se ověřováním zabraňuje duplicitě informací nebo zobrazení nerelevantní informace, kvůli např. shodě slov.

Od roku 2014 působnost svého nástroje postupně rozšířil o další světové regiony. Nástroj se dá efektivně využít zejména v regionech, v nichž probíhají válečné a jiné konflikty. Krom v této době nejsledovanějšího konfliktu na Ukrajině lze sledovat aktualizace z bojů v Sýrii, Izraele a Palestiny, Kavkazu, Kašmíru, Libye, Afghánistánu, Íráku a mnoha dalších. Krom vojenských aktivit také sleduje vládní rozhodnutí jednotlivých zemí, aktivity dalších nestátních aktérů, ve státech bez probíhajících válečných konfliktů sleduje zprávy o kriminálních aktivitách, přírodních katastrofách, protestech a celkové politické situaci.



Obrázek 15 - Mapa Liveuamap.com vyobrazující hranice válečné fronty na Ukrajině dne 4.července 2022, s ikonami zobrazující události se sloupkem napravo, kde jsou tyto události chronologicky seřazeny. Zdroj : https://liveuamap.com/

Pro uživatele se na stránce o konkrétním regionu zobrazí mapa s vytvořenými upozorněními upřesňující lokaci incidentu nebo vydání například vydání důležitého prohlášení. Tento incident je poté možné samostatně zobrazit. Okénko incidentu zobrazuje čas, ve který informace vyšla najevo, krátký odstavec s jádrem informace a zdroj ze kterého automatizovaný systém čerpal.

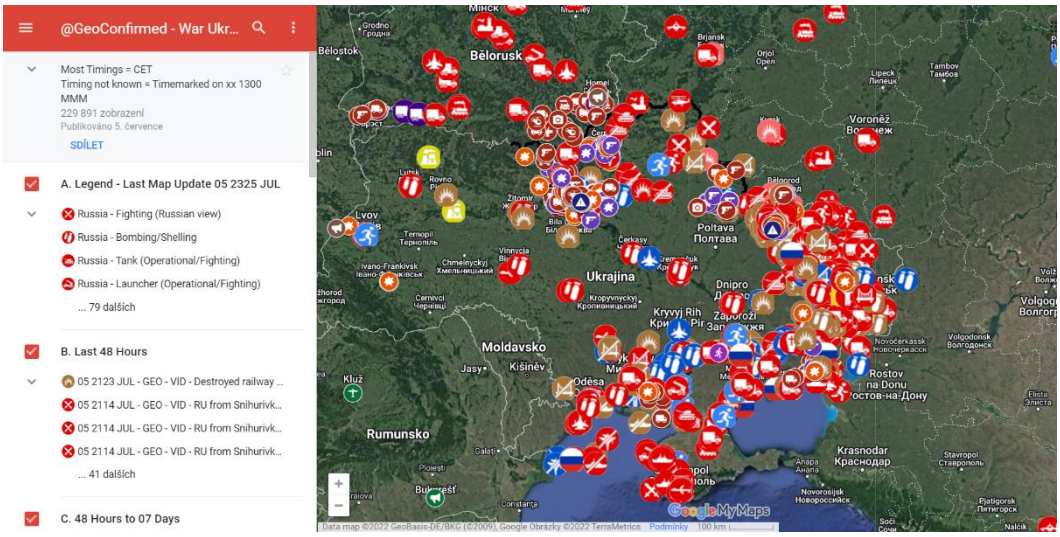
Případně je v incidentu vyobrazen odkaz na audiovizuální soubor, který je možno si pomocí výchozího pluginu ihned zobrazit. Osoba provádějící zpravodajství z otevřených zdrojů tak může sama ověřit, odkud se daná informace nachází, zda je pravdivá a zda se dá zdroj považovat za důvěryhodný.

4.5.2 Geoconfirmed

Nástrojem podobným Liveuamap je GeoConfirmed. Tento nástroj je celkově unikátní tím, že je tvořen komunitou nadšenců zabývajících se zpravodajstvím z otevřených zdrojů. Jeho účelem je přesně alokovat proběhlé události, které byly nafoceny nebo natočeny na video a třídit informace o proběhlých událostech v mnoha aspektech válečného konfliktu na Ukrajině.

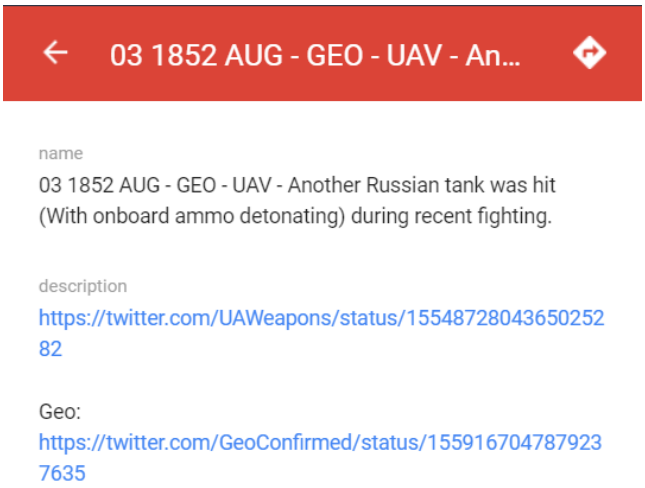
Většina těchto příspěvků je sdílena na sociálních sítích, nejčastěji je to Twitter, Telegram, TikTok, Youtube atp. Na základě nich je porovnáno video nebo obrázek se snímky z aplikace Google Maps, pokud bylo místo alokováno a její souřadnice jsou sdíleny na Twitter a dále přidány do mapy, kde se roztřídí podle druhu události.

