POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostně právní

Katedra kriminální policie

Zpravodajství z otevřených zdrojů (OSINT) v oblasti kriminálního zpravodajství-zdroje, metody, postupy a nástroje

Bakalářská práce

Open Source Intelligence (OSINT) in Criminal Intelligence - Sources, Methods, Procedures and Tools

VEDOUCÍ PRÁCE

Ing. Bc. Luděk Michálek, Ph.D.

AUTOR PRÁCE

Michal Skuhrovec

PRAHA

2023

ČESTNÉ PROHLÁŠENÍ

Prohlašuji, že jsem bakalářskou práci na téma „Zpravodajství z otevřených zdrojů (OSINT) v oblasti kriminálního zpravodajství-zdroje, metody, postupy a nástroje“ vypracoval samostatně a s použitím uvedené literatury a pramenů.

V Praze, dne 10. 03. 2023 Michal Skuhrovec

Poděkování

Chci poděkovat panu Ing. Bc. Luďku Michálkovi, Ph. D. za jeho vedení při zpracování bakalářské práce, za odborné vedení a navrhování věcných bodů do bakalářské práce.

Anotace

Následující text bakalářské práce má v krátkém souhrnu přiblížit historii informací uveřejněných v tzv. otevřených zdrojích, vymezeně na území Čech, přes období Studené války, až po digitalizaci otevřených zdrojů. V další části bakalářská práce uvádíme obecnou definici metody OSINT, základní pojmy a rozdělení. Další část se věnuje vybraným otevřeným zdrojům dostupným na internetu. Závěr je zaměřen na cíl této práce, a sice praktické využití informací získaných ze zpravodajství z otevřených zdrojů ve formě checklistu – souhrn možných informací, které lze získat metodou OSINT pro využití policistů zařazených na SKPV, jehož cílem je usnadnění a zjednodušení práce při vyhledávání informací o osobách (FO/PO) prověřovaných ze strany SKPV.

Klíčová slova

OSINT * otevřené zdroje * zpravodajství * checklist * lustrační nástroj * kriminální zpravodajství*

Annotation

The following text of the bachelor's thesis is intended to give a brief summary of the history of information published in the so-called open sources, defined in the territory of Bohemia, through the Cold War period to the digitization of open sources. In the next part of the bachelor thesis we present a general definition of the OSINT method, basic concepts and classifications. The next part is dedicated to selected open sources available on the Internet. Finally, we conclude with the aim of this thesis, namely the practical use of information obtained from open source intelligence in the form of a checklist - a summary of possible information that can be obtained by the OSINT method for the use of police officers assigned to the SKPV, the objective of which is to facilitate and simplify the work of searching for information on persons (FO/PO) screened by the SKPV.

Keywords

OSINT * open source * intelligence * checklist * lustration tools * criminal intelligence*

Obsah

Úvod

Zvolené téma této bakalářské práce pojednává o zpravodajství z otevřených zdrojů (OSINT) v kriminální oblasti. Ono zpravodajství je tak jasně situováno do specifické výseče, které se věnují orgány činné v trestním řízení, konkrétně Policie ČR, policisté zařazení do Služby kriminální policie a vyšetřování (SKPV), zabývající se vyšetřování těch nejsložitějších trestných činů, přičemž kriminální prostředí je pro ně studnice informací. Metoda zpravodajství z otevřených zdrojů je jen jedna z metod používaná policisty, kterými jsou zjišťovány kriminalisticky relevantní informace o osobách, věcech, ale i událostech. Nicméně tato metoda má velký potenciál, policisté dnes a denně nevědomky používají metodu OSINT a dostávají se tak mnohdy k informacím, které je posunou v prověřování trestné činnosti dopředu. Nutno však podotknout, že vyhledávání informací z otevřených zdrojů je pro policisty bez znalosti některých nástrojů či metod vyhledávání mnohdy časově náročné a je tak podceňován význam OSINTu, jakožto prostředku pro získaní kriminalisticky relevantní informace. V současné době je tak práce s metodou OSINT vyčleněna pouze na malý počet policistů SKPV, kteří jsou na tuto metodu školeni. Zbytek příslušníků PČR je odkázán na svou laickou znalost, získanou především užíváním prostředí internetu ze svého soukromého života, což může vést k nižší úspěšnosti vyhledání konkrétní informace. V takovém případě je výsledek použití metody OSINT neúměrný k vynaložené snaze o získaní hledané informace.

Cílem této bakalářské práce je navrhnout dílčí řešení tohoto problému za pomoci využití checklistu nebo lustrační karty. Lustrační karta by svým obsahem zrychlila, zefektivnila a zjednodušila práci spojenou se zpravodajstvím z otevřených zdrojů na takovou míru, aby ušetřila čas a získala prostor pro policisty v dalších oblastech jejich činností, vedoucí k řádnému objasňování nebo předcházení trestné činnosti. Cíl bakalářské práce na toto téma je zároveň motivací, jelikož policisté, kteří jsou zařazeni na operativě SKPV, se často setkávají s výše zmíněnými strastmi při vyhledávání informací z otevřených

zdrojů. Policisté jsou si tak vědomi, kolik času stráví základní rešerší o zájmové osobě a dostupných informacích k takové osobě, ať už se jedná o základní informace, týkající se například jejího podnikání, tak i otázky jejích koníčků, rodiny, ale i jejího vzhledu a chování.

Ke stanovenému cíli bakalářské práce se dostaneme přes úvodní seznámení s metodou OSINT z historického pohledu, který by měl kontrastně poukázat na posun v používání této metody. Zejména co se týče nosičů informací, jejich vytěžování, uložení a následné využití. Po seznámení s historií otevřených zdrojů bude dalším bodem bakalářské práce seznámení s otevřenými zdroji v internetovém prostředí, soustředící se na možnosti vyhledávání jak v internetových prohlížečích, tak na sociálních sítích. Pokud je řeč o internetovém prostředí a bavíme-li se o kriminálním zpravodajství, které by mělo být skryto jak před zdrojem informace, tak před nositelem informace musí být automaticky řeč i o bezpečnosti pohybu v internetovém prostředí tak, aby naše zpravodajské aktivity zůstaly neodhalené. Bakalářská práce se bude okrajově zabývat i Dark netem, který je pro kriminální zpravodajství neméně důležitou složkou, ba složkou zcela neopominutelnou. Na závěr bude v bakalářské práci pracováno s možnostmi ulehčení metody OSINT a její přenesení k policistům takovým způsobem, aby došlo k zefektivnění jejich činností. Řešená problematika, tedy její výsledek, by měl být jakýmsi informačním odrazovým můstkem, rychlým prvním náhledem na osobu a její datovou stopu v internetovém prostředí z pohledu otevřených zdrojů.

1. Historie vyhledávání informací v otevřených zdrojích

Informace, jako součást každodenního života, je součástí lidstva od doby jeho vzniku. V dnešním světě je pojem informace naprosto běžným termínem.

Samotné slovo informace pochází z latinského informatio (představa, obrys), které je odvozeno ze slovesa informare (dodávat tvar, formovat). V období středověku byl termín informace ve filozofii užíván ve smyslu ´´formulovat myšlenku´´. V moderní době je tento pojem vykládán také jako ´´komunikování něčeho k někomu´´, přičemž tato formulace je základním kamenem definice pojmu informace ve společenských vědách. Význam slova informace v dnešní digitální době byl pojat jako energie, která snižuje nebo odstraňuje neurčitost. Další důležitou definicí pojmu informace můžeme nalézt v dokumentační či knihovnické vědě, kde je informace chápána jako záznam nebo data, která je třeba popisovat, ukládat a třídit. [1]

V historii bylo vyhledávání informací podstatně odlišné od dnešní rychlé a digitalizované doby. Ve starověkém Římě vznikaly první veřejné knihovny, ke kterým měla přístup široká veřejnost, tedy alespoň ta, která byla gramotná. V tehdejším Římě byl vzděláván každý občan od sedmi let věku. Jelikož v Římě neměli občané povinnost manuálně pracovat, dostávalo se jim dostatek volného času pro čtení. Využívání veřejných knihoven tak nebylo ničím neobvyklým. V těchto veřejných knihovnách byla dostupná nejen poezie a prózy, ale také i projevy, císařské dokumenty a odborné práce. Člověk, který do veřejné knihovny došel, mohl vyhledávat informace z tehdejších otevřených zdrojů, a to i díky úředníkům, kteří knihovnu spravovali. [2]

---

[1] BAWDEN DAVID a ROBINSON LYN. Introduction to information science. London: Facet publishing, 2012, ISBN 9781856048101, S. 351

[2] HÁLOVÁ, Marie. Veřejné knihovny antické Římské říše. Duha: Informace o knihách a knihovnách z Moravy [online]. 2012, [cit. 2022-11-27]. ISSN 1804-4255. Dostupné z: http://duha.mzk.cz/clanky/verejne-knihovny-anticke-rimske-rise

Vyhledávání informací v otevřených zdrojích bylo tak umožněno již ve starověkém Římě a v další kapitole se práce bude věnovat historií otevřených zdrojů na území Čech.

1.1. Historie otevřených zdrojů na území Čech

Na začátek je nutné se zmínit o faktu, že využití a sdílení otevřených zdrojů bylo v období, o kterém bude hovořeno, velmi omezené možnostmi tehdejší doby. Využití informací získaných z otevřených zdrojů nebylo z pohledu tehdejších bezpečnostních sil, dohlížejících na veřejný pořádek a dodržování zákona, zdaleka tak využívané. Důvodem byl vznik novin, či jiných zpravodajských listin, které byly veřejně dostupné tak, jak to známe z moderní doby. Rozmach novinového zpravodajství na území Čech byl nejmarkantněji zaznamenán v 17. století. Právě počátek 17. století je spojen s pravidelně tištěnými novinami, což znamenalo pravidelné a častější zveřejnění událostí ve zdroji, který byl veřejně dostupný s ohledem na život v raném novověku.

Mimo klasických tištěných novin byly alespoň z počátku využívány i takzvané jednorázové zpravodajské tisky – letáky. Tyto letáky obsahovaly vždy nejdůležitější události, které se odehrávaly na území Českého království a v Markrabství moravském. Události byly shrnuty v jednom zpravodajském tisku. Jednalo se vždy o věrohodné události shromážděné v letáku, kdy tyto informace byly vždy různé a sloužily k poznání okolností a podmínek jednoho určitého děje.[3]

Za největší zásluhu na rozšíření pravidelných tiskových novin na území Českého království označuje Stejskalová následující: *„Bylo již konstatováno, že náboženské, politické a posléze vojenské konflikty, počínaje událostmi stavovského povstání v Čechách v letech 1618-22 a zájem o ně, způsobily rychlé*

[3] STEJSKALOVÁ, Eva. Novinové zpravodajství a noviny v Čechách od 17. století do roku 1740. Praha: Univerzita Karlova v Praze, nakladatelství Karolinum, 2015. ISBN 978-80-246-2613-0, s. 13

šíření nového média – pravidelných tištěných novin.“[4] Lze tak hovořit o rozšiřování informací zasazených do veřejně dostupných zdrojů. Z historických událostí však víme, že na počátku 17. století byla gramotnost obyvatelstva velmi nízká a byla výsadou šlechty a církve. Z toho vyplývá, že v tomto případě můžeme sice hovořit o otevřených zdrojích, které byly veřejně dostupné prostřednictvím právě uvedených zpravodajských letáků nebo tištěných novin, ale reálná dostupnost byla omezena na gramotné obyvatelstvo. To je svým způsobem s ohledem na tehdejší dobu jisté omezení a pojem ‘‘otevřené zdroje‘‘ je tak relativní.

Dalším důležitým milníkem v uveřejňování událostí v otevřených zdrojích bylo odloučení Českých zemí z Rakousko-uherské monarchie do samostatného demokratického celku Československé republiky.

Po vzniku Československa došlo k rozmachu tištěných médií, která se již velmi podobala tištěným médiím z moderní doby. Pokud hovoříme o rozmachu, nešlo jen o počet tisků, ale i o kvalitu poskytovaného zpravodajství. Na pořadu dne byl denní tisk, který informoval o aktuálních událostech a současně byl využíván politickými stranami jako jejich mluvčí, což ze strany politických uskupení znamenalo sponzorování zpravodajských redakcí. Otázkou pak zůstává objektivita těchto redakcí. Nicméně pro kriminální zpravodajství bylo důležité především zpravodajství na kriminální téma, ne tolik téma politické, i když to jsou občas spojené nádoby. Období první republiky je specifické i pro nástup rozhlasového a filmového zpravodajství. S tím přicházejí nové možnosti využívání informací z otevřených zdrojů, které jsou spatřovány v ustálenosti denního tisku a žurnalistiky jako takové a používání nových technologií za účelem usnadnění přeonsu informace a způsobu interpretace. Ovšem zásadní novinkou po vzniku Československa bylo propojení Československa se zahraničím. „*Významným krokem na poli československé žurnalistiky se stalo založení Československé tiskové kanceláře, která vznikla hned 28. října 1918 a zpočátku plnila funkci*

[4] STEJSKALOVÁ, Eva. Novinové zpravodajství a noviny v Čechách od 17. století do roku 1740. Praha: Univerzita Karlova v Praze, nakladatelství Karolinum, 2015. ISBN 978-80-246-2613-0, s. 108

tiskového odboru Národního výboru československého. Záhy však navázala kontakt se zahraničními zpravodajskými agenturami, a stala se tak důležitým mezičlánkem mezi zahraničním a domácími novináři.“ [5]

Tímto vstupem na mezinárodní scénu žurnalistiky a zpravodajství dostávají otevřené zdroje nový rozměr, který byl využíván jak v kriminálním zpravodajství, tak ve zpravodajské činnosti tehdejších zpravodajských služeb. Rozšířil se rozhled a pomyslná viditelnost orgánů činných v trestním řízení a zpravodajských služeb. Postupem dějinnými událostmi naší země bychom narazili na různé způsoby cenzurování otevřených zdrojů, ne však způsob šíření informací v otevřených zdrojích a nosičích otevřených zdrojů. V období první republiky, a i v období následujícím bylo využívání otevřených zdrojů pro kriminální zpravodajství teprve na začátku. To stejné neplatilo v USA a na mezinárodní scéně, a to hlavně v době studené války, kdy se metoda OSINT těšila přízni, především na úrovni zpravodajských služeb, a to jak v USA, tak i v tehdejším SSSR.

V dalších letech, zejména v období II. světové války a v době komunistického režimu, docházelo v Československu k více či méně přísné cenzuře všech informací. Cenzura se týkala nejen tiskových, ale i rozhlasových, ba i mluvených informací. Zpravodajství v otevřených zdrojích dostávalo nové rozměry, zejména s vývojem technologií a přizpůsobování se aktuální době. K tomuto období, období studené války, se přesuneme z Československa do celého světa a další kapitola bude věnována otevřeným zdrojům za doby studené války ve světovém měřítku.

1.1. Otevřené zdroje za studené války

V období po konci II. světové války můžeme poprvé mluvit o cíleném zpravodajství z otevřených zdrojů. Samotný prvopočátek byl dán v roce 1939

[5] Reindlová, Nikola. Tisk za 1. republiky: Památník Karla Čapka [online]. 2012, [cit. 2022-12-27]. Dostupné z: https://www.capek-karel-pamatnik.cz/vismo/dokumenty2.asp?id_org=200013&id=14311

britskou vládou, která podala žádost adresovanou na British Broadcasting Corporation, známou pod zkratkou BBC, týkající se puštění civilní, později i komerční služby. Úkolem této služby bylo zkoumat otevřené zdroje, a to zejména zahraniční tištěnou žurnalistiku a rozhlasové vysílání. Dále prováděla analýzu zahraničního vysílání, které bylo nazváno jako Souhrn světového vysílání (SWB), v současnosti je známý pod názvem BBC Monitoring. [6]

Lze tak říci, že nedošlo k posunu nově vzniklých veřejně dostupných zdrojů, ale spíše došlo k prvnímu využití již existujících otevřených zdrojů, a to ještě subjektem, kterým byla vláda Spojeného království Velké Británie a Severního Irska. Stále však nelze hovořit o kriminálním zpravodajství.

