Policejní akademie České republiky v Praze

Fakulta bezpečnostně právní

Katedra kriminální policie

Zpravodajství z otevřených zdrojů (OSINT) a sociálních médií (SOCMINT) jako zdroj informací v rámci aktivit služby kriminální police a vyšetřování

Diplomová práce

Open Source Intelligence (OSINT) and Social Media Intelligence (SOCMINT) as a source of information in the area of activities of Criminial Police and Investigation Service)

VEDOUCÍ PRÁCE

Ing. Bc. Luděk MICHÁLEK, Ph.D.

AUTOR PRÁCE

Bc. Adam Omasta, DiS.

PRAHA

2022

Čestné prohlášení

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

V Praze, dne 27. 02. 2022

Bc. Adam Omasta, DiS.

Poděkování

Rád bych poděkoval vedoucímu práce Ing. Bc. Luďku Michálkovi, Ph.D. za cenné rady a vstřícnost při zpracování diplomové práce.

ANOTACE

Diplomová práce pojednává o trendu užití OSINT A SOCMINT metod jako zdroj informací pro kriminální analýzy v rámci činnosti služby kriminální policie s kazuistikou několika případů, u kterých byly teoretické základy aplikovány do praxe jako hlavní metoda zdroje informací. V teoretické rovině je primárně objektem zájmu OSINT metoda s lokalizací SOCMINT metod jakožto součástí OSINT. Empirická část pojednává o aplikaci teoretických metod od všední práce s informacemi po speciální operace, včetně kazuistiky. Součástí práce je i výzkum užívání zmiňovaných metod v rámci kriminální policie formou dotazníku. Cílem práce je přirozeně vysvětlit výše uvedené metody od obecného ke konkrétnímu a následně poukázat na aplikaci těchto teoretických základů na aplikaci v několika případových studiích. Součásti cíle je i výstup výzkumu současného stavu vzdělání těchto metod a jejich aplikace v daných podmínkách kriminální policie.

KLÍČOVÁ SLOVA

OSINT, SOCMINT, kriminální analýza, darknet, TOR, sociální sítě, otevřené zdroje, databáze, internet

ANNOTATION

The diploma thesis deals with the trend of using OSINT and SOCMINT methods as a source of information for criminal analyzes in activities of the criminal police service with a several cases study were theoretical foundations was applied in practice as the main method of information. At theoretical level, the primary object of interest is the OSINT method with the localization of SOCMINT methods as part of OSINT. The empirical part deals with the application of theoretical methods from everyday work with information to special operations, including case studies. Part of the work is includes research of use of the mentioned methods criminal police in the form of a questionnaire. The aim of the work is naturally explain the above methods from general to specific and then to point out the application of these theoretical foundations to the application in several case studies. Part of the goal is the output of research into the current state of teaching these methods and their application in the current conditions of the criminal police.

KEYWORDS

OSINT, SOCMINT, criminla analysis, darknet, social network, open soureces, databases, internet

Obsah

1 Úvod

Tak jak se rozvíjela kriminální scéna napříč staletími, tak ani rozvoj analytických metod kriminální policie nezůstává pozadu. Ukázalo se, že hlavním a efektivním nástrojem boje se zločinem jsou kvalitní informace a to takové, které hlavně pocházejí ze zájmového prostředí. Právě tyto informace jsou v informačním věku výsledkem synergie a naprosté kolaborace analytických metod jako jsou Open Source Intelligence dále jen „OSINT“, Social Media Intelligence, dále jen „SOCMINT“, Web Intelligence dále jen „WEBINT“, apod. I když hlavním zdrojem těchto metod jsou veřejně dostupné informace, tak i tyto informace doplňují fragmenty v pomyslném obraze, který je složen z informací získaných dalšími metodami jako třeba Human Intelligence dále jen „HUMINT“ a Signal Intelligence dále jen „SIGINT“, nebo z poznatkové databáze kriminální policie.[1] Tato práce odkazuje na moderní využití výše uvedených metod, a to především OSINT, SOCMINT metod a jejich velmi úzké prolínání v rámci získávání dat. Z obecné teorie k praktické aplikaci ve formě kazuistik ze světa i domácí scény, kde bylo jako hlavní a efektivní metoda sběru dat právě OSINT a SOCMINT. To vše je završeno výzkumem formou dotazníků, k poměru vzdělaní policistů z hlediska těchto procesů a reálného využití dat z takovýchto metod u kriminální policie.

[1] PHYTHIAN, M. (ed.). Understanding the Intelligence Cycle. USA: Routledge, 2013. ISBN 978-0-203-55847-8.

2 Analýzy a zdroje informací

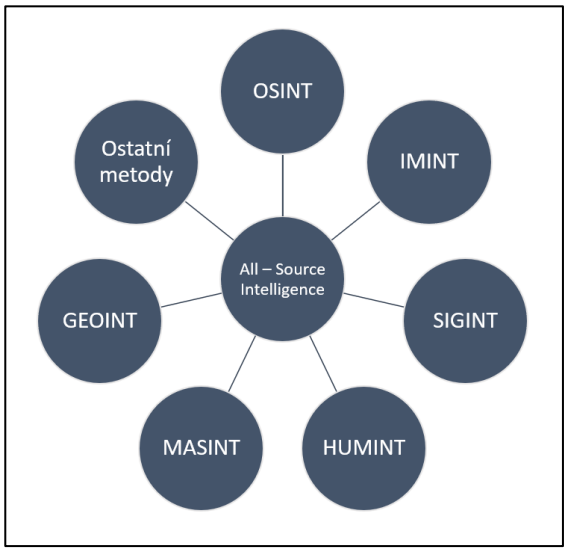
Data jsou velmi komplexní, a aby mohlo dojít k jejich rozčlení a efektivnímu vyhodnocení formou analýzy je nutná taky správná katalogizace. V případě zpravodajských analýz se jedná především o různé metody a oblasti původu informací. Již v úvodu jsou zmíněný typy analýz a sběry dat jako jsou HUMINT, SOCMINT, OSINT apod., těchto metod je nesčetně a teoreticky můžete přídavek významu „INT“ aplikovat na jakoukoliv oblast, jako např. Pizza Intelligence dále jen „PIZZINT“. Ačkoliv se tato záložka řadí mezi komické záležitosti, veskutečnosti se jedná o pravdiví sběr informací. Za studené války sledovaly zástupci SSSR v USA nejdůležitější administrativní budovy USA a když zaznamenali, že do těchto budov jsou v nočních hodinách velké donášky pizzy, věděli že se děje něco velkého. Stejně komický je i Lavatory Intelligence dále jen „LAVINT“, jinak řečeno odposlechnuto na toaletách.[2] Jak je shora uvedeno metod sběru dat a analýz je nespočetné množství, ale pro potřeby této práce budou irelevantní a budou označovány jako ostatní. Všechny tyto metody se shlukují do jednoho celku známého jako All – Source Intelligence dále jen „ASI“.

2.1 All – Source Intelligence

V odborné zpravodajské komunitě, je pojem ASI znám jako souhrn všech relevantních metod sběru dat a jejich následných analýz[3], viz. obr. č. 1. Jak je zmíněno v počátku druhé kapitoly, metod je celá řada a pro svou přehlednost jsou často uváděny ty nejsilnější v oblasti zdrojů dat. Obvykle se tak jedná o domény jako je OSINT cílený na sběr dat z otevřených zdrojů, HUMINT sběr dat pocházejících z lidských zdrojů, Imagery Intelligence dále jen „IMINT“, zkoumající satelitní snímky či běžné fotografie, Geospatial Intelligence dále jen „GEOINT“ zkoumající zemský terén v souvislosti s lidským působením, Signals Intelligence dále jen „SIGINT“ sběr a vyhodnocování datové komunikace jako jsou odposlechy telefonních hovorů apod., dále se jedná o Measure and Signature Intelligence dále jen jako „MASINT“ zabývající se sběrem a sledováním změn

[2] PASEMAN, Floyd L. A spy's journey: a CIA memoir. St. Paul, MN: Zenith, [2004]. ISBN 978-0-7603-2066-2.
[3] PHYTHIAN, M. (ed.). Understanding the Intelligence Cycle. USA: Routledge, 2013. ISBN 978-0-203-55847-8.

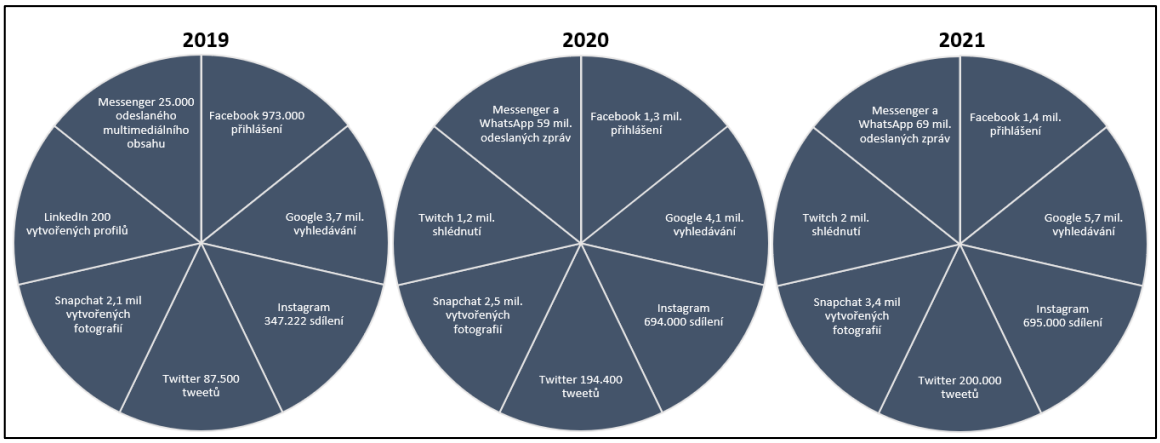
z fyzikálního či chemického hlediska objektů zájmu. Tím, že neuvádím další nepotlačuji jejich klíčový význam jako je třeba Technical Intelligence, zkráceně TECHINT zabývající se analýzou užívaných bojových prostředků a zařízeních, ale pro potřeby této práce je tento zdroj irelevantní. Jak jsem naznačil mezi hlavní pilíře patří OSINT, do jeho součásti můžeme zařadit i SOCMINT či WEBINT apod. Jedná se stále o vzájemně na sebe působící podmnožiny hlavního směru OSINT.



Obr. č. 1 – Grafické zpracování ASI mapy, zdroj: archiv autora

2.2 OSINT

Jak už bylo zmíněno OSINT, je metoda sběru dat a jejich analýza pocházející z tzv. otevřených zdrojů. Dříve byl OSINT aplikován na tištěná média jako noviny, časopisy, knihy a další média jako rádio, televize apod. Velká změna přišla s internetem a jak se informační věk vyvíjel, tak se i objem a typ dat ve virtuálním prostředí internetu zvětšoval, viz obr. č. 2. Tímto milníkem, který způsobil téměř neomezený zdroj dat, začali vznikat i nové metody sběru dat a jejich vyhodnocení. Právě v této chvíli začal mít OSINT velký potenciál, který se dále rozvíjel.



Obr. č. 2 – Data internetu v jedné minutě, zdroj: archiv autora

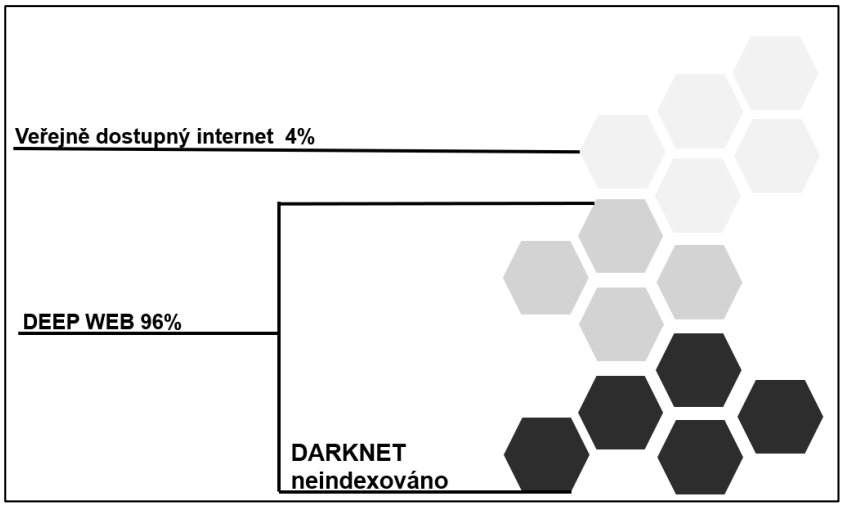
I samotný depot informací, jako virtuální prostředí internetu, v průběhu času procházelo neustálým zvětšováním a rozvojem sítí. V případě internetu pak dělíme úrovně na veřejně dostupný internet mezinárodně známý a uznávaný výraz „clearnet“ nebo „surfacenet“ a část, která je zabezpečena šifrováním a pro prohlížení obsahu jsou nutná hesla, tato část je nazývána jako „deep web“. Součástí „deep webu“ je i „darknet“, viz obr. č.3. Darknet jsou decentralizované sítě vně internetu, které zpřístupní svůj obsah pouze za využití aplikací pro vstup do konkrétní sítě. V případu darknetu neexistuje doména pro regulaci obsahu, a proto velmi často dochází k její zneužit pro trestnou činnost[4]. Nejznámější sítě darknetu jsou TOR[5], Freenet[6], I2P[7].

[4] GEHL, R. W. Weaving the Dark Web. London, England: The MIT Press, 2018. ISBN 978-0-262-03826-3

[5] Zkratka z anglického názvu The Onion Router, jedná se o jednu z darknet sítí. Dostupné online z www.torproject.org.

[6] Freenet, je jedna ze sítí darknetu, dostupný online na www.freenetproject.org.

[7] I2P zkratka pro jednu z darknet sítí stojící na principu peer to peer sdílení dat, dostupné online www.geti2p.net.



Obr. č. 3 – Grafické zpracování úrovní internetu, zdroj: archiv autora

Analýza webových stránek

Kompletní množina tištěných i živých médií se přesunula do virtuálního prostředí internetu a v souvislosti s tím vznikla úplně nová data například ve formě webový stránek, které byly rovněž velkým zdrojem dat jako jsou DNS[8] záznamy, NS[9] a jeho archívy, MX protokoly[10], nebo rozbor grafického obsahu. Vznikem těchto dat vnikla i nová metoda sběru dat a jejich analýzy WEBINT. Do roku 2021 bylo registrováno 1,2 miliardy webových domén ze kterých je cca. 200 mil. aktívních. viz tabulka č. 1.

Pořadí	Společnost	Počet aktívních hostovaných domén
1.	CloudFlare	49,834,342
2.	Amazon	34,488,723
3.	Verotel	29,020,004
4.	Ionos	11,759,286
5.	NameCheap	11,439,596
6.	Amazon	10,619,557
7.	OVH	9,285,419
8.	Godaddy	9,089,909
9.	Unifiedlayer	8,742,473
10.	Alibaba	8,626,207

Tabulka č. 1 – Statistika serverových hostingů, zdroj: www.host.io

[8] Zkratka z anglického názvu Domain Name System, veřejný registr webových adres.
[9] Zkratka z anglického slova Network System, veřejný registr hostovaných domén.
[10] Jedná se o parametr s adresou e-mail serveru.

Blockchain virtuálních měn

Stejně tak s příchodem blockchain technologie virtuálních měn, která stojí u většiny virtuálních měn na transparentnosti transakcí, ve kterých lze vyhledávat jako v účetní knize a díky obsáhlým databázím majitelů peněženek virtuálních měn, lze v nich sledovat i tok transakcí. I zde je možné, že brzy vznikne metoda Virtual Currencies Intelligence jako VCINT nebo Blockchain Intelligence jako BLOCKINT.

Státem sdílená data

Zájmová i klíčová data nemusíme hledat jen mezi soukromými subjekty, v dnešní digitální době stát distribuuje zcela přirozeně i kdysi nedostupná data. Především se jedná o data jako veřejné databáze ve formě různých registrů smluv, veřejných zakázek, statistických dat, katastr nemovitostí či databázi podnikajících subjektů apod. Stát a jeho orgány distribuuje digitální formou i výroční zprávy různých institucí nebo průběžné a mimořádné zprávy.

Aktivisti, neziskové organizace a novináři

Data sdílená se záměrem transparentnosti státní exekuce. Aktivisti, neziskové organizace, jedinci či skupiny s cílem zpřehlednit státní data do uchopitelnějších dat, vytváří webové stránky s indexovanými daty veřejných registrů spravovaných státem. Obvykle se mezi těmito daty nacházejí i data požadované dle zákona č. 106/1999 Sb. o svobodném přístupu k informacím, která nejsou obvykle státem automaticky zveřejňována. Tyto data obvykle procházejí procesem schvalování dle typu dotazu a může dojít o zamítnutí takovéhoto dotazu.

2.3 SOCMINT

Sociální sítě jsou virtuální platformy internetu, kde uživatelé umisťují svůj osobní obsah ve formách myšlenek a multimediálního obsahu. Dle adiktologů jsou sociální sítě stejně silně návykové jako drogy. V současné době je ze 20 nejnavštěvovanějších webových stránek světa, 18 portálů se sociální sítí. Když

v roce 2004 vznikla sociální síť Facebook, nyní Meta[11] a v roce 2005 YouTube, nikoho nenapadlo, jaký velký historický milník v oblasti zdrojů personálních informací a multimediálních dat to může být. V současné době je globálně 4,66 mld. aktivních uživatelů internetu a z toho 4,2 miliardy jsou aktivní uživatelé sociálních sítí. V globálním průměru 99,2 % těchto uživatelů má paralelně 8 účtů na různých sociálních sítích. Určitým vybočením z globálních statistik je Japonsko, kde se v průměru jedná o 3,8 účtu na aktivního uživatele. V ČR je dle aktuální statistických dat z roku 2021 celkem 9,43 milionů aktívních internetových uživatelů z toho 7,39 milionů aktivních uživatelů sociálních sítí. Meziroční růst je 7 % což je analogický stejně jako v každé zemi světa.[12] Za poměrně velkým meziročním růstem stojí i fakt, že některé stránky, se ve snaze adaptovat na vývoj internetu transformovali na sociální síť. Jedna z takových webových stránek s názvem PronHub teď už sociálních sítí je jedenáctou nejhledanější webovou stránkou v celosvětovém měřítku, která nyní obsahuje i sdílený erotický multimediální obsah. Původně se však jednalo o webovou stránku pro předplacení profesionálního erotického obsahu, či z části bezplatného erotického multimediálního obsahu. Jak se internet vyvíjel i provozovatele tohoto webu, pochopili sílu sociálních sítí a dokázali jak technickou stránku, tak i komunitní ideologii sdílení multimediálního obsahu, zapracovat do svých stránek. Velkou přeměnu zažilo i komunitní internetové fórum Reddit[13], které se rovněž adaptovalo a konvertovalo celou platformu na regulérní sociální síť. Pokud se na sociální sítě podíváme z úhlu běžného uživatele zjistíme, že mnoho sítí je administrováno stejným provozovatelem a podporují i stejná přihlášení s jedním účtem na více sociálních sítí. Právě z důvodu dynamického nárustu uživatelů od roku 2004 doposud a velmi velkému zdroji personálních informací, nejenom začali vznikat nové obchodní odbory, ale i analytické metody a odvětví zabývající se právě sociálními sítěmi. Více v tabulce č. 2[14], reflektující počet aktivních uživatelů v přeních sociálních sítích za rok 2021. Mezi takovéto metody se zařadil i tzv.

[11] V roce 2021 se společnost Facebook přejmenovala na Meta, chtěla tak řešit poškozený mediální obraz společnosti.
[12] Datareportal.com [online]. [cit.25.2.2022]. Dostupné z: https://datareportal.com/social-media-users https://datareportal.com/reports/digital-2021-global-overview-report
[13] Velmi rozšíření a populární fórum dostupné online na z adresy: https://www.reddit.com/
[14] Datareportal.com [online]. [cit.25.2.2022]. Dostupné z: https://datareportal.com/social-media-users

SOCMINT, který je synonymem pro zisk zájmových dat právě ze sociálních sítích. V počátcích sociálních sítí, uživatel nahrával na veřejné stránky svého profilu jakékoliv personální informace bez rozmyslu a obavy ze zneužití. Po krátkém čase, kdy uživateli začalo docházet, že sociální sítě sbírají telemetrii z ICT[15], která je analyzována a optimalizována pro nabídky reklam. Algoritmy společností se vylepšovali tak, že začali analyzovat i nahrávaný obsah uživatelem, a proto tyto aktivity začala podporovat ve formě pasivního nátlaku s dotazy na zaměstnání, vzdělaní, rodinné příslušníky, plány na dovolenou apod. Tyto metody však nevyužívaly jen samotní provozovatelé sociálních sítí, ale i společnosti, které za účelem zisku dat začali tzv. tyto data těžit za využití SW, který byl vytvořen přímo na míru každé sociální síti. Provozovatelé sociálních sítí si uvědomovali konkurence, které využívá jejich platformy a snažili se s touto konkurencí bojovat na technické úrovni, jako změnou algoritmu tak, aby nebylo možné data sbírat. Často samotný provozovatel sociální sítě stojí před kritiky ze strany státu nebo medií, že nedokázal ochránit citlivá data svých uživatelů, která byla zneužita.

Pořadí	Sociální síť	Počet aktívních uživatelů v miliardách
1.	Facebook (Meta)	2,74
2.	YouTube	2,29
3.	Instagram	1,22
4.	TikTok	0,69
5.	Telegram	0,5
6.	Pinterest	0,4
7.	Redit	0,43
8.	Twitter	0,35
9.	VK	0,1
10.	MeWe	0,016

Tabulka č. 2 – Statistika aktívních uživatelů sociálních sítí v roce 2021, zdroj: dataportal.com

Na základě uzamčení informací za registrační zeď, kdy se každý podezřelí profil hlídá za účelem odhalení tzv. agenty společnosti využívající sociální sítě jako zdroj obchodních dat, je čím dál těžší SOCMINT aplikovat. V dnešní době, je příprava k SOCMINT metodě velmi složitá a je nutná všeobecná nejen obecná znalost kontrolních a bezpečnostních mechanismů sociálních sítí, ale i konkrétní cílové sociální sítě, protože i když často se jedná o stejného pořizovatele s jinou obchodní značkou, ale pořád může být platforma vystavena velmi rozdílnému algoritmu. Infiltrovat konspiračním způsobem sociální síť je čím dál těžší, a to

[15] Mezinárodně uznávaná zkratka z anglického Information and Communication Technologi (ICT), zahrnující veškerou informační a komunikační technologii.

hovoříme pouze o sběru dat, pokud bychom konspirační profil chtěli využít pro digitální HUMINT pak je zde kumulativně několik problému včetně důvěryhodnosti profilu a nejde zde již jen o konspiraci před administrátory, ale i před objektem zájmu. Z hlediska SOCMINT metod rozdělujeme sociální sítě i na určité oblasti demografického a geopolitického hlediska. Konkrétně se tak jedná o sociální sítě globální, ale i místní. V případě globálních se jedná například o Facebook (Meta), Instgram, Twitter, Tik Tok, tyto sítě jsou užívaný globálně, ale rovněž například ruskojazyční uživatele Facebook platformy využívají i ruské platformy, VK, Mail.ru, Odnokalssinki (OK). Stejně tak Asiati využívají rovněž globální sociální sítě, ale k tomu využívají WEchat, Weibo, Baidu. V případě TOR sítě v darknet oblasti se jedná o sociální sítě s názvy Galaxy 2, Galaxy 3, Dread, Social a dnes již nefunkční Atalyo. Jako alternativa necenzurovaného, ale zcel legálního obsahu balancující na hraně zákonnosti a svobody projevu, bychom mohly zařadit sociální síť MeWe.