Typy událostí se dělí na ruské a ukrajinské ztráty na životech, ruská a ukrajinská zničená vojenská technika a vojenská infrastruktura, pohyby a pozice ruských jednotek, civilní ztráty na životech, zničená civilní infrastruktura; zaznamenané bombardování, ostřelování a exploze; střelba, záznamy z boje; snímky z proběhlých výměn zajatců a kde k nim došlo, masové hroby a další místa pohřbených osob atp.



Obrázek 16 - Mapa GeoConfirmed s ikonami zobrazující události se sloupkem nalevo, kde jsou tyto události chronologicky seřazeny.
Zdroj : https://www.google.com/maps/d/u/0/viewer?mid=10YK14-QB25penu8jeS4hBVarzGKZsVgj&ll=48.00921100052718%2C-17.637229600000005&z=4

Do databází těchto map může přidávat informace každý, pouze se musí řídit postupem, který je sdílen správci tohoto projektu na jejich twitterovém profilu @GeoConfirmed. Přidaný obsah je pravděpodobně moderován, aby byly všechny přidané informace průkazné a se správně zanesenou lokací. Po potvrzení je událost uložena do mapy na Google Maps.



Obrázek 17 - Detail ikony zobrazující událost, doplněny odkazem k příspěvkům s důkaznými materiály potvrzující přesnou lokaci události.
Zdroj : https://www.google.com/maps/d/u/0/viewer?mid=10YK14-QB25penu8jeS4hBVarzGKZsVgj&ll=48.883412000000014%2C38.23492900000001&z=8

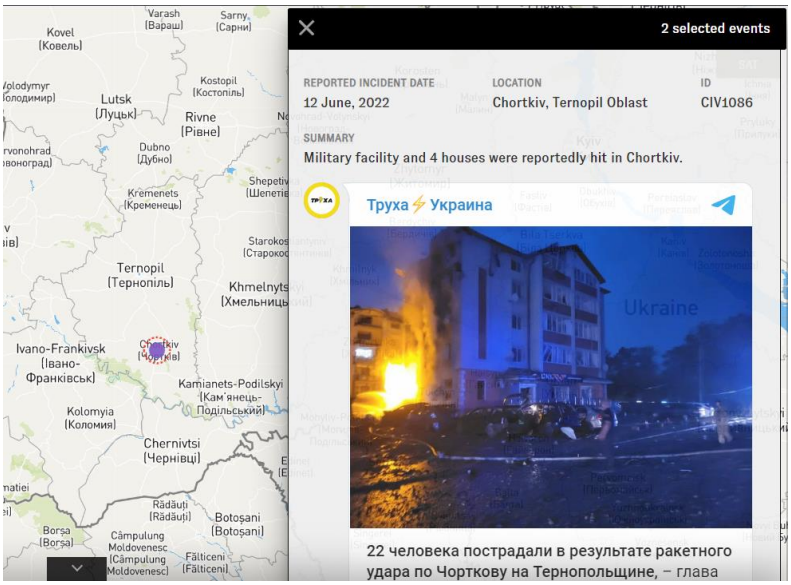
4.5.3 Mapa civilních škod

Tato mapa vykresluje a zdůrazňuje události, které měly za následek potenciální civilní dopad nebo újmu od doby, kdy Rusko zahájilo svou invazi na Ukrajinu. Podrobné incidenty byly shromážděny výzkumníky Bellingcat. Na mapě jsou zahrnuty případy, kdy byly poškozeny nebo zničeny civilní oblasti a infrastruktura, tam kde jsou viditelná zranění civilistů, nebo je přítomnost nehybných civilistů. Shromažďování incidentů obsažených v této mapě začalo 24. února 2022. Uživatelé mohou prozkoumat události podle data a místa. [79]

Uživatelé mohou nastavit časovou osu ve spodní části mapy tak, aby se zaměřila na události, které se staly v konkrétních dnech. Kliknutím na konkrétní den se na pravé straně obrazovky objeví seznam událostí, které se dni udály a byly dostatečně podloženy a zdokumentovány. Uživatelé nástroje si mohou také zobrazit události podle týdenních, dvoutýdenních, jednoměsíčních a tříměsíčních období. Na mapě se poté objeví vyznačení oblastí fialově vyplněnými kruhy v oblastech, čím větší jsou, tím více se události v určité lokaci událo. [80]

[79] Civilian Harm in Ukraine. Bellingcat [online]. 2022 [cit. 2022-07-18]. Dostupné z: https://ukraine.bellingcat.com/

[80] Hospitals Bombed and Apartments Destroyed: Mapping Incidents of Civilian Harm in Ukraine. Bellingcat [online]. 17.3.2022 [cit. 2022-07-18]. Dostupné z: https://www.bellingcat.com/news/2022/03/17/hospitals-bombed-and-apartments-destroyed-mapping-incidents-of-civilian-harm-in-ukraine/



Obrázek 18 - Legenda události na mapě civilních škod zobrazující a popisující událost se zdrojem informace.
Zdroj : https://ukraine.bellingcat.com/