Studenou válku lze datovat k roku 1947 a její konec k roku 1991, kdy se rozpadl Sovětský svaz. O studené válce hovoříme jako o střetu mezi velmocemi, a sice USA a SSSR, který nepřerostl ve válečný konflikt, jeho propuknutí by však znamenalo válku jadernou. Můžeme hovořit o III. světové válce, jelikož by se jednalo o konflikt, do kterého by byla zapojena celá planeta. Po celé zemi v tomto období vypuklo několik válečných konfliktů, v nichž soupeřící mocnosti bojovaly tzv. ‘‘v zastoupení‘‘. Ozbrojené konflikty se nevyhýbaly civilistům, byly vedeny ozbrojenými silami válčících zemí, výjimkou v té době nebyly ani občanské války a nově se hovořilo i o teroristické válce a válce proti teroru.[7]

V průběhu studené války hlavní soupeřící mocnosti, tedy USA a SSSR, do svých tajných služeb implementovaly kapacity, určené pro shromažďování otevřených zdrojů, které z počátku tvořily hlavní část veškerého zpravodajství a poté se staly hlavním zdrojem informací v otázce vojenských a politických kroků

[6]Schaurer, Florian and Störger, Jan. AFIO-Association of Former Intelligence Officers [online]. 2013. [cit. 16.01.2023]. Dostupné z: https://www.afio.com/publications/Schauer_Storger_Evo_of_OSINT_WINTERSPRING2013.pdf

[7] LABANCA, Nicola. *Válečné konflikty dneška od roku 1945 do současnosti*. Praha: Fortuna Libri, c2009. ISBN 978-80-7321-465-4. s. 10-21.

protivníka. Poprvé byl pak použit termín OSINT na konci 80. letech americkou armádou. [8]

V USA vznikla agentura se zkratkou FBIS – Foreign Broadcast Information Service, jejímž úkolem bylo shromažďování, analýza a podávání zpráv z otevřených zdrojů. Za úspěchy této agentury lze považovat například rok 1962 a kubánskou raketovou krizi, kdy FBIS při své činnosti, spočívající v monitorování rádia Moskva, mohla tehdejšímu prezidentovi Kennedymu podat zásadní informaci o rozhodnutí SSSR, a sice stáhnout rakety z Kuby. Nejednou byly veřejné informace jediné informace pro zpravodajské analytiky, jako v roce 1968 při invazi vojsk Varšavské smlouvy do Československa, kdy rozhlasové vysílání bylo pro zpravodajské služby zásadním zdrojem informací o situaci v ulicích Prahy. [9]

V období studené války bylo zpravodajskými službami plně využíváno otevřených zdrojů. Jak se ukázalo, veřejně dostupné informace z novin a rozhlasového vysílání byly pilířem zpravodajské činnosti, zaměřené na odhalování rizik a slabin protivníka v této složité době, ve které se proti sobě postavil komunistický východní blok řízený Sovětským svazem a západní mocnosti v čele s USA. V další části této práce bude hovořeno o samotných nosičích informací, kdy na konci období studené války v roce 1987 vzniká pojem internet, jenž mimo jiné vznikl i díky snaze vyvinout komunikační síť, která by nebyla tak lehce zničitelná jadernými zbraněmi.

---

8 Schaurer, Florian and Störger, Jan. AFIO-Association of Former Intelligence Officers [online]. Copyright © [cit. 16.01.2023]. Dostupné z: https://www.afio.com/publications/Schauer_Storger_Evo_of_OSINT_WINTERSPRING2013.pdf. S. 53, 54

9 Studeman, W. Historie Foreign Broadcast Information Service, [přednáška-online]. 1992. [cit. 29.12. 2022]. Dostupné z: https://irp.fas.org/fbis/studem.html

1.2. Historie otevřených zdrojů z pohledu jejich nosičů

Od počátku úsvitu lidské rasy byly zaznamenány pokusy sdělit informaci prostřednictvím přenesení myšlenky na nosič, na kterém myšlenka bude udržitelná po dlouhý čas. Pro potřeby nosičů informací v otevřených zdrojích nemá cenu hovořit o kamenných tabulkách, do kterých byly vytesáváním vyobrazovány činnosti tehdejších lidí, jako například lov zvěře. Přesuneme se k vývoji dnes již známých nosičů veřejně dostupných informací tzv. v otevřených zdrojích, jako jsou tištěné noviny, rozhlas nebo například televize. Mimo tato známá média byly v historii veřejně dostupné ještě další listiny, a sice matriky.

1.2.1. Matrika

Matrikou z historického pohledu lze označit úřední knihu, ve které byla zapsána jména osob a další osobní údaje potřebné pro právní evidence, jako byla například univerzitní matrika studentů, matrika šlechticů. Jednou z matrik byla i matrika církevní, jenž byla také úřední knihou, vedenou duchovními správci na jednotlivých farností, ale i laiky, kteří byli vyškoleni k zápisům do matriky. Do této matriky evidovali osoby, kterým byly udělovány svátosti. Tato duchovní matrika procházela jistým vývojem a ustálila se na podobě, ve které byla zapisována data narozených, pokřtěných, oddaných a zemřelých osob. Potřeba vést matriky je datována až k roku 1137, kdy byla v rámci lateránského koncilu zmíněna potřeba vést tyto knihy. V románských zemích matriky vznikaly až ve 14.-15. století a v českých zemích se vedení matrik datuje do poloviny 16. století.[10]

Zapsané údaje v matrikách lze přirovnat k dnešním veřejným rejstříkům či evidencím, obsahující osobní údaje. Samozřejmě pravidla pro nakládání s osobními údaji se tehdy výrazně lišila, a proto by se na rozdíl od dnešních veřejných rejstříků v tehdejších matrikách našly i osobní údaje zavedených osob.

[10]Répásová, Marie, Krátce k historii římskokatolických matrik, SOA v Třeboni-DIGITÁLNÍ ARCHIV [online]. [cit. 30.12. 2022]. Dostupné z: https://digi.ceskearchivy.cz/Matriky-Rimskokatolicka-cirkev-Kratce-k-historii-rimskokatolickych-matrik

Jedním z nejrozšířenějších veřejně dostupných – otevřených zdrojů v historii byly tištěné noviny.

1.2.2. Noviny

Jako první je nutné uvést pojem noviny, a co si pod tímto pojmem představit. Noviny dle Reifové lze charakterizovat takto: „*Podle tradičních teoretických koncepcí se n. charakterizují jako médium vykazující: a) aktuálnost, časovou blízkost, zpravodajství k události; b) periodicitu, tedy dlouhodobé vydávání v pravidelných cyklech; c) univerzálnost, tj. obsahovou pestrost; d) publicitu, tj. nikým neomezenou dostupnost pro všechny.*“ Proti rozhlasu a televizi lze noviny rozlišit ještě dvěma body. Jeden bod je neomezené využití nezávisle na času a místě, a ztvárnění písmem a tiskem. Za první dochované periodicky vycházející tištěné noviny se pokládají listy ,,Relationen‘‘, pocházející z roku 1605, autor Johann Carolus, Štrasburk a dále ,,Aviso‘‘ z roku 1609, autorem byl Julius Adolph von Söhne, Wolfenbüttel. V průběhu 17. století se tištěné noviny rozšířily do celé Evropy, alespoň ty které vycházely periodicky každý týden. [11]

Tištěné noviny tak lze označit jako první masivně rozšířený nosič informací, který bylo možno využít jako otevřený zdroj – veřejně dostupný zdroj informací, jenž se vyvíjel tak, jako zbytek světa. V průběhu dějin tištěné noviny nezaznamenaly výrazný posun, svou formou dosáhly cíle již prvním výtiskem. V dalších staletích se zkrátka tištěné noviny stále tiskly na papír, měnil se jen způsob a technologie tisku a psaní. Prvním útlumem tištěných novin byl příchod rozhlasu.

1.2.3. Rozhlas

Za úsvit rozhlasových dějin je považován rok 1906, kdy v rozhlasové stanici Brant Rock, Massachusetss byly vysílány první hudební signály. Obliba rozhlasu vzrůstala před první světovou válkou, ale v domácnostech nebylo dostatek přijímačů. V roce 1917 došlo v USA ze strany federální vlády k omezení rádiových

[11] REIFOVÁ, Irena. *Slovník mediální komunikace*. Praha: Portál, 2004. ISBN 80-7178-926-7. S. 164-165

vysílačů, které trvalo až do konce první světové války. V roce 1927 se pak rozhlasové přijímače opět rozšířily, a to i díky reproduktorům, které do té doby nebyly součástí přijímače. Rozhlas se tak začal rychleji rozšiřovat. Zprávy patřily k rozkvětu rozhlasu, a to mimo jiné i díky faktu, že rozhlas mohl zprávy hlásit tak, jak se staly, což tištěné noviny nemohly.[12]

Co se týče počátků rozhlasu, jednalo se spíše o hudební produkce. Po začlenění zpráv do vysílání došlo k rychlejšímu rozmachu rozhlasu a vývoj rozhlasu i nadále pokračoval, a to přes období první a druhé světové války, studené války, až do dnešní moderní doby. Zprávy vysílané na tomto nosiči, patřily mezi otevřené zdroje značně využívané zpravodajskými službami všech zemí, přičemž tento nosič se stal ve zpravodajství otevřených zdrojů značně používaným, jak již bylo názorně uvedeno v kapitole 1.2. při Kubánské krizi. Dalším nosičem otevřených zdrojů se s rozvojem technologií stala televize. Opět hovoříme pouze o nosiči, přičemž podstatné je, aby v nosiči, v tomto případě televizi, byly vysílány informace, využitelné ve zpravodajství z otevřených zdrojů.

1.2.4. Televize

V naprostém začátku představovala televizi tzv. Nipkowův disk, který měl spirálovitý vzor otvorů a při rotaci každý otvor naskenoval řádek obrazu. Tento způsob zobrazování si nechal v roce 1884 patentovat Paul Julius Gottlieb Nipkow. Sám Nipkow nikdy nepostavil funkční model tohoto modelu. V roce 1900 pak Constantin Perskyi jako první použil slovo ‘‘televize‘‘, a to ve své práci, kterou přednesl na Mezinárodním kongresu o elektřině na Mezinárodní světové výstavě, ve které byly zhodnoceny tehdejší elektromechanické technologie a zmíněna byla právě práce Nipkowa.[13]

---

[12] Sterling, H. Christopher. Radio. Definition, History, & Facts. Britannica. Encyclopedia Britannica. [online]. [cit. 18.01.2023]. Dostupné z: https://www.britannica.com/topic/radio

[13] SHIERS. G; SHIERS. M. Early Television: A Bibliographic Guide to 1940. New York and London: Garland Publishing Inc. 1997. ISBN 978-0-8240-7782-2. S. 13, 22

Začátky televize zdaleka nepřipomínaly tu televizi, jak jí známe dnes, nicméně v průběhu let došlo k rozvoji, alespoň do podoby, která umožnila její rozšíření a využití v předávání informací o událostech domácích a zahraničních.

Po útoku na Pearl Harbor v roce 1941 se vývoj televize výrazně zadrhl, veškerá snaha výzkumných společností byla upnuta na válečný výzkum zahrnující například výzkum radaru. I tak, během války jakoby mimoděk, válečným vývojem došlo k vývoji pokročilejších technologií jako byly nové kamery, přijímače, obvody nebo čočky obrazovek. Nové technologie mohly být použity nejen do válečných technologií, ale i do technologie televizní. S koncem druhé světové války se pak ve Spojených státech vrátilo 15 televizních stanic. Nicméně v této době bylo televizní vysílání oproti rozhlasovému vysílání dost podceňované a méně rozšířené.[14]

Stejně jako u rozhlasu či tištěných novin byl velmi důležitý vývoj těchto nosičů. Co je ale důležité z hlediska otevřených zdrojů, je fakt, že stejně jako na předchozích dvou jmenovaných nosičích, tak i v televizi vysílali různé pořady informující o událostech jak z domácí scény, tak i ze zahraničí. Jinými slovy v televizním vysílání byla odvysílána informace s jistou zpravodajskou hodnotou, kdy televize byly veřejné dostupné a z televize se tak stal další z otevřených zdrojů. Televize svým potenciálem, který jí byl dán díky obrazovému vjemu předkládané informaci, jenž byl nadstavbou oproti rozhlasu, který poskytoval pouze zvukovou informaci, vedla k rozvoji, který se nezastavuje ani v dnešní době. Dnes jsou televizory stále zdokonalovány a jsou možná nejrozšířenějším nosičem z hlavní trojice historických nosičů a sice tištěné noviny, rozhlas, televize. V dnešní době je vyhledávání v těchto otevřených zdrojích zjednodušeno, jelikož z velké většiny je možné všechny tyto otevřené zdroje nalézt na internetové síti, která se stala dominantním nosičem otevřených zdrojů moderní doby.

[14] ABRAMSON, A. The History of Television, 1942 to 200. McFarland, 2003. ISBN 978-0-7864-1220-4. S. 3

2. Otevřené zdroje na internetu

Jak bylo v závěru předchozí kapitoly řečeno, svět novin, rozhlasu, televize, ale i třeba starých matričních záznamů prošel digitalizací, která umožňuje uvedené otevřené zdroje vyhledávat na internetové síti. Nesmíme však zapomenout i na nové otevřené zdroje určené přímo pro internet, jako například sociální sítě nebo na otevřené zdroje vycházející z veřejných rejstříků, kupříkladu obchodní rejstřík, rejstřík trestů právnických osob, které jsou dnes již běžně dostupné na internetu. Internet sám o sobě poskytuje spousty informací a pro uživatele, který chce tyto informace vytěžit, je důležité vědět, kde má jakou informaci hledat. Zejména v kriminálním zpravodajství je velkou výhodou, že ten, kdo bude informaci vyhledávat, má k dispozici i tzv. tvrdá data – data dostupná v neveřejných zdrojích, data, která se nacházejí v informačních systémech, která jsou dostupná například právě Policii ČR. Tvrdá data lze pak porovnávat s daty získanými z otevřených zdrojů. Obrázek utvořený pomocí metody OSINT, je díky tvrdým datům ucelenější i důvěryhodnější. Rizikem kriminálního zpravodajství ze strany OČTŘ je nebezpečí, že bude jejich vyhledávání odhaleno a bude tak odhalen i důvod, proč tato data o tom, kterém konkrétním objektu jsou vyhledávána. Z tohoto důvodu je ze strany OČTŘ nebo i zpravodajských služeb velmi důležité OSINT provádět bezpečně. I tomuto tématu se bude práce věnovat, nicméně v další části práce si definujeme pojem OSINT a základní informace o této metodě.

2.1. Definice OSINT metody, základní rozdělení

Otevřenými zdroji jsou podle Alexe O'Briena: „*Informace s otevřeným zdrojem jsou informace, ke kterým má široká veřejnost snadný a legální přístup. Byl používán ve válce a diplomacii dávno před internetem – spolu s informacemi ukradenými nebo jinak tajně získanými a úzce drženými. Ale jeho rozšířenost dnes znamená, že to, co bylo kdysi pro mnohé cenově nedostupné, je nyní dostupné*

pro nespočet aktérů, ať už jde o Severní Koreu, CIA, novináře, teroristy nebo kyberzločince.“[15]

Ve stručnosti lze shrnout, že otevřenými zdroji jsou noviny, časopisy, rozhlasové a televizní vysílání, internet, knihy, ale mohou jím být i různé přednášky, sympózia, konference, veškeré činnosti, kterou mohou být zdrojem informací a odehrávají se ve veřejném, volně přístupném prostoru.[16]

Zpravodajství otevřených zdrojů pod zkratkou OSINT dle Michaela Bazzella: „*Open Source Intelligence, často označována jako OSINT, může pro mnoho lidí znamenat mnoho věcí. Oficiálně je definována jako jakékoli zpravodajské informace vytvořené z veřejně dostupných informací, které jsou shromažďovány, zkoumány a šířeny včas vhodnému publiky za účelem řešení konkrétního zpravodajského požadavku.*“[17]

2.1.1. Základní rozdělení

Jedním ze základních rozdělení OSINT by mohlo být rozdělení podle vyhledávání na **pasivní** a **aktivní** metodou:

a) **pasivní** metodu představuje vyhledávání pomocí zadání vstupních dat do nástroje OSINT, jímž mají být vyhledány požadované informace a tím umožňují získat další informace. Jedná se o vyhledávání v širokém záběru sběru požadovaných informací.

---

[15] O’BRIEN, A. Open Source Intelligence May Be Changing Old-School War | WIRED. WIRED-The Latest in Technology, Science, Culture and Business | WIRED [online]. [cit. 22.01.2023]. Dostupné z: https://www.wired.com/story/open-source-intelligence-war-russia-ukraine/

[16] Otevřené zdroje. Bezpečnostní informační služba České republiky. [online]. 2023. [cit. 22.01.2023]. Dostupné z: https://www.bis.cz/otevrene-zdroje/

[17] BAZZELL, M. Open Source Intelligence Resources For Searching and Analyzing Online Information fifth edition, CreateSpace Independent Publishing Platform, 2016. ISBN 978-1530508907. S. III, IV

b) **aktivní** metodou rozumíme cílenější vyhledávání dat/informací, které se mohou zpočátku tvářit jako informace skryté. Hovoříme tedy o užším, konkretizovanějším záběru požadovaného cíle vyhledávání.