2.4 Kolaborace OSINT a SOCMINT metod

Metody jako OSINT jsou spíše kategorie prostého zisku dat bez sebevětších obstrukcí. Oproti tomu SOCMINT, který se zaměřuje hlavně na sociální sítě, do kterých se dnes už řadí většina komunikátorů je velmi náročný, a to právě kvůli přípravě pro svůj proces. Na rozdíl od získávání informací z tzv. otevřených zdrojů, si musíme uvědomit, že sociální účty jsou pro uživatelé z venku leckdy uzavřeny a pokud na platformě nemáte ověřený účet, nemáte možnost zobrazit ani profilové informace či fotografii. Důvodem jsou nespočetné problémy s tzv. data miningem [16] svých uživatelů. Společnosti spravující tyto virtuální platformy sociálních sítí se snaží bránit takovému procesu sběru dat, proto je příprava konspirativního prostředku nejdůležitějším krokem. Pro překonání všech klíčových příprav je zdroj dat, naprosto diametrální od dat z otevřených zdrojů. Tyto data jsou obvykle kusé bez celistvosti a je nutné tyto data analyzovat a pokusit se je prověřit ještě v otevřených zdrojích pro další informace. Takto vzájemná kolaborace OSINT a SOCMINT metod maximalizují efektivitu sběru dat k subjektu zájmu.

[16] Data mining, je anglicky výraz pro analytickou metodu sběru dat z velkého zdroje.

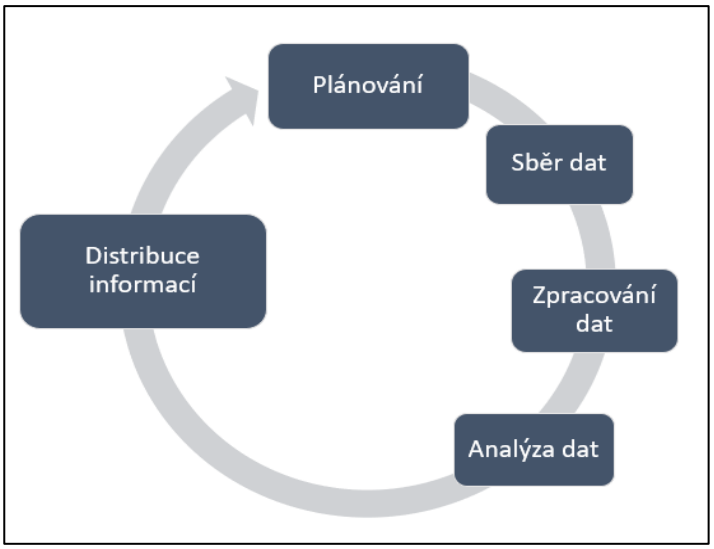
3 Zpravodajský cyklus jako proces sběru a vyhodnocení dat

Při každé efektivní analytické práci, je třeba znát cíl a sestavit si racionální plán od stanovení objektu zájmu, přes oblast zdroje dat až po výsledky analýzy. Tento plán je nazýván v oblasti práce s daty jako zpravodajský cyklus. Zpravodajských cyklů je několik druhů s cílem reflektovat konkrétní potřeby jejich aplikace v rámci svých oborů. Každý analytický obor může mít diametrální požadavky na celý proces, avšak jádro zpravodajského cyklu zůstává vždy stejný. Pokud si představíme zpravodajský cyklus, vždy by se mělo jednat o racionálně přirozený proces zpracovaní dat od plánu až po výstup. Jedná se o složky jako je plánování, sběr dat, zpracování dat, analýza dat, distribuce informací. První procesy zhruba podobající se procesům z dnešního obecného pojetí zpravodajského cyklu bylo využíváno již v 1. světové válce, ale skutečně první zadokumentovaný byl v roce1944, následně největší rozmach a úpravy do dnešní podoby proběhlo za studené války, která trvala mezi západními a východními mocnostmi v letech 1947–1991.[17]

3.1 Zpravodajský cyklus z hlediska kriminálních analýz

Každý zpravodajský cyklus, musí vycházet z analytických potřeb dané oblasti pro kterou bude využíván jako metodická šablona manipulace s daty. Pro potřeby kriminální policie a kriminálních analýz[18], je v podstatě tato oblast v několika fázích neustále netraktující a opakující se složkami procesu, jako analýza dat, sběr dat a zpracováním dat. Pro potřeby kriminální policie a kriminálních analýz, je v podstatě tato oblast v několika fázích neustále interaktivním a opakujícím se procesem se složkami jako analýza dat, sběr dat a zpracováním dat.

[17] CARL, L. D. The International Dictionary of Intelligence. USA: University Press of America, 1993. ISBN 978-1878292032.
[18] Interpol.com [online]. [cit.25.2.2022]. Dostupné z: https://www.interpol.int/content/download/7253/file/27_CAS01_05_2014_EN_web.pdf



Obr. č. 4 – Grafické zpracování zpravodajského cyklu, zdroj: archiv autora

Plánování

Plánování je jedna z nejdůležitějších fází zpravodajského cyklu a odráží potřeby a směr cíle. Pro vymezení objektu zájmu, je z efektivního hlediska nutné stanovit, jaké prostředky budou na tuto činnost vyčleněny, jaké informační zdroje a metody budou použity. Důvodem je optimalizace procesu pro kvalitní výstup. Někdy se mohou v rámci procesu změnit relevantní potřeby sběru dat, čímž v procesu zpravodajské cyklu dochází k návratu do fáze opětovného plánování za účelem přehodnocení zdrojů a vyřazení nebo zařazení nové metody.

Sběr dat

Samotný sběr dat, je jedna z nejsložitějších operací zpravodajského cyklu, protože obsahuje nejen příležitosti, ale i možné hrozby. Na základě předem definovaných prostředků a metod z procesu plánování, dochází ke sběru dat. V této fázi procesu záleží na metodě, u kterých je postup velmi specifický. V této fázi dochází k samotné realizaci sběru dat za využít různých technik, metod. Pod tímto sběrem dat si můžeme představit nejen odposlech komunikačního a datového provozu, práci s lidskými zdroji, nebo data z internetu, ale i výstupy z technických zařízení jako jsou družice a různé typy sond. U internetových dat může sběr probíhat automatizovanou formou nebo manuální.

Zpracování dat

Několik sub fází jako řazení, vyhodnocení, analýzy integrace a expedice dat ke komplexní analýze složky zpravodajského cyklu. Nedochází jen k očištění informací na relevantní informace jako vstupní data k analýze, ale k transformování informací do dat vhodné pro vložení do databází. V dnešní záplavě informací se data již nevyhledávají manuálně tak, že je do procesu zahrnut rozpoznávací lidský proces. Dnes jsou informace vyhledávány automatizovaně za využití analytických SW, které jsou naskytovány zájmové procesy. Takovýto proces velmi zefektivnil práci s daty, ale má to i své nevýhody, a to je problematika z hlediska struktury dat. Pokud informace není upravena pro použití v databázi, SW ji nedokáže zpracovat či vyhledat a tím jako by neexistovala. Z těchto důvodů musí být například z hlediska HUMINT poznatků, jako jsou třeba poznatky informátorů, zpracovány do kontextu s informací a dle manuálu či metodiky pro vklad takových to informací. Pro pochopení uvedu příklad, práce s lidmi je jeden z nejsložitějších procesů a v případě HUMINT metod, se může jednat i o práci s informátory. Pokud bychom se ohlédli po informátorech v rámci policejní praxe a vybrali statisticky nejprůměrnějšího a nejběžnějšího informátora, byla by to oblast drogové problematiky. Organizování trestné činnosti a výroba OPL[19] by jim šla, ale formulace či odborné názvy samozřejmě už ne. Navíc pro subjektivní hodnocení informací pro databáze dle indexu validity 1-5 A-F, je nutná správná charakteristika a prověření informace. Právě proto, je důležité forma zpracování a hodnocení informace pro vklad. Prakticky se jedná o stejný proces, kdy je informace transformována, klasifikována a vložena do databáze pro analytické využití, jako je například extrakce metadat[20] ze získaných souborů, dešifrování zachycených zpráv, filtrace a očištění ICT telemetrie, očištění grafického obsahu či extrakci grafického obsahu ze zvukových souborů. Těchto procesů je celá řada.

[19] Omamné a psychotropní látky
[20] Metadata jsou doprovodná data každého elektronického objektu ve formě technických atributů objektu.

Analýza dat

Jedná se o fázi procesu, ve které analytici data dávají do souvislostí s daty z předchozích procesů, čímž vytváří finální rysy výstupu. Tento proces je velmi složitý a klade na analytika velkou zodpovědnost nejen ke znalosti daného tématu, ale i k určité predikci možného vývoje. Nejedná se jen o analýzu zpracovaných dat, ale i tvorbu vlastích alternativních schémat hrozeb včetně jejich možných řešení.

Distribuce informací

Zpracovaný výstup ve formě zprávy, je komplexní odraz veškerých procesů ve zpravodajském cyklu, který shrne i možnosti a doporučené postupy. Tento výstup je odevzdán zadavateli úkolu.

4 Nástroje a metody sběru dat

V dnešní době jsou data velmi ceněnou komoditou. Jak bylo řečeno v předchozí kapitole ve spojitosti se sociálními sítěmi a vzniku nových dat s příchodem a rozvojem internetu, společnosti se snaží získat personální data nejen pro cílenou reklamu nebo spotřební trendy ve společnosti, ale i k ovlivňování veřejného mínění nebo politických voleb. Informace mohou mít velkou moc a nejvíce jich je právě ve virtuálním prostředí internetu. Záleží na typu poptávaných dat a jaký účel mají data plnit. V případě lidí můžeme hovořit o plošném sběru dat za účelem tvorby statistik nebo cílený sběr informací za účelem buď sledovat objekt zájmu napříč internetu a shromažďovat sensitivní informace napříč virtuálním prostředí internetu. Při sběru dat se nemusí jednat jen data okolo lidských objektů zájmu rovněž se může jednat o archívy, multimédia, datové kontejnery, pod. V obou případech jsou data zjišťována, jak automatizovaně za pomocí pokročilých SW, nebo manuálně za využít dílčích nástrojů.

4.1 Manuální sběr dat

Vzhledem k rozsahu a zaměření tématu OSINT, budou zmíněna jen teorie v základním rozsahu k nástrojům a využitelným metodám. Pro účely manuálního sběru dat je možné využít nejen webová rozhraní, ale i softwarová řešení, které ale stále nabízejí jen základní dobývání surových dat.

4.1.1 Internetové vyhledávače

Pokud jde o obecné hledisko každá země má své vnitrostátní vyhledávače, které obvykle vyhledávají informace z lokálních zdrojů a nejsou tak globálně zaměřeny, jako například webová stránka s rozdělovníkem vyhledávačů dle států www.searchenginesoftheworld.com. Existují i různé webové stránky nabízející i konsolidované vyhledávaní, které skrze jeden vyhledávač, prohledavá v algoritmech předem definovaných vyhledávačů. Tyto vyhledávače je dobré využívat při šetření v lokálních reálií, kde nám globální vyhledávače zisk informací deformují. Mezi populární vyhledávače patří i weby s komplexním vyhledáváním www.all-io.net, www.alltheinternet.com, wwwweboas.is. Dále exotické

vyhledávače jako je vyhledávač www.parseek.com. Jeden z nejmazavějších vyhledávačů srovnatelný s algoritmem Google vyhledávače, ale s preferovaným vyhledáváním v ruskojazyčných zemích je www.yandex.com. I když bylo v předchozích kapitolách zmíněno, že darknet webové stránky nejsou indexovány, tak i v prostředí TOR se nacházejí vyhledávače. Princip tkví v manuálním indexování nebo registrování adres tvůrci takových webových domén v daném vyhledávači. V darknet prostředí TOR se jedná především o vyhledávače Ahmia na www.juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibsot4csyd.onion, a ne příliš známy, ale využitelný vyhledávač Phobos na webové adrese www.phobosxilamwcg75xt22id7aywkzol6q6rfl2flipcqoc4e4ahima5id.onion.

4.1.2 Google Search Operators

U globálního vyhledávače, jakým je Google, nám ve své podstatě nabízí nejen svůj špičkový, ale i vyhledávací algoritmus, ale i samotnou filtraci díky funkci vyhledávání za pomocí operátorů[21]. Pro přehled je v tabulce č. 3 uvedeno několik základních příkazů s následnou aplikací a výsledkem.[22]

Operátor	Význam
""	Vyhledání přesného výrazu, který je umístěn v uvozovkách. Například "brusný kámen", výstupem bude jen stránky obsahující tvar pro brusný kámen.
OR	Užíváno pro vyhledávání dvou výrazů, obvykle ve spojení s dalšími operátory. Například site:pojistovna.cz Novák OR Novotný, vyhledá na webové stránce www.pojistovna.cz obsah, kde figuruje Novák nebo Novotný.
AND	Užíváno pro vyhledávání dvou výrazu s podmíněním přítomnosti obou slov, obvykle ve spojení s dalšími operátory. Například site:pojistovna.cz Novák AND Novotný, vyhledá na webové stránce www.pojistovna.cz vyhledá obsah jen, kde figuruje Novák a současně i Novotný.
filetype:	Vyhledávání konkrétního slova či slov v předem definovaném typu dokumentu. Například červený fosfor filetype:pdf, výstupem jsou

[21] Známo taky jako výrazy v anglickém jazyce Google Hack nebo Google Dorks
[22] Exploit-db.com:Google Hacking Database. [online]. [cit.25.2.2022]. Dostupné z: https://www.exploit-db.com/

	odkazy na stránky obsahují dokument formátu PDF obsahující slova červený fosfor.
site:	Zúžení vyhledávání na konkrétní síť obvykle užívání s dalšími operátory. Příklad červený fosfor site:alchema.cz, výstupem jsou obrázky či texty vně webové stránky www.alchema.cz obsahující slova červený fosfor.
inurl:	Vyhledá stránky, které mají v názvu předem definované nebo definovaná slova. Například inurl:apple vyhledá web, který má v URL obsaženo slovo apple.
intext:	Vyhledá webové stránky, které mají ve svém obsahu předem definované nebo definovaná slova vhodné za využití dalších operátorů. Příklad intext:″slepice″ OR ″drůbež″ vyhledá webové stránky s konkrétním textem slepice nebo drůbež.
cache:	Výsledkem je zobrazení poslední verze webové stránky, která je v mezipaměti za předpokladu, že byla indexována.
#	Vyhledá označené příspěvky předem definovaného výrazu na indexovaných sociálních sítích. Příklad #funwithdrugs, výstupem jsou odkazy na Instagram s fotografiemi #funwithdrugs
*	Nahrazení slova nebo operátora, lze jej využít pro vyhledávání i subdomén. Například site:*.seznam.cz -www
-	Vyloučení daného výrazu nebo celé webové stránky. Rovněž použití jako diskriminace nedůvěryhodných zdrojů.

Tabulka č. 3 – Přehled základních Google operátorů, zdroj: www.exploit-db.com

4.1.3 Veřejné databáze a registry

Mezi další zásadní zdroje, mohou být i veřejnosti přístupné databáze spravovány státem jako jsou například různé registry jako je třeba státní správa zeměměřičství a katastru dostupné online na www.cuzk.cz, registr živnostenského podnikání dostupné online na www.rzp.cz, databáze českého statistického úřadu dostupné online na www.czso.cz, registr smluv mezi státem a právnickými nebo fyzickými subjekty dostupné online na www.smlouvy.gov.cz. Povinnost zveřejňování zmíněných dat, nemá jen ČR ale i všechny státy světa, proto je možné se dostat k podobným datům i rámci jiných zemí jako například u Spojené království Velké Británie a Severního Irska, kde se na vládní webové stránce dostupné online www.gov.uk, nachází rozdělovník veřejných registrů jako například živnostenský rejstřík na www.find-and-update.company-information.service.gov.uk. Takovéto

informace je možné získat ze všech možných koutů světa, pokud zde došlo k základní digitalizaci.

4.1.4 Rozbor grafického materiálu

V rámci OSINT analýz, dochází k záchytů dat v podobě obrázků či jiného grafického obsahu, který lze opět vyhodnotit jak na přítomnost exif dat[23], popřípadě možnou úpravu dat s grafickým obsahem, tak i možný původ, či duplicitu tohoto obsahu na jiných místech. Ve své podstatě se do této analýzy zapojuje mnoho oborů, a to včetně steganografie[24] a steganalýzy[25]. Obvykle se jedná o grafiku v podobě upravených obrázků jako součást webové stránky v rámci WEBINT nebo fotografii na webových stránkách či sociálních sítí. Ke zjištění exif dat poslouží prosté zobrazení vlastností obrázku, kde můžeme nalézt data ve formě GPS koordinátu, kde byl obrázek pořízen, jakým zařízením byla fotografie pořízena, jako je například typ a značka zařízení, dále čas a datum pořízení. U exif dat je velmi snadné uvedená data zfalšovat nebo smazat, proto je důležité k těmto datům přistupovat obezřetně a ověřovat důvěryhodnost těchto dat. Z grafického obsahu lze zjistit i změny v grafické bitmapě, zda došlo k nějaké úpravě fotografie, popřípadě v jak velkém rozsahu. Nebo zda v takovémto grafickém materiálu nejsou záměrně ukrytá data za využití digitální steganografie. Rovněž jde zhodnotit i samotnou fotografii s obsahem co se na ní nachází.[26] Jako například obr. č. 4, na kterém jsou zachyceny diametrální místa příznačná pro dvě místa na planetě, kde se nachází na levé straně vyfrézované bezpečnostní drážky na dálnici v USA a na pravé straně svislé opravní značení s losem. V případě dostatku vstupních dat z obsahu, který se nachází na fotografii, lze rozpoznat místo, osoby, věci i přibližný čas pořízení. Možnost procvičování takovýchto dovedností na webové stránce www.geogussr.com, kde se generují nahodilé fotografie na základě Google maps, které se snažíte identifikovat na základě obsahu grafiky.

[23] Exif data je forma metadat ve formě doprovodných technických atributů fotografie.
[24] Steganografie je typ utajené komunikace, kdy jsou data ukryty tak, aby nebyla zjistitelná.
[25] Steganalýza je metoda detekce skrytých dat.
[26] BAZZELL, M. Open Source Intelligence Techniques. 6th ed. Poland: Amazon, 2018. ISBN 978-1984201577.

Obr. č. 4 – Vlevo drážky v silnici USA, vpravo dopravní značení Skandinávie, zdroj: archiv autora

Reversní vyhledávání obrázků a fotografií, obvykle pocházející z WEBINT jako grafický obsah webových stránek. Za využití vyhledávacích algoritmů ze stránek www.google.com, www.yandex.com, www.tineye.com, lze vyhledat podobný ne-li stejný grafický obsah s odkazy nálezu v internetu.[27]

4.1.5 Password OSINT

V oblasti OSINT metod je tato nejvíce morálně rozporuplná, protože zdrojem dat jsou data pocházející z trestné činnosti, jako je tzv. data leak[28] a data breach[29] obsahující základní data a telemetrii uživatelů různých služeb. Obvykle se jedná o data jako jméno, příjmení, e-mailová adresa, heslo k registrovanému účtu, popřípadě telefonní číslo, IP adresa a základní telemetrie ICT ze kterého byl účet

[27] PICOLET, J. Operator Handbook. USA: Netmux LLC, 2020. ISBN 9798605493952.
[28] Data leak je anglický výraz pro vynesení dat z jinak veřejně nedostupných databází a systémů obvykle úmyslně zaměstnancem z osobních pohnutek nebo neúmyslně pochybením.
[29] Data breach je anglický výraz pro získání dat z dat z databází nebo systémů kybernetickým útokem.

registrován, či z něj přistupováno k účtu, ale to záleží na rozsahu tzv. logování[30]. Bezpečnostní komunita tvrdí, že v současné době je dostupných 12 mld. záznamů, což by statisticky znamenalo, že minimálně u každého aktivního uživatele internetu došlo ve dvou případech zveřejnění hesla. Společnost Apple v nové aktualizaci přidala funkci, automatického prověření hesla, zda se nenachází ve výše uvedených seznamech exponovaných hesel. Právě, zde je ten morální rozpor, jelikož využívání těchto zdrojů může vést k velmi efektivnímu vyhledávání dat a spojovat anonymní uživatele s účty a s totožnostmi na všech úsecích a úrovních internetu. Mezi nejvýznamnější vyhledávače hesel a ICT telemetrie patří tyto webové stránky: www.dehashed.com, www.hashes.org, www.weleakinfo.to, www.havibeenpwned.com.

4.1.6 Analýza webové stránky a dat

Jedním z relativně nových dat z chronologického hlediska příchodu internetu do společnosti, jsou data v souvislosti s provozem webových stránek a jejich obsah. U webových stránek tak analyzujeme tzv DNS, NS záznam, MX záznam, subdomény. Každá webová stránka je zavedena v tzv. Domain Name Systém, ve které je zapsán majitel, adresa a kontaktní údaje webové domény[31]. Na základě GDPR je většina těchto údajů cenzurována za účelem ochrany osobních dat. Název webové stránky je ve skutečnosti odkaz na IP adresu s daty webového obsahu na serverech. Tyto údaje může využít pro analýzu NS, ve vztahu k historii hostováním, jaké webové stránky byly na stejném místě hostovány. Analýzou MX záznamu, získáme informace o posčítaných klientech v rámci webové stránky či případného přesměrování e-mailových adres k webové doméně. Další technické informace pocházejí z algoritmu samotné webové stránky, ve formě zdrojového kódu, který stojí za provozem. Ve zdrojovém kódu webové stránky se často nacházejí metadata, která nejsou viditelná v náhledu webové stránky. Obvykle se jedná o informace tvůrce a technické poznámky a komentáře vývojáře ve

[30] Logování je výraz z anglického slova „Log“, což je obecně známo jako zápis informací z monitorování prostředí činnosti systému a jeho okolí.
[31] KUBECKA, Ch. Hack the World with OSINT. Netherland: HypaSec, 2019. ISBN 978-0-9956875-9-2.

zdrojovém kódů PHP[32] nebo HTML[33]. Komentáře v PHP kódu jsou v jednoho řádku začínají znakem „//“ nebo znak „#“ a následuje text komentáře, nebo více řádkový komentář, který je uzavřen znaky „/* text komentáře */“. U HTML kódů se jedná o „<!-- text komentáře -->“. Komentáře mohou obsahovat informace jako e-mailová adrese, a jiné kontaktní údaje tvůrce stránek nebo skryté odkazy a informace.[34] Rovněž se může analyzovat kousek zdrojového kódu, zda není duplikován i na jiných webových stránek, které souvisejí s daným webem. Dalším aspektem je rozbor obsahu webových stránek a odkazů na sociální sítě. Různé reklamní bannery nebo fotografie mohou být analyzovány IMINT metodou, včetně komparace duplicitního užití na jiných webech. Součásti WEBINT analýz je i zjišťování subdomén[35]. K tomu je možné využít jak již zmíněné Google operátory ve formátu site:*.test.cz -www, tak i různé SW jako například Sublister, který subdomény detekuje podobným způsobem, dostupný online na webové adrese https://github.com/aboul3la/Sublist3r.