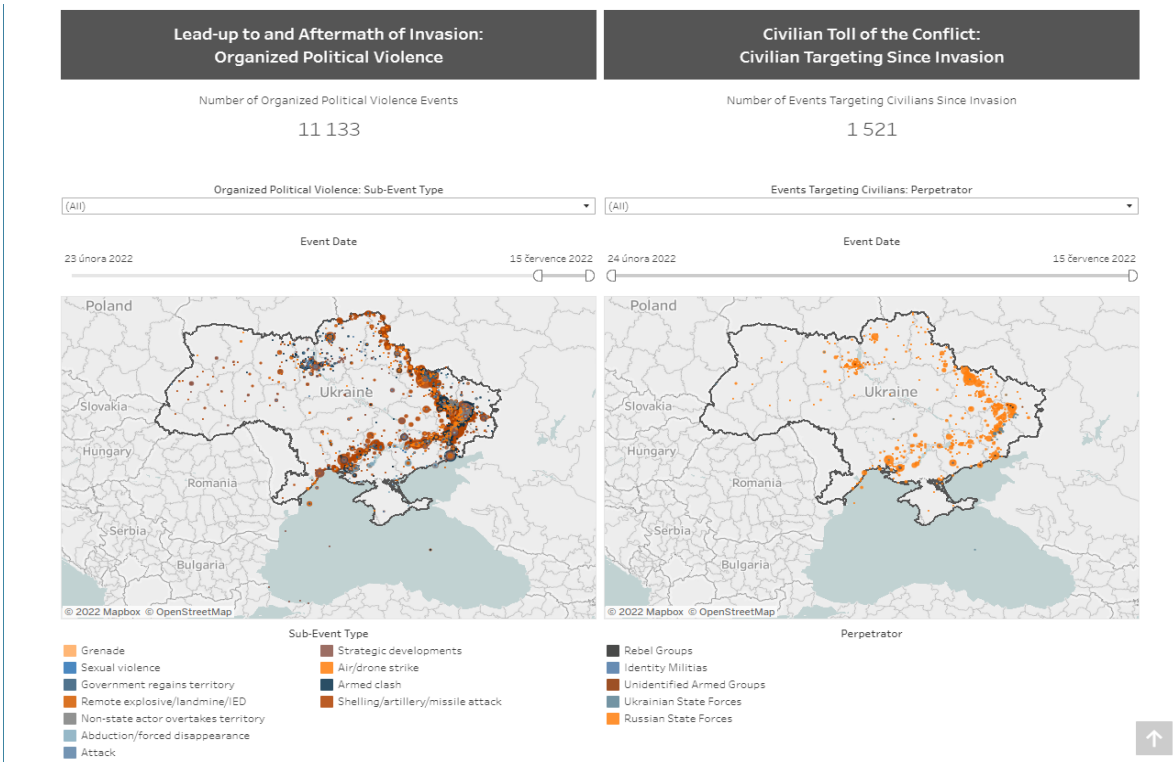
Filtry na levé straně obrazovky také umožňují vyhledávat na časové mapě podle konkrétních typů incidentů. Filtry například umožňují vybrat události, které poničily obytná, průmyslová, zdravotnická zařízení atd. Ty se pak objeví na mapě s ostatními odfiltrovanými výsledky.

Pokud lze s jistotou zjistit druh munice nebo zbraně, které způsobily civilní újmu nebo škodu je to také uvedeno v zobrazené události. Uživatelé mohou používat filtry k vyhledávání konkrétních typů zbraňových systémů, které mohly být nasazeny, jako je kazetová munice, řízené střely nebo dokonce ruční zbraně.

4.5.4 ACLED

ACLED neboli The Armed Conflict Location & Event Data Project je projekt shromažďování, analýzy a krizového mapování po celém světě. ACLED shromažďuje data o místech, úmrtích, všech hlášených násilných dalších protestních politických akcí po celém světě a jejich aktérech a účastnících.

ACLED všechny svoje analýzy sdílí na svých platformách a jsou veřejně přístupné bez jakýchkoliv poplatků.[81]



Obrázek 19 - Mapa organizace ACLED vyobrazující polohu a povahu událostí proběhlých na Ukrajině od počátku války do 15.7.2022 s barevně znázorněnými legendami.
Zdroj: https://acleddata.com/ukraine-crisis/

Co se týče konfliktu na Ukrajině jsou na dostupné reporty jednotlivých týdnů války, vývoj na frontě, na jakých místech probíhají intenzivní boje, mapa událostí a informací v týdnu, statistiky proběhlých událostí a jejich grafická zobrazení. Jako zdroje jsou využívány oficiální dokumenty ukrajinských, ale i ruských vojenských jednotek, které vytváří denní zprávy podrobně popisující např. porušování příměří spáchané proti cílům na územích, která ovládají.

Jejich hlášení obecně nehlásí směr palby ani zpětnou palbu z druhé strany. Dalším zdrojem jsou denní reporty organizace Organizace pro bezpečnost

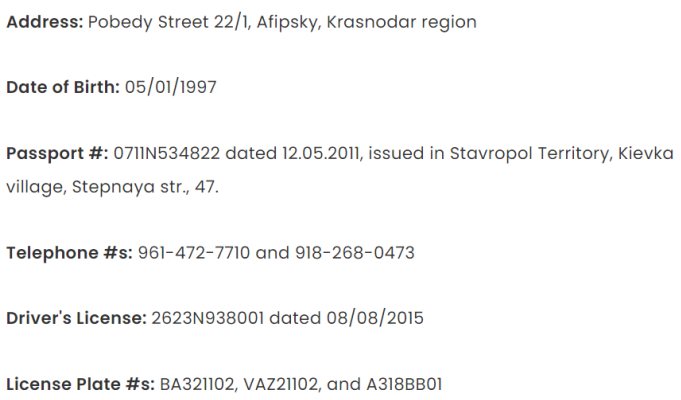
[81] ACLED History: [online]. The Armed Conflict Location & Event Data Project, 2022, 1 s. [cit. 2022-07-18]. Dostupné z: https://acleddata.com/acleddatanew//wp-content/uploads/dlm_uploads/2021/11/ACLED-History_v2_February_2022.pdf

a spolupráci v Evropě a dalších nespecifikovaných zdrojů, které přímo informují z místa události o konkrétních škodách nebo obětech.[82]