Rozdělit vyhledávaná data v OSINT metodě můžeme podle dostupnosti:

a) **zveřejněné nebo odvysílané** – média, online příspěvky, zprávy, rozhlasový pořad

b) **dostupné na základě veřejné žádosti** – informace získané na základě žádosti některého ze subjektu státní správy (jedná se o vládní informace ze sčítání lidu pozn. aplikovatelné spíše v zahraničí – v tuzemsku veřejně dostupné na internetových stránkách czso.cz)

c) **dostupné na základě předplatného nebo nákupu** (dálkový přístup do katastru nemovitostí, placené publikace)

d) **veřejně vyhledatelné** (internetové weby)[18]

Metodu OSINT je možné také rozdělit následovně:

a) **podle zdroje – osoby, věci**, čímž není pro tyto účely myšleno zdroj, který nám informaci sděluje nebo od kterého informaci dotazujeme, ale zdroj, který je nositelem požadované informace, kdy v tomto případě se jedná o vyhledávání informace o osobách či věcech (např. František Mrázek, Resort Čapí hnízdo)

b) **podle témat – situace, událost**, v tomto případě nebude hledat informace o konkrétní osobě či věci, ale o nějaké situaci nebo události (například válka na Ukrajině, covidová pandemie).[19]

---

[18] KADAR, T. Top 10 OSINT (Open Source Intelligence) Software & Tools. SEON Fraud Prevention: The Best Tools for Fraud Fighters [online]. 2023. [cit. 18.01.2023]. Dostupné z: https://seon.io/resources/the-best-tools-for-osint/?utm_term=&utm_campaign=%5BS%5D+Blog+-+dynamic+%5BGlobal%5D&utm_source=google&utm_medium=cpc&hsa_acc=4202831505&hsa_cam=18737907277&hsa_grp=139814728781&hsa_ad=631421714770&hsa_src=g&hsa_tgt=dsa-1465635799605&hsa_kw=&hsa_mt=&hsa_net=adwords&hsa_ver=3&gclid=EAIaIQobChMI-pqvi4Tc_AIV5UiRBR1YKw4tEAAYASAAEgKysvD_BwE

[19] Dokument z neveřejného školení pro pracovníky SKPV. 2022

Dalším důležitým rozdělením, které nespadá pod základní rozdělení metody OSINT, ale je neméně důležitý pro metody kriminálního zpravodajství je podle druhu dat:

a) **tvrdá data** – jedná se o data, která jsou přímo měřitelná časově i prostorově, podpořená statistikou, data objektivní, v kriminálním zpravodajství pro potřeby Policie ČR jsou tvrdá data, data dostupná z evidencí PČR a informačních systémů – zde nelze hovořit o otevřených zdrojích, nicméně pro kriminální zpravodajství je tento pojem důležitý, jelikož při kriminálním zpravodajství je podstatné získaná data pomocí metody OSINT prověřit, či alespoň komparovat právě s těmito tvrdými daty tak, aby došlo k získání ucelené kriminalisticky relevantní informace

b) **měkká data** – data založená na základě postojů či názorů lidí, data subjektivní, pro účely OSINT v kriminálním zpravodajství hovoříme o měkkých datech jako o datech, získaných právě OSINT metodou, tedy datech ze sociálních sítích, zpráv, rozhlasu, novin atd., takto získaná data mohou být manipulována, zkreslena nebo dokonce můžou pocházet z dezinformací a je nutno k nim takto i přistupovat [20,21]

Z pohledu využívání měkkých a tvrdých dat by se mělo hledět na relevantnost získaných dat. Pro úspěšné prověřování by měly být cíleně vyhledávány takové informace, které lze ověřit, alespoň pokud je chceme v trestním řízení využít jako důkaz. Pro operativní, taktický postup nám stačí informace nepodložená, protože i taková informace může operativnímu rozpracování pomoci. Při vyhledávání měkkých dat (například příspěvky na sociálních sítích) můžeme zjistit skutečnost, kterou je ale třeba komparovat se skutečným stavem, což lze provést osobní prověrkou takové informace, nebo prověrkou v dostupných evidencích a informačních systémech. Takovým ověřením pomocí tvrdých dat a potvrzením hledané informace, pocházející

[20]BURIÁNEK, J. Data měkká a tvrdá – Sociologická encyklopedie. [online]. 2017. [cit. 18.01.2023]. Dostupné z: https://encyklopedie.soc.cas.cz/w/Data_měkká_a_tvrdá

[21] Dokument z neveřejného školení pro pracovníky SKPV PČR. 2022

z měkkých dat dochází ke vzniku kriminalisticky relevantní informace. Jedná se o informaci, která je využitelná v prověřování a která toto prověřování posouvá k objasnění celé věci, ať už z pohledu objasnění děje a okolností prověřované trestné činnosti, tak z pohledu ztotožnění pachatele.

Obecně vzato, metody zpravodajství z otevřených zdrojů vycházejí z metod zpravodajství jako takového, a tak jde OSINT při získávání informací ruku v ruce se zpravodajskými cykly, které jsou jakousi metodickou kuchařkou pro zpravodajskou činnost.

2.1.2. Zpravodajský cyklus

Předtím než budeme hovořit o zpravodajských cyklech, je důležité definovat dva základní pojmy, které se v této práci často vyskytují. Jedním z nich je zpravodajská činnost. Zde si pomůžeme citací dle Luďka Michálka: „*Cílem zpravodajské činnosti je zejména získávání shromažďování a vyhodnocováni (souhrnně zabezpečování) informací potřebných pro rozhodovací proces a požadovaných vládou či jiným oprávněnými zadavateli a uživateli. Informace jsou získávány všemi dostupnými prostředky a postupy, tedy jak otevřenými, tak i utajovanými. Zpravodajská činnost může také zahrnovat provádění tzv. skrytých akcí (covert action, aktivní opatření), tedy operací zaměřených na přímé ovlivňování situace v cizí zemi požadovaným způsobem tak, aby nebylo zjevné zapojení vlastní vlády do takové akce nebo aby toto zapojení bylo možné uvěřitelným (hodnověrným) způsobem popřít (plausible denial). Nedílnou součástí zpravodajské činnosti je také ochrana vlastních utajovaných skutečností před činností cizích zpravodajských organizací.*

Zpravodajská informace je výsledek zpracování shromážděných dat a informací týkajících se informačních požadavků zadavatele.“[22]

[22] MICHÁLEK, Luděk, POKORNÝ, Ladislav, STIERANKA, Jozef, MARKO, Michal. Zpravodajství a zpravodajské služby. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2013. ISBN: 978-80-7380-428-2. S. 15

Druhým definovaným pojmem je kriminální zpravodajství. Zde můžeme uvést, že kriminální zpravodajství je souhrn činností OČTŘ v trestním řízení a činností policie nebo jiného subjektu při získávání poznatků o trestné činnosti nebo předcházení trestné činnosti. Tyto činnosti jsou prováděny v rámci jednotlivých zákonů a v nich vymezených oprávnění. Předmětná oprávnění umožňují uvedeným subjektům utajovaně bez vědomí dotčených osob získávat, shromažďovat a také vyhodnocovat informace o těchto dotčených osobách. Dotčenou osobou je myšlena ta osoba, proti které se tr. řízení vede nebo o jejíchž tr. činnosti jsou získávány poznatky nebo jejíchž tr. činnosti má být předcházeno.[23]

Zpravodajský cyklus popisuje Luděk Michálek takto: „*Zpravodajský cyklus je základním metodologickým postupem zpravodajské činnosti. Je to sled postupných, vzájemně na sebe navazujících a cyklicky se opakujících kroků, v jejichž průběhu jsou získávány a shromažďovány data a informace, zpracovány do podoby zpravodajských informací a předáván oprávněnému uživateli.*“[24]

Nyní můžeme hovořit o konceptu zpravodajského cyklu jenž by mohl mít následující schéma:

1) požadavek (requirements) – prvním spouštěčem zpravodajské činnosti je vznesení požadavku na vyhledání, získání nedostupných informací, které jsou potřebné, nebo lze také definovat problém, v případě kriminálního zpravodajství bude požadavek k získání informace zadávat určený policista zodpovědný za vedení prověřování nebo jeho nadřízený

2) plánování (planning) – nutnost naplánování a stanovení postupu při vyhledávání požadované informace (kde, za jakou cenu, kdo atd.), plánování

[23] MICHÁLEK, Luděk a kol. Kriminální zpravodajství jako nástroj kontroly trestné činnosti a zajišťování vnitřní bezpečnosti. Praha: Policejní akademie České republiky v Praze, 2020. ISBN: 978-80-7251-506-6. S. 12

[24] MICHÁLEK, Luděk, POKORNÝ, Ladislav, STIERANKA, Jozef, MARKO, Michal. Zpravodajství a zpravodajské služby. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2013. ISBN: 978-80-7380-428-2. S. 130

v případě kriminálního zpravodajství bude provádět oprávněný pracovník, který bude pověřen vyhledáním požadované informace

3) sběr (collection) – samotný sběr dat a informací utajeným i neutajovaným způsoby a prostředky – zdroje sběru lze rozdělit následovně:

A) veřejně dostupné zdroje (otevřené zdroje), odtud zkratka ‘‘OSINT‘‘

B) utajené zdroje a metody – tyto dále dělíme na:

a) kontaktní

- HUMINT (Human Inteligence) -získané lidmi od lidí

b) získané na dálku technickými prostředky:

- SIGINT (Signal Inteligence) – rádiové zpravodajství
- IMINT (Image Inteligence) – zobrazovací zpravodajství
- MASINT (Measurement and Signature Inteligence) – zpravodajství vyvozené z technických příznaků

4) zpracování (processing) – jedná se o prvotní zpracování získaných záznamů z velkého množství dat do přijatelnější formy, která bude uspořádanější a čitelnější i pro analytika, který není přímo specializovaný na tuto činnost. Tato fáze zpravodajského cyklu je velmi náročná, jelikož pracuje opravdu s velkým množstvím dat různého formátu. Ať už jde o informaci datovou, tvořící jedničky a nuly, či zašifrované soubory, které je potřeba převést například do obrázku, textu nebo i překladu z nejrůznějších jazyků rozhlasového vysílání. Dále je potřeba získaná data následně roztřídit a ukládat do zabezpečených uložišť, a sice ve formě, která je za pomoci počítačů lehce dohledatelná.

5) analýza (analysis) – pravděpodobně rozhodující fáze probíhá vytyčením důležitých částí ze surových dat, která se čerpají ze širokého spektra utajovaných i neutajovaných zdrojů. Z takto získaných dat se dále vypracuje analytická zpráva. Při jejím vypracování jsou aplikovány expertní znalosti, spočívající v zacházení s daty a komentáři k vypracované zprávě, které přidávají finální zprávě jakousi nadstavbu. Při vytváření analýzy je důležitá znalost zdrojů ze strany analytika, což obnáší povědomí o možnostech, limitech a slabinách

těchto zdrojů. Další podstatnou činností analytika je označení důvěryhodnosti zdroje a důvěryhodnost konkrétní informace. Popsaná činnost je důležitá pro stanovení priorit využívání vyhledaných informací a současně může pomoci při stanovení ověření takové informace.

Hodnocení důvěryhodnosti a spolehlivosti lidských zdrojů podle metodik NATO:

a) zcela spolehlivý – dlouhodobě prověřený zdroj, zdroj je kvalifikovaný, autentický a vždy mluví pravdu

b) obvykle spolehlivý – zdroj nemá vždy přímý přístup k věci, je možnost drobné pochybnosti o kvalifikaci a autenticitě zdroje, většinou pravdomluvný

c) asi spolehlivý – možnost záměrného vytěsnění některých skutečností, pochybnosti o jeho kvalifikaci, zdroj občas přináší pravdivé informace

d) obvykle nespolehlivý – většinou se jedná o zdroj nekvalifikovaný a neautentický

e) nespolehlivý – zprávy mohou být podvržené, překroucené, zdroj poskytuje nekvalifikované a neautentické vstupy

f) nelze posoudit – jedná se o nový zdroj, neznámý nebo neprověřený zdroj informace, stupeň autenticity a kvalifikovanosti nelze dosud posoudit

Škála důvěryhodnosti a konkrétní informace:

a) pravdivá informace – ověřená i z jiných informačních zdrojů

b) pravděpodobně pravdivá – zapadá do kontextu, navazuje na jiné informace, není jinak potvrzená

c) asi pravdivá – nepotvrzená, nevyvrácená informace, která je ovšem logická, nicméně není možné z takové informace učinit nějaké závěry, např. je příliš obecná

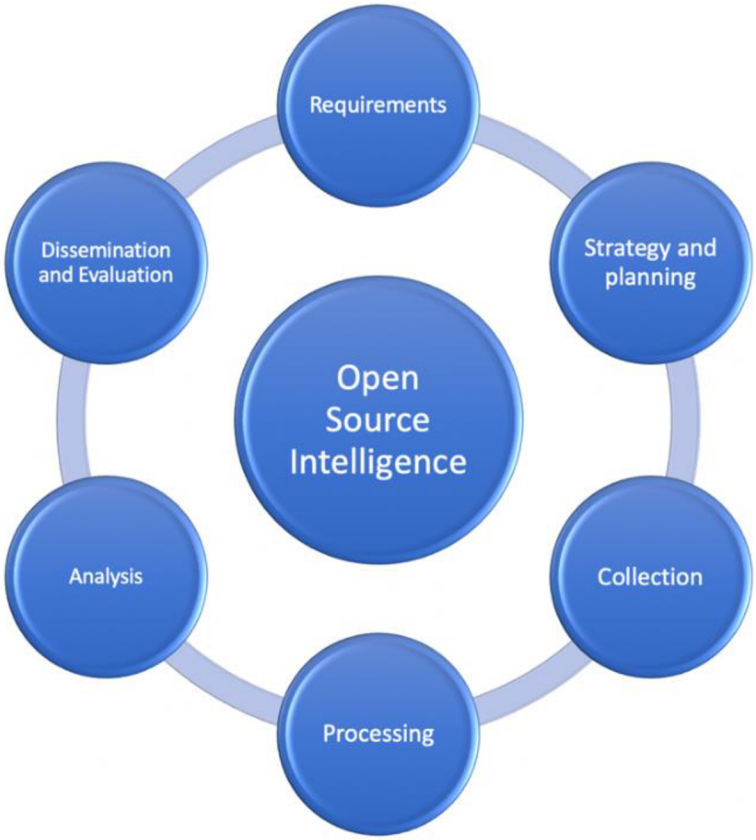
d) pochybná, ale možná pravdivá – je nepravděpodobná, ale není logicky vyloučitelná, nelze přijmout ani odmítnou a je možné, že v dalším vývoji získá platnost

e) **nepravděpodobná** – v rozporu s jinými informacemi, postrádá logiku a není v kontextu s ostatními dosud zjištěnými skutečnostmi

f) **nelze posoudit** – není dostatek dat k porovnání

6) **vytvoření výstupního produktu (někdy uváděno jako součástí 5. fáze)** – odevzdání odpovědi na zadaný požadavek, tedy předání vypracované zprávy, která uvede zjištění informací na základě zadání

7) **předání uživatelům (dissemination)** – doručení zpracované zprávy k zadavateli[25]



Obrázek č. 1: Zpravodajský cyklus dle Roberta André Furuhaug[26]

[25] ZEMAN, Petr. Zpravodajský cyklus-klišé nebo nosný koncept?. Obrana a strategie. Brno: Univerzita obrany. 2010. 45-64, 115. DOI: 10.3849/1802-7199.10.2010.01.045-064. S 46-58

[26] FURUHAUG, André, Robert. Open Source Inteligence Methodology. AI-Powered Research Tool. [online]. 2019. [cit. 18.01.2023]. Dostupné z: https://www.semanticscholar.org/paper/Open-Source-Intelligence-Methodology-Furuhaug/56e8ea14b1279cb77c91df8898957a4f71b90ea4

Zpravodajskými cykly lze definovat metody zpravodajské činnosti. Jak bylo již zmíněno, metoda OSINT vychází z těchto cyklů, kdy se liší některými body, především způsobem provedení těchto metod. Jednoduše řečeno, OSINT probíhá převážně vytěžováním informací dálkovým přístupem k veřejným zdrojům. Ve výše uvedených fázích zpravodajského cyklu se však liší pouze v jednom bodě, a sice v bodě č. 5 – sběr. Odlišení není správný výraz, nýbrž se jedná spíše o vyloučení jedné části sběru informací. Nebude zvolena utajená metoda a utajené zdroje. Zvolením metody vyhledávání v otevřených zdrojích tak dojde k naplnění podstaty metody OSINT. V případě, že zvolíme kriminální zpravodajství prováděné metodou OSINT, bude tak zpravodajství probíhat v popsaném cyklu: zvolíme si jakou informaci hledáme, naplánujeme, jak nejlépe informaci nalézt, posbíráme co nejvíce informací o daném objektu vyhledávání, informaci zpracujeme tak, aby byla co nejsrozumitelnější. Poté data vyhodnotíme, tedy zanalyzujeme a na závěr vyhotovíme finální zprávu. Pro potřeby kriminálního zpravodajství je pak důležitá i skutečnost, jestli dokážeme získanou informaci procesně řádně zavést do prověřovaní trestné činnosti tak, aby mohla být použita jako důkaz, nebo se bude jednat jen o informaci taktickou pro operativní využití.