4.1.7 Sociální sítě

Skrze OSINT se dostáváme na platformy sociálních sítí a komunitních fór. Z pohledu manuálního sběru dat, jsou tyto platformy nejproblematičtější, protože zde platí určitá bezpečnostní pravidla, bez kterých nelze data sbírat nebo analyzovat. Data lze sbírat za využití krycích profilu viz. kapitola 5.1. Působení v prostředí internetu. Na uvedených sociálních platformách je velký zdroj dat tykající se objektů zájmu, které nám dokážou poskytnout k analýze grafický materiál ve formě fotografií, vazby přátel apod. Za předpokladu efektivního pronikání do zájmových skupin i informace a obsah z uzavřených skupin.

Jedna z hlavních oblastí aktivního sběru dat na sociálních sítích jsou vazby na předmětný cíl. Zde je velmi důležitá myšlenka s názvem 6 stupňů odloučení. Jedná se o myšlenku, že všichni lidé na světě jsou ve spojení přes šest sociálních

[32] PHP je anglickou zkratkou pro Hypertext Preprocessor, což je programovací jazyk k tvorbě webových stránek
[33] HTML je anglickou zkratkou pro Hypertext Markup Language, což je programovací jazyk k tvorbě webových stránek.
[34] TAYEBI, M. A., et al. Open Source Intelligence and Cyber Crime. Switzerland: Springer, 2019. ISBN 978-3-030-41251-7
[35] Subdoména je součásti hlavní internetové domény.

kontaktů. V roce 1967 americký vědec Stanley Milgram[36] na základě myšlenky spisovatele Frygiese Karinthyho[37] provedl experiment, který tuto myšlenku potvrdil. Společnost Facebook v roce 2011 publikovala vlastní studii, kde je při 727 mil. uživatelů toto číslo již 4,74 a v roce 2016 při 1,6 mld. již číslo 4,57. Za předpokladu snižujícího se čísla sociální vazeb v závislosti na počtu uživatelů, je při počtu uživatelů Facbook 2,74 mld. ze statistických dat z roku 2021, racionálně číslo 4. I když se jedná o data ze sociální sítě Facebook, nyní Meta, je tato rovnice zastoupena na každé sociální síti, a to včetně i reálného světa. Právě na základě této informace, je důležité při aktivním sběru dat dbát na zúžený okruh objektu zájmu a nepřecházet na více než dvě sociální vazby, protože se zvětšovaným okruhem se zvětšuje i irelevantnost získaných dat.

Mezi základní metodu manuálního sběru dat ze sociálních sítí patří i použitelnost Google operátorů, které lze aplikovat na mnoho sociálních sítí, a to i vně těchto sítí. Například v Google vyhledávači lze použít parametr k osobě a místu vyhledávání „karel novak“ site:twitter.com. Při tomto parametru lze následně v google prohlížeči změnit záložku na obrázky a zobrazí se fotografie a jiný grafický materiál z účtu, které jsou v parametrech syntaxe předmětného vyhledávání. Stejně tak jako tzv. označení neboli „tag“ za využití symbolu #, například „#drugsonsale“ from:twitter.com.[38] Za těchto podmínek v syntaxi je vyhledám obsah s označením drogy na sociální síti Twitter. Z hlediska pasivního sběru dat je možné využití různých statistických a kompilačních stránek, www.socialbearing.com, www.twitonomy.com, www.twitterdeck.com. V dnešní době však sběr dat ze sociálních sítí už není tak jednoduchý, jak před rokem 2018, kdy si společnosti uvědomili sílu a cenu personálních dat obsahující sociální sítě a s cílem vytěžit maximu těchto dat rozpoutaly boj mezi provozovateli sociálních sítí a společnostmi, které sítě využívají pro sběr dat. Tento boj se začal odrážet do politiky a pak i zejména do ochrany osobních údajů či práva na soukromí. Následkem byla bezpečnostní opatření provozovatelů sociálních sítí a odstraňování některých personálních dat nebo možnost zamykat své účty na

[36] Stanley Milgram 15.7.133 – 20.12.1984, byl americký pedagog a sociolog, absolvent Harvardu, USA sociální psychologie.
[37] Frigyes Karinthy 24.6.1887-2971938, byl maďarký spisovatel a novinář.
[38] RUSSELL, M. A., et al. Mining the Social Web. 3rd ed. Canada: OREILLY, 2019. ISBN 9781491985045.

sociálních sítích tak, aby nebyly vyhledatelné nebo nebyl viditelný obsah. Toto jednání změnilo mnoho metod sběru dat na sociálních sítí do nepoužitelného stavu, a to včetně zálohování obsahu. V současné době je prakticky nemožné zjistit komplexní informace než za využití komplikovaného pronikání do zájmového prostředí nebo rozboru interakcí v rámci profilu. V případě sociální sítě Facebook se jedná například o interakci při sdílení nezbytných informací jako je například profilová fotka, u které jde vidět sociální interakce formou emotikon a komentářů. Pravděpodobně nejbližší a blízcí přátelé budou takovouto událost komentovat nebo hodnotit. Stejně tak i povinný obsah, jako jsou oblíbené stránky, místa a zájmy. I zde lze vyčíst a vykreslit charakteristické rysy osoby či získat data pro rozšíření oblasti informačního depotu.

Jeden z největších zdrojů informací, jsou pravděpodobně diskuze ve virtuálním prostředí, do které se zapojí celá komunita. Tyto zdroje dat nenajdeme vně sociálních sítí, ale na diskuzních fórech, které se velkým rozmachem sociálních sítí transformovali do jakéhosi hybrida diskuzního fóra sociální sítě Facebook formátu. V každé oblasti zájmu je možné fórum, které lze využít pro kriminální analýzy v obecné rovině. Nejznámější a nejrozsáhlejší taková forma je Reddit v oblasti clearnetu a Dread v oblasti darknetu, a to konkrétně TOR sítě.

U sociální sítě Instagram je problematika sběru opět v uzavřeném profilu a případně s extrakcí grafického obsahu profilu, protože se nacházejí pod ochranným filtrem, který je nastaven ve zdrojovém kódu samotné platformy. Pro účely extrakce komplexního grafické obsahu zájmového profilu lze využít webový nástroj www.instadp.com a v případě změny algoritmu vně platformy sociální sítě, který takový to nástroj vyřadí z provozu manuálního zajištění formou printscreen funkcí nebo jiného SW nástroje pro výřezy obrazovky.

4.1.8 Virtuální měny

I když BTC je formou POC[39] popsáno od roku 2008 a zprovozněno v roce 2009, fakticky je policejní zájem na virtuálních měnách až od roku 2013, kdy začal prorážet do společnosti jako investiční a platební nástroj. V tom druhém případě

[39] POC je anglická zkratka Proof of concept, což je realizace důkazu o proveditelnosti teorie.

se jedná hlavně o kriminalizaci virtuálních měn jako platební prostředek za ilegální zboží, a to nejen na virtuálních platformách ilegálních tržišť vně darknetu, ale i v clearnetu formou utajených skupin sociálních sítí. V rámci manuálního sběru dat poslouží webové stránky každého provozovatele virtuální měny, které jsou pokládany za měnu s viditelným blockchainem. V případě kriminálních analýz, poslouží i webová stránka www.walletexplorer.com, která byla vytvořena českým vývojářem, který nyní pracuje ve společnosti poskytující profesionální nástroj plně automatizovaného typu www.chainalysis.com. V rámci kriminálních analýz nás bude převážně zajímat 4 nejužívanější virtuální měny na světě, a to k poměru investičního nástroje nebo jako platební prostředek za ilegální zboží a to BTC, XMR, LTC, ETH. Pouze XMR je naprosto anonymní a jeho blockchain není veřejný, proto v něm nelze vyhledávat jako ve veřejném účetnictví. U těch s veřejným blockchainem jsme schopni tzv. Trasovat transakci napříč blockchainem od adresy k adrese, ale problémem je, že adresy jsou anonymní. Nástroj jako wallet explorer dokáže některé z BTC adres identifikovat a tím začínáte odhalovat směr transakce a její povahu. V rámci manuálního trasování je to velmi náročný úkol a s neaktuálními informacemi, které wallet explorer i celkem neefektivní.

4.2 Automatizovaný sběr dat

V předešlém oddílu byly popisovány metody manuálního sběru dat, ale právě základní metody manuálního sběru dat souvisejí s tím plně automatizovaným. Některé SW obvykle open source [40] typy SW využívají právě postupy z manuálního sběru dat jako například Google operátory. Graficky zpracovaný SW, je nic jiného než syntaxe příkazů, které uživatel používá bez hlubší znalosti a nutnosti manuálního zadávání. Například grafické zpracování vyhledávacího pole, do kterého zadáte e-mailovou adresu a tel. číslo následně máte na výběr tlačítko pouze ve spojením s dalším objektem nebo vyhledat obojí. Pouze si vybíráte mezi tlačítky s funkcemi, ale za grafickým zobrazením není nic jiného než prostá syntaxe Google operator, kterou analytik zadával do Google vyhledávače,

[40] Open source známy taky jako open software je, program s otevřeným zdrojovým kódem pro možnou modifikaci či nakládání.

tak to udělá SW za něj. Například fórum www.github.com, které původně fungovalo jako poradní programátorské fórum, kde se programátoři radili o svých projektech a vzájemně si je opravovali a propagovali. Dnes má tato platforma stejný účel, ale lze ji již považovat za sociální síť v rámci, které sdílíte vlastní obsah, myšlenky a dáváte k dispozici i vlastní SW. Právě zde se nachází mnoho SW pro OSINT od primitivnějších až po sofistikovanější, které se dokáží rovnat i profesionální konkurenci.

Software as a service

Mezi často nabízených programů se často setkáme s nabídkou SaaS[41]forem, které mají svou velkou výhodu, a to přístup k datům odkudkoliv a za pomoci rozhraní webového prohlížeče nebo SW ve formě klienta bez licenčního omezení vztahující se k ICT. Jako další výhoda je výpočetní výkon, který v případě SaaS není tak důležitý, protože všechny procesy běží na ICT u poskytovatele a grafické rozhraní je pouze náhled a ovládací panel. Tyto formy mají sice výhody, ale i nevýhody, a to v rychlosti zpracování dat nebo možných výpadků služeb apod.

Software řešení

Jsou obvykle programy vně počítače, které čerpají data ze vzdálených serverů, ale oproti SaaS řešení komplexní procesy běží v programu, který je hostován na přítomném HW. Nevýhody mohou spočívat velkém nákladu kvůli HW náročnosti analytického SW nebo licenci, která je vázaná na HW a jakékoliv poškození či opotřebování, které učiní hlavní složku ICT neprovozuschopnou může mít vliv na licenci, která obvykle je vázáná právě na HW v ICT.

U takto řešených SW je třeba tyto skupiny rozdělit na dvě. Ve skupině první se jedná o SW, který shromažďuje data pro vyhodnocení analytikem a skupinu druhou, kde jsou data již v raném procesu vyhodnocováno samotným algoritmem SW. U skupiny druhé jsou tyto řešení velmi populární a téměř neustále vznikají nové projekty. Obvykle je životní cyklus takovéhoto SW kratší než obvykle. Obvykle se jedná o studentské projekty, které tvůrci ponechají bez aktualizací, čímž se neadaptují na dynamicky se vyvíjecí prostředí internetu. Někteří tvůrci na

[41] SaaS je anglická zkratka Software as a Service, což je výraz pro formu provozu programu tím, že je hostován provozovatelem služby.

základě těchto projektů dostanou pracovní nabídku s podmínkou, že se dále svému projektu nebudou věnovat v žádné formě aktualizace nebo úpravy. Tohle byl i případ tvůrce webu pro OSINT analýzu BTC blockchain dat dostupných online na www.walletexplorer.com, který přijal nabídku od společnost Chainalysis a proto je stránka neaktualizována a propaguje komerční nástroje zmíněné společnosti pro stejnou činnost. Níže jsou uvedeny dle skupin příklady několika nejznámějších a nejužívanějších programů OSINT komunitou.

4.2.1 Software jako nástroj sběru dat

Třízení nástrojů pro OSINT je velmi složité, protože mnoho z nich je spíše nástroj pro vizualizaci již držených dat než jako nástroj extrakce a část z takových SW je i nástrojem, který následně data vizualizuje. Níže jsou zmíněny nejznámější a nevyužívanější nástroje OSINT komunitou z obojího zastoupení.

FOCA

Veřejně dostupný nástroj od společnosti Telfonica Tech dříve proslulé Eleven Paths. Nástroj s názvem FOCA[42] je využíván jako všestranný nástroj pro DNS analýzu apod., ale z velkého množství stejných SW vystupuje z řady pro plošnou identifikaci souborů a extrakci meta dat z těchto souborů z předem definovaných zdrojů nebo za využití Google operátorů. Dostupná online na sociální síti GitHub na odkazu www.github.com/ElevenPaths/FOCA.[43] Software FOCA má i svého stinného bratra s názvem Evil FOCA, který se věnuje testování bezpečnosti sítí z hlediska útoků MITM[44].

Recon – ng

Nástroj od společnosti Balck Hills kompilující všeobecné příkazy pro komplexní průzkum objektu zájmu a získaní dat k DNS, subdoménám, NS, MX protokolům a podobných záznamů v jednoduchým rozhraním, dostupný online na webové adrese www.github.com/lanmaster53/recon-ng.[45]

[42] FOCA je zkratka z anglických slov Fingerprinting Organizations with Collected Archives
[43] GitHub.com [online]. [cit.25.2.2022]. Dostupné z: www.github.com/ElevenPaths/FOCA
[44] MITM je zkratka anglického výrazu Man in the middle, což je druh kybernetického útoku.
[45] GitHub.com [online]. [cit.25.2.2022]. Dostupné z: www.github.com/lanmaster53/recon-ng

Nmap/Zenmap

Velmi rozšířený nástroj vytvořený Gordonem Lyonem pro mapování jak vnitřní sítě, tak aktivní vyhledávaní vně internetu na základě dotazu k dané doméně. Jedná se především o zjištění dat v podobě IP adres, otevřených portech a identifikaci služeb běžících na těchto portech OS serveru. Tento program je v GUI jak pro WIN OS pod názvem ZenMap tak pro OS s Linux s jádrem s názvem Nmap, oba programy dostupné online na webové stránce www.nmap.org.[46]

TheHarvester

Pasivní OSINT nástroj pro data minig informací v podobě e-mail adres, telefonních čísel a podobných údajů na předem vymezené oblasti zájmu. Nástroj podporuje jak globální, tak i lokální internetové vyhledávače, včetně možnosti zařazení vlastního API ze zdrojů jako jsou databáze Censys, BynaryEdge, Shodan, SecurityTrails apod. Nástroj dostupný online na webové adrese www.github.com/laramies/theHarvester.[47]

Reactor

Vizualizační a analytický nástroj formou SaaS od společnosti Chainalysis, využívajíc veřejné blockchainy virtuálních měn BTC, ETH a další dle nabídky společnosti, společně s OSINT daty k transakcím. Vzhledem k obsáhlým databází ztotožněných adres virtuálních měn se jedná o jeden z nejvýkonnějších nástrojů v globálním měřítku, pomáhající bezpečnostním složkám a finančním institucím po celém světě. Informace dostupné online na webové adrese www.chainalysis.com.[48]

Elliptic

Rovněž se jedná o analytický a vizualizační nástroj ve formě SaaS pro transakce virtuálních měn ve veřejném blockchainu, využívající nejen vnitřních databázi ztotožněných adres virtuálních měn. Není tak populární a databázemi obsáhlý jako Reactor, ale má právoplatné zastoupení v oblíbenosti bezpečnostní komunitě

[46] Nmap.org [online]. [cit.25.2.2022]. Dostupné z: www.nmap.org
[47] GitHub.com [online]. [cit.25.2.2022]. Dostupné z: www.github.com/laramies/theHarvester
[48] Chainalysis.com [online]. [cit.25.2.2022]. Dostupné z: https://www.chainalysis.com/chainalysis-reactor/

a využití v globálním měřítku. Informace k nástroji dostupné online na webové adrese www.elliptic.co.[49]

Voyager

Software formou SaaS od společnosti WEB-IQ se věnuje vizualizaci dat, která pocházejí z procesu data mininigu ve všech zájmových oblastí internetu z hlediska bezpečnosti, a to včetně darknet sítí. Zejména pak z oblasti TOR sítě. Jedná se o jeden z nejrozšířenějších nástrojů u bezpečnostních složek, nejen pro svůj objem dat, ale kvalitních relevantních informací. Nástroj disponuje možností nastavovaní různých filtrů a prohlížení historických dat, proto je cenným nástrojem. Informace dostupné online na webové doméně www.web-iq.com.[50]

Vision

Vizualizační nástroj formou SaaS pro analytické účely od společnosti DarkOwl, který využívá bezpochyby největší a nejlepší databází dat pocházející z data miningu internetu všech oblastí internetu především zaměřenou na darknet oblast. Společnost si je vědoma, že síla nástroje není jen ve vizualizaci dat, ale i v datech v samotných. Tyto data jsou tak kvalitní, že společnosti DarkOwl se více soustředí na jejich prodej formou API. V současné době se jedná o číslo jedna v nejprodávanějších digitálních komodit v této oblasti segmentu trhu. Klientem nejsou jen bezpečnostní složky z celého světa, ale i společnosti, které výše zmíněné API využívají, jako zdrojová data pro vstupní data vlastního SW využívající AI post-processing[51] dat. Informace dostupné online webové adrese www.darkowl.com.[52]

4.2.2 Software s AI a data z post-processingu

Některé softwarová řešení mají zakomponovaný AI systém s cílem vyhodnocení tzv. Big Dat, která by jinak analytik pracující s nástrojem nebyl schopen třídit, natož

[49] Elliptic.co [online]. [cit.25.2.2022]. Dostupné z: https://www.elliptic.co/solutions/crypto-wallet-screening
[50] Web-iq.com [online]. [cit.25.2.2022]. Dostupné z: https://web-iq.com/solutions
[51] AI post-processing dat je anglický výraz pro automatizovanou analýzu a zpracování za pomocí předem nastaveného algoritmu za účelem filtrace dat nebo umělé inteligence.
[52] Darkowl.com [online]. [cit.25.2.2022]. Dostupné z: https://www.darkowl.com/products/vision-app/

zpracovat. Data se třídí zcela automatizovaně na základě bodového hodnocení relevance. Níže jsou uvedená na trhu nejznámější řešení pro bezpečnostní účely z hlediska kriminálních analýz, která se nachází jen v komerční sféře a často jsou i velmi nákladná.[53]

IRIS

IRIS, je analytický a vizualizační nástroj od společnosti Hyperids, v němž jsou integrovány unikátní moduly pro online práci v internetu, které rovněž dokáží třídit data a nabízet pravděpodobnost propojení objektů zájmu s dalšími daty či objekty. Společnost Hyperids na svých webových stránkách www.hyperids.com zmiňuje unikátní moduly jako je platforma pro HUMINT metody a modul pro správu krycích profilů.[54]

WebintPro

Jedná se analytický a vizualizační nástroj od společnosti Cognyte, který se specializuje na data ze sociálních sítí a konektivitu mezi objekty zájmu, kterou vyhodnocuje v post-processingu algoritmus programu. Mezi jeho domény patří i rozpoznávaní obličejů z fotografií a identifikaci objektu vně sociálních sítí. Informace dostupné na webových stránkách společnosti www.cognyte.com.[55]

Gotham

Jeden z nástroj od společnosti Palantir, který je cílen přímo na bezpečností složky. Palantir na svých produktových stránkách na webovém portálu www.palantir.com uvádí, že se jedná o nástroj s pokročilými funkcemi AI a strojového učení, které na základě sledování práce analytika dokáže filtrovat a následně nabízet pouze relevantní data v rámci kriminálních analýz.[56]

[53] TAYEBI, M. A., et al. Open Source Intelligence and Cyber Crime. Switzerland: Springer, 2019. ISBN 978-3-030-41251-7.
[54] Hyperids.com [online]. [cit.25.2.2022]. Dostupné z: https://www.hyperids.com/products-solutions
[55] Cognyte.com [online]. [cit.25.2.2022]. Dostupné z: https://www.cognyte.com/web-intelligence/web-intelligence-investigations/#
[56] Palantir.com [online]. [cit.25.2.2022]. Dostupné z: https://www.palantir.com/platforms/gotham/

Videris

Je vizualizační nástroj pro mapování dat pocházejících z více zdrojů v interaktivním grafu zvýrazněného propojení mezi objekty na základě vnitřního algoritmu a post-procesingu dat. Do platformy lze použít jak vlastní data sety, tak i veřejné nebo zdroje společnosti. Více informaci na webovém portálu společnosti www.blackdotsolutions.com.[57]

Social Links

Nástroj v SaaS formě dostávající se do popředí především v SOCMINT analýzách, kde je možné využít GUI verzi tak i API token pro modulární platformu. Nástroj dokáže korelovat data s databázemi pocházejícími z data miningu, tak i real-time daty a spojovat profily sociálních sítí s objekty zájmu. Informace dostupná online webové adrese www.sociallinks.io.[58]

4.2.3 Modulární forma řešení softwaru

Jedená se o platformu se základními OSINT funkcemi, s možností vlastního zavedení API[59] tokenu ze zakoupené služby u jiných provozovatelů, a to téměř bez omezení. Obvykle jsou takovéto modulární platformy prodávány v licenci s časovým omezením s možností dalšího prodloužení. Platformy jsou velmi lákavé pro svou malou cenu, protože prioritu a zaměření si vybere sám analytik, čímž se celá kompilace těchto SW stává velmi efektivní k poměru ceny a výkonu, jinými slovy pronajímatel neplatí za zbytečné a nevyužité funkce. Provozovatelé takových to platforem zároveň neručí za funkčnost modulů a distancují se od možných výpadků služeb, protože poskytují pouze platformu nikoliv samotné moduly.

[57] Blackdotsolutions.com [online]. [cit.25.2.2022]. Dostupné z: https://blackdotsolutions.com/industries/government/
[58] Sociallinks.io [online]. [cit.25.2.2022]. Dostupné z: https://sociallinks.io/industries/leas-and-government
[59] Zkratka v anglickém jazyce pro Application Programming Interface, sloužící jako data interface z datového zdroje

Maltego

Mezi nejznámější modulární platformy patří SW Maltego od společnosti Paterva. Maltego poskytuje ze základu pouze funkce jako vyhledávání v internetu za pomocí syntaxí Google operátorů, ale plně automatizovaně. V základním menu je možné si doinstalovat moduly od externích dodavatelů jak třeba k DNS analýzám apod., ale obvykle nejsou přesné nebo jsou omezené na počet výsledků či možných vyhledávání. V případě nákupu přístupu do různých DB, lze aplikovat vyhledávání i v takových to DB. Velmi mnoho společností se orientuje nejen na vlastní SW, ale i na moduly nebo API využitelných v rámci Maltega.[60] Pokud pomineme společnosti, které paralelně nabízejí i API přístup k data setům, jsou zde i společnosti zaměřující se na data sety a veškeré náklady jsou směřovány právě na data mining. Jedna z takových společností je Webz.io, která nabízí i aktuální data sety i zdarma[61].