4.5.5 Cargo200

Cargo200 (topcargo200.com) je internetová stránka, která zaznamenává potvrzené ztráty vysoce postavených vojáků na ruské straně v konfliktu na Ukrajině. Tyto informace byly shromážděny pomocí zpravodajství z otevřených zdrojů s přídavkem pravděpodobného využitím uniklých informací o mnohých ruských vojácích, díky proběhlým hackerským útokům na databáze. Jedná se o vojáky od generálů, plukovníků, podplukovníků, majorů až po důstojníky. Je v nich uvedeno celé jejich jméno; jednotka či rota, které byli součástí, jejich fotografie; u některých datum narození, vzdělání, životopis a číslo jejich odznaku.

Část stránky se zabývá ruskými oligarchy, kteří zemřeli z různých důvodů od počátku války na Ukrajině. V poslední řadě jsou zde podrobněji vypsáni i lidé, kteří by podle autora stránky spáchali válečné zločiny. Je zde popsán důvod proč tomu tak je, důkazový materiál, ještě podrobnější popis těchto osob, čísla pasu, čísla řidičských oprávnění, partneři vojáků, odkaz na jejich sociální sítě apod.


Address: Pobedy Street 22/1, Afipsky, Krasnodar region

Date of Birth: 05/01/1997

Passport #: 0711N534822 dated 12.05.2011, issued in Stavropol Territory, Kievka village, Stepnaya str., 47.

Telephone #s: 961-472-7710 and 918-268-0473

Driver's License: 2623N938001 dated 08/08/2015

License Plate #s: BA321102, VAZ21102, and A318BB01

Obrázek 20 - Příklad údajů uvedených u jednoho z ruských vojáků.
Zdroj: https://topcargo200.com/

[82] ACLED Methodology and Coding Decisions around Conflict in Ukraine [online]. The Armed Conflict Location & Event Data Project, 2022, 9 s. [cit. 2022-07-18]. Dostupné z: https://acleddata.com/acleddatanew//wp-content/uploads/dlm_uploads/2021/11/ACLED-History_v2_February_2022.pdf

Využití takového typu informací může pomoci při představě o ztrátách vysoce postavených vojáků a predikcích o schopnostech velení ruské armády v budoucnu. U zemřelých oligarchů může ukazovat, v případě podezřelých úmrtí, na vnitřní politické rozbroje a snahu odstraňovat osoby, které například nesouhlasí nebo přímo bojují proti ideám a povaze směřování ruské politiky. V případě potvrzených či domnělých osob, které spáchaly válečné zločiny, je hlavní motivací této stránky shromáždit a uložit zde informace o nich a důkazy o domnělých zločinech, které mohou ve výsledku sloužit k jejich odsouzení.

Závěr

V práci jsem dokázal pomocí literárních a internetových zdrojů shrnout v současné době aktuální a relevantní zdroje, metody a nástroje obecně a také z hlediska konkrétního zaměření na konflikt na Ukrajině. Cílem mé diplomové práce bylo představit a vytvořit ucelený obraz o zpravodajství z otevřených zdrojů, primárně zaměřený na získávání dat z elektronických zdrojů a jejich zpracování.

V obecné části práce byly popsány základní pojmy týkající se zpravodajství a národní bezpečnosti. Následně se práce zabývala zpravodajstvím z otevřených zdrojů, kde jsem popsal princip, na kterém funguje, zdroje tohoto typu zpravodajství a výhody a výzvy spojené s prací s informacemi z otevřených zdrojů.

Konkrétněji jsem se zaměřil na problematiku, princip platforem a vyhledávání dat a informací na sociálních sítích, Deep Webu a Dark Webu. Uvedl jsem také mnohé jejich nástroje, které lze na těchto platformách použít a jaké data a informace na nich lze nalézt. V návaznosti na to jsem uvedl několik široce používaných softwarových nástrojů, kde jsem uvedl jakým způsobem se používají a který typ dat a informací z nich lze získat.

V praktické části diplomové práce jsem se zaměřil na případovou studii zahrnující kvalitativní analýzu zdrojů, metod a nástrojů zpravodajství z otevřených zdrojů, týkající se aktuální situace stále probíhajícího konfliktu na Ukrajině. Proto považuji vše, co jsem si v úvodu práce zadal, za splněné.

Je nezbytné dodat, že o tématu jsem čerpal čistě z odborné literatury a dalších veřejně přístupných zdrojů, takže je můj vhled na reálnou praxi při zpravodajství z otevřených zdrojů, prováděných například v rámci činnosti bezpečnostních sborů, v některých ohledech omezený.