Veškeré dosud zmíněné informace slouží k naplnění cíle této práce. Vytvářený checklist by měl být co nejefektivnější a z tohoto důvodu je nutné poznat a orientovat se v základní problematice OSINT. Požadovaná finální podoba checklistu by měla obsahovat informace o osobách (FO i PO), přičemž předtím, než budou data zanesena do checklistu, bude nutné tyto informace vyhledat a získat. K tomuto vyhledávání budou použity mimo jiné právě zpravodajské cykly.

OSINT, oproti klasickému zpravodajství, kde se využívají jako zdroj informací fyzické osoby, nepřináší žádné přímé nebezpečí, směřující k ohrožení příslušníka bezpečnostního sboru nebo zpravodajské služby, provádějící zpravodajskou činnost. Není nutné vystavovat tyto pracovníky v zájmovém prostředí, protože vše probíhá vzdáleným přístupem k veřejně dostupnému zdroji. Neznamená to však, že OSINT je metodou zcela bezpečnou. Existuje zde totiž riziko odhalení zájmu o danou konkrétní informaci, či odhalení samotné

vyhledávací činnosti, která by dekonspirovala úřad, službu či orgán, pátrající po informacích. V další kapitole bude práce zaměřena na bezpečné vyhledávání v otevřených zdrojích, tak aby riziko odhalení bylo úměrné ke kvalitě získané informace.

2.2. Bezpečnost vyhledávání z pohledu uživatele vytěžujícího otevřené zdroje

Bezpečnost byla v této práci několikrát zmiňována, zejména v souvislosti se zajištěním konspirace činnosti při vyhledávání v otevřených zdrojích. Z pohledu laiků by se mohlo zdát, že je jednoduché zabezpečit svou činnost na počítači na kterém pracují. Přímým řešením je pořízení antiviru, ať už v podobě bezplatné licence, tak v podobě placené licence. V případě pořízení antivirového programu určitě nelze mluvit o dostatečné ochraně proti sledování našeho pohybu v internetovém prostředí. U placených licencí je důležité hlídat, co vlastně je placeno. Ne všechno, co je placené, musí automaticky znamenat, že je bezpečné. Některé programy nabízí ochranu proti sledování činností na internetu nebo tzv. ‘‘anonymní surfování‘‘. Ne vždy je anonymní surfování opravdu anonymní, co do viditelnosti v síti internet. Některé anonymní režimy totiž nabízejí pouze nevysledovatelné sledování a prohlížení webových stránek na konkrétním PC nebo v domácí síti. Proto lze říci, že antivirový program je jasnou volbou do běžné domácnosti. Nicméně pro potřeby zpravodajství je nutné volit komplexní řešení ochrany, které zahrnuje použití bezpečnostních programů a služeb. Důležitým faktorem bezpečnosti na internetu je i chování uživatele při konkrétní zpravodajské činnosti.

V případě bezpečnosti při využívání metody OSINT hovoříme o tzv. defenzivním OSINTu. Tedy zabezpečení naší činnosti tak, abychom byli nedohledatelní. Je nutné uvědomit si, kdo je naším nepřítelem při snaze utajit naši činnost. Jsou jimi internetové vyhledávače, kdy největším naším ‘‘protivníkem‘‘ je Google. Dále také zprostředkovatelé internetového připojení, kteří už ve své podstatě mají dostupné velké množství dat o připojení uživatele. Dalším

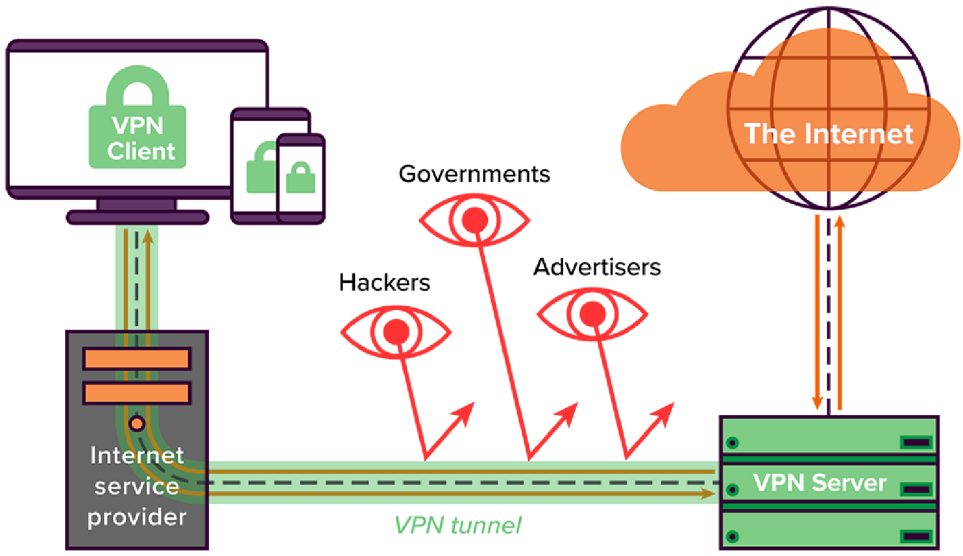
potenciálním nebezpečím na internetu jsou samotné zpravodajské služby cizích mocností, antivirové programy, operační systémy, hackeři a v neposlední řadě cíle našeho vyhledávání. Musíme si také uvědomit, co je nutné utajovat z naší strany. Budeme se snažit utajit příslušnost k PČR, vlastní identitu, místo připojení a zařízení, ze kterého se připojujeme a o koho se zajímáme. Lze nastavit protiopatření, abychom minimalizovali nebezpečí odhalení, některá základní protiopatření uvedeme v následujícím rozdělení:

1) **důsledné oddělení soukromých a pracovních záležitostí** – k dispozici bychom měli mít zařízení vyčleněné pro potřeby vytěžování veřejných zdrojů

2) **anonymizace sítě** – naší snahou by mělo být docílení neviditelnosti při vyhledávání na internetu, tedy nezanechání datové stopy, podle které by bylo možné nás dohledat, což lze docílit využitím šifrování a skrytí našeho připojení pomocí následujících způsobů:

   a) **VPN (Virtuální Privátní Síť)** – jedná se o šifrované připojení přes internet ze zařízení do sítě. Toto šifrované připojení zajišťuje bezpečný přenos citlivých dat, zabraňuje vysledování provozu a umožňuje uživatelům vzdálený přístup do sítě. Programy na provoz VPN můžeme pořídit bezplatně, což pro nás znamená omezená rychlost připojení a méně lokalit připojení. Jako příklad neplacených VPN programů můžeme uvést DewVPN, PrivadoVPN, Windscribe, VPNHub. VPN programy, které se platí, mají neomezenou rychlost datového toku a více lokalit připojení, je ale nutné se registrovat a zaplatit licenci. Příklad programů: ProtonVPN, Nord VPN, Surfshark, Cyberghost.[27]

[27] What Is a VPN? - Virtual Private Network-Cisco. Networking, Cloud, and Cybersecurity Solutions – Cisco. [online]. 2023. [cit. 26.01.2023] Dostupné z: https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html

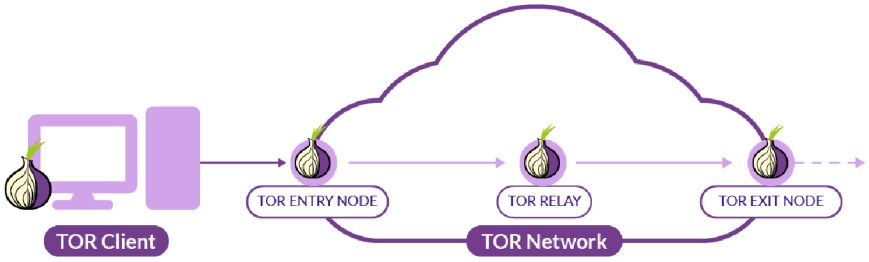


Obrázek č. 2 – schéma připojení přes VPN, autor neuveden[28]

b) TOR – zkratka TOR znamená ‘‘The Onion Router‘‘, jedná se o bezplatný prohlížeč, který má otevřený zdrojový kód, umožňující anonymně surfovat po internetu. Po každém uzavření internetového prohlížeče prohlížeč TOR automaticky vymaže historii vyhledávání a zašifruje veškerý provoz. Další specifickou vlastností je přístup k Dark Webu. Síť TOR byla vyvinuta americkým námořnictvem pro potřeby anonymní online komunikace této vojenské organizace. V roce 2006 projekt převzala nezisková organizace a dnes se TOR project zaměřuje na svůj prohlížeč a vývoj dalších nástrojů na ochranu soukromí jeho uživatelů. TOR umožňuje šifrovaný provoz přes řadu 3 prostředníků, tím oddělí vaši IP adresu od prohlížené stránky a vaše stopa je tak jen velmi těžko dohledatelná. Existují ovšem služby jako například sociální sítě, které připojení přes TOR blokují.[29]

[28] Autor neuveden. Co je VPN a jak ji můžeme využít? *Forescope* [online]. 2020. [cit. 30.1.2023]. Dostupné z: https://www.forscope.cz/blog/co-je-vpn/

[29] PORUTIU, Theodor. What is the Tor Browser? A Guide to the Dark Web Browser. VPNOverview.com | News and Reviews, Privacy and Anonymity [online]. 2014. [cit. 30.01.2023]. Dostupné z: https://vpnoverview.com/privacy/anonymous-browsing/tor/



Obrázek č. 3 – schéma připojení přes TOR dle Jason DONAHUE[30]

c) **mobilní hotspot** – jedná se o připojení k internetu prostřednictvím vytvořeného mobilního přístupového bodu. Díky připojení prostřednictvím mobilního hotspotu docílíme dynamické IP adresy, která se po každém připojení mění, není stálá, a tudíž je velmi obtížné určit dle IP adresy koncového uživatele.

3) **volba operačního systému** – v tomto případě máme na výběr ze dvou základních variant operačních systémů a sice Linux či Windows. V porovnání těchto dvou systémů vychází pro potřeby OSINTu jednoznačně lépe Linux. U systému Linux má plnou kontrolu nad systémem uživatel, běží zde naprosté minimum procesů. Jinými slovy, spouští se jen to, co uživatel opravdu spustit chce a není vyžadováno nastavování dalších uživatelských bezpečnostních nastavení. Oproti tomu systém Windows vyžaduje doplňková bezpečnostní nastavení, jakým je například Firewall, čištění systému nebo antivirus a na pozadí běží všechny aplikace, které by mohl uživatel potřebovat. Jednou z dalších nevýhod u Windows, z pohledu užívání metody OSINT, je kontrola systému, kterou má v rukou společnost Microsoft.

4) **volba internetového prohlížeče** – již samotným nastavením prohlížeče si můžeme pomoci k bezpečnějšímu vytěžování internetu v prostředí internetových prohlížečů. Jedná se například o nastavení zobrazování polohy,

[30] DONAHUE, Jason. How to detect TOR network connections with Falco. *Sysdig*. [online]. 2022. [cit. 29.1.2023]. Dostupné z: https://sysdig.com/blog/detect-tor-network-connection-falco/

automatické mazání souboru cookies, ukládání, respektive neukládání hesel a historie. Lze si pořídit i doplňky, které dokáží bezpečnost vyhledávání v prohlížečích zvýšit. Adblock, který blokuje reklamy, CookieAutoDelete, který automaticky maže soubory cookies, doplňky pro blokaci sledovacích prvků (Ghostery, Privac Badger). Uvedeme zde i několik základních internetových prohlížečů, které jsou pro OSINT vhodnější:

a) **Firefox, Brave** – možnost nastavení soukromí, správa rozšiřujících aplikací, jedná se o menší firmy, a proto ztráty uživatelů jsou v případě jejich zklamání o to větší. Již z této podstaty lze předpokládat lepší ochranu soukromí uživatelů.

b) **Chrome, Edge** – jsou to dominantní hráči na trhu a existuje zde riziko zneužití tohoto postavení. Rizikem je myšleno historie vytěžování a následná profilace uživatelů (reklamy na míru) a dále v minulosti identifikovaná spolupráce s agenturami cizích mocností.

5) **volba internetového vyhledávače** - pokusíme se rozdělit vyhledávače podle bezpečnosti pro potřeby zpravodajství z otevřených zdrojů:

a) **bezpečné** – Startpage, DuckDuckGo, Swisscows
b) **víceméně bezpečné** – Metager, Brave
c) **nebezpečné** – Google, Yahoo, Yandex

Z pohledu defenzivního OSINTu by si policisté měli dávat pozor i na detaily jako je pojmenování jejich zařízení, kterými se připojují k WiFi nebo Bluetooth. I nastavení hardwaru počítače, který bude pro OSINT používán, je velmi důležité. V případě přítomnosti vestavěné kamery a mikrofonu by měl být mikrofon vypnut a kamera překryta. Za využití výše popsaných bodů by datová stopa uživatelů provádějící OSINT měla být zanedbatelná. [31]

Při využití znalostí k zabezpečení uživatele vyhledávajícího v internetovém prostředí bychom měli dosáhnout minimalizování rizik spojených s odhalením naší činnosti.

[31] Prezentace z neveřejného školení pracovníků SKPV PČR ze dne 16.06. 2021.

2.3. Sociální sítě

O sociálních sítích lze říci, že je běžně využíváme jako okno do životů jiných osob, prohlížíme si činnosti našich přátel, sousedů, bývalých partnerů, spolužáků, ale také celebrit nebo našich vzorů. Důvodem, proč takto nahlížíme do životů ostatních, je snaha nenechat si nic ujít. S nadsázkou můžeme říci, že je to jako jedna velká reality show, do které si své hrdiny vybereme my sami.[32]

Současnost lze nazvat jako věk sociálních médií. Známé sociální sítě Facebook, Twitter, Google a LinkedIn jsou zástupci rychlého přenosu lidských životů, jejich interakcí, identit, argumentů a názorů do jakési veřejné a soukromé sféry, kterou můžeme pojmenovat jako digitální sociální společenství. To vše je realizováno v bezprecedentním měřítku. Pro příklad, denně je na Facebook nahráno 250 miliónů fotografií, na Twitter 200 miliónů tweetu a na YouTube je denně shlédnuto 4 miliardy videí. Reakcí na takový trend je vznik nové zpravodajské metody ‘‘SOCMINT‘‘ – zpravodajství sociálních médií, což je vlastně příbuzný metody OSINT. SOCMINT vznikl jako reakce bezpečnostních složek států do národního zpravodajského rámce, kdy nejdříve bylo nutné vytvořit pevný metodologický základ shromažďování, evidence, ověřování, porozumění a aplikace. Ve Spojeném království již vznikl legislativní rámec, který umožnil tamním donucovacím orgánům udržet si schopnost bojovat proti zločinu s ohledem na to, že pachatelé využívají moderní technologie a objevují nové způsoby ve společné komunikaci prostřednictvím digitálního prostoru. V digitálním prostoru plánují i páchají trestnou činnost. Orgány činné v trestním řízení se snaží využít zpravodajství sociálních medií, kdy je na pořadu dne otázka metodologického a etického rámce využívání metody SOCMINT. Shromažďování

[32]LOSEKOOT, Michelle; VYHNÁNKOVÁ Eliška. Jak na sítě: ovládněte čtyři principy úspěchu na sociálních sítích. Brno: Jan Melvil Publishing, 2019. Žádná velká věda. ISBN 978-80-7555-084-2. S. 35.

informací metodou SOCMINT bude veřejně přijatelné jen v případě, že bude prováděno správně a autorizovaně.[33]

Kriminální zpravodajství prostřednictvím sociálních sítí patří k velmi užitečným zdrojům. Prostřednictvím sítí jako je Facebook, Instagram nebo moderní Tik Tok lze vyhledat osoby a někdy i společnosti. Těmi největšími hráči na poli sociálních sítí jsou Facebook, Twitter, Instagram, Youtube. Díky zpravodajství, obsaženém v těchto veřejně dostupných zdrojích, můžeme vyhledat pro potřeby orgánů činných v trestním řízení poměrně zajímavé informace, které nejsou dostupné v žádných evidencích ani informačních systémech. Informace, které nejsou dostupné ani v jiném druhu veřejně dostupného zdroje. Mezi informacemi, zveřejněnými na těchto sociálních sítích jsou fotografie, videa, přátelské struktury uživatelů, informace o zájmech osob, ale i vztahy mezi jednotlivými uživately. V případě, že si uživatel nastaví soukromí tak, aby citlivě chránil své údaje, je těžké se k těmto datům dostat. Při zpravodajství na sociálních sítích tak vše závisí na samotném nastavení účtu toho daného uživatele.