4.3 Operační systémy a webové stránky pro OSINT nástroje

Vzhledem k rozmanitosti veřejně dostupných dat, vznikají stejně tak rychle i různé primitivní, ale efektivní nástroje pro OSINT. Logicky se tady nabízí snaha kumulovat ty nejefektivnější nástroje vně OS, jako operační místo pro komplexní dobývání dat, a to včetně jejich analýz. Tyto OS jsou obvykle založeny na Linux jádru. Ty historicky nejpopulárnější a s původní originální myšlenkou, které jsou zároveň nejvíce využívané bezpečnostní komunitou jsou uvedený níže. Stejně tak jako OS, vznikají i různé digitální manuály či souhrny webových nástrojů v rámci webového rozhraní s odkazy na weby či jednotlivé nástroje.

OSINT Operační systémy

OS Kali

I když se jedná o OS distribuci Linuxu především pro penetrační testování ICT a SW, jedná se taky o ideální operační prostředí pro OSINT a analýzu dat.

[60] Maltego.com [online]. [cit.25.2.2022]. Dostupné z: https://www.maltego.com/product-features/
[61] Webz.io [online]. [cit.25.2.2022]. Dostupné z: https://webz.io/data-apis/archived-web-data

Distribuce je dostupná, včetně všech informací na webovém portálu společnosti OffSec Services www.kali.org, která OS vyvinula. OS obsahuje velmi velké množství především open source nástroje nebo SW pro komunitní užití bez poplatků z každé oblasti kybernetické bezpečnosti a analýzy dat.[62] Náhled OS obr. č. 5.

Obr. č. 5 – Náhled OS Kali a vybraných OSINT nástrojů, zdroj: archiv autora

OS Buscador

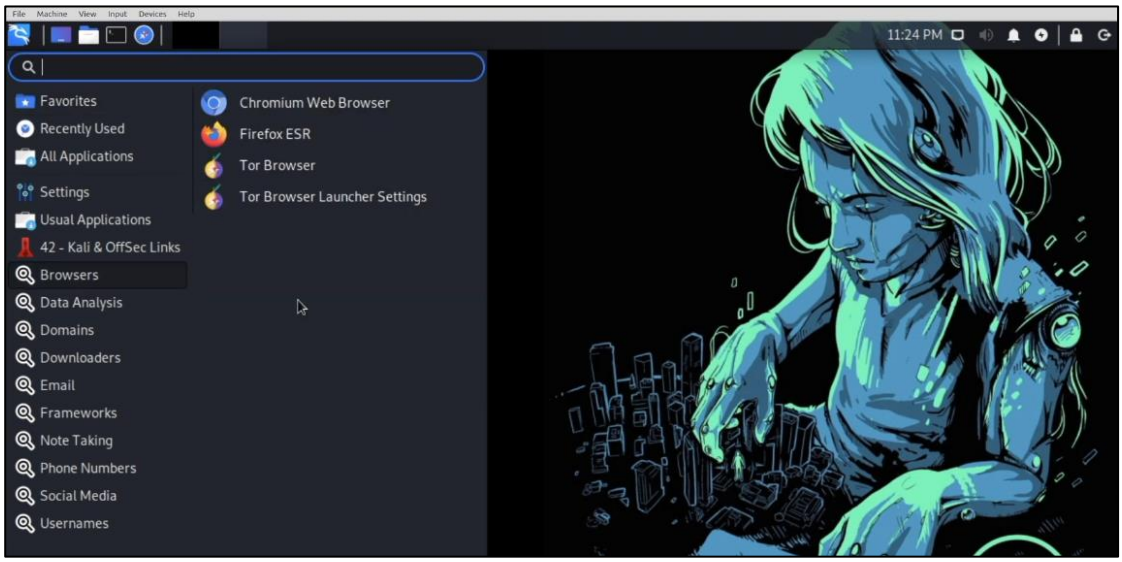
Operační systém Buscador, byl OS s Linuxovým jádrem distribuován OSINT expertem Michael Bazzelem skrze webový portál www.inteltechniques.com, jakož to OS s předinstalovaným SW pro OSINT práci v expertní rovině. OS Není nadále aktualizován, a proto byly z bezpečnostních důvodů ze zdroje odstraněny odkazy pro stažení. Nicméně i když ve své podstatě obsahuje zcela identické nástroje jako v neustále aktualizovaném OS Kali, je zcela namístě zaslouženě tento OS zmínit po boku již zmíněných OS. I když není dostupný přímo u zdroje tak je stále k dispozici v hybridních verzích v OSINT darknet komunitě.[63] Náhled OS obr. č. 6.

[62] Kali.org [online]. [cit.25.2.2022]. Dostupné z: https://www.kali.org/features/
[63] Null-byte.wonderhowto.com [online]. [cit.25.2.2022]. Dostupné z: https://null-byte.wonderhowto.com/how-to/use-buscador-osint-vm-for-conducting-online-investigations-0186611/

Obr. č. 6 – Náhled OS Buscador a vybraných OSINT nástrojů, zdroj: archiv autora

Trace Labs OSINT VM

Jedná se o v kontextu s ostatními OS velmi mladou distribuci OS pro OSINT práci, i když je primárně zaměřen na penetrační testování v oblasti bezpečnosti ICT stejně tak jako distribuce OS Kali, ale obsahuje i velmi kvalitní operační prostředí pro OSINT práci včetně analýzy dat. Distribuci je možné stáhnout na webovém portálu společnosti www.tracelabs.org.[64] Náhled OS s předinstalovanými nástroji a definování oblastí nástrojů jako obr. č. 7.



Obr. č. 7 – Náhled OS Trace Labs OSINT VM s oblastí nástrojů, zdroj: archiv autora

[64] Tracelabs.org [online]. [cit.25.2.2022]. Dostupné z: https://www.tracelabs.org/initiatives/osint-vm

Webové stránky pro OSINT

Krom výše uvedených SW a známých postupů je dobré sledovat vývoj nových metod, které se obvykle objevují jako různé formy publikací, které shrnují například webové odkazy s popisy funkcí, nebo webové rozhraní které komplexně obsahuje kompilaci nástrojů a metod dle objektu zájmu v interaktivní formě. V této formě se objevuje například web www.osintframework.com.[65] Nevýhoda takovýchto služeb je v bezpečnostním riziku. Dle premisy nikdo nic nedělá zadarmo, i zde lze předpokládat, že tyto weby a weby na které se odkazují sbírají nejen telemetrii ICT ze kterých je veden dotaz, ale data k dotazu samotnému. Z těchto důvodů je nutností mít o takových to stránkách všeobecný přehled a paralelně sledovat i OSINT komunitu a jejich názory ohledně těchto nástrojů.

4.4 Komparace metod automatizovaného a manuálního sběru dat

Abychom dokázali komparovat silné a slabé stránky automatizovaného sběru dat, který rovněž zahrnuje post-procesing sebraných dat a manuálního sběru dat musíme si nejdříve připomenou jejich potenciály a možné hrozby.

Pokud si vybavíme kauzu „Cambridge Analytica“ ve spojení s „data mining“ SW „Palantir“, kde došlo k revolučnímu nápadu využití zmíněného SW ke „kolektování“ dat 50 mil. Američanů s následnou analýzou u společnosti Cambridge Analytica, díky které věděl přesně, co má nynější prezident říct, aby získal zmíněných 50 mil. potenciálních voličů v roce 2016. Po této manipulaci byl hnán k zodpovědnosti právě zakladatel a majitel FB Mark Zuckerberg, protože dovolil uživatelům až příliš exponovat svá osobní data na jeho sociální síti.[66] Od roku 2016 prochází FB neustálými změnami tak, aby společnostem jako Palantir, Cognyte, Hyperis apod., byla co nejvíce ztížena práce s těmito daty. Nejen soukromé společnosti, ale i vlády se postavili zneužívaní exponovaných dat uživatelů, a to nejen v oblasti sociálních sítí, ale v obecné rovině sdílených dat

[65] GitHub.com [online]. [cit.25.2.2022]. Dostupné z: https://github.com/lockfale/osint-framework
[66] Cnbc.com [online]. [cit.25.2.2022]. Dostupné z: https://www.cnbc.com/2018/03/27/palantir-worked-with-cambridge-analytica-on-the-facebook-data-whistleblower.html

mezi společnostmi. Jako nástroj pro regulaci byl v EU roku 2016 použit GDPR[67] a v USA roku 2020 Kalifornský CCPA.[68] Již toto opatření má za následek stižené vyhledávání za pomoci OSINT metod u obou forem kolektování dat, ale u té automatizované je to ve větším poměru, protože SW s tak sofistikovaným zdrojovým kódem nelze adaptovat tak lehce, jak v rovině manuálního sběru dat. U takové změny je třeba velkého týmu programátorů a času.

V roce 2018 se majitel FB nyní Mety Mark Zuckerberg zavázal k aktivnímu boji proti falešným účtům za využití nejmodernějších technologií jako je AI se strojovým učením a k zřízení divize, která budu tento nástroj aktivně užívat a vylepšovat k lokalizaci a následnému mazání těchto účtů.[69] Tento krok zasáhl obě formy sběru dat, ale opět citelněji automatizované SW, které využívají své krycí profily rytmicky a opakovaně stejným způsobem, kdy AI lehce tyto profily dokáže identifikovat. U manuálního sběru dat je činnost mnohem důmyslnější a lépe krycí profil spravován.

Dalším problémem automatizovaného sběru dat v obecné rovině je příliš velké zaměření na jednu sociální síť a to Facebook. Dnes můžeme s naprostou přesností na základě statistických dat říct, že sociální sítě jsou užívány na základě věku v kontextu s obsahem. Což znamená, že se společnost dělí na užívaní sociálních sítí dle věku. Například u Facebooku je to ve věkové kategorii od 25 roku dále a u Instagramu je to do 25 let. Nemluvě o sociálních sítích dle globálně kulturního ukazatele jako je Ruskojazyčná, Asijská a Americko-evropská uživatelská základna, která užívá lokální sociální sítě. Právě u tohoto hlediska je automatizovaný sběr z velké míry omezen a nedokáže být tak efektivní jako manuální sběr dat, který je v tomto případě velmi přesný.

Jeden z dalších stránek je i role operátora chceme-li analytika využívající tyto metody. Z jedné strany je automatizovaný sběr naprosto rychlý a na první pohled mnohem efektivnější než operátor využívající metody manuálního sběru. Jak už

[67] Zkratkou z anglických slov General Data Protection Regulation, nařízení evropského parlamentu a rady EU 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.
[68] Je anglickou zkratkou slov The California Consumer Privacy Act z roku 2018 dnes již aktualizován z roku 2020
[69] Fortune.com [online]. [cit.25.2.2022]. Dostupné z: https://fortune.com/2020/03/04/facebook-a-i-fake-accounts-disinformation/

bylo zmíněno, programy pro plně automatizované sběry dat a programy, které mají funkci post-procesingu dělají vše za analytika, nicméně analytik není schopen kontrolovat všechny procesy a případně i chybovosti. Navíc u takovéhoto operátora dochází k degradaci znalostní báze. I když je manuální sběr dat mnohem pomalejší je většinou ve výstupu mnohem více informací než z automatizovaného sběru dat. Navíc analytik manuální sběru je schopen v reálném čase reagovat na hrozby a odstraňovat závady takřka v raném čase, což u automatizovaného sběru leckdy může trvat i týdny.

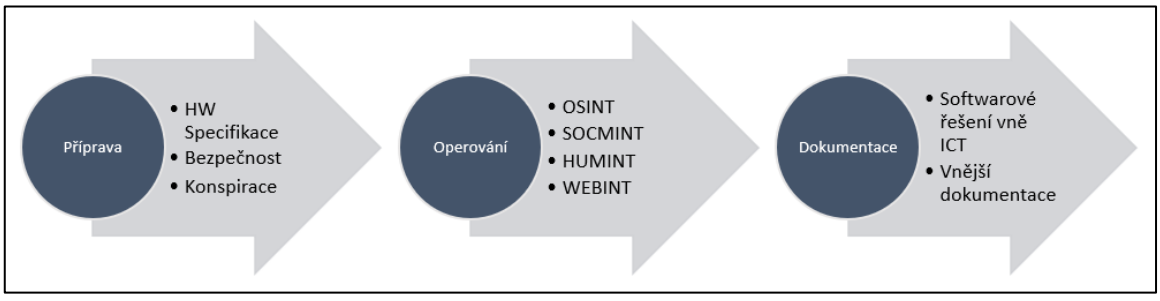
Z výše uvedené komparace je evidentní, že v případě aktivního využití OSINT metod je manuální metoda sběru dat zcela efektivnější a méně nákladná než automatizovaná. Nevýhodou je pouze rychlost zpracování dat a náročnost získání dovedností. To, ale neplatí u tzv. big data analýzách, kde automatizovaná forma sběru a vyhodnocení dat za využití AI a strojového učení je mnohem efektivnější.

5 Využití OSINT a SOCMINT metod v rámci kriminální policie

V počátcích informačního věku byla data teprve na vzestupu a nasycenost relevantními daty pro kriminální policii byla irelevantní a nedostatečná. Zprvu zde fungovali jen komunitní fóra, řekněme předchůdce reálných sociálních sítí a fragmenty denních informací. Skutečný rozvoj digitálních dat přišel až se sociálními sítěmi, které způsobili opravdový rozmach ve sdílení osobních dat. Na zcela nový fenomén virtuálních platforem internetu se začali v pozdějších letech adaptovat i policisté, kteří předchozí užívání OSINT metod měli spojené pouze s denním tiskem a dalšími medií jako je televize a rádio vysílání. V dnešní době je OSINT jeden z největších zdrojů informací na planetě a získávání těchto dat se stává čím dál sofistikovanější. Jak už bylo v předchozích kapitolách uvedeno, každá zmíněná metoda potřebuje určitou přípravu, a to nejen pro efektivní sběr dat s následnou analýzou, ale taky pro svou ochranu. Každá zdrojová oblast dat má svoje určitá specifika, a to nejen pro fázi přípravy a možného provedení, ale i z bezpečnostního hlediska.

5.1 Působení v prostředí internetu

Pro působení vně internetu jsou určitá profesní pravidla, která zahrnují nejen bezpečnost, ale i odborná specifika pro zacházení se získanými daty. Celý proces přípravy lze charakterizovat do tří fází, viz. obr. č. 8.



Obr. č. 8 – Fáze působení v internetu, zdroj: archiv autora

Fáze první – Příprava

Jedna z nejzákladnějších zásad je HW, bez kterého není možné bezpečně a systematicky působit v internetu. Pro efektivní a bezpečnou práci je třeba na HW naistalovat mnoho SW ať už virtualizující OS tak i zabezpečující záznam dat či

jejich možnou analýzu. V těchto případech ICT hovoříme vždy o dostatečném procesorovém výkonu ve formě počtu jader, které potřebujeme pro virtualizaci[70]. Stejně tak jako RAM paměti potřebujeme rovněž dostatečně prostorná úložiště. V souhrnu vše závisí na plánu a prostředí cílových dat.

Virtualizace je jedna z nejzákladnějších nástrojů, kdy za pomocí SW vytvoříme jakýkoliv jiný OS v ně stávajícího, tak aby procesy ve virtualizovaném OS nezasahovali a byly separátní od hlavního OS. Pokud například je vaším cílem zkoumání funkčnosti a možných dat z ramsonware[71], je možné jej spustit v takovém to prostředí, bez újmy na hlavním OS, pod kterým tento proces běží. Stejně tak lze toto pravidlo aplikovat na jakékoliv jiné práci vně internetu, kdy při extrakci surových dat chráníte HW a hlavní OS, zároveň se vám ponechává možnost průzkumu metadat.

Mezi klíčové bezpečnostní opatření je konspirace IP[72] adresy internetového připojení. Za využití Virtual Private Network dále jen „VPN“, Proxy či jiného ekvivalentu anonymizačních služeb jako je TOR apod.

Sock puppet, není nic jiného než předem vytvořený krycí profil, s jehož účelem je konspirace pronikání do zájmového prostředí. Jeden z účelů je bezpečnostní. V celé řadě sociálních sítí k efektivnímu vytěžování je potřeba mít založený účet. V rámci bezpečnosti, aby byla zaručena profesionální stránka celého pronikání do zájmových prostředí a s cílem získávání informací je nutný takovýto profil, protože využívání vlastního účtu na sociálních sítích nebo krycího profilu na vlastním ICT, kde jsou soukromé účty užívány, vede k dekonspiraci, a navíc díky propojovacím algoritmům i exponování totožnosti operátora. Krycí profil je možné připravit dle potřeb, a to pro obecnou OSINT a SOCMINT aplikaci, nebo pro cílené potřeby s konkrétním cílem. V případě konkrétních potřeb se profily obvykle připraví pro nejpravděpodobněji úspěšnou interakci nebo proniknutí. V zásadě se jedná o vytvoření krycího profilu, aby pro administrátora vnitřních skupin nebyl podezřelý a prošel, popřípadě ověřováním bez sebemenšího podezření. Nejedná se zde jen

[70] Virtualizace, je proces vytvoření jiného prostoru se stejným využití zdroje, např. Další OS ve stejném ICT.
[71] Druh škodlivého SW, který obvykle znepřístupní obsah nebo zamezí užívaní ICT s cílem vydírat majitele.
[72] Zkratka z anglického jazyka Internet Protocol

o nezdar, ale i o možné upoutání negativní pozornosti. Profily k interakci jsou profily vytvořeny jen za jedním účelem a jen pro daný úkol a obvykle před samotným vytvořením takovéhoto profilu, probíhá již OSINT a SOCMINT šetření, jehož výstup je nejideálnější profil pro interakci.[73]

Tvorba profilů obsahuje několik specifikací, mezi ty nejsložitější spadají důvěryhodnost a historie. Rovněž je zde hrozba ze strany provozovatele sociální sítě, který je něco jako hlídač vstupní brány jeho platformy. Zde dochází jen k základní kontrole, zda nesplňuje kumulativně několik znaků krycího účtu, obvykle se z této fáze ověřování lze dostat pouhým 2FA[74] ověřováním díky tel. číslům, protože algoritmus většiny sociálních sítí bere přidání tel. čísla do profilu jako splnění jedné z podmínek kompletního profilu, čímž se stává důvěryhodným a zkoumány jsou jen profily pod 60% důvěryhodnosti. Jako další krok je grafický obsah ve formě profilové fotografie, nebo grafiky tzv. avatara[75], dále doplnění maličkostí z cílových skupin jako jsou zájmy, koníčky apod. U grafického materiálu pro krycí profil, zde operátor stojí před morálníma zásadami. Jednou z nich je profilová fotka a fotografický obsah ve formě fotografií z dovolené či podobných věcí zvyšující důvěru profilu. Vzhledem k využívání krycího profilu na sociální síti, kde platí všeobecně přijatá norma společnosti, že profil na sociální síti zastupuje danou personu ve virtuálním světě, a to i za cenu reakce na vlastní reakce či prezentování názorů, je zcela vyloučeno užívání jako profilové fotografie nebo fotografií jakýchkoliv osob z virtuálního prostředí internetu bez jejich svolení. Je celá řada nástrojů, jak vytvořit a upravit profilové fotografie, aby nedošlo k zneužití něčí podoby. Stejně tak jako údaje v profilu, kde opět platí pravidlo, že operátor bez povolení nevytváří na cizí osobu účet na sociálních sítí s cílem tento profil užívat pro výše uvedená šetření. Switch agent je působivá utilita, která upraví telemetrii prohlížeče a ICT připojovaného na webové stránky.

U některých úkolů může být vytvořena i virtuální platební karta bez nutnosti reálných identifikačních údajů, která slouží k pronikání za tzv. pay wall,[76] kam se

[73] BAZZELL, M. Hiding from the Internet. 3rd ed. USA, 2016. ISBN 978-1522914907.
[74] 2FA z anglického slova Two-factor authentication, volně přeloženo jako dvoufázové ověřování.
[75] Avatar, výraz pro profilový obrázek bez vlastní fotografie zastoupenou formou jakékoliv individuální grafiky.
[76] Pay wall, volně přeloženo jako platební zeď, je výraz pro dostupnost obsahu jen v rámci placeného členství nebo individuální platby.

v dnešní době ukrývají informace, které balancují na hraně zákona a často se tak jedná o kvalitní zdroj informací z prostředí.

Fáze druhá – Operování

Po první fázi přípravy přichází na řadu fáze druhá, a to je samotné operování ve virtuálním prostorou internetu v rámci OSINT a SOCMINT šetření. Jak už bylo zmíněno v předchozích kapitolách existuje výraz aktivní a pasivní OSINT, analogicky lze aplikovat i na SOCMINT. Zda operátor ve formě aktivního sběru dat sbírá data k nějakému cíli či pasivně zda operátor sbírá data plošně pro vytvoření statistiky či mapy hrozeb. U Aktivního OSINTU lze metody dělit ještě na obecné místo působení a dalších metod využívaných v rámci OSINT metod jako je WEBINT či IMINT.

Fáze třetí – Dokumentace dat

Jak už bylo zmíněno v kapitole o zpravodajském cyklu, každý sběr dat se upravuje pro vklad do databází nebo jiné informačního depotu, ze kterého je na základě analýz tvořen výstup. Při sběru dat, v rámci OSINT a SOCMINT metodách, je několik metod, jak zajistit data. Buď formou kopie, což je zachycení dat za pomocí vnitřních procesů ICT jako je SW na zachycení obrazovky. Konkrétně se může jednat i o tzv. addon[77] prohlížeč, který dokáže zachytit celou grafickou podobu webu ve formě jedné fotografie, mezi komunitou uznávané nástroje bezpochyby patří Fire Shot[78] a Nimbus[79]. Dále SW instalovaných vně OS ať už Linux či Windows, který zachycuje výřezy aktuálního grafického objektu obrazovky nebo grafický obsah zachycuje do video podoby. Všestranný a bezpečnostní komunitou uznávaný SW OBS Studio. V případě prostých dat se pořizují kopie souborů, které se analyzují za dodržení prostředí, které si operátor připravil v první fázi.