V dnešní době je, kvůli technologickému posunu a velkému množství produkovaných dat, nutné neustále přizpůsobovat metody a aktualizovat funkčnost nástrojů. Je třeba využívat více automatizovaných procesů, aby shromažďování a zpracovávání informací bylo rychlé a použitelné pro libovolné účely. Pokud se zkoumají mezinárodní vztahy, mezinárodní konflikty, socioekonomické poměry ve státech, je také potřebná vysoká úroveň znalosti dané problematiky. A na to nepomohou ani ty nejlepší zdroje, metody a nástroje pro zpravodajství z otevřených zdrojů.

Taková znalost, porozumění a schopnost dosazování si informací do méně omezeného kontextu však není přesně měřitelná. Kvůli neměřitelnosti úrovně znalosti celkové problematiky mohou být některé informace na sociálních sítích a v hromadně sdělovacích prostředcích označeny za pravdivé a skutečné, když nejsou; nebo pravdivé informace za dezinformaci a “fake news“. Měla osoba nebo více osob, kteří rozhodli o pravdivosti nebo nepravdivosti informace natolik znalostí a dostatek podkladů, které ji dokazují? A právě to dokáže být velkým problémem při zpracovávání informací z otevřených zdrojů, které mohly být zveřejněny jako součást informační války. Je potom na lidech, kteří se o problematiku opravdu zajímají posoudit jejich pravdivost, ale i tehdy může být posouzena špatně.

Účel takových informací má své racionální odůvodnění a je zcela pochopitelné, proč se tak děje. Zároveň však sdílení takových zpráv celkově nepřidává na důvěryhodnosti informací přijímaných z “prestižních“ hromadně sdělovacích prostředků. Pokud se médium o takových událostech rozhodne informovat a informace se později ukáží jako nepravdivé nebo zkreslené, je porušena celková důvěra tohoto zdroje a mělo by se ke každé další informaci ze stejného zdroje postupovat s větším skepticismem. V případě mnou uvedené metody týkající se spolehlivosti informací tedy snížit úroveň důvěryhodnosti zdroje.

Pokud se však pomocí nástrojů hledají informace o osobách, IP adresách, doménách a podobných záležitostech, je většinou vidět vše černé na bílém. Ale

i v těchto případech je možné, že jsou pravdivé informace skryty nebo se vydávají za jiné a mohou tak vést analýzu na špatnou stopu. Právě proto bývá zpravodajství z otevřených zdrojů spojeno i s dalšími druhy zpravodajství, aby mohli upozornit na klam a nepravdivé informace obsažené v otevřených zdrojích. Ve stejnou chvíli je při analýze určité problematiky ideální spolupráce více osob najednou, snaha o spolupráci s dalšími institucemi, které by se mohli zajímat o stejnou problematiku a o výměnu informací s nimi.

Specifické na dnešní situaci je, že pokud má kdokoliv zájem informace o dění kdekoliv na planetě, může je pomocí otevřených zdrojů analyzovat sám nebo se spojit i na dálku s více dalšími lidmi. Nemusí se tak spoléhat pouze na informace ze státních nebo komerčních hromadně sdělovacích prostředků jako v minulosti. Pokud tedy žije v zemi s podobnými pravidly jako v České republice.

Závěrem bych rád zhodnotil celkovou situaci války na Ukrajině, ale nemám zde zájem polemizovat o správnosti jakýchkoliv rozhodnutí na obou stranách konfliktu. Mým záměrem je jen naznačit to, že v konfliktech obdobného rozsahu s celkem podobnými parametry (např. válka v Jugoslávii nebo válka v Iráku) trvaly boje několik let a po konci následovala pro poražené země minimálně další dekáda plná nestability, ekonomických problémů a strádání obyvatelstva. Což znamená, že predikce dalšího vývoje z mé strany předpokládá s tím, že konflikt bude trvat několik let, tak jako ty výše zmíněné. S ohledem na současný vývoj konfliktu mít nebude ani jedna strana zájem snížit ze svých požadavků.

Současně mají války velkých rozměrů negativní vliv na ceny surovin a velké množství uprchlých osob v jiných státech. V případě nedalekého konfliktu je tu možnost rozšíření bojů do vlastního státu. To vše nepřispívá větší národní bezpečnosti států do války přímo nezapojených, v konfliktu na Ukrajině tedy i u České republiky.

Seznam zkratek

API : Application Programming Interface

BBC : British Broadcasting Corporation

CIDR : Classless Inter-Domain Routing (beztřídní směrování)