Jak bylo výše naznačeno SOCMINT je typem zpravodajské metody OSINT, která je zaměřená na sběr a analýzu dat z platforem sociálních médií. V otázce, v čem se liší OSINT a SOCMINT, by mělo být řečeno, že OSINT se zaměřuje pouze na informace, které jsou veřejně dostupné a existují názory, že i sociální sítě jsou veřejně dostupné. Stejný názor nesdílí uživatelé a zastánci soukromí na sociálních médiích, kde určitou míru soukromí předpokládají. Existuje však aspekt, který je nutný minimálně zvážit a brát na něj do jisté míry ohled. SOCMINT může vyhledávat a následně i použít informace obsažené na platformě sociálních médií, které byly určeny pro konkrétní publikum. Otázkou zákonnosti pak zůstává případ, kdy pro využití SOCMINT metody je založen falešný účet, přes který se subjekt, který využívá metodu SOCMINT, snaží připojit k soukromé

[33] CHRISTOPHER, Andrew, Richard; ALDRICH J. Richard; WARK K. Wesley. Secret Intelligence. A Reader. Second Edition. New Yor, USA: Routledge, 2020. ISBN 978-0-415-70567-7. S. 77, 78.

skupině nebo se snaží dostat k obsahu, který má na svém profilu zájmová osoba.[34]

Sociální sítě jsou fenoménem v posledních 15 letech. Není se čemu divit, že počet uživatelů vzrůstá, a to i v zájmovém prostředí. Vyhledávání v sociálních sítích je často podmiňováno registrací uživatelského účtu. V současné době již pro potřeby OČTŘ probíhá vytěžování sociálních sítí a získávání informací vedoucí k ustanovení zájmových osob. Toto vytěžování však musí probíhat se skrytou identitou. Za tímto účelem se na sociálních sítích vytvářejí falešné profily.

Služby jako je Google, poskytnou komukoliv více účtů na Gmail a Google+ jen s minimálním ověřením. Kdežto Facebook, Twitter, Instagram nebo Yahoo nutí uživatele překonat mnoho překážek k udělení přístupu. Níže uvedeme souhrn nejoblíbenějších služeb, včetně požadavků na ověření a náhradních řešení. Tyto techniky byly ověřeny na jiných službách, které blokují skryté účty.

1) **Facebook** – nejtěžší založení nového účtu, u většiny nově zakládaných účtů vyžaduje Facebook ověření zadáním telefonního čísla. Na toto telefonní číslo je pak zasílán ověřovací text. Řešením je vypnout VPN nebo například Tor Browser tak, aby nedocházelo k zakrývání IP adresy. Poté se přihlásit z domácího internetového připojení a založit účet pod emailovou adresou,vytvořenou na bezplatné emailové platformě, která není populární jako například Google nebo Yahoo. Jedná se například o emailovou platformu založenou na serveru My Way (mayway.com). Na Facebooku je pod takto založeným emailem registrováno málo lidí a tyto účty nejsou Facebookem označené jako podezřelé.

[34] MALTEGO. Everytthing About Social Media Intelligence (SOCMINT) and Investigations. [online]. 2022. [cit. 26.01.2023]. Dostupné z: https://www.maltego.com/blog/everything-about-social-media-intelligence-socmint-and-investigations/

2) **Twitter** – zde bude vyžadováno přihlášení pod účtem Twitteru, u kterého bude stačit registrace účtu pod legitimní emailovou adresou z domácího nebo firemního internetového připojení, nikoliv však veřejné Wi-Fi.

3) **Instagram** – pokud nebudeme vytvářet více účtu za jeden den ze stejného internetového připojení, budou podmínky stejné jako v předchozím případě u Twitteru. V tomto případě by neměl být kladen žádný odpor při vytváření anonymních účtů.

4) **Yahoo** – pro jednu z důležitých vyhledávácích technik na Facebooku je email, založený na Yahoo, velmi podstatnou součástí, bohužel. Bohužel i proto, že k založení účtu Yahoo má nový uživatel povinnost poskytnou telefonní číslo jako je tomu u Facebooku. Tuto překážku lze překonat použitím emailu od méně známého poskytovatele emailové platformy. Registrace musí být vytvořena z IP adresy, která za posledních 30 dní nevytvořila žádný nový účet.[35]

Jednou věcí je založení účtu na některé ze sociálních sítí. Druhou věcí je samotné vyhledávání informací. Jako příklad uvedeme úskalí vyhledávání na sociální síti Facebook. Současná doba je mírně nepříznivá pro cílený sběr informací ze sociálních sítí. Je to způsobeno uvědomováním si bezpečnostních rizik, která jsou spojena s užíváním sociálních sítí. V následujících letech je předpoklad, že znalosti, spojené s ochranou sdílených informací, budou lepší. O to složitější bude sběr těchto informací. Na začátku vyhledávání informací o osobách je nutné si uvědomit, že nemusí být dostačující znalost jména a příjmení vyhledávané osoby. Uživatelé si nemusí při registraci zadávat svá pravá jména. Problém nastane i při poznávání podle fotografie, která nemusí být přidaná, nebo může být značně zkreslující. Odlišnost uživatelského jména či neexistence fotografie osoby nemusí znamenat, že se jedná o zájmovou osobu se špatnou pověstí. Řešením může být vyhledání osoby v dostupných evidencích PČR, kde nám může pomoci jak fotografie, tak osoby v příbuzenském vztahu. Stejně tak se můžeme při vyhledávání osoby na sociálních sítích

[35] BAZZELL, M. Open Source Intelligence Resources For Searching and Analyzing Online Information fifth edition, CreateSpace Independent Publishing Platform, 2016. ISBN 978-1530508907. S. 75, 76

posunout, pokud budeme znát telefonní číslo zájmové osoby. Pokud toto číslo bylo registrováno s profilem na sociální síti, může nám to velice usnadnit ustanovení osoby. Často můžeme zájmovou osobu dohledat i přes účty rodinných příslušníků. Rodinní příslušníci mohou mít zájmovou osobu v seznamu přátel, nebo označenou na fotografii či zadanou v rodinné vazbě. Pokud vyhledáváme skupinu osob, u nichž známe účet alespoň jedné z nich, můžeme najít propojení v seznamu přátel nebo označení na fotografiích na tom známém účtu, a tím se dostat k ostatním osobám. V případě dohledání osob nastává situace:

a) **profil je veřejný** – informace jsou nabídnuty samotným uživatelem (přístup k fotografiím, přístupný seznam přátel)

b) **profil je soukromý** – uživatel nesdílí žádné informace, v tomto případě je nutné vyhledat user name uživatele, převést ho do ID Facebooku a pro vyhledávání použít dodatečné nástroje.

Po vyhledání či ustanovení dotyčné osoby je potřeba provést analýzu toho, co nám vlastně uživatelský účet říká. Například s kým je osoba často na fotografiích, komu dala k fotce ‘‘laik‘‘, komu přidala komentář k příspěvku, jaká má oblíbená místa, která navštěvuje. Z uvedených dat si lze udělat obrázek o osobě, o které jsme do té doby měli jen minimum základních údajů.[36]

Pro usnadnění vyhledávání a analýzy informací z účtů na sociální síti Facebook existuje i několik online nástrojů. Pokusíme se vyjmenovat alespoň ty nejužitečnější:

a) **Lookup ID** (https//lookup-id.com) – na této stránce můžeme dohledat osobní ID Facebooku, které je důležité pro používání jakékoliv jiné online služby, jenž je používaná k doplnění standartního vyhledávání klíčových slov na Facebooku

b) **Facebook Page Barometer** (http://barometer.agorapulse.com) – zde nalezneme statistiky a informace o konkrétních účtech nebo stránkách na sociální síti Facebook

[36] Dokument z neveřejného školení pro pracovníky SKPV PČR. 2022

c) Informace pro OČTŘ

(https://ww.facebook.com/safety/groups/law/guidelines) – stránky, jejichž obsahem jsou pokyny pro orgány činné v trestním řízení při vyhledávání informací na Facebooku a Instagramu

d) Whopostedwhat

(https://whopostedwhat.com) jedná se o generátor, který po vyplnění příslušného formuláře vyhledá na základě klíčových slov příspěvky na Facebooku, vyhledávání lze omezit na určitý časový výsek.[37]

Sociální sítě za pomoci metody OSINT nebo spíše SOCMINT jsou v dnešní době nepostradatelnou studnicí informací, kterou nelze při kriminálním zpravodajství přehlížet nebo opomíjet. Úspěch při vytěžování informací ze sociálních sítí není zaručen. Ovšem v případě, že budeme při vyhledávání informací na soc. sítích úspěšní, můžeme si tím v probíhajícím prověřování poskytnout hodnotná data.

2.4. Vyhledávání pomocí internetových vyhledávačů

Do většiny internetových vyhledávačů lze k vyhledávání využít příkazů zadaných do vyhledávacího pole. Tyto výrazy ovšem nejsou součástí hledaných výrazů a jsou označovány jako ‘‘operátory‘‘. Vyhledávání pomocí těchto operátorů má dvě části. Každá část je oddělena dvojtečkou. Na levé straně od dvojtečky je typ operátoru, jako je web, webový odkaz nebo text (přípona souboru). Vpravo je pravidlo pro operátora, tím je cílová doména nebo typ souboru. Příklad site operátora: ‘‘site:forbes.com Michael Bazzell‘‘, výsledkem bude vyhledání všech informací obsahující jméno Michael Bazzell na serveru forbes.com.[38]

[37]SOCradar. How to Use SOCMINT for Better Cause? [online]. 2021. [cit. 30.01. 2023]. Dostupné z: https://socradar.io/how-to-use-socmint-for-better-cause/#_ftn1

[38] BAZZELL, M. Open Source Intelligence Resources For Searching and Analyzing Online Information fifth edition, CreateSpace Independent Publishing Platform, 2016. ISBN 978-1530508907. S. 40

Světově nejrozšířenější vyhledávače jako je Google a Bing mají na svých serverech indexovány miliardy webových stránek. Uživatelům, používající tyto vyhledávače, to umožňuje zúžit a rozšířit výsledky vyhledávání díky pokročilým vyhledávacím operátorům. Umět ovládat operátory pokročilého vyhledávání je základní dovedností pro metodu OSINT ze dvou důvodů:

a) obrovské množství informací, které jsou obsažené ve vyhledávačích, je nutné umět co nejefektivněji přetvořit na konkrétní požadovanou informaci

b) mimo Google a Bing používají vyhledávací operátory i ostatní stránky jako například Twitter, který má pokročilé vyhledávání a též přijímá vyhledávání pomocí operátorů.[39]

Vyhledávací operátory podporuje i ryze český server seznam.cz. V sekci ‘‘nápověda‘‘ lze nalézt detaily popisu vyhledávacích operátorů. Níže uvedeme význam a použití operátorů dle serveru seznam.cz:

- **uvozovky (" ")**: k vyhledání přesné fráze se hledaná fráze zapisuje do uvozovek, stránka, na které je fráze dohledána, obsahuje všechna uvedená slova v zadaném tvaru a pořadí těsně u sebe, lze zadat i jednotlivé slovo, které bude vyhledáno bez skloňování (příklad zadání fráze "najdu tam co hledám" – vyhledá stránky, které obsahují text ve stejném znění, jako zadaný dotaz, "autem" – vyhledá slovo v zadaném tvaru)
- **intitle:** vyhledávání požadovaného výrazu v titulku stránky, v případě více hledaných slov se příkaz musí zopakovat (příklad použití operátoru intitle: seznam-vyhledá slovo ‘‘seznam‘‘ v titulku stránky, intitle:seznam intitle: nápověda - vyhledá slova ‘‘seznam‘‘ a ‘‘nápověda‘‘ v titulku stránky)
- **inurl:** vyhledává slova prvotně v URL stránky (příklad použití operátoru inurl: inurl:fulltext-vyhledá slovo ‘‘fulltext‘‘ v URL stránky, příkaz inurl:fultext,napoveda – vyhledá slova ‘‘fulltext‘‘ a ‘‘nápověda‘‘ v URL)

[39] Advanced Googleing. Open Source Intelligence Training for Law Enforcement. It's Our Business to Know. [online]. 2020. [cit. 03.02.2023]. Dostupné z: https://osinttraining.net/introduction-to-osint/advanced-googleing/

- **intext:** vyhledá zadané slovo přednostně přímo v obsahu stránku (příklad použití operátoru intext: intext:nápověda-vyhledá slovo nápověda v obsahu stránky)
- **lang:** omezuje vyhledávání jen na dokumenty v požadovaném jazyce, lze nalézt ty dokumenty, u nichž je možné jednoznačně určit jediný hlavní jazyk (příklad použití operátoru lang: cars lang:cs-vyhledá dokumenty, které obsahují výraz ‘‘cars‘‘ a zároveň mají detekovanou pouze češtinu - do výsledků nebudou zahrnuty cizojazyčné ani vícejazyčné dokumenty)
- **site:** je určen k ohraničení vyhledávání na zaindexované stránky z požadované domény, více domén je nutné oddělit čárkou (příklad použití operátoru site: site:seznam.cz – vypíše veškeré stránky z domény seznam.cz včetně všech jejich subdomén např. napoveda.seznam.cz, dalším příkladem je příkaz sklik site:seznam.cz, který umí vyhledávat stránky z domény seznam.cz obsahující slovo ‘‘sklik‘‘ a ty jsou seřazeny podle relevance s ohledem na hledaný text, příkaz prezident site:novinky.cz site:lidovky.cz – zapsáno více domén, ve kterých vyhledává slovo prezident)
- **notsite:** vyhledává veškeré informace až na stránky z požadované domény, použití stejné jako u operátoru site
- **filetype:** filtruje dokumenty na základě jejich formátu, omezit lze na formáty html, doc, rtf, pdf, ppt, txt (příklad použití operátoru filetype: borovice filetype:doc – vyhledá dokumenty ve formátu doc obsahující slovo ‘‘borovice‘‘, borovice filetype:pdf site:sofronka.cz – vyhledá dokumenty ve formátu pdf obsahující slovo ‘‘borovice‘‘, které se nacházejí na doméně sofronka.cz), tímto operátorem lze vyhledat pouze ty soubory, které Seznam standartně indexuje a nelze vyhledávat soubory bez textového obsahu jakou jsou například obrázky ve formátu .jpg
- **kombinace operátorů:** lze při zadávání operátorů kombinovat několik operátorů a tím zpřesnit výsledky vyhledávání (příkladem může být kombinace operátorů rod, pinus ‘‘borovice lesní‘‘site:sofronka.cz filetype:pdf –

tento příkaz dokáže vyhledat jen ty dokumenty ve formátu pdf, které jsou umístěny na doméně sofronka.cz a obsahují přesnou frázi borovice lesní).[40]

Uvedené operátory jsou ušité na míru serveru seznam.cz, nicméně většinu z nich lze použít i například na Google vyhledávači. Obecně platí, že zadávání těchto operátorů funguje stejným způsobem, jen se občas liší ve své formě, nicméně fakticky se jedná o stejný princip vyhledávání.

Pro porovnání uvedeme pár příkazů určené přímo pro Google:

- **mapa (map):** příkaz v Googlu ukáže mapové podklady pro zadanou oblast (příklad příkazu: map:silicon valley)
- **zdroj (source):** tento příkaz vyhledá zprávy z určitého zdroje (příklad příkazu: apple source:the verge)
- **loc:placeman:** vyhledává výsledky z dané oblasti (příklad příkazu: loc:"san francisco" apple)
- **film (movie):** vyhledá informace o konkrétním filmu i případné promítání filmu v blízkosti zadavatele (příklad příkazu: movie:steve jobs) Google neustále své operátorské příkazy odstraňuje, proto tyto byly tyto příkazy vybrány a vyzkoušeny podle aktuální funkčnosti.[41]

Vyhledávaní pomocí vyhledávače Google, jak už bylo zmíněno, je velmi nebezpečné, alespoň z pohledu snadného odhalení uživatele, který informaci vyhledává. Před vyhledáváním informací tímto způsobem je nutné zvážit, zdali jsme ochotni podstoupit riziko našeho možného odhalení, odhalení naší činnosti nebo našeho zájmu.