5.1.1 Vyhledávací a monitorovací činnost

Mezi jednou ze základních činností v této kategorii je vyhledávací a monitorovací činnost. V rámci vyhledávání se jedná o aktivní působení v internetu

[77] Výraz, pro volitelný externí SW modul pro prohlížeč.
[78] Getfireshot.com [online]. [cit.25.2.2022]. Dostupné z: https://getfireshot.com/
[79] Nimbusweb.me [online]. [cit.25.2.2022]. Dostupné z: https://nimbusweb.me/screenshot.php

vyhledáváním ilegálního obsahu v internetu na všech úrovních a dle specifikací problematiky. Tyto iniciativní aktivity nelze aplikovat u každé kriminální problematiky pouze u kterých je evidentní latence trestního jednání. V tomto případě se jedná obvykle o trestné činy spojené s nabídkou či poptávkou ilegálních služeb nebo zboží. Převážně se tak jedná o nabídky OPL a ilegálních virtuálních služeb, jako jsou služby z portfolia hackingu nebo digitálního zboží ve formě grafického obsahu v oblasti pedofile nebo porušování autorských práv apod. V rámci takových to aktivit je možné se zaměřit na kritické oblasti, které se monitorují pasivním způsobem nebo je aktivně vyhledávat za využití OSINT metod. Monitorování může být dlouhodobé, jehož účelem je pochopení „modusu operandi“ [80] trestní činnosti nebo mapování konektivity mezi objekty zájmu. Současně může být prováděna i záloha obsahu, ať manuálně či pomocí SW řešení s následným vyhodnocením, jehož výstup může vést k dalšímu místu monitorovaní. Praktická ukázka typického vyhledávání a následného monitorování objektu zájmu je uvedená v kapitole 6.3., s názvem „Sociální síť a virtuální tržiště s ilegálním obsahem v DarkNet síti“.

5.1.2 Infiltrace zájmového prostředí a HUMINT

Infiltrace zájmového virtuálního prostředí v internetu je velmi problematický proces, protože mimo standartních bezpečnostních postupů je nutné ještě vytvořit cílený krycí profil na základě již sesbíraných dat k objektu zájmu, tak aby infiltrace byla nejen možná, ale i co nejvíce pravděpodobná. U takových to operací se běžně stává, že se povede na několikátý pokus a veškerá práce při vytváření krycích profilu vyjde nazbyt, protože jsou nadále takto vytvořené profily nepoužitelné pro stejný účel. V případě úspěšné infiltrace se v další fázi tohoto procesu objevuje psychologická stránka. Krycí profil není jen kompilace grafického obsahu a smyšlených údajů, ale taky osoba, která musí být připravena k interakci v infiltrovaném prostředí. V téhle fázi to vypadá, že do celého procesu vstupuje psychologie, ale není tomu tak. Psychologie do tohoto procesu vstupuje už ve fázi přípravy krycího profilu, protože už napřed definuje oblast a možnosti interakce

[80] Modus operandi je latinský výraz užívaný v kriminalistice jako styl nebo postup charakterizující individuálnost pachatele.

s možnými zájmovými objektem v infiltrovaném prostředí. Samozřejmě velkou roli hraje účel takového to působení, zda se jedná jen infiltrace za účelem pasivního monitoringu, nebo zda je účelem aktivita ve směru podpory TŘ, nebo aktivního vyhledávání. V tomto procesu je třeba rovněž neustále zhodnocovat hrozby a příležitosti, protože každý krok může dekonspirovat nejen samotný profil, ale samotnou operaci.

5.2 Podpůrná činnost v prověřování TŘ

I když platí stejná pravidla jako v kapitole 5.1. o působení v internetu, zde se jedná spíše o podpůrnou činnost, jako dokládání materiálu pro procesní úkony v rámci trestního řízení, jako je například propojování strategických osob věcí a míst nebo jako důkaz o situaci. Současně pokud to podstata TŘ umožňuje, nebo objekty zájmu jsou v prostředí internetu aktivní, může sběr z virtuálního pestření jako důležitá data pro dozorujícího státního zástupce nebo soudce k povolení úkonů dle trestního řádu.

5.2.1 Screening před a při realizaci operativně pátracích prostředků

Jak už bylo zmíněno OSINT a SOCMINT, může být základním kamenem operativně pátrací činnosti v samotném počátku trestního řízení. Pokud je objekt zájmu aktivní ve virtuálním prostředí internetu a splňuje předpoklady, jako zdroj informací, je možné získat velké množství dat. Z pohledu kriminálních analýz se ve své podstatě jedná o sběr veřejných dat k objektům zájmu, jako je konektivita k jiným objektům zájmu ve vztahu k profilům na různých sociálních sítích nebo osobní aktivita na internetu jako jsou inzeráty, veřejné komentáře reflektující názory, recenze hotelů a navštěvovaných gastronomických míst, zveřejňovaní fotografií apod. Tyto data mohou pomoct zmapovat nejen okolí subjektu zájmu a připravit podpůrné podklady pro povolení úkonů nasazovaných v rámci trestního řízení, ale i vykreslit osobnost objektu zájmu pro případné návrhy a realizaci operativně pátracích prostředků, která jsou uvedená v §158b/1 zák. č. 141/1961 Sb., trestní řád, jako je sledování, předstírané převody, či nasazení agenta.

V případě sledování osob a věcí je žádoucí OSINT a SOCMINT prověrka, kdy tyto data mohou poskytnout předpokládaný pohyb objektu či míru problematičnosti jeho sledování. Nebo zájmová místa subjektu v okolí jeho pohybu, v případě ztráty kontaktu může být opět navázán právě na jedné z oblíbených destinací z OSINT prověrky.

U nasazení agenta či předstíraného převodu mohou informace doplnit bezpečnostní hledisko, kdy například v evidencích není objekt majitelem zbrojního průkazu či střelné zbraně, ale na sociálních sítích je focena anebo natáčen při střelbách. Může se jednat i o sportovní aktivity, jako je třeba zveřejňování fotografie z různých tréninku nebo výcviku v rámci bojových aktivit. Stejně tak, jako uvedená data, mohou identifikovat možné hrozby ze strany objektu zájmu, mohou pomoct i vykreslit osobnost subjektu či zájmová místa pro případný kontakt, jako oblíbená místa ve formách barů, heren, hotelů či holičství. Výše uvedená data jsou v praxi velmi důležitá a v mnoha případech se k takovým to datům jiným způsobem nelze dostat.

5.2.2 Monitoring zájmových objektů a prostředí v prověřování TŘ

V předchozí kapitole se jednalo o shromažďování dat v první fázi trestního řízení, v rámci mapování okolí zájmových subjektů či přípravy na operativně pátrací prostředky. Za předpokladu nalezení dat k objektům zájmu v první fázi je důležité monitorování těchto subjektů a změn, která provádí ať už na sociálních sítích nebo vně internetu formou inzerce a je velmi důležitá pro sledování vývoje operativně pátrací činnosti. V dnešní době šifrovaných standartu se velmi často stávají sociální sítě jediné místo, které umožňuje monitorování činnosti objektů zájmu. V některých případech může být i monitorování pohybu a činnosti v zahraniční, které opět napomáhají v rozhodování o nasazení či usnadnění povolení operativně pátracích prostředků. Stejně tak se může jednat například o monitorování virtuálního prostředí, jako jsou různá fóra poskytující relevantní informace pro trestní řízení nebo virtuální platformy s prodejem ilegálního zboží, kde se může sledovat změna nabídek či monitorování aktivit pseudonymu pro účely trestní řízení. Taková činnost je dlouhodobá a dokumentuje se v případě nálezu zájmové informace, která se přikládá spolu s úředním záznamem ke

spisovému materiálu. Některá data jsou shromažďována za účelem dalších analýz, jehož cílem je souhrnná aktivita v rámci tohoto prostředí.

6 Kazuistika využití OSINT a SOCMINT metod

V této kapitole bude zvýrazněna aplikace teorie z výše uvedených kapitol do praktických scénářů v rámci kazuistiky, které byly realizovány v posledních třech letech. Zejména se pak jedná o kazuistiku FBI, v rámci využití OSINT metod v rámci trasování BTC a SOMINT metod na objekty zájmu vně sociálních sítí. Jako další kazuistika bude aplikovaný WEBINT a OSINT, díky kterému bylo možné zmapovat kompletní síť webových domén se záměrem podvodů. Jako poslední kazuistika se věnuje OSINT, SOCMINT a WEBINT metodám z oblasti darknet sítí, a to konkrétně TOR sítě, ze které bylo možné ztotožnit pachatele včetně místa působení.

6.1 Odhalení a dopadení organizované skupiny nigerijských podvodů

Tato kazuistika poukazuje na důležité využití OSINT metod v oblasti blockchainu, který byl klíčoví ke ztotožnění pachatele v roli organizátora a využití SOCMINT nebo IMINIT metod ke ztotožnění místa, kde se pachatel nachází.

Tak jak se rozšiřoval internet do celého světa, tak i zločinecké struktury se začaly adaptovat na nové pole působnosti. Nejrozšířenější podvody za využití internetu skrze e-mailových služeb známe taky jako „Yahoo Boys“[81] nebo „Scam 419“[82], je sada triků využívající sociálního inženýrství, kdy si útočník vyhlídne svoji oběť za účelem vylákání finanční částky, a to pouze s digitálním kontaktem za využití konspirace.

V roce 2019 došlo k finančním podvodům skrze internet. Obětí se stali dvě společnosti se sídlem v Chicagu, USA. Jedna byla podvedena celkem o 2,3 mil. USD a druhá o 15,3 milionu USD. Podvody spočívali v důmyslném schématu e-mailů a sociálního inženýringu. Útočník získal e-maily velkých společností ze starých uniklých databází a následně za využití OSINT metod si provedli screening těchto společností, jehož cílem bylo získat co nejvíce informací o položkách, které nakupovali a jaké bankovní toky k tomu požívali. Následně si útočník založil e-mailové účty s podobným názvy, jako byly adresáti poškozených, a to včetně

[81] Název slupiny podvodníků, je dle společnosti americké Yahoo, která poskytuje e-mail účet bez poplatku.
[82] Mezinárodní výraz pro tzv. „Nigerijské podvody“.

bankovních účtů se stejnými názvy jako společnosti, a to za využití lokálních kompliců. Poté byly oběti kontaktovány ve stejném smyslu, jako v minulých případech obchodního jednání. Oběti bez sebemenšího tušení posílali peníze na obdržené platební informace, které se jevili jako bankovní účty společností, s kterými dlouhodobě obchodují. Pachatelé následně za obdrženou FIAT měnu[83] pořídili virtuální měnu Bitcoin dále jen „BTC“[84], kterou odeslali na adresu hlavního pachatele. Ten BTC opět směnil na FIAT měnu v USD, které se však už tvářili jako výnos z obchodování s virtuální měnou. Tyto transakce byly prováděni v rámci směnárenské platformy LocalBitcoin.

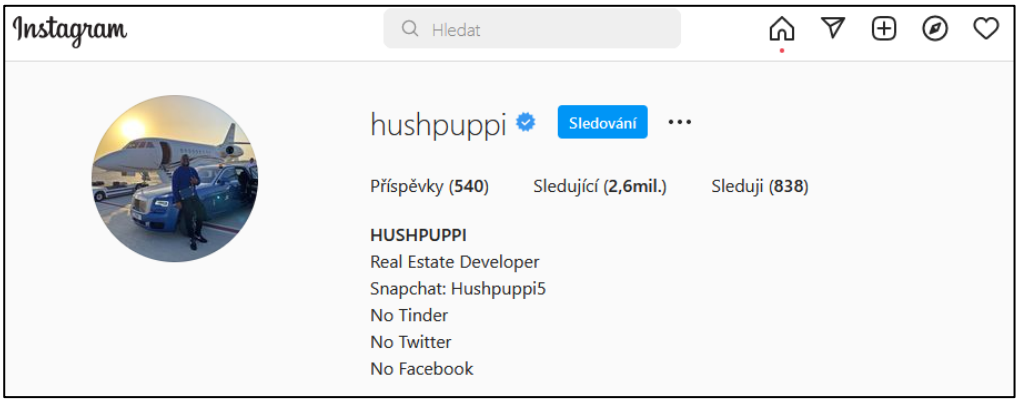
Případu se chopila FBI, která měla výhodu v podobě domácího území, na kterém se nacházeli společnosti, které pachatel využil pro podvody. Po analýze získaných dat a zmapovaných e-mailových účtů bylo zjištěno, že bankovní účty v USA byly založeny osobami, které byly kontaktováni osobu užívající pseudonym Mark Kain. Dle majitelů zmíněných bankovních podvodných účtů Mark Kain jim zaplatil, aby po připsání, nakoupili BTC a následně mu jej poslal na konkrétní BTC adresu.

Po získání těchto informací a provedené blockchain, analýza ukázala, že skutečně došlo k nákupu a převodu 1494 BTC, které přímo souvisejí s podvodem spáchaným na společnostech v Chicagu. Konkrétně se jednalo o BTC adresu „16AtGJbaxL2kmzx4mW5ocpT2ysTWxmacWn“, která figurovala v tomto podvodu nejméně v devíti případech. Záznamy, které se podařilo FBI získat od společnosti Bitpay[85], poukázala na používaní této adresy již v letech 2015 propojených s e-mail účtem od společnosti Google „husleandbustle@gmail.com“. E-mail byl použit jako Aple ID. FBI získala od společnosti Apple data o zřízení účtu ze kterého byl zjištěn Olalekan Jacob Ponle, narozený v roce 1991 ve městě Lagosu v Nigérii.

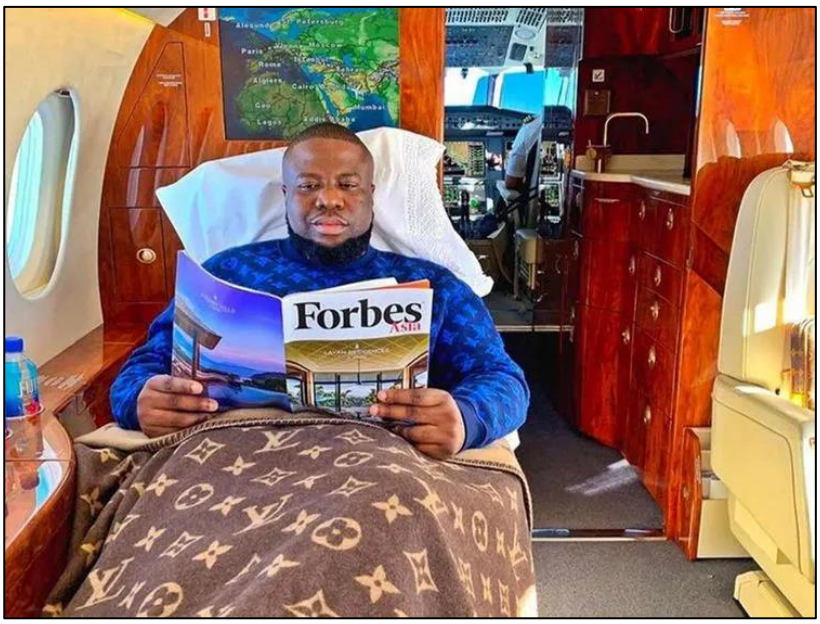
Sice FBI znala jméno pachatele, ale nevěděla, kde se Ponle v danou chvíli nachází. V tuto chvíli přichází na řadu SOCMINT a odražení veškerých údajů, které se v průběhu OSINT šetření k osobě nashromažďovali. Na základě těchto

[83] FIAT měna je výraz pro tzv. měnu s nuceným oběhem, která je vydávaná na základě zákona.
[84] Bitcoin je nejrozšířenější virtuální měna využívající jak v rámci transakcí, tak i jako investiční nástroj.
[85] Společnost provozující platební brány v oblasti oboustranné konverze FIAT na VC.

dat byly zjištěna přezdívka, pod kterou byl ve světě sociálních sítí znám jako „Mr. Woodbery“ a „Hushpuppi“ s odkazem na jeho účet sociální sítě Instagram https://www.instagram.com/hushpuppi viz. náhled profilů na sociální síti Instagram jako obr. č. 9, 10. Bezpečnostní složky byly v šoku ze sociálních sítí, kde se hlavní pachatel organizované skupiny Ponle choval jako podnikatel žijící na velmi vysoké úrovni.



Obr. č. 9 – Náhled Instagram profilu hushpuppi, zdroj: https://www.instagram.com/hushpuppi



Obr. č. 10 – Náhled fotografie životního stylu z profilu Instagramu, zdroj: https://www.instagram.com/hushpuppi

Na základě rozboru fotografií z Instagram profilu bylo zjištěno, že se tato osoba zdržuje ve Spojených Emirátech v Dubaji. Na základě tagu u fotografií bylo

zjištěno, že se jedná o hotel Palazzo Versace Dubai at Jaddaf Waterfront v Dubaji. Mimo tagu byla tato skutečnost zjištěna rozborem fotografií, kde pachatel sedí na balkonu s výhledem na město Dubai se zálivem zbožněným Google Maps, jako výhled právě z hotelu Palazzo Versace obr. č. 11.

Obr. č. 11 – Fotografie pachatele s výhledem z hotelu Palazzo Versace, zdroj: https://www.instagram.com/hushpuppi

Na dalším snímku je ukázka možné komparace fotografií, kde obrázek č. 12, pochází z Instagram účtu https://www.instagram.com/hushpuppi, na kterém jsou Ponleho vozidla, včetně značky vozidla Porsche červené barvy. Na fotografii obr. č. 13, je fotografie nalezena mezi sdílenými fotografiemi návštěvníků Dubaje, kde nezjištěná osoba vyfotila záběr od vstupu hotelu Palazzo Versace a následně tuto fotografii sdílel do veřejných sbírek Google maps k místu Palazzo Versace. Na fotografii je nejen místo, kde došlo k focení Ponleho vozidel, ale na levé straně fotografie bylo zachyceno zaparkované Ponleho červené vozidlo Porsche, před hotelem Palazzo Versace v Dubaji.

Obr. č. 12 – Fotografie pachatele jeho vozového parku, zdroj: https://www.instagram.com/hushpuppi

Obr. č. 13 – Fotografie neznámého turisty z hotelu Palazzo Versace, zdroj: https://www.google.com/travel/hotels/palazzo

Poté co FBI informovala policejní úřady v SAE, spustili saudské policejní úřady operaci se jménem Fox Hunt 2. V hotelu Palazzo Versace v Dubjai úspěšně zadrželi hlavního pachatele Ponlehho, včetně celé organizované skupiny. Saudské úřady informovali veřejnost, že v rámci domovních prohlídek bylo zajištěno 27 počítačů, 47 mobilních teflonů, 15 USB flash disků, 5 externích HDD, 13 luxusních vozidel a hotovost ve FIAT měně USD v přepočtu se jednalo o cca.

750 mil. Kč. Všechny pachatele a zajištěné věci byly předány FBI k dalšímu opatření. FBI později v tiskové zprávě uvedla, že na základě vyhodnocení bylo zjištěno celkem 1.926.400 obětí v celkové škodě 9,3 mld. Kč.[86]

I když v rámci legislativního procesu případ u soudu neobstál a Ponle byl propuštěn na svobodu[87], je zde evidentně profesionálně zpracovaná linka dat vedoucí od pseudonymu a sítě nastrčených obětních beránků až k pachateli, který byl ztotožněn skrze BTC transakce a následně díky sociálním sítím lokalizován na místě, kde rovněž došlo k jeho zadržení a zajištění důkazů.

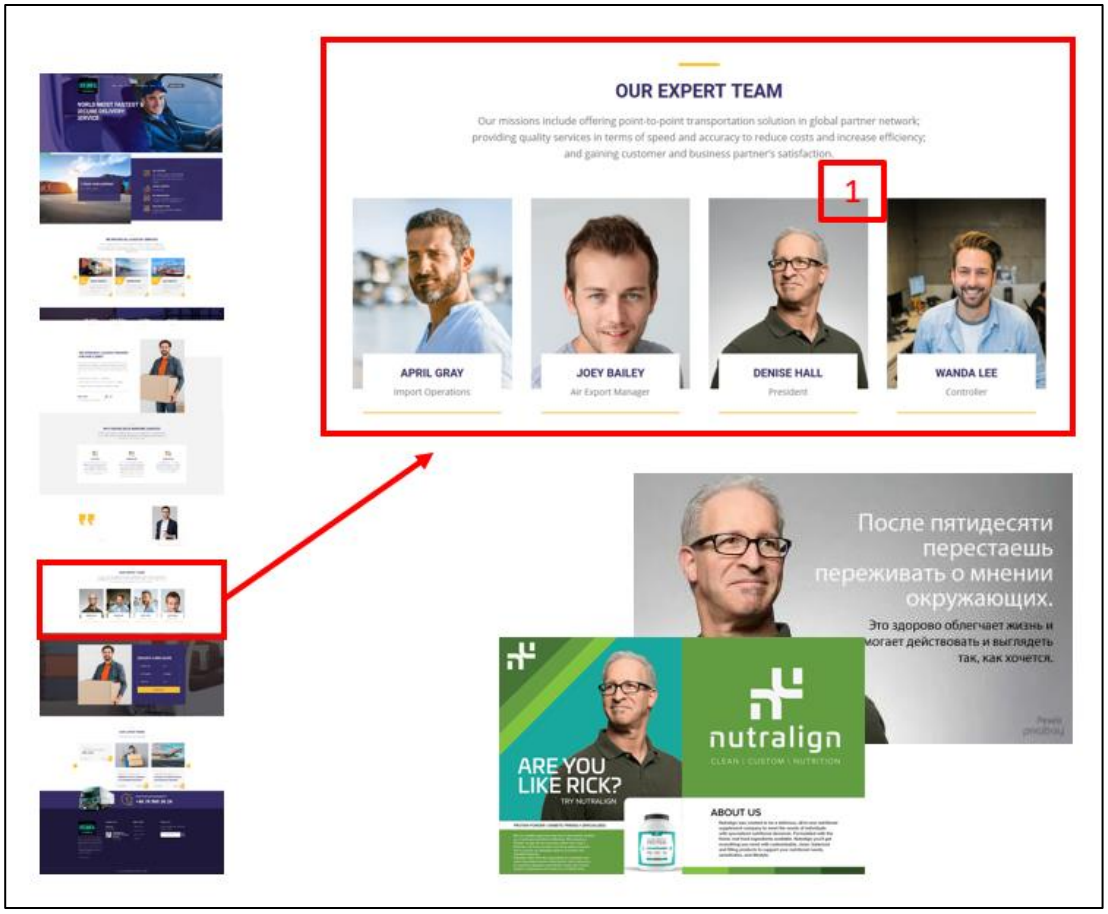
6.2 Podvody se zdravotním materiálem pro COVID-19

Tato kazuistika poukazuje na jeden z nejdůležitější metod v rámci OSINT analýz, a to je WEBINT. Na začátku byla v rámci monitorování prodeje OPL v internetu objevena podezřelá aktivita, spojující tyto aktivity s webovou stránkou spediční společností a pokročilou WEBINT metodami byla následně rozkryta síť podvodních stránek týkající zdravotního materiálu a potřeb spojené s COVID-19 situací. Na základě těchto informací byl informován Interpol, který vydal veřejné varování.

V roce 2020 bylo při monitorování zájmového prostředí internetu s nabídkami OPL zjištěna podezřelá aktivita pseudonymu, jež nabízel širokou NPS včetně těch, která jsou i na seznamu přílohy Nařízení vlády č. 463/2013 Sb. V rámci OSINT šetření bylo zjištěno několik zkušeností s tímto pseudonymem, kdy většina z těchto reakcí na sociálních sítích byla negativního rázu. Při komunikaci bylo evidentní, že se nejedná o prodej OPL, ale cílem je vylákání finančních prostředků skrze BTC finančních transakcí. Osoba využívající pseudonym v komunikaci popisovala odeslání látek, skrze dnes již neexistující společnost a webové stránky, www.deltamaritimelogistics.com.