COMINT : Komunikační inteligence

DDos : distributed denial-of-service

DNS : Domain Name System

ELINT : Elektronické zpravodajství

EU : Evropská Unie

FISINT : Signálové zpravodajství týkající se přístrojové komunikace

GDPR : Obecné nařízení o ochraně osobních údajů

GEOINT : Geospatiální zpravodajství

HUMINT : Zpravodajství z lidských zdrojů

IMINT : Obrazové zpravodajství

IP : internetový protokol

NATO : The North Atlantic Treaty Organization

OSINT : Zpravodajství z otevřených zdrojů

RT : Russia Today

SIGINT : Signálové zpravodajství

SOCMINT : Zpravodajství ze sociálních sítí

TASS : Informatsionnoye Agentstvo Rossii

URL : Uniform Resource Locator

VK : VKontakte

VPN : Virtual Private Network

Seznam použitých zdrojů

Monografie

1. AKHGAR, Babak, P. Saskia BAYERL a Fraser SAMPSON. *Open Source Intelligence Investigation: From Strategy to Implementation*. Cham, CH: Springer, 2016, 248 s. ISBN 978-3-319-47671-1.
2. BAZZELL, M. *Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information*. Ninth edition. 2022. ISBN: 979-8761090064.
3. CHRISTOPHER, Andrew, Richard J. ALDRICH a Wesley K. WARK, ed. *Secret Intelligence: A Reader*. Second Edition. New York, USA: Routledge, 2020. 679 s. ISBN 978-0-415-70567-7.
4. GEORGE, Roger Z. *Intelligence in the National Security Enterprise: An Introduction*. USA: Georgetown University Press, 2020, 345 s. ISBN 9781626167445.
5. GOLDSTEIN, Frank L. *Psychological Operations: Principles and Case Studies.* Maxwell Airforce Base, Alabama: Air University, Press, 1996, 378 s. ISBN 1-58566-016-7.
6. HASSAN, Nihad A.. Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence. Ontario, Canada, 2018. ISBN 978-1-4842-3213-2.
7. KALPAKIS, George a Theodora TSIKRIKA a spol. OSINT and the Dark Web. In: AKHGAR, Babak a spol. *Open Source Intelligence Investigation: From Strategy to Implementation*. Cham, CH: Springer, 2016, s. 111-132. ISBN 978-3-319-47671-1.
8. MCDOWELL, Don. *Strategic Intelligence: A Handbook for Practitioners, Managers, and Users* [online]. Revised. Scarecrow Press, 2009, 287 s. [cit. 2022-04-16]. ISBN 978-0-8108-6285-2. Dostupné z: http://www.lander.odessa.ua/doc/Strategic_Intelligence-_A_Handbook_for_Practitioners,_Managers_and_Users.pdf
9. PALERI, Prabhakaran. Revisiting National Security: Prospecting Governance for Human Well-Being. Singapur: Springer, 2022. 1047 s. ISBN 978-981-16-8292-6.
10. SCHÄFFNER, Christina. *Analysing Political Speeches*. Londýn, UK: Multilingual Matters, 1997. 95 s. ISBN 9780585147000
11. SCHÄFFNER, Christina a Paul CHILTON. *Discourse Studies: A Multidisciplinary Introduction*. Vol.2. Londýn, UK: Sage, 1997. 680 s. ISBN 9781848606487.
12. TROIA, Vinny. *Hunting Cyber Criminals: A Hacker's Guide to Online Intelligence Gathering Tools and Techniques*. Indianapolis, USA: John Wiley & Sons, 2020. 514 s. ISBN 978-1-119-54092-2.

Zákonná úprava

1. Zákon č. *153/1994 Sb., o zpravodajských službách České republiky*

Akademické práce

1. BEDNÁŘ, Jaroslav. Vývoj mediálního obrazu válečných konfliktů a reflexe jeho utváření v českých internetových denících [online]. Olomouc, 2020 [cit. 2022-07-14]. Dostupné z:

https://theses.cz/id/vr2zau/Bednar_Jaroslav_BP.pdf. Bakalářská. Univerzita Palackého v Olomouci. Vedoucí práce Mgr. Eva Lebedová, Ph.D.

2. GIBSON, Stevyn D. , *Open Source Intelligence a contemporary intelligence lifeline,* PhD Thesis, Cranfield University, Defence College of Management and Technology, 2007, p.33. Dostupné z: https://www.scribd.com/document/552940969/2007-OPEN-SOURCE-INTELLIGENCE-a-Contemporary-Intelligence-Lifeline

Webové stránky a elektronické zdroje

1. ACLED History: [online]. The Armed Conflict Location & Event Data Project, 2022, 1 s. [cit. 2022-07-18]. Dostupné z: https://acleddata.com/acleddatanew//wp-content/uploads/dlm_uploads/2021/11/ACLED-History_v2_February_2022.pdf
2. ACLED Methodology and Coding Decisions around Conflict in Ukraine [online]. The Armed Conflict Location & Event Data Project, 2022, 9 s. [cit. 2022-07-18]. Dostupné z: https://acleddata.com/acleddatanew//wp-content/uploads/dlm_uploads/2021/11/ACLED-History_v2_February_2022.pdf
3. *Address by the President of the Russian Federation*. Kremlin [online]. 21.2.2022 [cit. 2022-07-10]. Dostupné z: http://en.kremlin.ru/events/president/news/67828
4. *Audit národní bezpečnosti* [online]. Praha: Ministerstvo vnitra ČR, 2016 [cit. 2022-05-05]. Dostupné z: https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf
5. A transcript of George Bush's war ultimatum speech from the Cross Hall in the White House. *Guardian* [online]. 18.3.2003 [cit. 2022-07-12]. Dostupné z: https://www.theguardian.com/world/2003/mar/18/usa.iraq
6. BALMFORTH, Tom. Ukraine's richest man announces his holding's exit from media business. The Moscow Times [online]. 11.7.2022 [cit. 2022-07-13]. Dostupné z: https://www.reuters.com/business/media-telecom/ukraines-richest-man-announces-his-holdings-exit-media-business-2022-07-11/
7. BERGENGRUEN, Vera. How Telegram Became the Digital Battlefield in the Russia-Ukraine War. The Time [online]. 21.3.2022 [cit. 2022-07-18]. Dostupné z: https://time.com/6158437/telegram-russia-ukraine-information-war/
8. *Bezpečnostní strategie ČR*. Praha: Ministerstvo zahraničních věcí České republiky, 2015. ISBN 978-80-7441-005-5. [cit. 2022-05-06].Dostupné z: https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf
9. CASANOVAS, Pompeu. Cyber Warfare and Organised Crime. A Regulatory Model and Meta-Model for Open Source Intelligence (OSINT). In: *Philosophical Studies Series* [online]. Švýcarsko: Springer International Publishing Switzerland, 2017, s. 139-167 [cit. 2022-05-20]. Dostupné z: https://uploads-ssl.webflow.com/5cd23e823ab9b1f01f815a54/5cff33b8bbb1f7b1327173ed_Cyber%20Warfare%