[40] Seznam.cz. Fultextové vyhledávání. Pokročilé vyhledávání s použitím operátorů. [online]. 2023. [cit. 03.02.2023]. Dostupné z: https://napoveda.seznam.cz/cz/fulltext-hledani-v-internetu/pokrocile-vyhledavani/

[41] HARDWICK, Joshua. Google Search Operators: The Complete List (42 Advanced Operators). Ahrefs - SEO Tools & Resources To Grow Your Search Traffic [online]. 2020. [cit. 03.02.2023]. Dostupné z: https://ahrefs.com/blog/google-advanced-search-operators/

2.5. Dark Web

Nejprve je důležité ujasnit si pár pojmů, se kterými se budeme v této kapitole setkávat. Na internetové síti se nachází značné množství informací. K některým informacím se dostaneme pomocí využití běžných vyhledávačů, nebo prostřednictvím vyhledávačů, které skrývají IP adresu, jako například TOR browser nebo VPN browser.

Informace vyhledatelné běžným vyhledávačem se nacházejí na takzvaném Surface webu, jenž tvoří pouhé 4% internetové sítě. Surface web používáme každý den a slouží k provádění našich běžných aktivit. Zkrátka to, co každý považuje za internet.[42,43]

Hluboký web, anglicky Deep Web není tak tajemný, jak by mohl napovídat jeho název. Za Deep Web lze označit i soukromou síť, která může být provozována kýmkoliv. Je to internet, který není dostupný pro standartní vyhledávače, příkladem může být síť, která je spravována placenou streamovací službou. Jedná se o nejrozšířenější kategorii nových informací na internetu. Deep Web našel využití na interních stránkách velkých společností, sdružení a obchodních organizací. Například systémy vysokých škol a univerzit Deep Web využívají pro přístup k online databázím. Můžeme říct, že Deep Web je používán pro legitimní účely, které vyžadují anonymitu. Deep Web potřebuje k přístupu zadání hesla a šifrování – typicky se jedná o internetové bankovnictví. [40,44]

---

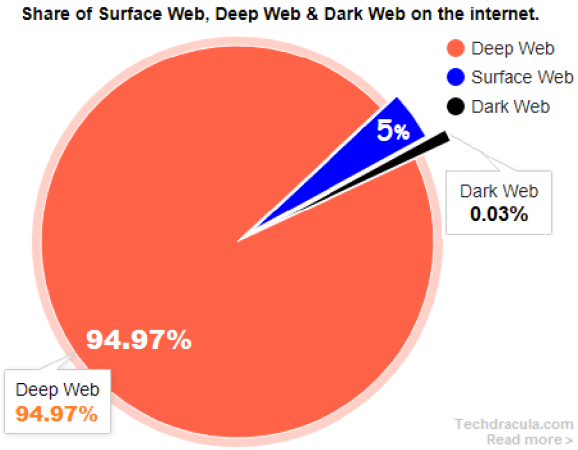
[42] ŠIMEK, Gabriel. Surface Web vs. Deep Web vs. Dark Web. CryptoNews.cz. Vše o kryptoměnách. [online].2021.[cit.05.02.2023]. Dostupné z: https://www.cryptonews.cz/bezpecnost/surface-web-vs-deep-web-vs-dark-web

[43] ALZA.CZ, Co je deep web? A jak se liší od dark webu?. [online]. 2019. [cit. 05.02.2023]. Dostupné z: https://www.alza.cz/co-je-deep-web

[44] TIWARI, Adytia. What Is The Difference Between Deep Web, Darknet, And Dark Web? Fossbytes-Technology Simplified [online]. 2020. [cit. 05.02.2023]. Dostupné z: https://fossbytes.com/difference-deep-web-darknet-dark-web/

Dark Web je součástí Deep Webu. Dark Web obsahuje internetové stránky, které nelze vyhledat v obvykle užívaných webových prohlížečích. K těmto internetovým stránkám, nacházejících se na Dark Webu, se lze dostat pouze za použití programů jako je TOR nebo například IP2. Uvedené programy jsou určeny ke skrytému přístupu na Dark Web, a to s ohledem na jejich schopnost zamaskovat IP adresu, díky čemuž je zajištěna anonymita uživatelů, kteří přistupují k internetovým stránkám. [45]

Jak již bylo zmíněno, běžný internet tzv. Surface net tvoří pouhé 4% internetové sítě. Pro lepší představu přikládáme znázornění podílu na internetové síti:



Obrázek č. 4 – podíl Dark Webu na internetové síti dle serveru Techdracula[46]

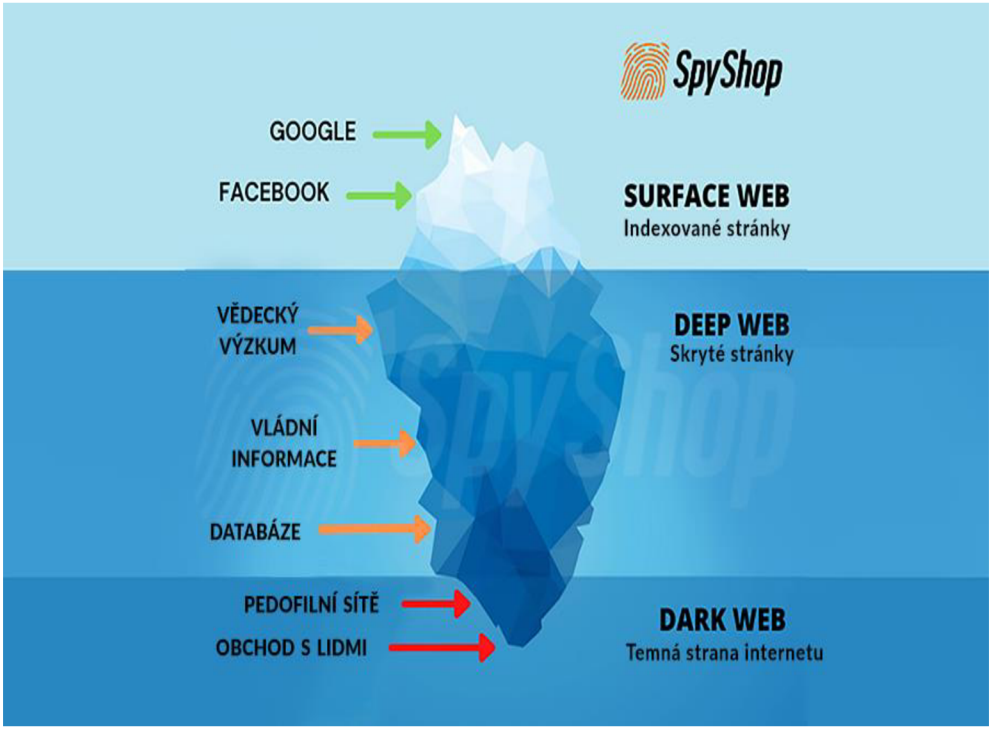
Dark Web je takřka neomezeným zdrojem nelegálního zboží a služeb, ke kterému se lze dostat prostřednictvím připojení k internetu odkudkoliv z celého světa. Prostřednictvím Dark Webu můžeme zakoupit nelegální zboží, a to od padělaných značkových oděvů, přes drogy, zbraně, dětskou pornografii,

---

[45] 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. ISBN: ISBN 978-3-319-47671-1. S. 111-112.

[46] TECHDRACULA. Surface web vs deep web vs dark web vs shadow web vs marianas web. Techdracula. [online]. [cit. 02.02.2023]. Dostupné z: https://techdracula.com/surface-vs-deep-vs-dark-vs-vs-shadow-vs-marianas-web/

bílé maso, brutální videa, která znázorňují násilí na skutečných lidech až po zakoupení lidských orgánů. Stejně tak zde lze objednat nelegální služby, jako například únosy, vraždy nebo legalizaci výnosů z trestné činnosti. Dark Web svou podstatou slouží také jako studnice poznatků a kriminalisticky relevantních informací o trestné činnosti včetně jejích pachatelů. Tyto poznatky využívají orgány činné v trestním řízení po celém světě. U našich útvarů PČR lze jistě dohledat několik kauz, při kterých bylo využito prostředí Dark Web k odhalení, zadokumentování a zastavení trestné činnosti. Stejně tak i rozkrytí organizovaných skupin, páchajících nelegální činnosti. Představu o tom, co vlastně znamená Dark Web v síti internet, si nejlépe uděláme prostřednictvím následujícího obrazového schéma:



Obrázek č. 5 – schéma Dark Webu podle Marie Novákové[47]

Vyhledávání na Dark Webu probíhá stejně jako na webu umístěném na běžné internetové síti, a to prostřednictvím nástrojů, které jsou určené k vyhledávání v indexech jednotlivých webů. Samozřejmě je důležité dodržovat

[47] NOVÁKOVÁ, Marie. ARK WEB - Temná strana internetu [+18] - SpyShop24.cz - detektivní blog. Spy Shop - Obchodní síť se špionážní technikou [online].2022, [cit. 04.02.2023]. Dostupné z: https://www.spyshop24.cz/blog_cz/dark-web-temna-strana-internetu-18/

bezpečnostní prvky vyhledávání, tím spíše, že se pohybujeme po Dark Webu, který je předurčen pro nelegální činnost. Lze tak předpokládat, že dojde k pokusu vysledovat naši činnost i naše umístění v síti. TOR sice maskuje naší IP adresu, ale je založen na vyhledávači Firefox a stejně jako ten, i TOR může mít bezpečnostní díry, které se zacelují aktualizací. Naskytuje se tak možnost nabourat naše vyhledávání na Dark Webu v době, kdy se čeká na aktualizaci a zalepení bezpečnostní díry. Při vyhledávání se používá tzv. information Slippage, což lze přeložit jako informační skluz. Při vyšetřování osob na Dark Webu je nutné provést atribuci mezi weby Surface netu a Dark Webem, a to díky informačnímu skluzu. To znamená nalezení podobných markantů, jako například uživatelská jména nebo adresy kryptoměn, která uživatel používá jak na webech Surface netu, tak na Dark Webu. Většina takto zjištěných kladných informací je způsobena chybnými návyky uživatelů. Tento informační skluz – chybné návyky uživatelů, může vést k ustanovení uživatele Dark Webu.[48]

Dark Web je velmi rozmanitá kapitola. Pro potřeby našeho checklistu, kterému se budeme věnovat v další kapitole, není zásadní. Důvodem je náročnost ustanovení osoby užívající Dark Web. Časová náročnost a možnosti ustanovování osoby, užívající Dark Web, je neefektivní k možnému výsledku. Důvodem je, že checklist má sloužit pro základní rozhled o umístění osoby v některém z veřejných zdrojů. Do tohoto základního rozhledu nepatří tak složitý úkon jako je prohledávání Dark Webu. Pro většinu prověřovaných trestných činů nemusí být taková informace použitelná ani uchopitelná. Z uvedených důvodů nebude na Checklistu uvedena informace o využívání Dark Webu. Získanou informaci lze uvést v případě, že v průběhu prověřování vyjde tato skutečnost najevo a její zjišťování nebude vykoupeno časem a náročností vyhledávání.

[48] OSINT COMBINE. Dark Web Searching. Open Source Intelligence. [online]. 2020. [cit. 05.02.2023]. Dostupné z: https://www.osintcombine.com/post/dark-web-searching

3. Praktická část, checklist jako základní pomůcka pro policisty

Poslední část této bakalářské práce nám má představit podobu tak zvaného checklistu, tedy lustračního nástroje. Nehovoříme o jeho vizuální podobě, co se úpravy a podoby jako takové týče. To je spíše otázka na IT specialisty, kteří vytvářejí informační a jiné systémy. V této práci se zabýváme obsahovou podobou checklistu.

Pokud chceme vytvořit nástroj, který má obsahovat nějaká data, je nutné nejprve vyspecifikovat jaká data to budou. Obecně lze říci, že checklist bude obsahovat informace o osobách fyzických i právnických. Bude se jednat o informace vytěžené z veřejně dostupných zdrojů prostřednictvím metody OSINT. Účelem vzniku checklistu je především zefektivnění vyhledávání informací k osobám, které jsou předmětem prověřování trestné činnosti. Na začátku každého prověřování stojí ustanovování osob, které se nějakým způsobem podílejí na trestné činnosti, která je PČR prověřována. Ustanovení takových osob probíhá prostřednictvím kombinace operativně pátrací činnosti, šetření a vytěžování jak tvrdých dat z informačních systémů dostupných pro PČR, tak měkkých dat dostupných z veřejných zdrojů. Při prověřování veřejných zdrojů nastává problém, který je možno spatřovat v množství otevřených zdrojů a možnou náročností na orientaci v nich. Potíže může působit i neznalost celého portfolia dostupných zdrojů a časová náročnost pro ‘‘operativce‘‘ v řadách SKPV. Není v časových možnostech operativy, aby důkladně prováděla metodu OSINT. To nehovoříme o chybějící osvětě těchto pracovníků, která by metodu OSINT představila jako možnost, jak si pomoci při ustanovování osob a zjišťování informací o nich.

Z výše uvedených skutečností vyplývá jeden fakt. Pokud by existoval nástroj, který by shromáždil podstatné informace získané metodou OSINT, o něco málo by byla zvýšena efektivita činností při prověřování trestné činnosti. A pokud si přiznáme, že zločin a zločinci samotní jsou ve většině případů vždy

o krok před OČTŘ, toto by mohl být krok, jak se jim opět o něco málo přiblížit. Lze se alespoň pokusit o přizpůsobení tempa rozvoje forem a metod prověřování trestné činnosti v souvislosti s tím, jakou rychlostí se vyvíjí způsob páchání trestné činnosti. Checklist by mohl být nástroj, který by se stal dalším dílkem skládačky, vedoucí ke zmiňovanému posunu.

3.1. Vydefinování tvrdých dat z dostupných evidencí PČR a jejich následná analýza pro použití v OSINT metodě

Tvrdá data z pohledu OSINTu jsou bezpečně ztotožňující informace o osobách a jsou dostupná z centrálních registrů a evidencí, které nejsou veřejně dostupné. Některé z evidencí spravuje sama PČR. Těmito policejními evidencemi je myšlena například Centrální databáze objektů, dále jen CDO. Naopak Centrální registr obyvatel spravuje Ministerstvo vnitra a pro PČR je dostupný prostřednictvím IS Bedrunka. Abychom mohli využívat tyto evidence, musíme znát alespoň jméno a příjmení osoby, kterou se snažíme ztotožnit. V kladném případě lustrace nalezneme pak soubor informací o osobě, které nám umožní její ztotožnění a získání základních informací o této osobě. V tomto bodě si můžeme udělat základní obrázek o osobě. Víme, jak se osoba jmenuje, včetně data narození a adresy jejího trvalého bydliště. Zobrazíme si fotografii osoby a zjistíme, zda je osoba držitelem ŘP či vlastní nebo provozuje nějaké vozidlo. Mimo to se můžeme dostat i k rodinným příslušníkům a dalším důležitým informacím.

Získané informace je důležité správně uchopit a provést jejich analýzu. V analýze je potřeba se zaměřit převážně na ty skutečnosti, které využijeme jako vstupní data při vyhledání dat ve veřejných zdrojích. Nedílnou součástí je analýza vzájemného propojení osob ať už s ohledem na rodinné vazby či vazby vytvořené v konkrétním spise. Dalšími informacemi, které nám pomohou před začátkem OSINTu jsou telefonní čísla osob, registr vozidel, registr držených zbraní. Čím více informací z dostupných neveřejných evidencí budeme mít,

tím spíše dosáhneme úspěchu při vyhledávání v otevřených zdrojích. Pokud tedy máme zanalyzovaná tvrdá data a poté vyhledaná a analyzovaná data z otevřených zdrojů, nastává jejich vzájemná komparace.