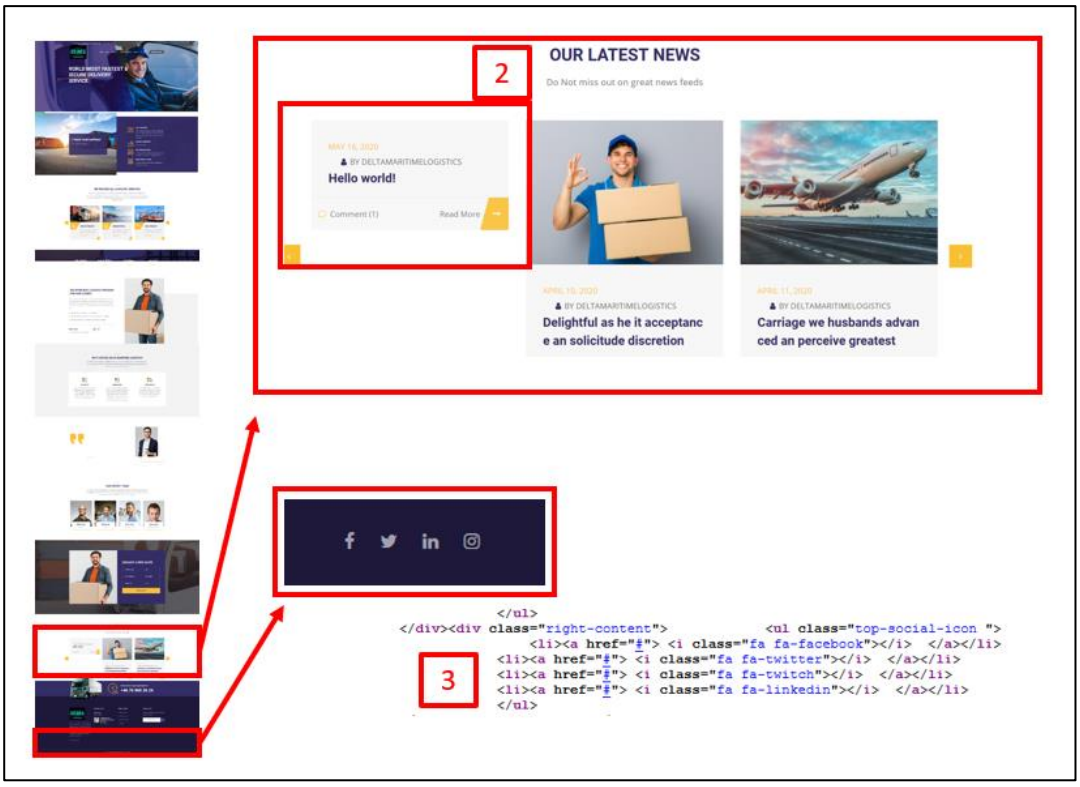
[86] Securityboulevard.com [online]. [cit.25.2.2022]. Dostupné z: https://securityboulevard.com/2020/07/hushpuppi-and-mr-woodbery-bec-scammers-welcome-to-chicago/
[87] Justice.gov: U.S. Department of Justice [online]. [cit.25.2.2022]. Dostupné z: https://www.justice.gov/usao-ndil/press-release/file/1292061/download

Z komunikace a recenzí vně sociálních sítí je patrné, že se jedná o důmyslný systém podvodů, spočívající ve snaze vylákat ze zájemce o omamné a psychotropní látky finanční prostředky nejen za tyto substance, ale i za poštovné a následnou zálohu za neexistující certifikát „Euro 1“. Dalším OSINT a WEBINT šetřením ke spediční společnosti, která požadovala dle referencí uhradit poplatky byly zjištěny data, které poukazují na nastrčenou webovou stránku tvářící se jako mezinárodní spediční společnost.



Obr. č. 14 – Náhled na webové stránky v části „Our expert team“ - nález bod 1, zdroj: archiv autora

Na webových stránkách v části věnované záložce „Our expert team“ jsou všechny fotografie zaměstnanců převzaty z internetu, jak lze vidět u bodu 1, obr. č. 14, kde osoba pojmenovaná jako Denise Hall vystupuje jako prezident společnosti. Stejnou osobu lze nalézt i na reklamních letácích či prezentacích, stejně tak jako všechny osoby z této sekce webové stránky.



Obr. č. 15 – Náhled na webové stránky v části „Our latest news“ a sociální sítě – nález bod 2 a 3, zdroj: archiv autora

Na webových stránkách v části věnované záložce Our latest news“ s označením bodu 2 je defaultně nastaveno pole pro komentáře, kdy bylo pravděpodobně v šabloně webové stránky nedopatřením vynecháno pole s klientským komentářem a ponechán výraz „Hello world!“, což je při programování forma uvítací hlášky nově vzniklého modulu nebo programu. Profesionální společnost by komentáře od klientů brala velmi vážně. Stejně tak se v zápatí webové stránky nachází odkazy společnosti na sociální sítě, jak lze vidět v bodu 3 obr. č. 15, kde se nachází náhled zdrojového kódu s nedefinovanými odkazy na vlastněné sociální sítě. Opět žádná společnost by neopomněla tuto propagaci propojit s webovou stránkou.

Webové stránky jsou velmi dobře neutrálně zpracovány, a to nejen graficky, ale i zdrojovým kódem, díky kterému je možné během několika minut kompletně změnit kontaktní údaje a nahradit stávající logo DML za jiné tak, že webová stránka bude vypadat jako jiná spediční služba. Grafické a textové podklady nejsou nijak vázány k logu DML, což je velmi podezřelé. V náhledu webové stránky (příloha č. 1) lze rovněž vidět, že logo společnosti zde zcela nezapadá a stránky tak

pravděpodobně slouží pouze jako šablona pro měnící se název spediční společnosti osoby „Dr. Solino“.

Šetřením k IP adresám pocházející z komunikace Dr. Solina byl zjištěn server Google provozovatele e-mail klienta Gmail, u komunikace se spediční společností www.deltamaritimelogistics.com z emailové adresy info@deltamaritimelogistics.com byla zjištěna IP adresa 199.188.200.216, což poukazuje na server server267-1.web-hosting.com společnosti Namecheap, Inc. s místem hostingu Chicago, USA.

Dalším šetřením k webové doméně http://www.deltamaritimelogistics.com bylo zjištěno, že je registrována společností WhoisGuard, Inc., sídlící v Panamě s P.O. Box 0823-03411 se službou anonymity majitele domény. V rámci dalšího šetření byl zjištěn NS domény dns2.namecheaphosting.com a dns1.namecheaphosting.com, čímž bylo zjištěno, že hosting webových stránek je provozován stejnou společností jako její MX protokol, a to společnosti Namecheap, Inc. AS22612 s místem hostingu Chicago, USA s IP adresou stránek 199.188.200.254, která má nastaveno SPF[88], na již výše zmíněnou IP adresu pocházející z hlavičky e-mailu 199.188.200.216. Rovněž byla zjištěna historie NS viz. tabulka č. 4.

Datum od prvního záznamu	IP adresa	Webová stránka hostujícího
13.9.2015	66.96.147.105	https://www.ipage.com/
14.6.2016	68.65.122.213	https://www.ipage.com/
26.7.2016	8.5.1.34	https://www.enom.com/
5.8.2020	199.188.200.254	https://www.namecheap.com/

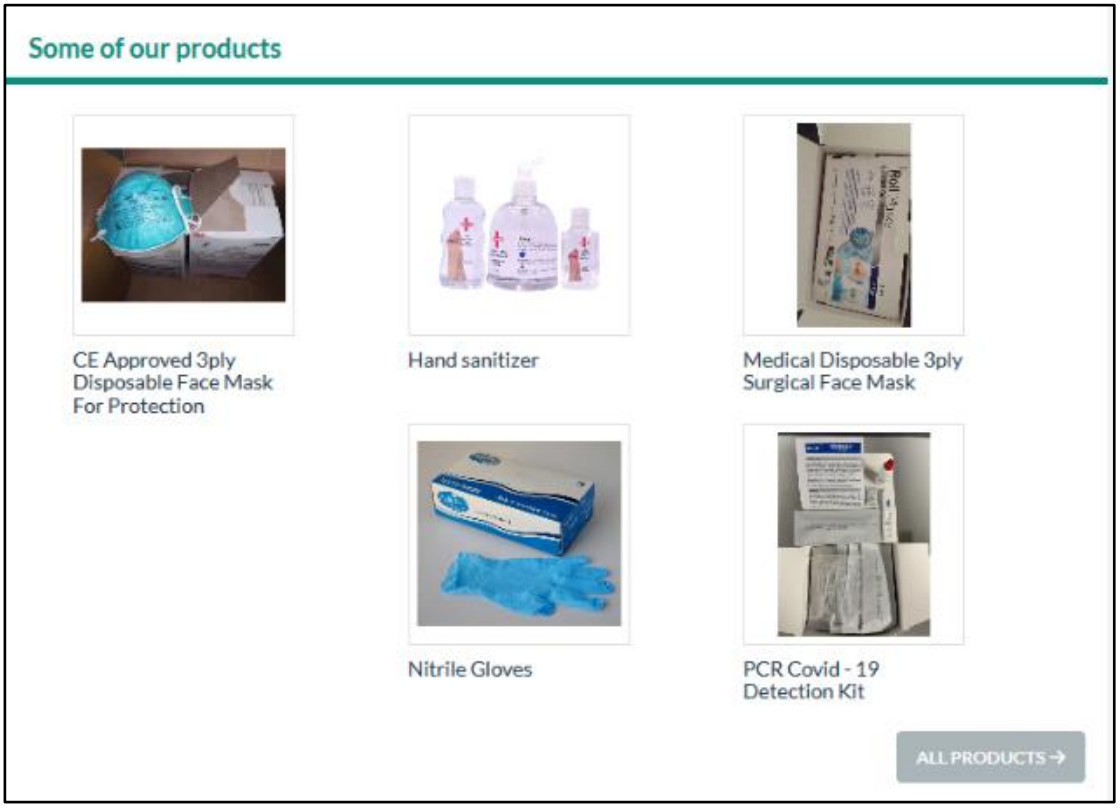
Tabulka č. 4 – Historie NS hostingu http://www.deltamaritimelogistics.com

Na základě výše uvedených informací bylo provedeno OSINT šetření, ze kterého bylo zjištěno, že osoba využívající pseudonym „Dr. Solino“ je spojená rovněž s těmito údaji jako jsou telefonní kontakty, e-mailové adresy a uživatelské jméno komunikační aplikace Skype, které nahodile uvádí nebo uváděl ve své inzerci k OPL, medikamentům či zdravotnickému materiálu.

Na základě šetření k tel. číslu „+37062886057“ byla zjištěna inzerce společnosti „Baumerteam“ s udávaným původem ze Slovenské republiky, nabízející

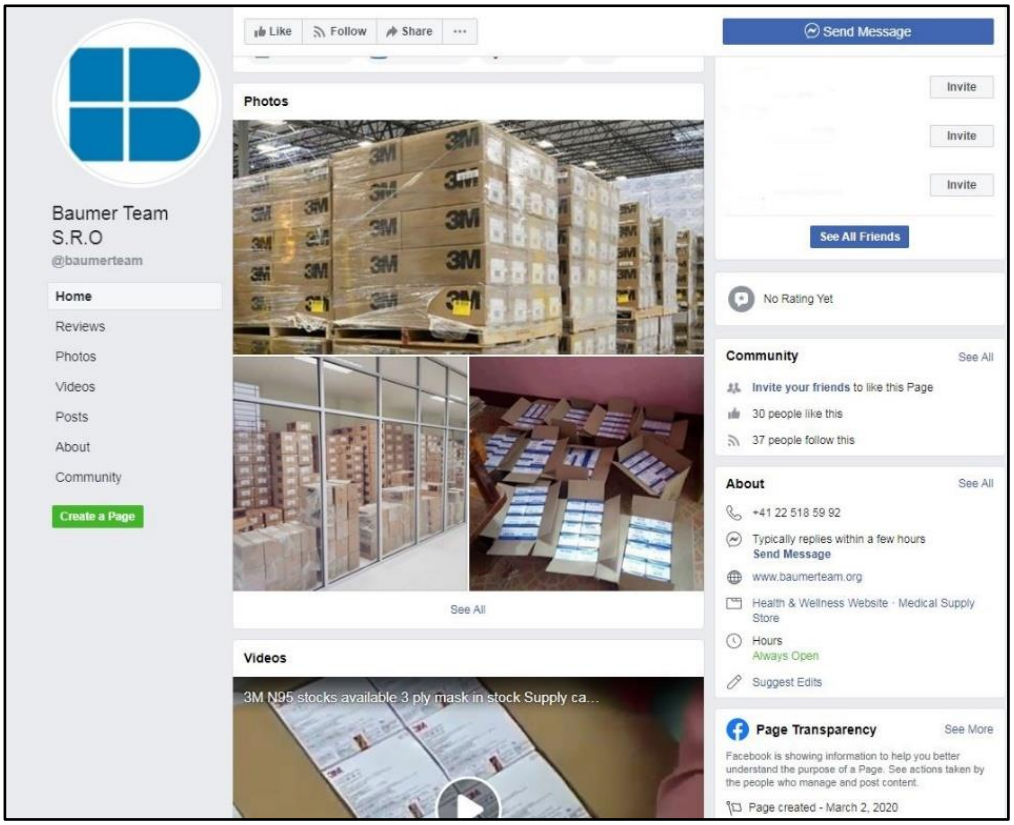
[88] SPF zkratka z anglického výrazu Sender Policy Framework. Jedná se o e-mailový autentizační systém sloužící jako obrana proti spamu.

zdravotnické výrobky – viz náhled inzerátu na obr. 16. Inzerát dostupný online: https://www.medicaldevices1.com/medical-device-suppliers/baumerteam.



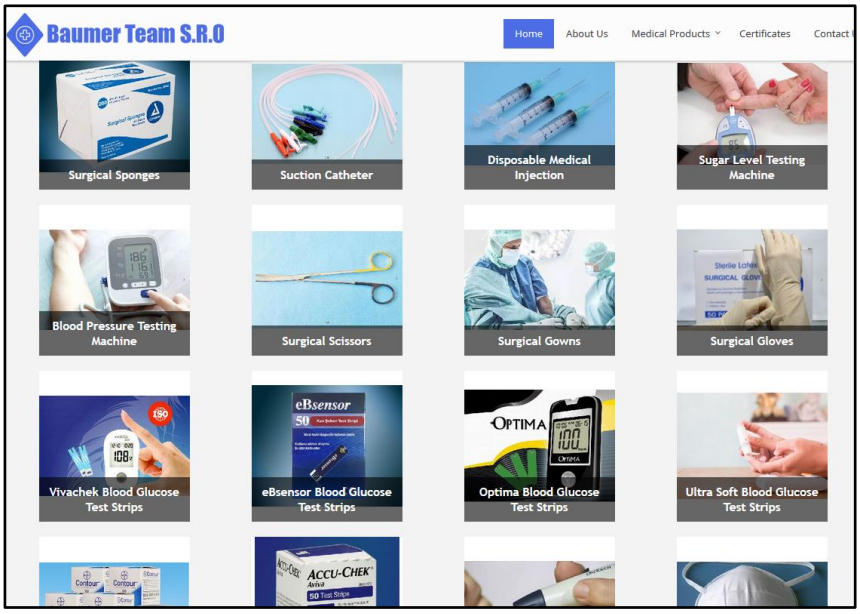
Obr. č. 16 – Náhled nabídky inzerátu Baumerteam, zdroj: https://www.medicaldevices1.com/medical-device-suppliers/baumerteam

Ke společnosti se pojí webové stránky www.baumerteam.com s udávanými kontaktními údaji jako sídlo společnosti: „Cintorinsky rad 1184.14 komarno, Republic of Slovakia“, telefonním kontaktem „+48422886920 / +17606185546“ a e-mail adresou info@baumerteam.com. Dále bylo zjištěno, že byl pravděpodobně provozován ještě jeden web se stejným původem, který je však již nedostupný, a to www.baumerteam.org. Tuto společnost doprovázely profily na sociálních sítích, které jsou již nedostupné – náhled obr. č 17.

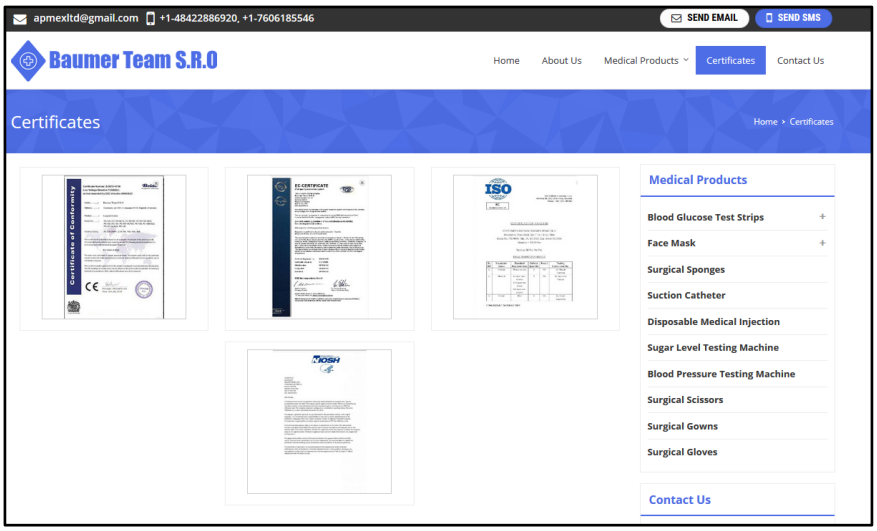


Obr. č. 17 – Náhled profilu sociální sítě Facebook na Baumer Team S.R.O, zdroj: archiv autora

Dalším šetřením k výše uvedeným webovým adresám se zdravotnických materiálem byla zjištěna webová stránka www.baumerteamus.com, která má v záložce s informacemi rovněž uvedeno, že se jedná o společnost pocházející ze Slovenska, a to konkrétně z Komarna. Kontaktní informace jsou od předchozích stránek odlišné, jako e-mail je uveden „apmexltd@gmail.com“ a jako telefonní kontakt je uváděn „+1-48422886920, +1-7606185546“. Náhled již neexistující webové stránky jako obr. č. 17, 18.



Obr. č. 17 – Náhled webové stránky www.baumerteamus.com, zdroj: archiv autora



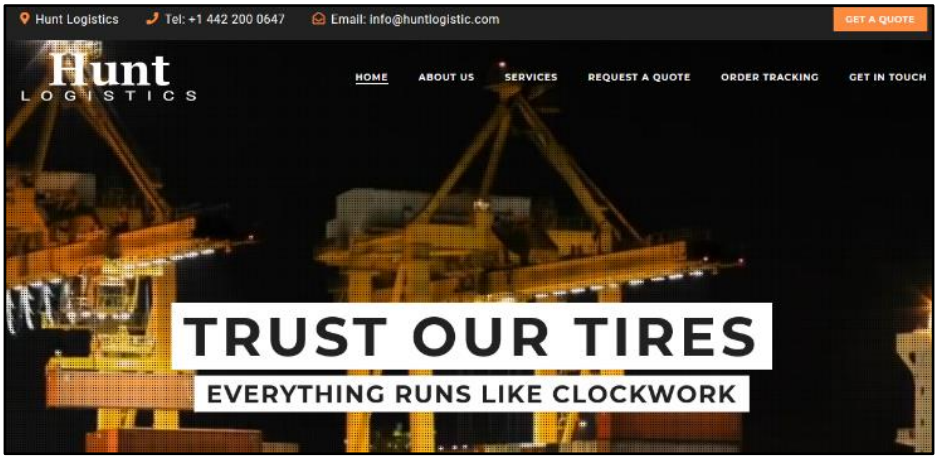
Obr. č. 17 – Náhled webové stránky s certifikáty www.baumerteamus.com, zdroj: archiv autora

Výše uvedená webová stránka je hostována u společnosti https://www.hosteurope.de/ a registrovaná společností https://uk.godaddy.com/. Webové stránky jsou hostovány na IP 166.62.85.22. Dalším šetřením bylo zjištěno, že se pravděpodobně jedná o VPS[89] s obsahem dalších webových stránek, které z hlediska použitých šablon odpovídají stránkám spedičních společností nebo

[89] Zkratka z anglického výrazu Virtual Private Server, volně přeloženo jako virtuální privátní server, který je virtualizovaný na HW.

webovým stránkám se zdravotnickým materiálem, prostředky souvisejícími s ochrannou před COVID-19 či webovým stránkám nabízejícím prodej NPS se stejným nebo podobným účinkem jako OPL k 68 webovým stránkám. Náhledy vybraných webových stránek z výše uvedeného seznamu jako obr. č 18, 19.

Obr. č. 18 – Náhled na abtlogisticsgroup.com, zdroj: archiv autora



Obr. č. 19 – Náhled na huntlogistic.com, zdroj: archiv autora

Závěrem lze konstatovat, že s největší pravděpodobností se jedná o dobře organizovanou skupinu působící ve virtuálním prostředí internetu, pravděpodobně od roku 2012 prakticky po celém světě, a to prostřednictvím nejen vlastních webových stránek, ale i inzertních portálů. Je velmi obtížné, až téměř nemožné, zjistit původ těchto pachatelů nebo místo, ze kterého operují. Lze se domnívat, že osoby skrývající se za přezdívkou „Dr. Solino“ nikdy neměli v plánu jakoukoliv položku z nabídky ať už ilegálního, nebo legálního zboží dodat a jejich záměrem

je vylákat ze zájemců v průběhu procesu objednávky a předstírané dodávky objednaného zboží finanční prostředky. Webové stránky jsou velmi profesionálně nejen navrženy, ale i zpracovány, včetně firemních MX protokolů, nabídky k zaměstnání, popřípadě certifikace zboží. S největší pravděpodobností se může jednat o značný počet webových stránek založených čistě za podvodným účelem. Odhadem lze konstatovat, že cca 30 % těchto webů se zaměřuje na zdravotnický materiál a testy v rámci COVID-19 opatření a využívá tak současné situace, kdy orgány veřejné moci v jednotlivých zemích mají v rámci zrychlených nákupů často snížené požadavky na prověření schvalovací procesy a prověření historie dodavatelských společností. Dalších 30 % webových stránek tvoří fiktivní spediční firmy se smyšlenými poplatky či vratnými kaucemi, jejichž cílem je vylákat další peníze. Vzhledem k tomu, že některé weby již mají negativní hodnocení, je velmi pravděpodobné, že zde dochází k podobnému psychologickému fenoménu jako u ransomware, kdy oběť v tichosti zaplatí a z důvodu studu či obavy o vyzrazení zájmu o nelegální komodity tuto platbu veřejně nepřizná nebo celou událost ani nenahlásí jako bezpečnostní incident. Nelze vyloučit, že i zde se může jednat o rostoucí latentní trestnou činnost, která zdánlivě vypadá jako ojedinělý případ, ale ve skutečnosti se může jednat o tisíce podvodů za měsíc.

Vzhledem k povaze době zjištění byl informován Interpol, který na základě četných informací ze všech státu vydal zprávu, která je dostupná online.[90] Náhled článku jako obr. č. 20.