20and%20Organised%20Crime.%20A%20Regulatory%20Model%20and%20Meta-Model%20for%20Open%20Source%20Intelligence%20(OSINT).pdf

10. CHAPPELL, Bill. Snake Island sailors are freed as Ukraine and Russia conduct a prisoner exchange. National Public Radio [online]. 24.3.2022 [cit. 2022-07-14]. Dostupné z: https://www.npr.org/2022/03/24/1088593653/snake-island-sailors-freed-prisoner-swap
11. CHAPPLE, Mike. *What Is Metadata?* [online]. 15.9.2020 [cit. 2022-04-16]. Dostupné z: https://www.thoughtco.com/metadata-definition-and-examples-1019177
12. CHEN, Emily a Emilio FERRARA. Tweets in Time of Conflict: A Public Dataset Tracking the Twitter Discourse on the War Between Ukraine and Russia [online]. Marina del Rey, CA, USA: University of Southern California, Information Sciences Institute, 2022 [cit. 2022-07-18]. Dostupné z: https://arxiv.org/pdf/2203.07488.pdf
13. CHIRINOS, Carmela. Anonymous takes revenge on Putin's brutal Ukraine invasion by leaking personal data of 120,000 Russian soldiers. Fortune [online]. 4.4.2022 [cit. 2022-07-18]. Dostupné z: https://fortune.com/2022/04/04/anonymous-leaks-russian-soldier-data-ukraine-invasion/
14. Civilian Harm in Ukraine. Bellingcat [online]. 2022 [cit. 2022-07-18]. Dostupné z: https://ukraine.bellingcat.com/
15. DAVYDOFF, Daniil. The cult of the search in open-source intelligence. Security Magazine [online]. 24.11.2020 [cit. 2022-05-10]. Dostupné z: https://www.securitymagazine.com/authors/2380-daniil-davydoff
16. DIXON, S. Most popular social networks worldwide as of January 2022: Ranked by number of monthly active users. Statista.com [online]. 26.7.2022 [cit. 2022-07-31]. Dostupné z: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/
17. DOKUMENT: Přepis projevu Volodymyra Zelenského před oběma komorami českého parlamentu. ČT 24 [online]. 15.6.2022 [cit. 2022-07-14]. Dostupné z: https://ct24.ceskatelevize.cz/domaci/3506574-dokument-prepis-projevu-volodymyra-zelenskeho-pred-obema-komorami-ceskeho-parlamentu
18. FLEISHER, Craig S. Using open source data indeveloping competitive andmarketing intelligence. In: *European Journal of Marketing* [online]. Windsor, Kanada: Emerald Group Publishing Limite, 2007, s. 852-586 [cit. 2022-05-18]. Vol. 42 No. 7/8, 2008. Dostupné z: https://www.researchgate.net/publication/273745484_Using_Open_Source_Data_in_Developing_Competitive_and_Market_Intelligence
19. Hospitals Bombed and Apartments Destroyed: Mapping Incidents of Civilian Harm in Ukraine. Bellingcat [online]. 17.3.2022 [cit. 2022-07-18]. Dostupné z: https://www.bellingcat.com/news/2022/03/17/hospitals-bombed-and-apartments-destroyed-mapping-incidents-of-civilian-harm-in-ukraine/
20. IntelTechniques Search Tools [online]. [cit. 2022-07-07]. Dostupné z: https://inteltechniques.com/tools/index.html