Tvrdá data jsou pro vytváření checklistu důležitá. Komparací tvrdých a měkkých dat, bychom měli dojít k potvrzení informace získané prostřednictvím metody OSINT. Pokud by nedošlo k pozitivní shodě mezi tvrdými a měkkými daty, nelze tyto údaje na checklist zanést. Jednoduše proto, že budou sloužit pro PČR jako spolehlivá informace, která je zjištěna ve veřejných zdrojích a zároveň je opřena o neveřejné zdroje (centrální registry atd.). S informací z checklistu se bude dále pracovat při rozkrývání trestné činnosti a podle toho by informace měla být vypracovávaná. Odpovídajícím postupem, který bude velmi náročný na vyhledávání i následnou analýzu, bychom měli dojít k takovému údaji, který bude mít v prověřování svou váhu. Pokud chceme checklist tvořit jako lustrační nástroj, nesmí obsahovat domnělá nebo dokonce smyšlená data. Tím by checklist nejenom ztratil kredit, ale mohl by nasměrovat policisty špatným směrem, což by vedlo k možné časové ztrátě a úniku jiných podstatných skutečností. Výsledkem uvedené komparace by měl být údaj, který bude zanesen do checklistu. Tímto zaneseným údajem bude konkretizování otevřeného zdroje, ve kterém se podařilo nalézt vyhledávanou osobu a další případné skutečnosti o osobě obsažené v konkrétním otevřeném zdroji.

3.2. Seznam veřejně dostupných zdrojů pro potřeby checklistu

Otevřených zdrojů pro potřeby českých OČTŘ je velké množství. Ne každý otevřený zdroj je pro potřeby prověřování Policií ČR zajímavý, alespoň co se potřebnosti informace týče. Níže pro orientaci uvedeme seznam některých veřejně dostupných rejstříků a registrů a dalších otevřených zdrojů, které lze považovat za důležité pro potřeby checklistu:

(1) Bydlení:

a) Katastr nemovitostí, nahlížení do katastru nemovitostí
b) Registr sčítacích obvodů a budov
c) Registr územní identifikace, adres a nemovitostí
d) Mapové podklady (mapy.cz, google maps)

(2) Daně:

a) Plátci DPH
b) Plátci spotřebních a ekologických daní

(3) Ekonomika a finance:

a) ARES – čerpá z databáze otevřených zdrojů veřejné správy
b) CEDR – otevřená data vedena Ministerstvem financí ČR

(4) Investice a exekuce

a) Evidence úpadců
b) Insolvenční rejstřík
c) Seznam insolvenčních správců

(5) Podnikání

a) Obchodní rejstřík
b) Portál živnostenského oprávnění
c) Obchodní věstník
d) Rejstřík trestů právnických osob
e) MagnusWeb

(6) Sociální sítě

a) Facebook
b) Instagram
c) Twitter
d) LinkedIn

Veškeré výše uvedené otevřené zdroje se nacházejí v internetovém prostředí. Při využívání shora uvedených otevřených zdrojů si nemůžeme být jistí, jakým způsobem a v jakém rozsahu je sledována činnost na těchto stránkách a sítích. Z tohoto důvodu je nutné dodržovat bezpečnostní pravidla, popsaná

ve výše uvedené kapitole zabývající se bezpečností vyhledávání. Nelze tak vyhledávat ze služebních počítačů, připojených do intranetové sítě. Checklist by ovšem naopak byl lustračním nástrojem dostupným pouze v policejní intranetové sítě. Samozřejmě množství veřejných zdrojů je daleko více, nicméně toto je výňatek těch zdrojů, které nám dokáží vypovědět hodnotnou informaci přímo k vyhledávané osobě (FO i PO).

V případě, že vznikne nová sociální síť nebo nový rejstřík, který je využitelný pro naše potřeby, je nutné i tyto nové zdroje postupně zavést na checklist. Obecně je důležité zdroje přístupné z checklistu aktualizovat. Otevřené zdroje použitelné pro checklist musí být omezeny co do počtu těchto zdrojů. Analýzou všech existujících otevřených zdrojů jako jsou i noviny, rozhlasové vysílání, ostatní rejstříky a všechny sociální sítě bychom zahltili jak provádějící analytiky, tak i cílové uživatele checklistu. Už při pohledu na seznam vytyčených otevřených zdrojů je zřejmé, že ne všechny zdroje se budou týkat právnických osob a naopak.

Máme-li hrubý seznam veřejných zdrojů a víme, že musíme informace poskytnuté těmito zdroji porovnat s daty, která byla vyhledána v neveřejných centrálních registrech, je na řadě otázka právního rámce a etické, morální odpovědnosti. V době, kdy existuje zákon o ochraně osobních údajů, GDPR a obecně vzato je velký tlak na ochranu osobních údajů občanů, se pokoušíme vytvořit shromaždiště dat, která nalezneme defacto ve volně dostupném internetu.

3.3. Legislativní rámec OSINTu z pohledu GDPR

Nejprve je nutné uvést, jak si obecně stojí GDPR ve vztahu k metodě OSINT. Při zpravodajské činnosti za použití OSINT metody dochází téměř ve všech aspektech k jistému druhu zpracování osobních údajů. Zpracováním myslíme shromažďování, ukládání, analyzování a reprodukování takových údajů jakými jsou adresy, jména, uživatelská jména, telefonní čísla, IP adresy, obrázky. V roce 2018 byla na půdě Evropské unie zavedena nová legislativa, která upravuje

obecné nařízení o ochraně osobních údajů a zpracování osobních údajů, známá pod zkratkou GDPR. Pracovníci využívající zpravodajství OSINT vlastně shromažďují data z veřejných zdrojů. I přesto by vše mělo být v souladu s GDPR, alespoň tam, kde je to relevantní. GDPR se pak vztahuje na OSINT zpravodajství ve dvou případech:

a) pracovník využívající OSINT metodu je příslušník členského státu EU

b) OSINTem jsou zpracovávány osobní údaje týkající se občana EU.[49]

Zmiňovaná legislativa GDPR je obsahově velmi rozsáhlá. Proto se pokusíme svým způsobem vytyčit klíčové zásady pro OSINT metodu s dodržováním nařízení GDPR:

a) je důležité správně pochopit, kdy se z nás stává správce údajů nebo zpracovatel údajů

b) pro samotné zpracování osobních údajů musíme mít nějaký právní podklad

c) při zpracování osobních údajů musíme dodržovat určité zásady

d) je důležité, abychom porozuměli a respektovali konkrétní práva na soukromí a ochranu údajů, která mají jednotlivé subjekty těchto dotčených údajů.[50]

V našem případě, kdy je checklist tvořen pro využití Policií ČR, je právní vymezení zacházení s osobními údaji upraveno v zákoně č. 273/2008 Sb. o Policii České republiky, a to přímo v hlavě X. Práce s informacemi. Z pohledu GDPR pak platí článek 2 odst. 2 písm. d), ze kterého vyplývá, že toto nařízení se nevztahuje na zpracování osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání nebo výkonů trestů, a to včetně

[49] BLOCK Ludo. GDPR essentials for OSINT research. Blockint – Research | Consulting | Training. [online]. 2021. [cit. 11.02.2023] Dostupné z: https://www.blockint.nl/methods/gdpr-essentials-for-osint-research/

[50] OSINT Central. OSINT and GDPR How is OSINT affected by GDPR. [online]. 2022. [cit. 13.02.2023]. Dostupné z: https://osint-central.com/osint-gdpr/

ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení. Naopak na činnost policie se vztahuje čl. 6 odst. 1, písm. c), e) GDPR, který hovoří o právní povinnosti, vztahující se na policii při plnění úkolů prováděných ve veřejném zájmu nebo při výkonu veřejné moci, kterými je policie pověřena.[51]

3.4. Postup vložení osoby na checklist

Snaha popsat teoretický postup při vytváření checklistu může mít své trhliny, které můžou být spatřovány v nedostatečné představivosti. Je však cílem naší práce se alespoň pokusit popsat postup vytvoření checklistu i kroky vedoucí k zanesení osoby na tento checklist. Lze pojmout checklist dvěma způsoby, z nichž jeden z nich není v současné době reálný. Tím nereálným scénářem je vytvoření centrálního lustračního prostředku, který by měl podobu centrální evidence osob. Tedy, každý občan starší 15 let, který by převzal občanský průkaz, by měl za povinnost aktualizovat údaje, které registroval při žádosti o vydání OP. Údaje o přítomnosti, registraci v předem jasně definovaných otevřených zdrojích a nejlépe včetně sociálních sítí. Tato představa je ideální z pohledu využitelnosti pro PČR. Nicméně sdělování takových údajů by bylo zřejmě v rozporu s některými z právních předpisů. Zmíněný postup by narazil na odpor jak u občanů ČR, tak u provozovatelů sociálních sítí. Provozovatelé sociálních sítí by se mohli cítit zneužiti pro potřeby Policie ČR. Dalším nezbytným dílkem pro tento postup by musela být digitalizace veřejné správy, tak, aby občan nemusel s každou informací docházet na úřad. Tuto variantu lze tedy rovnou zavrhnout. Další a reálnou variantou by mohl být postup podobný jako například při snímání otisků prstů. Abychom byli přesnější, každé osobě, které bylo sděleno podezření ze spáchání trestného činu podle ustanovení § 179b odst. 3 tr. řádu, nebo které bylo sděleno zahájení trestního stíhání jako osobě obviněné dle § 160 odst. 1 tr. řádu, se do připraveného formuláře vyplní data ke každému předem určenému otevřenému zdroji, ve kterém lze takovou osobu najít, a to včetně

[51] Policie ČR. Zpracování osobních údajů Policií České republiky. [online]. 2023. [cit. 10.02.2023]. Dostupné z: https://www.policie.cz/clanek/zpracovani-osobnich-udaju-policii-ceske-republiky.aspx?q=Y2hudW09Mw%3d%3d

uživatelských jmen. Oba dva výše uvedené postupy jsou pouze naivní představou o tom, že osoby vše řádně uvedou nebo, že si ihned poté, co údaje uvedou policejnímu orgánu, nezaloží nové účty, nebo se nepokusí skrýt své údaje jiným způsobem. Jiným způsobem můžeme rozumět například založení nové společnosti s novým zápisem do obchodního rejstříku.

Jediným možným způsobem tak zůstává vytěžení potřebných údajů zpravodajstvím z otevřených zdrojů, a to takovým způsobem, aby se o tom dotčené osoby nedozvěděly. Máme tedy trestní spis ve fázi prověřování, kde máme zavedenou potenciální podezřelou osobu. Úkolem operativy je v tuto chvíli mít řádně ustanovenou osobu tak, aby nebyl pochyb nejen o její existenci, ale také o její pravé totožnosti. V případě, že máme ověřenou totožnost osoby, můžeme tyto údaje považovat za vstupní údaje. Získané vstupní údaje spolu s žádostí o lustraci osoby a zavedení na checklist předáme pracovníkovi z analytické skupiny SKPV. V tuto chvíli je břemeno na bedrech analytika. Nutností je důkladné proškolení takového analytika jak z postupů v metodě OSINT, tak v jejich pečlivé komparaci s tvrdými daty, finálním vyhodnocením zjištěných dat a jejich řádným zavedením do checklistu. Takto proškolený analytik by lustroval v otevřených zdrojích. V těch, které by musely být dopředu jasně definovány jako zájmové pro potřeby checklistu. V případně kladného zjištění – tedy, že prověřovaná osoba se nachází například v obchodním rejstříků, bude tato informace zanesena jako kladný výsledek lustrace, a to včetně informací, které tento rejstřík o dané osobě poskytne. Tudíž budeme vědět IČO osoby nebo celé společnosti, ve které daná osoba vystupuje a další dostupné údaje v obchodním rejstříku. Vzhledem k novému zjištění máme defacto další vstupní údaj a tím je IČO a například adresa podnikání. Zjištěné údaje můžeme vložit do dalších evidencí jako například ARES, CEDR (u těchto systému se nám mohou informace dvojit), nebo rejstřík trestů fyzických osob. Všechny další kladné výsledky lustrací v těchto otevřených zdrojích je nutné opakovaně zadat a přidat zjištěné informace pod daným rejstříkem. Rovněž můžeme například zjistit v katastru nemovitostí majitele domu, kde je společnost provozována a tím si ustanovit další osobu, která může být zájmová. Pro potřeby checklistu

nemůžeme větvit lustrace na nové osoby. Větvení lustrace bez automatizovaného systému by bylo časově velmi náročné a je spíše na příjemci dat z checklistu, aby si sám zhodnotil, zdali je pro něho tato osoba zájmová, či nikoliv. V případě, že ano, musí jí ustanovit a poskytnou nová vstupní data pro analytika. Tím by se celý koloběh opakoval. Pokud bude osoba ustanovena, ale nebude v prověřované věci figurovat jako zájmová osoba, nebude přidána do checklistu.

Specifickou úlohou bude OSINT nebo chcete-li SOCMINT, tedy lustrace v sociálních sítích. SOCMINT bude probíhat souběžně s lustrací ostatních otevřených zdrojů. Lišil by se pouze ve výsledném výstupu zadávaném do checklistu. V případě kladného zjištění by se do checklistu vyplnilo uživatelské jméno v dané sociální síti. Společně s tím by se neuváděly informace vytěžené z tohoto účtu, ale pouze by se poznamenalo, zdali se jedná o otevřený účet nebo soukromý. V případě, že by účet byl soukromý, uvedl by se rozsah informací, které účet poskytuje (například pouze úvodní fotografie nebo seznám přátel). Dalším odlišným způsobem od lustrace v ostatních otevřených zdrojích je například vyhledávání předmětné osoby pomocí účtu jejích rodinných příslušníků. Důvod je zřejmý. Předmětná osoba nemusí mít uživatelské jméno stejné jako své pravé jméno, ale její rodinný příslušník může mít uživatelské jméno shodné s tím pravým. Na účtu tohoto rodinného příslušníka pak můžeme spojit uživatelské jméno vyhledávané osoby například podle fotografie, komentáře nebo označení rodinné vazby v profilu účtu a tím ustanovit uživatelské jméno na sociální síti. Samotné vytěžení účtu na sociálních sítí by bylo opět na zadavateli požadavku. Zadavatel, operativec, nebo jinak zpracovatel spisu by z checklistu dostal informaci o uživatelském jménu a otevřenosti přístupu k účtu na sociální síti. Vyhodnocení dostupných dat by bylo zcela na něm, a to z toho důvodu, že má přehled o celém prověřování a dostupná data si umí dát do kontextu jen on sám. V poslední fázi před konečným uzavřením checklistu by měla být komparace zjištěných dat s tvrdými daty. Pro příklad komparace je naše představa taková, že zjistíme-li z policejních evidencí data k matce vyhledávané osoby, pokusíme se jí spojit v některém z otevřených zdrojů a tím si potvrdit relevantnost vyhledaných dat. Můžeme například najít jméno matky v KN jako spolumajitelku

domu, ve kterém bydlí vyhledávaná osoba, nebo jak již bylo výše zmíněno, můžeme přes účet na sociální síti matky ustanovit uživatelské jméno předmětné osoby.

Vstupní požadavek na uvedení osoby do checklistu byl zadán, bylo provedeno zpravodajství metodou OSINT, výsledek byl analyzován, komparován s tvrdými daty pro ověření relevantnosti zjištěných údajů. Poslední fází je zpráva o splnění požadavku. O zprávě jako takové není třeba se příliš zmiňovat. Jednalo by se o sdělení, že osoba byla zavedena do checklistu a lze ji v tomto systému lustrovat. Jen v případě negativního OSINTU by bylo sděleno, že osobu se nepodařilo v otevřených zdrojích vyhledat. Předmětným výsledkem by bylo samotné zavedení osoby na checklist. Teoretická podoba a využitelnost checklistu v praxi bude předmětem další kapitoly.

3.5. Výsledná podoba checklistu a jeho využitelnost v policejní praxi

V této kapitole se pokusíme nastínit podobu checklistu z pohledu informačního systému a zařazení do skupiny těchto informačních systému. Dále se pokusíme přiblížit využitelnost checklistu pro příslušníky PČR, a to jak ze strany policistů za základních útvarů, tak ze strany příslušníků SKPV. Mimo jiné se i pokusíme nastínit podobu checklistu z pohledu lustračního nástroje. Přístup k informačnímu systému checklistu rozdělíme do tří úrovní:

1. **dožádání k vložení osoby do checklistu** – požadavek zanést osobu do checklistu by mohl každý policista zařazený na SKPV, a to již v době před zahájením trestního řízení. Tedy i v době, kdy je teprve prověřován poznatek o možné trestné činnosti. Ve fázi prověřování před zahájením úkonů v trestním řízení můžou být informace OSINTu velmi podstatné pro zjišťování dalších informací, které dovedou prověřování poznatku až do zahájení úkonu trestního řízení. Policisté zařazení na základním útvaru by měli žádat o vložení osoby do checklistu v případě, že budou sdělovat osobě podezření ze spáchání

trestného činu podle ustanovení § 179b odst. 3 tr. řádu. Dalším důvodem pro vložení osoby do checklistu, by mohla být situace, kdy bude po osobě vyhlášeno pátrání. Žádost by měla být směrována na příslušného analytika SKPV s oprávněním vkládání údajů do checklistu.