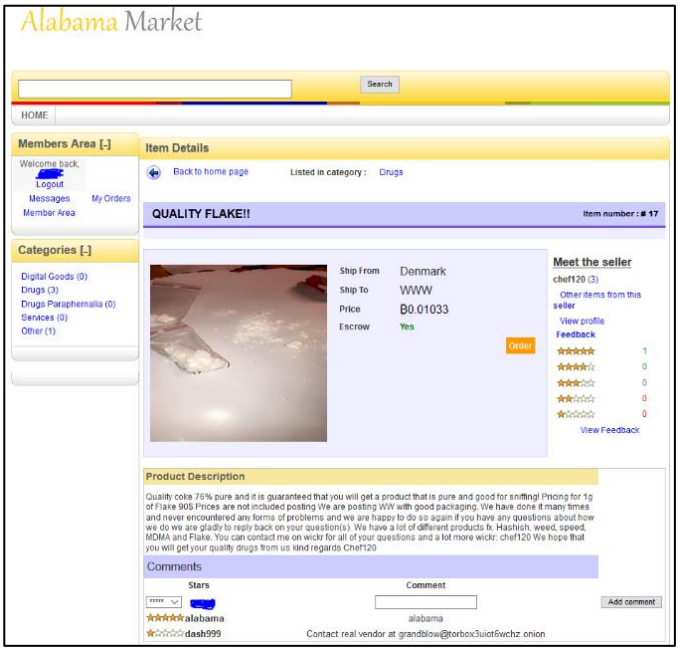
Obr. č. 20 – Náhled varování zprávy Interpolu k výše zpracovanému tématu, zdroj: https://www.interpol.int/News-and-Events/News/2020/INTERPOL-warns-of-organized-crime-threat-to-COVID-19-vaccines

[90] Interpol.com [online]. [cit.25.2.2022]. Dostupné z: https://www.interpol.int/News-and-Events/News/2020/INTERPOL-warns-of-organized-crime-threat-to-COVID-19-vaccines (accessed Feb 25, 2022).

6.3 Sociální síť a virtuální tržiště s ilegálním obsahem v DarkNet síti

Tato kazuistika poukazuje na aplikaci OSINT, WEBINT a SOCMINT metod v rámci pronikání do zájmového prostředí, vyhledávaní zájmového obsahu a následné ztotožnění pachatele. S ohledem na citlivost odhalování metod SKPV PČR nebudou zveřejňovaný vyvinuté nové nebo na základě této akce vyvinuté metody.

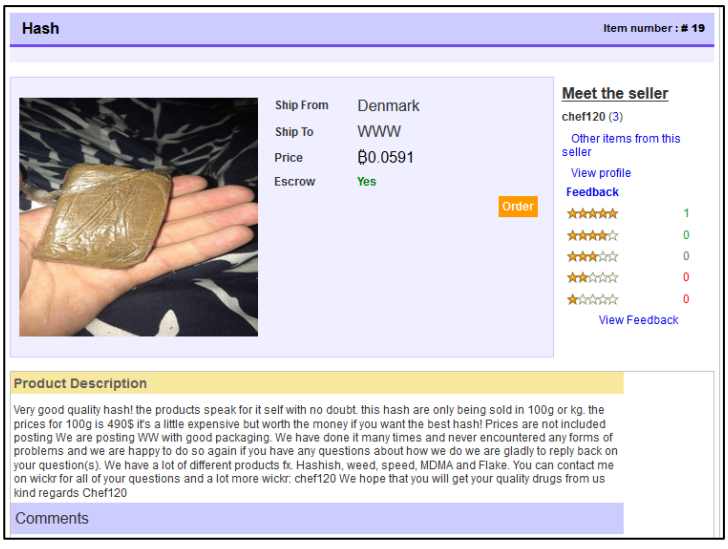
V rámci monitoringu TOR sítě, bylo v roce 2019, zjištěno virtuální tržiště s názvem „Alabama Market“, které bylo umístěné v TOR síti. Na první pohled běžná virtuální platforma s ilegálním obsahem obr. č. 21, však ukrývala v doprovodných datech stránky údaje: „Copyright © 2019“, dále datum pravděpodobně spuštění tržiště „Launched: 05/30/19“, a nastavení serveru v den monitoringu: „Server date: 06/25/2019“. Na základě provedené WEBINT analýzy bylo zjištěno, že je na tržišti registrováno celkem 516 uživatelů. Odkazy na profily uživatelů jsou ve formátu: http://i7e53wyud4ljkmd4.onion/view_profile.php?id=X, vzestupně od čísla 1, čímž se dalo toto číslo dopočítat. Stejně tak jako profil „admin“, který byl založen 26. 5. 2019, a profil pořadově číslo 2, před zprovozněním samotného tržiště dne 30. 5. 2019, jako profil s názvem „uzivatel2“ bez diakritiky a v českém jazyce, „http://i7e53wyud4ljkmd4.onion/view_profile.php?id=2“, což poukazuje na česky hovořící osobu v roli tvůrce tržiště náhled obr. č. 22.



Obr. č 21 – Náhled ilegálního tržiště Alabama market, zdroj: archiv autora

Obr. č 22 – Náhled profilu „uzivatel2“, zdroj: archiv autora

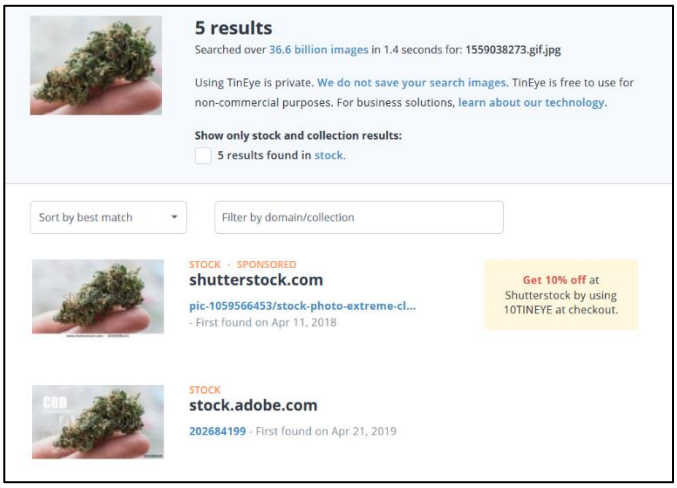
Při průzkumu virtuálního tržiště byla zjištěna nabídka s grafickým vyobrazením OPL. Detail nabídky OPL je zobrazen univerzálně ve tvaru id=X, kde X je číslo nabídky: http://i7e53wyud4ljkmd4.onion/view_product.php?id=X a to konkrétně u nabídky, s adresou na nabídku: http://i7e53wyud4ljkmd4.onion/view_product.php?id=19, náhled jako obr. č. 22



Obr. č 22 – Náhled detailu nabídky OPL, zdroj: archiv autora

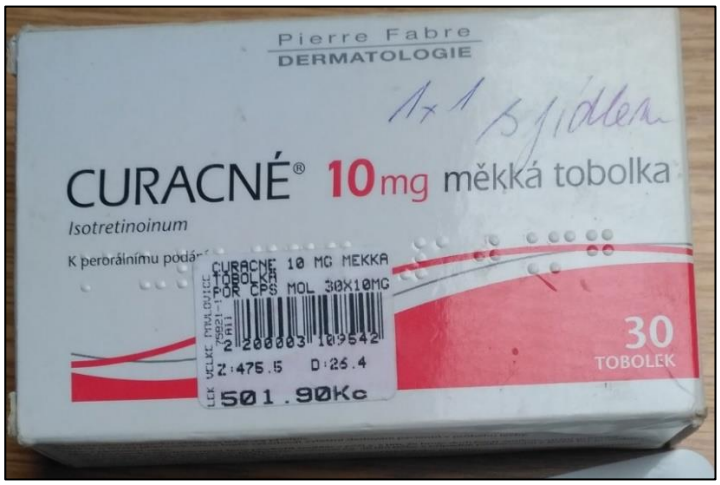
Fotografie OPL byly umístěny na adrese http://i7e53wyud4ljkmd4.onion ve tvaru: „http://i7e53wyud4ljkmd4.onion/uploads/1559291023.gif“. Na této adrese byl

dostupný index dané složky, ze které je patrné, že celkem 7 souborů, bylo nahráno 29. 5. 2019, tedy ještě před spuštěním tržiště a je tedy pravděpodobné, že jsou nahrány přímo administrátorem tržiště. Soubory jsou všechny shodné, liší se pouze v názvu. Neobsahují žádná relevantní metadata a jedná se o fotografie stažené z internetu, které jsou dostupné v komerčních databázích fotografií na www.shutterstock.com, komparace příkladu fotografie obr. č. 23.



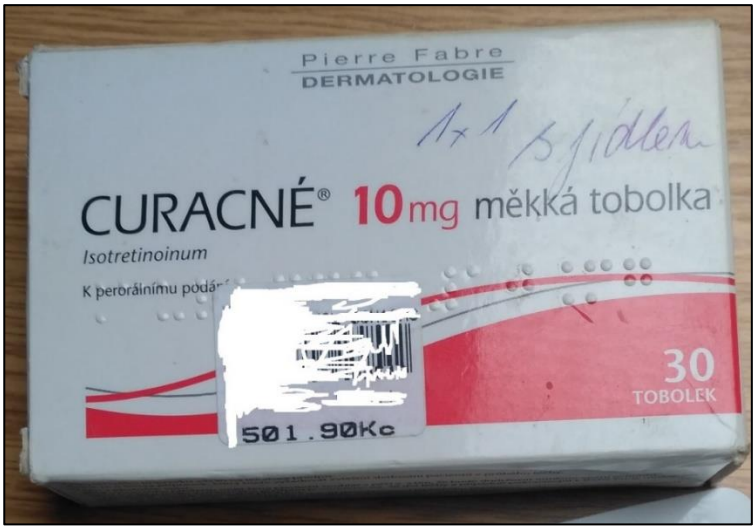
Obr. č 23 – Náhled komparace fotografie OPL, zdroj: archiv autora

Adresář „upload“, obsahují fotografie českých SIM karet: T-mobile, O2, Oskarta, Vodafone. Dále na dvou fotografiích je zachycen lék „CURACNÉ,“ zakoupený dle nalepené etikety s čárovým kódem a místem lékárny obr. č. 24, díky této etiketě byla zjištěna lékárna odkud byl lék pořízen.



Obr. č 24 – Náhled fotografie se štítkem lékárny, zdroj: archiv autora

Na druhé fotografii léku CURACNÉ je čárový kód a název lékárny vymazán, z čehož je patrné, že si autor pravděpodobně uvědomil svou chybu a snažil se ji napravit obr. č. 25.

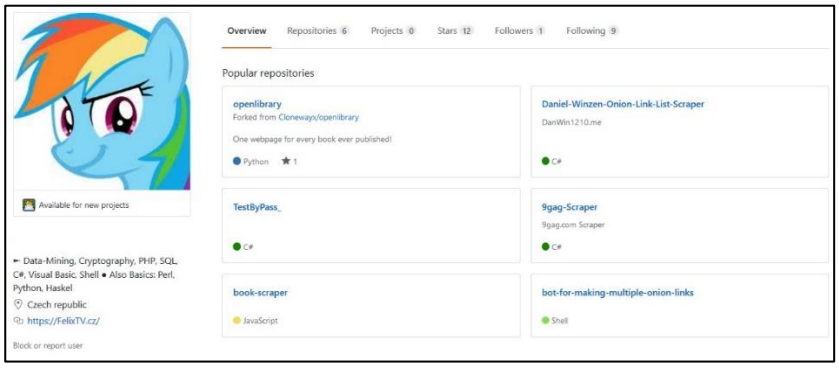


Obr. č 25 – Náhled fotografie s odstraněným štítkem lékárny, zdroj archiv autora

Obě fotografie mají shodná exif data, která obsahují informace o zařízení, kterým byly fotografie pořízeny a GPS data, kde byly fotografie pořízeny. V tomto případě se tak jedná o ICT Xiaomi Redmi 3S, ve kterých je uvedena GPS poloha, která skutečně odpovídá místu poblíž lékárny, kde bylo léčivo zakoupeno. Stejně tak i fotografie výše zmíněných SIM karet obsahují exif data ve formě GPS koordinátu, s použitím shodného mobilního zařízením Xiaomi Redmi 3S. Na základě těchto dat bylo zjištěno přesné místo pořízení fotografií. Toto místo se nachází v obydleném domě v malé vesnici na jihu Moravy. Toto místo odpovídalo bydlišti pachatele. Následným OSINT šetřením k místu za pomocí katastru nemovitostí o osobě bylo zjištěno bydliště a jméno pachatele. Sekundárním šetřením v okolí osoby pachatele a k jeho schopnostem, bylo zjištěno, že studuje informatiku a zapojuje se do spoustu vlastních projektů vně internetu ve formě vytváření webových stránek a SQL[91] databází. Rovněž byl zjištěn profil na webu Github s profilovou fotografií vyobrazení kreslené postavy modrého poníka z pohádky „My little ponny“ obr. č. 26. I když se zprvu jedná o irelevantní poznámku, v dalších

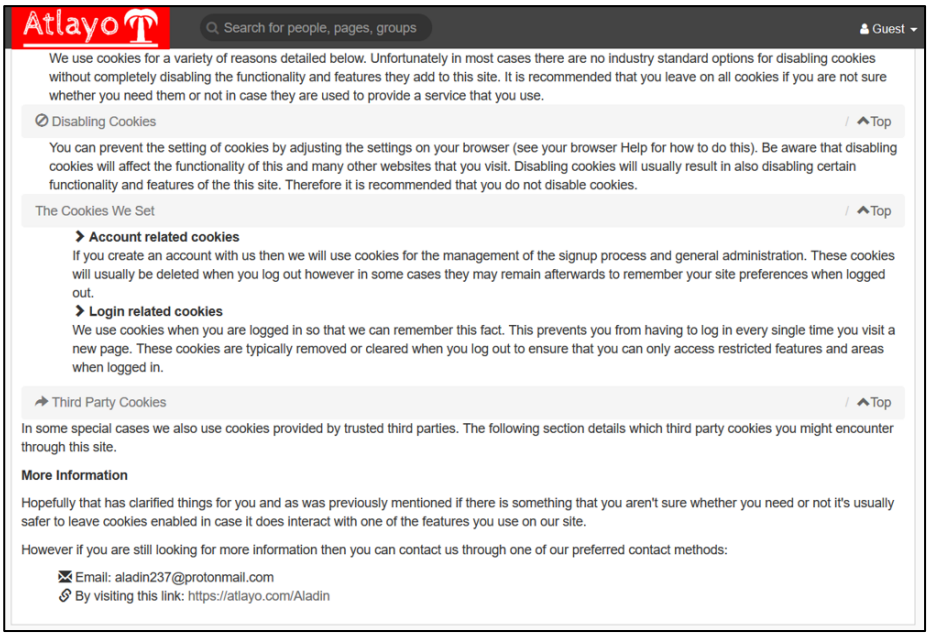
[91] Je zkratka z anglického Structured Query Language, což je typ pro dotazování v relačních databázích.

krocích dojde právě k využití této informace, jako potvrzující identitu pseudonymu se ztotožněnou osobou. Na profilu uvádí dovednosti PHP a SQL, což jsou přesně dovednosti potřebné pro vznik virtuálního tržiště „Alabama Market“.



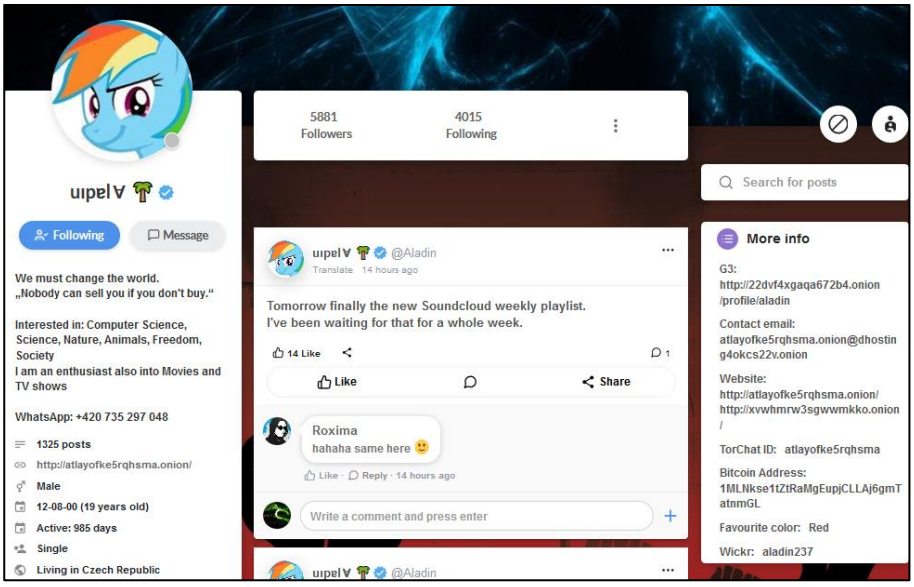
Obr. č 26 – Náhled profilu na Github, zdroj: archiv autora

Vzhledem k věku a možným zálibám byla oblast rozšířena i na herní klienty a přidružené sociální sítě. Zde byl pachatel nalezen na Steam platformě, kde užíval identický profilový obrázek z pohádky „My little ponny“ a jako herní pseudonym využíval nick: „Aladin237“. Na tomto profile měl i skupinu s názvem „Atlayo“. Socialní síť Atlayo vznikla v roce 2018 a nacházela se v darknetu sítě TOR. Tato sociální síť byla známá pro svou absenci cenzury či dozorující morální domény, proto mohlo docházet ke sdílení jakéhokoliv i ilegálního obsahu bez postihu pod rouškou naprosté anonymity. V polovině roku 2019 došlo k promazání obsahu a ke spuštění stejného obsahu v clearnetu na adrese www.atalyo.com. V dostupných podmínkách a FAQ zmíněné sociální sítě Atlayo bylo zjištěno, že správce a držitel této sociální sítě odkazuje na sebe profilem na stejnojmenné sociální síti: „https://atlayo.com/Aladin“ a s e-mailovým kontaktem: aladin237@protonmail.com obr. č. 27.



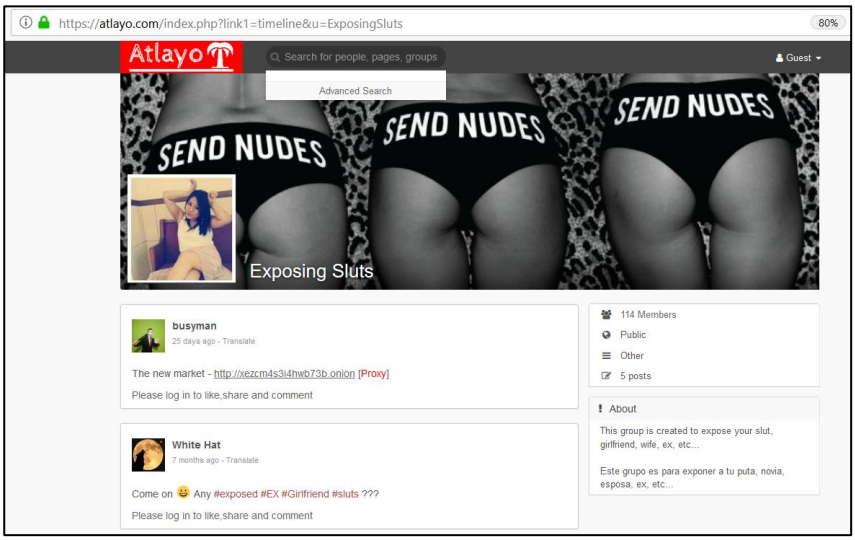
Obr. č 27 – Náhled FAQ www.atlayo.com, zdroj: archiv autora

Na adrese https://atlayo.com/Aladin, na které by se měl nacházet profil administrátora a majitele sociální stránky, je stejný profilový obrázek z pohádky „My little ponny," který se nachází na profilech u webových stránek Steam a Github. Náhled profilu jako obr. č. 28.



Obr. č 28 – Náhled profilu administrátora Atlayo „Aladin", zdroj: archiv autora

Na výše uvedené sociální síti s webovou adresou byla www.atlayo.com, se nachází skupina „Exposing Sluts“, ve které osoba využívající uživatelské jméno „busyman“ sdílela odkaz na nově vzniklé virtuální tržiště s ilegálním zbožím v rámci sítě TOR „Alabama Market“. Náhled skupiny jako obr. č. 29.

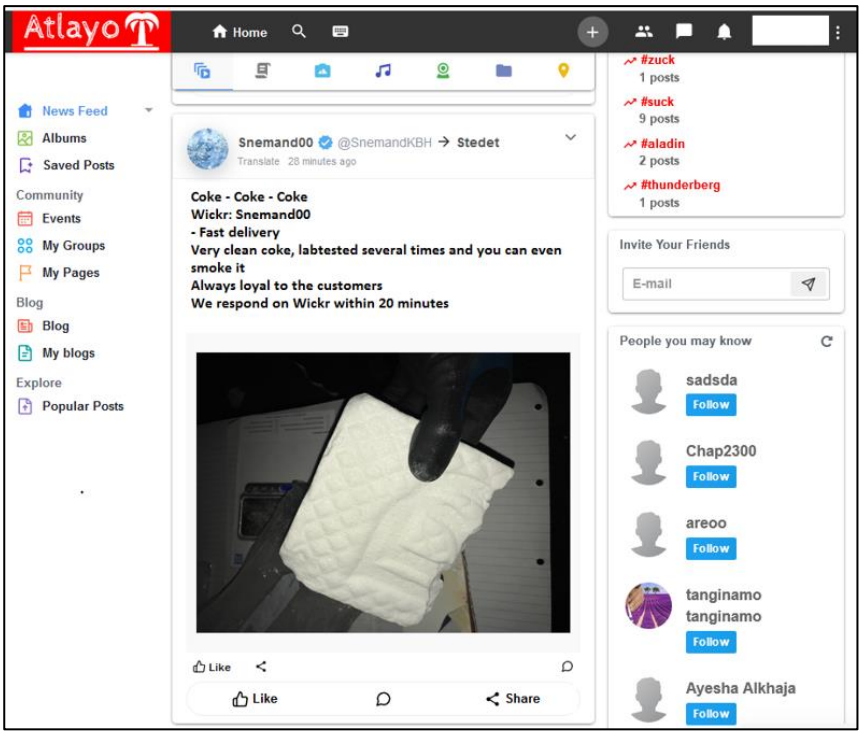


Obr. č 29 – Náhled sdílení odkazu Alabama Market vně skupiny „Exposing Sluts“ profilem „busyman“, zdroj: archiv autora

Výše zmíněný admin „Aladin“ a osoba využívající profil: „busyman“ jsou spolu na sociální síti: „Atlayo“ ve spojení a na základě šetření k tomuto účtu je nanejvýš pravděpodobné, že je to další z falešných účtu osoby využívající pseudonymu Aladin a tento profil využívá k šíření linku vně sociální sítě jen jako iluze komunitního zájmu o odkaz k virtuálnímu tržišti s ilegálním obsahem v TOR síti darknetu.