21. KLEČKOVÁ, Adéla. OPEN SOURCE INTELLIGENCE AND TERRORISM. PSSI ALUMNI BRIEF [online]. Praha: Prague Security Studies Institute, 2021. Dostupné z: https://www.pssi.cz/download//docs/8539_pssi-alumni-brief-01-osint-4.pdf
22. GANDOMI, Amir a Murtaza HAIDER. Beyond the hype: Big data concepts, methods, and analytics. International Journal of Information Management [online]. 3.12.2014, s. 137-144 [cit. 2022-05-12]. Dostupné z: https://doi.org/10.1016/j.ijinfomgt.2014.10.007
23. GALPEROVICH, Danila. Russia Using Foreign Agent Law to Attack Journalism, Media Say. Voice of America [online]. 10.7.2022 [cit. 2022-07-12]. Dostupné z: https://www.voanews.com/a/press-freedom_russia-using-foreign-agent-law-attack-journalism-media-say/6206858.html
24. GEOINT – Geospatial Intelligence. Heavy.ai [online]. [cit. 2022-05-05]. Dostupné z: https://www.heavy.ai/technical-glossary/geoint
25. KEMP, Simon. Digital 2022: Global Overview Report. Data Reportal [online]. 26.1.2022 [cit. 2022-07-18]. Dostupné z: https://datareportal.com/reports/digital-2022-global-overview-report
26. LAURENCE, Peter. How Ukraine's 'Ghost of Kyiv' legendary pilot was born. BBC [online]. 1.5.2022 [cit. 2022-07-15]. Dostupné z: https://www.bbc.com/news/world-europe-61285833
27. Maltego [online]. [cit. 2022-07-06]. Dostupné z: https://www.maltego.com/product-features/?utm_source=paterva.com&utm_medium=referral&utm_campaign=301
28. Putin Signs Law Introducing Jail Terms for 'Fake News' on Army. The Moscow Times [online]. 4.3.2022 [cit. 2022-07-13]. Dostupné z: https://www.themoscowtimes.com/2022/03/04/putin-signs-law-introducing-jail-terms-for-fake-news-on-army-a76768
29. Recon-ng [online]. GitHub. [cit. 2022-07-07]. Dostupné z: https://github.com/lanmaster53/recon-ng
30. Russia tightens legislation on 'foreign agents'. Deutsche Welle [online]. 29.6.2022 [cit. 2022-07-12]. Dostupné z: https://www.dw.com/en/russia-tightens-legislation-on-foreign-agents/a-62307066
31. RYŠÁNEK, Adam. Rusko plánuje největší válku v Evropě od roku 1945, tvrdí Johnson. *Seznam Zprávy* [online]. 20.2.2022 [cit. 2022-07-10]. Dostupné z: https://www.seznamzpravy.cz/clanek/zahranicni-rusko-planuje-nejvetsi-valku-v-evrope-od-roku-1945-tvrdi-johnson-189307
32. Sci-Hub. Sci-hub.com [online]. 26.7.2022 [cit. 2022-07-04]. Dostupné z: https://sci-hub.se/about
33. SCHRECK, Carl. Holy Slight: How Russia Prosecutes For 'Insulting Religious Feelings'. Radio Free Europe [online]. 2020 [cit. 2022-07-11]. Dostupné z: https://www.rferl.org/a/russia-prosecuting-insults-to-religious-feelings/28678284.html
34. SCHWIMMER, David. Žádosti o poskytnutí informací o uživatelích Facebooku, Googlu, Microsoftu a Seznamu. *Policie.cz* [online]. 20. 4. 2020 [cit. 2022-05-25]. Dostupné z: https://www.policie.cz/clanek/zadosti-o-poskytnuti-informaci-o-uzivatelich-facebooku-googlu-microsoftu-a-seznamu.aspx

35. Securedrop Overview. Securedrop [online]. [cit. 2022-07-04]. Dostupné z: https://securedrop.org/overview/
36. SHAH, Hasit. Full text of Ukrainian president Volodymyr Zelenskyy's speech to the US Congress. Quartz [online]. 16.3.2022 [cit. 2022-07-14]. Dostupné z: https://qz.com/2142992/transcript-of-volodymyr-zelenskyys-speech-to-the-us-congress/
37. Shodan [online]. [cit. 2022-07-04]. Dostupné z: https://help.shodan.io/the-basics/what-is-shodan
38. Snake Island: Ukraine says troops who swore at Russian warship are alive. BBC [online]. 28.2.2022 [cit. 2022-07-14]. Dostupné z: https://www.bbc.com/news/world-europe-60554959
39. Social Media Stats Russian Federation. StatCounter [online]. [cit. 2022-07-18]. Dostupné z: https://gs.statcounter.com/social-media-stats/all/russian-federation
40. Social Media Stats Ukraine. StatCounter [online]. [cit. 2022-07-18]. Dostupné z: https://gs.statcounter.com/social-media-stats/all/ukraine
41. Speech by President of Ukraine Volodymyr Zelenskyy at the NATO Summit. President of Ukraine [online]. 24.2.2022 [cit. 2022-07-13]. Dostupné z: https://www.president.gov.ua/en/news/vistup-prezidenta-ukrayini-volodimira-zelenskogo-na-samiti-n-73785
42. Spiderfoot. Spiderfoot [online]. [cit. 2022-07-06]. Dostupné z: https://www.spiderfoot.net/documentation/
43. This New Tool Lets You Analyse TikTok Hashtags. *Bellingcat.com* [online]. 11.5.2022 [cit. 2022-07-01]. Dostupné z: https://www.bellingcat.com/resources/how-tos/2022/05/11/this-new-tool-lets-you-analyse-tiktok-hashtags/
44. TheHarvester [online]. [cit. 2022-07-07]. Dostupné z: https://github.com/laramies/theHarvester
45. Tor at the Heart: The Ahmia project. Tor Blog [online]. 5.12.2016 [cit. 2022-07-04]. Dostupné z: https://blog.torproject.org/tor-heart-ahmia-project/
46. Ukraine. Reporters Without Borders [online]. 2022 [cit. 2022-07-14]. Dostupné z: https://rsf.org/en/country/ukraine
47. US DEPARTMENT OF THE ARMY. Open-Source Intelligence [online]. Washington, DC: Army Techniques Publication, 2012 [cit. 2022-07-17]. S.8 Dostupné z: https://irp.fas.org/doddir/army/atp2-22-9.pdf
48. *What is intelligence?* Office of the Director of National Intelligence [online]. [cit. 2021-12-01]. https://www.dni.gov/index.php/what-we-do/what-is-intelligence
49. What is the Deep and Dark Web? Kaspersky.com [online]. 2022 [cit. 2022-07-04]. Dostupné z: https://www.kaspersky.com/resource-center/threats/deep-web
50. YAQUB, M. How Many Tweets per Day 2022 (New Data). The Time [online]. 8.7.2022 [cit. 2022-07-18]. Dostupné z: https://www.renolon.com/number-of-tweets-per-day/
51. ZEMAN, Petr. Co je zpravodajství [online]. 2008 [cit. 2022-05-02]. Dostupné z: https://www.absd.sk/co_je_zpravodajstvi#_ftn3

Seznam obrázků

Seznam tabulek