2. **vkládání/editace údajů** – vkládání údajů je úzce spojeno se samotným vyhledáním informací OSINTem, tudíž by vkládáním údajů byli určeni analytici SKPV od úrovně Územních odborů, přes Krajská ředitelství až po celostátní útvary jako je NPC či NCOZ. V případě nutnosti by bylo možné data i editovat, aktualizovat,

3. **vytěžování údajů** – vytěžovat checklist by v plné míře mohli pracovníci SKPV opět od úrovně Územních odborů, přes Krajská ředitelství až po celostátní útvary jako je NPC či NCOZ. Policisté základních útvarů by pak měli možnost vytěžovat tento systém k osobám, proti nímž by vedli trestní řízení pouze na základě odůvodněné žádosti směrované na analytickou skupinu SKPV příslušného Územního obvodu. V tomto případě by analytik odpověděl na takovou žádost sjetinou z checklistu k dožadované osobě. Tím předejdeme svévolnému lustrování osob v checklistu. Pokud stanovíme taková pravidla, je důležité si obhájit omezený přístup policistů základních útvarů k checklistu. Důvodem je možná zneužitelnost ani ne tak samotných údajů, které si ve finále může každý pomocí OSINTu najít sám, ale samotné podstaty toho, že se ta která osoba nachází v checklistu. Jak jsme již uváděli, v checklistu by byly evidovány všechny zájmové osoby, které probíhají nebo probíhaly spisem jako osoby prověřované, podezřelé či obviněné. Pokud by každý policista měl přístup k checklistu, snadno by se tak mohl dopátrat informace o tom, že některá z osob, kterou si zadá do vyhledávání je nebo byla prověřována. Taková informace už je zneužitelná a mohla by ohrozit živé spisy. Samozřejmě nelze tomu předejít ani vymezením pracovníků SKPV jako neomezenými uživately, kteří mohou checklist prohledávat a potenciální únik informací hrozí i v tomto směru. Zde se nabízí varianta zadávání důvodu dotazu do checklistu, tak jak to známe u ostatních informačních systémů. Policisté, kteří jsou zařazeni na SKPV mají bezpečnostní prověrku na minimální úrovni ‘‘VYHRAZENÉ‘‘, což již samo o sobě přináší rozšířenější oprávnění.

Checklist jako policejní evidence by odpovídal systému, jakým je například CDO. Spravovala by si ho sama Policie ČR a nebyl by dostupný žádnému jinému OČTŘ. Checklist je zamýšlen jako součást policejních evidencí s nutností zadávat přihlašovací údaje. Užívání checklistu by vypadalo následovně. Oprávněný policista by zadal jméno, příjmení a datum narození osoby, kterou by chtěl vyhledat v checklistu. Po zadání by proběhla lustrace v checklistu, jejíchž výsledek by mohl být negativní s oznámením, že osoba nebyla dosud do checklistu zadána. Pozitivní výsledek by znamenal výpis předdefinovaných otevřených zdrojů. U každého otevřeného zdroje zvlášť by se mělo dát prokliknout k informaci, zdali vyhledávaná osoba je v tom konkrétním otevřeném zdroji k nalezení. Pokud ano bude tento otevřený zdroj označen jako pozitivní a bude v něm informace k osobě, která v otevřeném zdroji byla dostupná. V opačném případě bude jen uvedeno, že otevřený zdroj je z pohledu vyhledávání osoby negativní, tudíž dotyčná osoba není v tomto zdroji zavedena. Což ovšem neznamená, že v jiném otevřeném zdroji není dostupná. Přehlednost checklistu, stejně jako u ostatních programů, systémů a nástrojů je odkázána na IT specialistu. Pro naší práci je důležité, co by checklist nabízel. Pro činnost policistů by checklist znamenal zjednodušení vyhledávání v otevřených zdrojích. Byť nemusí taková informace zásadním způsobem posunout prověřování vpřed, může významně pomoci při získávání informací o prověřovaných osobách. Můžeme zjistit i propojení vzájemných vazeb prověřovaných osob, lze získat fotografii, která by mohla sloužit jako důležitý segment prověřování. Pokud zamýšlíme použít informaci z checklistu jako důkaz, bude nutné takovou informaci oficiálně vyžádat i u provozovatele rejstříku nebo toho daného otevřeného zdroje, a to s ohledem na to, aby předložená informace nemohla být před soudem napadena a označena jako informace podvrhnutá policejním orgánem.

Závěr

OSINT jako metoda v řadách Policie ČR je prozatím méně využívanou metodou při sběru dat o zájmových osobách. Bylo shrnuto několik základních informací o historii otevřených zdrojů. Několik dalších kapitol a podkapitol vedlo k seznámení se s tím, co je metoda OSINT a jak ji lze využívat. Přes několik definic a uvedení metody OSINT do provozu, alespoň obrazně řečeno, byly nově získané vědomosti a informace využity pro praktický nástroj, kterým je v naší práci checklist. Checklist byl vytvořený v této práci jako čistě teoretický nástroj, určený k usnadnění vyhledávání dat v otevřených zdrojích o osobách pro potřeby PČR. Vznik takového programu, jakým by byl checklist není tak snadný. Je zapotřebí spojení IT specialistů, kompetentních policistů a samozřejmě i vůle vedení PČR, aby došlo k vývoji zmiňovaného programu. V začátku vývoje by jistou překážku mohla tvořit nedostatečná, vlastně nulová databáze. Ta by se tvořila dlouhou dobu, nejspíše roky. Množství dat vložených do checklistu by logicky ze začátku bylo mizivé. Až po dostatečném nasycení checklistu, by tento začal plnit svou funkci naplno. Z tohoto důvodu by musel být kladen důraz na vkládání osob do checklistu. Po pár letech, kdy bude checklist naplněn daty a bude prověřena jeho využitelnost, bychom mohli vymýšlet další nové způsoby využití checklistu. Například vykreslováním vzájemných vazeb osob nebo automatického propojení s ETŘ. Tím je myšleno vložení osoby do ETŘ a po označení osoby jako prověřované, podezřelé by se automaticky propojila s checklistem a byla by provedena její lustrace. Checklist by mohl plnit funkci další pomůcky pro policisty, ale je velmi důležité správně uchopit tento nástroj tak, aby se nestal protizákonným, zneužitelným, neefektivním a uživatelsky nedostupným. Cíl práce bylo teoretické vytvoření lustračního nástroje checklist a k tomu seznámení s historií otevřených zdrojů a seznámení s moderní metodou OSINT. Pokud checklist bude někdy vytvořen a pokud k vytvoření přispěje, byť jen malým dílkem, tato práce, můžeme teprve v tomto případě považovat cíl práce za splněný.

Seznam použitých zdrojů

Monografie

1. ABRAMSON, A. The History of Television, 1942 to 200. McFarland, 2003. ISBN 978-0-7864-1220-4. S. 3.
2. BAWDEN DAVID a ROBINSON LYN. Introduction to information science. London: Facet publishing, 2012, ISBN 9781856048101, S. 351.
3. BAZZELL, M. Open Source Intelligence Resources For Searching and Analyzing Online Information fifth edition, CreateSpace Independent Publishing Platform, 2016. ISBN 978-1530508907.
4. CHRISTOPHER, Andrew, Richard; ALDRICH J. Richard; WARK K. Wesley. Secret Intelligence. A Reader. Second Edition. New Yor, USA: Routledge, 2020. ISBN 978-0-415-70567-7. S. 77, 78.
5. 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. ISBN: ISBN 978-3-319-47671-1. S. 111-112.
6. LABANCA, Nicola. *Válečné konflikty dneška od roku 1945 do současnosti*. Praha: Fortuna Libri, c2009. ISBN 978-80-7321-465-4. s. 10-21.
7. LOSEKOOT, Michelle; VYHNÁNKOVÁ Eliška. Jak na sítě: ovládněte čtyři principy úspěchu na sociálních sítích. Brno: Jan Melvil Publishing, 2019. Žádná velká věda. ISBN 978-80-7555-084-2. S. 35.
8. MICHÁLEK, Luděk a kol. Kriminální zpravodajství jako nástroj kontroly trestné činnosti a zajišťování vnitřní bezpečnosti. Praha: Policejní akademie České republiky v Praze, 2020. ISBN: 978-80-7251-506-6. S. 12.
9. MICHÁLEK, Luděk, POKORNÝ, Ladislav, STIERANKA, Jozef, MARKO, Michal. Zpravodajství a zpravodajské služby. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2013. ISBN: 978-80-7380-428-2.
10. REIFOVÁ, Irena. *Slovník mediální komunikace*. Praha: Portál, 2004. ISBN 80-7178-926-7. S. 164–165.
11. SHIERS. G; SHIERS. M. Early Television: A Bibliographic Guide to 1940. New York and London: Garland Publishing Inc. 1997. ISBN 978-0-8240-7782-2. S. 13, 22.

12. STEJSKALOVÁ, Eva. Novinové zpravodajství a noviny v Čechách od 17. století do roku 1740. Praha: Univerzita Karlova v Praze, nakladatelství Karolinum, 2015. ISBN 978-80-246-2613-0

Zákonná úprava

1. Zákon č. 273/2008 Sb., o Policii ČR

Webové stránky a elektronické zdroje

1. HÁLOVÁ, Marie. Veřejné knihovny antické Římské říše. Duha: Informace. o knihách a knihovnách z Moravy. [online]. 2012. [cit. 2022-11-27]. ISSN 1804-4255. Dostupné z: http://duha.mzk.cz/clanky/verejne-knihovny-anticke-rimske-rise
2. Reindlová, Nikola. Tisk za 1. republiky: Památník Karla Čapka [online]. 2012. [cit. 2022-12-27]. Dostupné z: https://www.capek-karel-pamatnik.cz/vismo/dokumenty2.asp?id_org=200013&id=14311
3. Schaurer, Florian and Störger, Jan. AFIO-Association of Former Intelligence Officers [online]. 2013. [cit. 16.01.2023]. Dostupné z: https://www.afio.com/publications/Schauer_Storger_Evo_of_OSINT_WINTERSPRING2013.pdf
4. Studeman, W. Historie Foreign Broadcast Information Service, [přednáška - online]. 1992. [cit. 29.12. 2022]. Dostupné z: https://irp.fas.org/fbis/studem.html
5. Répásová, Marie, Krátce k historii římskokatolických matrik, SOA v Třeboni - DIGITÁLNÍ ARCHIV [online]. [cit. 30.12. 2022]. Dostupné z: https://digi.ceskearchivy.cz/Matriky-Rimskokatolicka-cirkev-Kratce-k-historii-rimskokatolickych-matrik
6. Sterling, H. Christopher. Radio. Definition, History, & Facts. Britannica. Encyclopedia Britannica. [online]. [cit. 18.01.2023]. Dostupné z: https://www.britannica.com/topic/radio
7. O'BRIEN, A. Open Source Intelligence May Be Changing Old-School War. WIRED-The Latest in Technology, Science, Culture and Business. [online].

[cit. 22.01.2023]. Dostupné z: https://www.wired.com/story/open-source-intelligence-war-russia-ukraine/

8. Otevřené zdroje. Bezpečnostní informační služba České republiky BIS. [online]. 2023. [cit. 22.01.2023]. Dostupné z: https://www.bis.cz/otevrene-zdroje/
9. KADAR, T. Top 10 OSINT (Open Source Intelligence) Software & Tools. [online]. 2023. [cit. 18.01.2023]. Dostupné z: https://seon.io/resources/the-best-tools-for-osint/?utm_term=&utm_campaign=%5BS%5D+Blog+-+dynamic+%5BGlobal%5D&utm_source=google&utm_medium=cpc&hsa_acc=4202831505&hsa_cam=18737907277&hsa_grp=139814728781&hsa_ad=631421714770&hsa_src=g&hsa_tgt=dsa-1465635799605&hsa_kw=&hsa_mt=&hsa_net=adwords&hsa_ver=3&gclid=EAIaIQobChMI-pqvi4Tc_AIV5UiRBR1YKw4tEAAYASAAEgKysvD_BwE
10. BURIÁNEK, J. Data měkká a tvrdá – Sociologická encyklopedie. [online]. 2017. [cit. 18.01.2023]. Dostupné z: https://encyklopedie.soc.cas.cz/w/Data_měkká_a_tvrdá
11. ZEMAN, Petr. Zpravodajský cyklus-klišé nebo nosný koncept? Obrana a strategie. Brno: Univerzita obrany. 2010. 45-64, 115. DOI: 10.3849/1802-7199.10.2010.01.045-064. S 46-58
12. FURUHAUG, André, Robert. Open Source Inteligence Methodology. AI-Powered Research Tool. [online]. 2019. [cit. 18.01.2023]. Dostupné z: https://www.semanticscholar.org/paper/Open-Source-Intelligence-Methodology-Furuhaug/56e8ea14b1279cb77c91df8898957a4f71b90ea4
13. What Is a VPN? - Virtual Private Network-Cisco. Networking, Cloud, and Cybersecurity Solutions – Cisco. [online]. 2023. [cit. 26.01.2023] Dostupné z: https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html
14. Autor neuveden. Co je VPN a jak ji můžeme využít? *Forescope* [online]. 2020. [cit. 30.1.2023]. Dostupné z: https://www.forscope.cz/blog/co-je-vpn/

15. PORUTIU, Theodor. What is the Tor Browser? A Guide to the Dark Web Browser. VPNOverview.com. [online]. 2014. [cit. 30.01.2023]. Dostupné z: https://vpnoverview.com/privacy/anonymous-browsing/tor/
16. DONAHUE, Jason. How to detect TOR network connections with Falco. *Sysdig*. [online]. 2022. [cit. 29.1.2023]. Dostupné z: https://sysdig.com/blog/detect-tor-network-connection-falco/
17. MALTEGO. Everytthing About Social Media Intelligence (SOCMINT) and Investigations. [online]. 2022. [cit. 26.01.2023].Dostupné z: https://www.maltego.com/blog/everything-about-social-media-intelligence-socmint-and-investigations/
18. SOCradar. How to Use SOCMINT for Better Cause? [online]. 2021. [cit. 30.01. 2023]. Dostupné z: https://socradar.io/how-to-use-socmint-for-better-cause/#_ftn1
19. Advanced Googleing. Open Source Intelligence Training for Law Enforcement. It's Our Business to Know. [online]. 2020. [cit. 03.02.2023]. Dostupné z: https://osinttraining.net/introduction-to-osint/advanced-googleing/
20. Seznam.cz. Fultextové vyhledávání. Pokročilé vyhledávání s použitím operátorů. [online]. 2023. [cit. 03.02.2023]. Dostupné z: https://napoveda.seznam.cz/cz/fulltext-hledani-v-internetu/pokrocile-vyhledavani/
21. HARDWICK, Joshua. Google Search Operators: The Complete List (42 Advanced Operators). Ahrefs-SEO Tools & Resources To Grow Your Search Traffic [online]. 2020. [cit. 03.02.2023]. Dostupné z: https://ahrefs.com/blog/google-advanced-search-operators/
22. ŠIMEK, Gabriel. Surface Web vs. Deep Web vs. Dark Web. CryptoNews.cz. [online].2021.[cit.05.02.2023].Dostupné z: https://www.cryptonews.cz/bezpecnost/surface-web-vs-deep-web-vs-dark-web
23. ALZA.CZ, Co je deep web? A jak se liší od dark webu? [online]. 2019. [cit. 05.02.2023]. Dostupné z: https://www.alza.cz/co-je-deep-web

24. TIWARI, Adytia. What Is The Difference Between Deep Web, Darknet, And Dark Web? Fossbytes-Technology Simplified [online]. 2020. [cit. 05.02.2023]. Dostupné z: https://fossbytes.com/difference-deep-web-darknet-dark-web/
25. TECHDRACULA. Surface web vs deep web vs dark web vs shadow web vs marianas web. Techdracula. [online]. [cit. 02.02.2023]. Dostupné z: https://techdracula.com/surface-vs-deep-vs-dark-vs-vs-shadow-vs-marianas-web/
26. NOVÁKOVÁ, Marie. ARK WEB-Temná strana internetu [+18] - SpyShop24.cz - detektivní blog. Spy Shop-Obchodní síť se špionážní technikou [online].2022, [cit. 04.02.2023]. Dostupné z: https://www.spyshop24.cz/blog_cz/dark-web-temna-strana-internetu-18/
27. OSINT COMBINE. Dark Web Searching. Open Source Intelligence. [online]. 2020. [cit. 05.02.2023]. Dostupné z: https://www.osintcombine.com/post/dark-web-searching

Prezentace a přednášky

1. Dokument z neveřejného školení pro pracovníky SKPV. 2022
2. Prezentace z neveřejného školení pracovníků SKPV PČR ze dne 16.06. 2021.

Seznam obrázků