Následně bylo zjištěno, že stejnou událost zpracovává kodaňská policie, a to konkrétně výše uvedenou sociální síť Atlayo, na které se nacházejí skryté skupiny čítající komunitu 10 až 20 tisíc uživatelů, ve které se nabízejí a dál distribuuje OPL ve formě kokainu, MDMA[92], XTC[93] a podobná syntetická OPL, náhled jako obr. č. 30.

[92] MDMA je zkratka 3,4-methylendioxy-N-methylamfetamin syntetické OPL
[93] XTC je tableta s obsahem MDMA a celulózy obvykle ražena s různými motivy a obsahem účinné látky MDMA obvykle od 150 mg až po 350 mg.

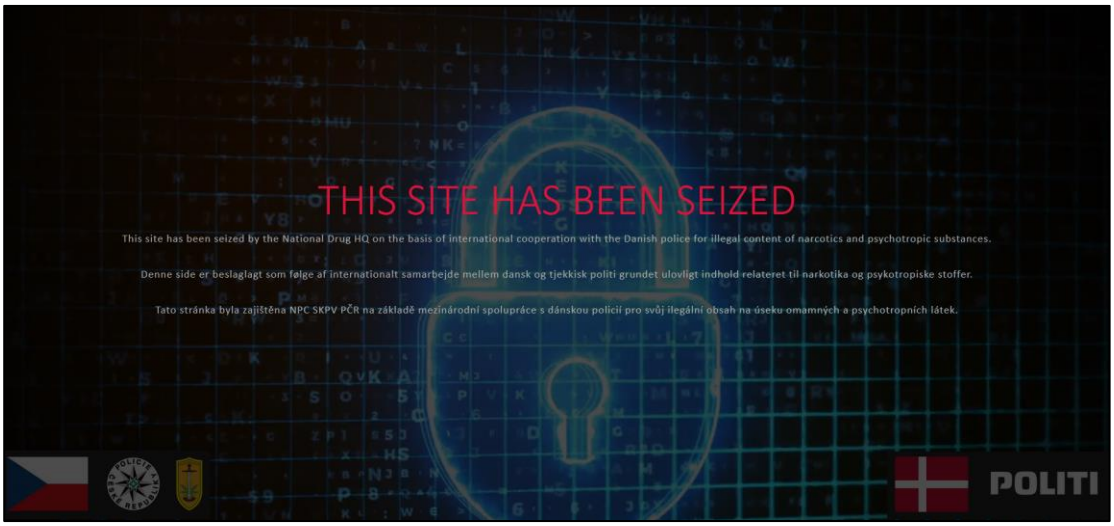


Obr. č. 30 – Náhled sociální sítě www.atlayo.com s OPL

Výše uvedený administrátor a tvůrce sociální sítě o tomto jednání věděl a osobně se přičinil k ochraně zájmů prodejců OPL. Následně ve společné operaci, byl v ČR zadržen tvůrce a administrátor Alabama Market tržiště a sociální sítě Atlayo, který byl ztotožněn na základě SOCMINT analýzách a na adrese, která byla zjištěna OSINT metodou. V Dánsku byly zadrženi dva pachatelé a velké množství OPL. V ČR se díky kvalitní přípravě podařilo zajistit nejen kompletní ICT zapojené do všech ilegálních činností, ale i převzít kontrolu nad celou sociální síti, která postrádala elementární základy cenzury ilegálního obsahu, a to včetně pedofilní tematiky, podpory náboženského a politického terorismu, nabídky ilegálních aktivit, a to včetně prodeje dalších ilegálních věcí jako zbraní, odcizených platebních prostředků apod. Sociální sít čítala 450.000 anonymních registrací a stovky uzavřených a anonymních skupin. Na základě těchto zjištění, byla sociální síť uzavřena jak na úrovni TOR sítě v darknetu, tak i v clearnetu viz. náhled obr. č. 31. [94] Všichni zadržení pachatelé byly dánským soudem odsouzeni k odnětí

[94] iRozhlas.cz [online]. [cit.25.2.2022]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/dansko-prodej-drog-atlayocom-darknet-socialni-sit-zbrane-porno_2007310941_jgr

svobody. Po podání odvolání s nesouhlasem na výši trestu, odvolacím soud uznal nedostatečnou výši odnětí svobody nově rozhodl o přísnějších trestech pro všechny v celé kauze a to 5 let odnětí svobody pro českého programátora, 10 a 12 let pro dánské prodejce OPL. Rozsudek je pravomocný.



Obr. č. 31 – Náhled zajištěné sociální sítě, zdroj: www.atlayo.com

Výše uvedená operace byla první svého druhu a zároveň je to i první případ v české kriminalistice, kdy bylo za pomocí pokročilých SOINT, WEBINT, SOCMIT metodami zjištěn nejen pachatele trestné činnosti, ale další trestná činnost vně internetu.[95] Od prostého monitoringu k pachateli a úspěšnému odsouzení.

[95] Policie.cz: Policie České republiky [online]. [cit.25.2.2022]. Dostupné z: https://www.policie.cz/clanek/operace-green.aspx

7 Hodnocení užívání OSINT a SOCMINT metod v rámci kriminální policie

Hlavním cílem průzkumu je objektivně zhodnotit užívání OSINT a SOCMINT metod v rámci služby kriminální policie a vyšetřování na základě zkušeností policistů zařazených na pozicích pro zpravování trestních spisů. Sekundárním cílem je vyhodnotit, zda mají některé faktory, jako biologický a služební věk vliv na využívaní takových to metod a zhodnocení subjektivního názoru na tyto metody. Pro tyto účely bude použit sběr relevantních dat formou dotazníků.

7.1 Popis průzkumu a sběr dat

Sběr dat je proveden formou elektronicky distribuovaného dotazníku, osobám zařazeným u policie české republiky dále jen „PČR“ na úrovni služby kriminální policie a vyšetřování dále jen „SKPV“ úrovně útvarů s celostátní působností dále jen „ÚCP“ jako je Národní protidrogová jednotka dále jen „NPC“ a Národní centrála organizovaného zločinu dále jen „NCOZ“, krajské úrovně a obvodní nebo územní úrovně. Vzhledem k hierarchické struktuře SKPV z hlediska věcné příslušnosti trestných činů, je relevantní a důležité do průzkumu zahrnout i spisovou službu místních oddělní policie dále jen „MOP“ a obvodních oddělení policie dále jen „OOP“, na kterých dochází ohlášení trestného činu jeho kvalifikace a sběr prvotních informací, pro postoupení na SKPV pro věcnou příslušnost nebo samy zpracovatelé z MOP a OOP takovou to věc zpracovávají, přičemž využívají stejných metod jako SKPV. Je zcela evidentní, že SKPV většinou rozpracují spis, který prošel prvotní analýzou zpracovatelů z úrovně MOP a OOP. Dotazník byl rozesílán na všechna výše zmíněná pracoviště v celé ČR, tak aby byla data rovnoměrně zastoupená z celé ČR a ze všech výše uvedených oblastí působnosti.

Otázky jsou zaměřené na využívání OSINT a SOCMNIT metod, v rámci trestního řízení. Dotazník obsahuje deset otázek s výběrem z několika předem definovaných možných odpovědí a předem definovaného rozsahu pro ucelenější výstup analýzy. Otázky jsou v obecné části dotazníku zaměřeny na služební praxi, biologický věk, vzdělání a služební zařazení. V praktické části jsou dotazy pokládány nejdříve na znalost oblasti OSINT a SOCMINT metod, následně jejich praktické využití v individuálních trestních řízeních a subjektivní hodnocení přínosu takových to metod na škále od 1 do 10.

Otázky a možnosti odpovědi:

1. V jaké úrovní organizačního článku jste zařazen/a
    - Služba pořádkové policie MOP/OOP
    - SKPV obvodní nebo územní úrovně
    - SKPV krajské úrovně
    - SKPV s celostátní působností
2. Váš biologický věk
    - do 30 let
    - 31–45 let
    - 46 a více let
3. Váš služební věk u PČR
    - do 5 let
    - 6–10 let
    - 11–16 let
    - od 17 a více let
4. Vaše nevyšším dosažené vzdělání
    - Středoškolské s vykonanou maturitní zkouškou
    - Vysokoškolské v bakalářském studijním programu
    - Vysokoškolské v magisterském studijním programu
    - Doktorát na základě rigorózního řízení
    - Vysokoškolské vzdělání v doktorském studijním programu
5. Víte, co znamená OSINT metoda?
    - Ano
    - Ne
6. Víte, co znamená SOMINT metoda?
    - Ano
    - Ne
7. Absolvoval/a jste seminář organizovaný PČR, CEPOL, EUROPOL nebo jinou organizací, u které rozhodování o vyslání spadá do kompetence PČR, k OSINT metodám sběru dat?
    - Ano

- Ne
- Absolvoval jsem takový kurz, ale mimo PČR na základě vlastní iniciativy a vlastních nákladů.

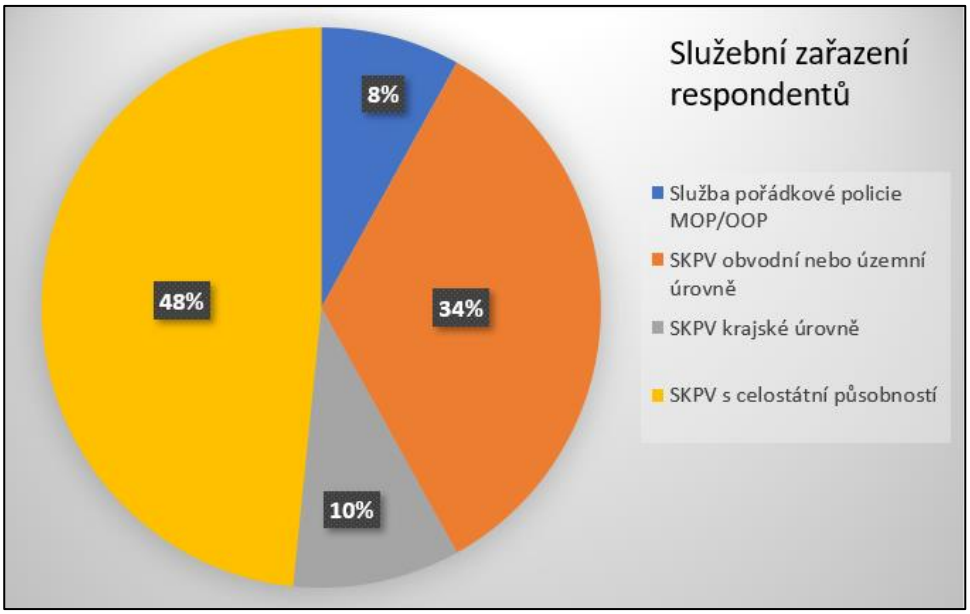
8. Využíváte sběr a následnou analýzu dat z otevřených zdrojů internetu a sociálních sítí v oblasti řešení již odhalené trestné činnosti v rámci prvotních úkonů či dalšího rozpracování?
    - Tyto metody nelze aplikovat sice u každé problematiky, ale pokud je zde možnost tak je využívám společně s policejními databázemi a poznatkovými fondy.
    - Významně takové metody nevyužívám. Vše, co potřebuji zjistím osobně nebo v policejních databázích či poznatkových fondech.
9. Přikládáte do spisového materiálu relevantní výstupy z otevřených zdrojů a sociálních sítí vztahující se k objektům zájmu?
    - Ano
    - Ne
10. Na základě vašeho subjektivního hodnocení, v jakém rozsahu za posledních 5 let vám sběr dat z otevřených zdrojů a jejich analýza ve vašich spisech pomohla získat úkony, vykreslit situaci a vazby či zadokumentovat data s důkazní hodnotou?
    - Grafické vyobrazení škály od 1 až 10 hvězd.

7.2 Vyhodnocení a analýza dat

Vyhodnocení dat bude probíhat na základě hodnocení odpovědí v kontextu s faktory prvních čtyř otázek vykreslující respondenty, jako je biologický a služební věk, zařazení společně s nejvyšším dosaženým vzdělání v souvislosti s otázkami, která reflektují znalosti, možnosti, praktickou aplikaci a subjektivního hodnocení respondenty přínosu OSINT metod.

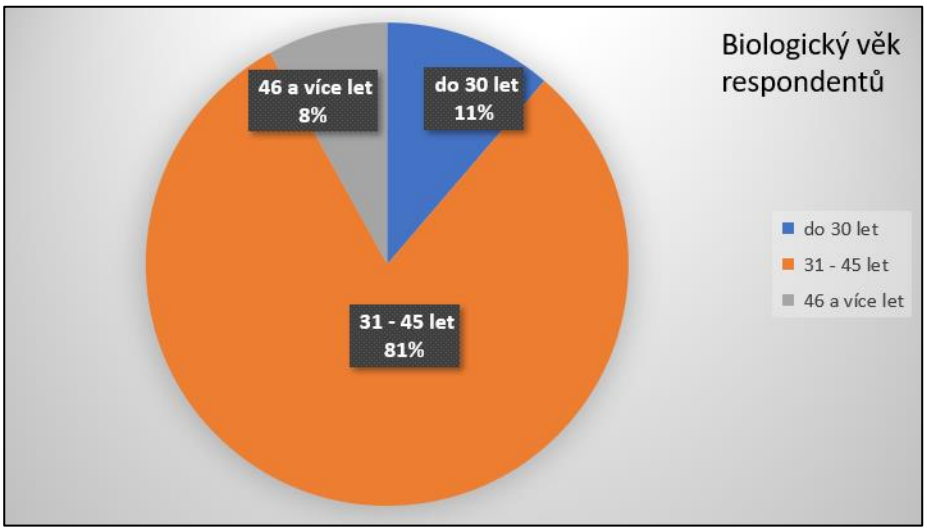
Dotazník vyplnilo 62 respondentů a to konkrétně 30 zařazených na ÚCP SKPV, 6 z KŘP, 21 z obvodní nebo územní úrovně a 5 z MOP nebo OOP, viz. procentuální vyjádření v grafickým znázornění obr. č. 32. Jak už bylo zmíněno sběr dat probíhal

skrze virtuálním prostředí s cíleným na konkrétní pracoviště pro ucelenější výsledky s rovnoměrným zdrojem dat z celé ČR.



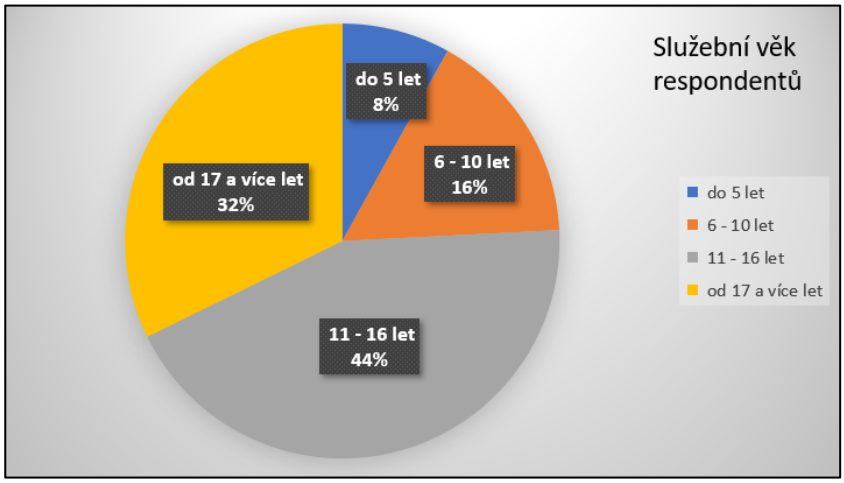
Obr. č. 32 – Graf s procentuálním vyjádřením služebního zařazení respondentů.

Do sběru dat se zapojili respondenti v rozsahu 7 respondentů do 30 let věku, 50 respondentů v rozmezí 31–45 let věku a 5 respondentů 46 a více věku. Tyto data byly důležité z hlediska odrazu vývoje společnosti z hlediska obliby užívání ICT. Grafické vyobrazení dat obr. č. 33.



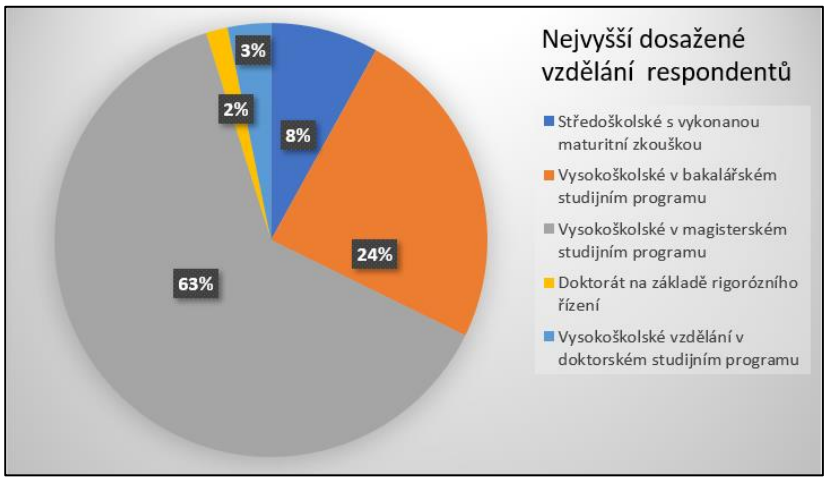
Obr. č. 33 – Graf s procentuálním vyjádřením biologického věku respondentů.

Součástí otázek, byl dotaz na délku služebního věku, kde bylo cílem zjistit, zda má tento věk vliv na znalosti daných témat jako je OSINT a SOCMINT s praktickou aplikací. Tento jev se prokazatelně neprojevil a data nejsou jednoznačná. Pro vyhodnocení tohoto cíle, by bylo třeba daleko většího vzorku respondentů s rovnoměrnějším zastoupením biologického věku.



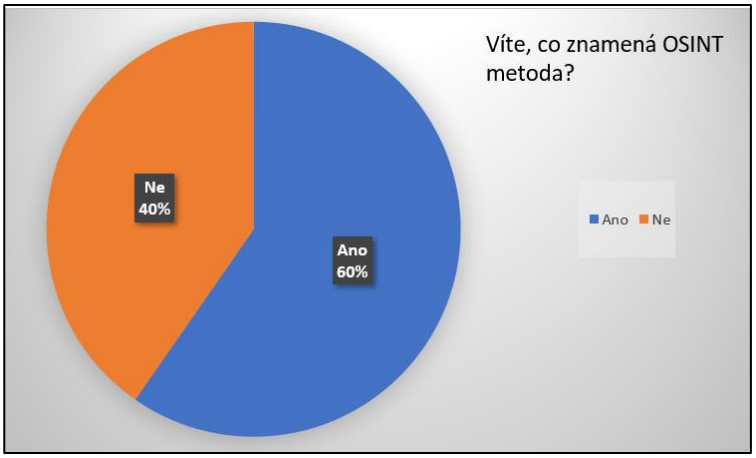
Obr. č. 34 – Graf s procentuálním vyjádřením služebního věku respondentů.

Vzhledem k povaze dotazníku a diametrálních požadavků na vzdělání v různých úrovních SKPV PČR, bylo důležité zjistit úroveň vzdělání respondentů a vytyčit průměr respondentů. I když se úroveň vzdělání jeví jako důležitý faktor, v hodnocení využívání OSINT metod, na základě vyhodnocených dat, jde jen o vykreslující faktor, jelikož se s obornou znalostí tohoto tématu pravděpodobně mohla setkat jen velmi nepatrný podíl respondentů v rámci svého vzdělání.



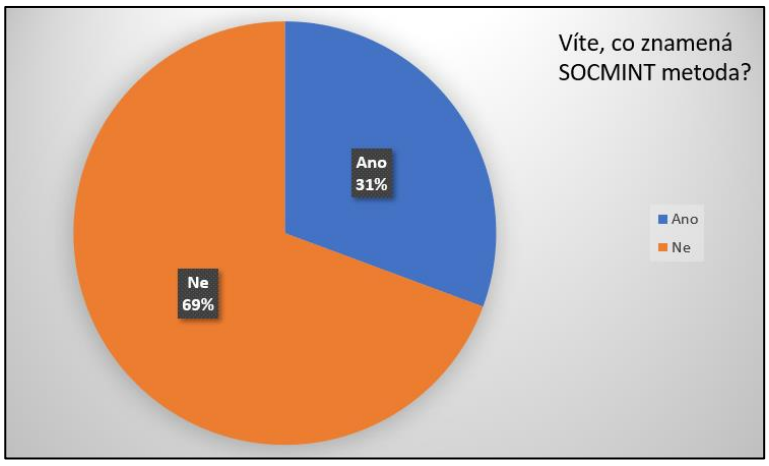
Obr. č. 35 – Graf s procentuálním vyjádřením vzdělání respondentů.

Na otázku „Víte, co znamená OSINT metoda“, bylo odpovězeno u policistů téměř rovnoměrně, ale vetší dominance je na straně odpovědi ANO. V této oblasti je vidět pozitivních odpovědí respondentů z ÚCP, které se v této oblasti více věnují vzdělávání. Což je vidět z dat, kdy ÚCP 25 z 30 respondentů odpovědělo ANO a z řad nižších organizačních článku PČR odpovědělo SPP ANO 1 a NE 4 respondentů, u obvodní nebo územní úrovně ANO 7 a NE 14 respondentů, a u SKPV Krajské úrovně top bylo ANO 4 a NE 2 respondenti.



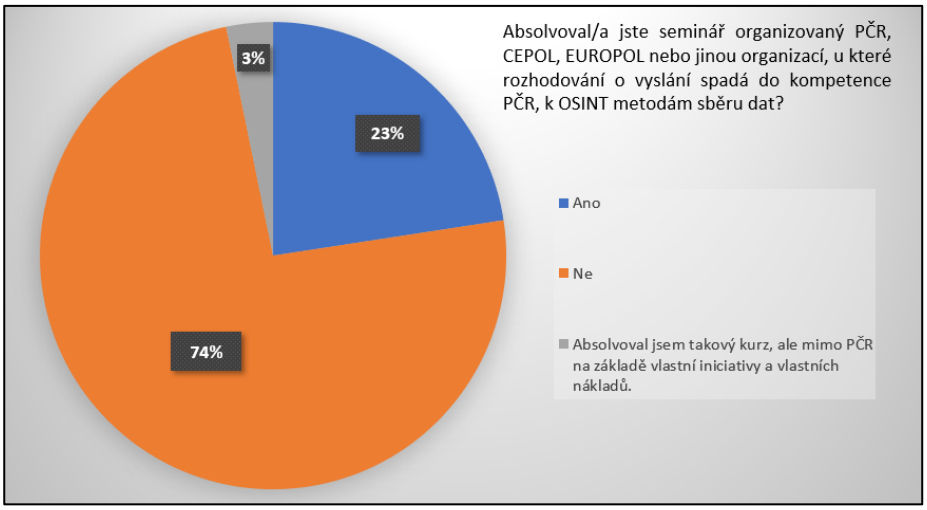
Obr. č. 36 – Graf s procentuálním vyjádřením znalosti OSINT metody.

Na otázku „Víte, co znamená SOCMINT metoda“, bylo odpovězeno u policistů spíše negativně, i když se to dalo očekávat z hlediska informovanosti či možnosti interního vzdělávaní v této oblasti. Opět je v odpovědích ANO dominující ÚCP, které má komplexní vzdělávací projekty pro tuto oblast. Grafické vyobrazení odpovědí obr. č. 36.



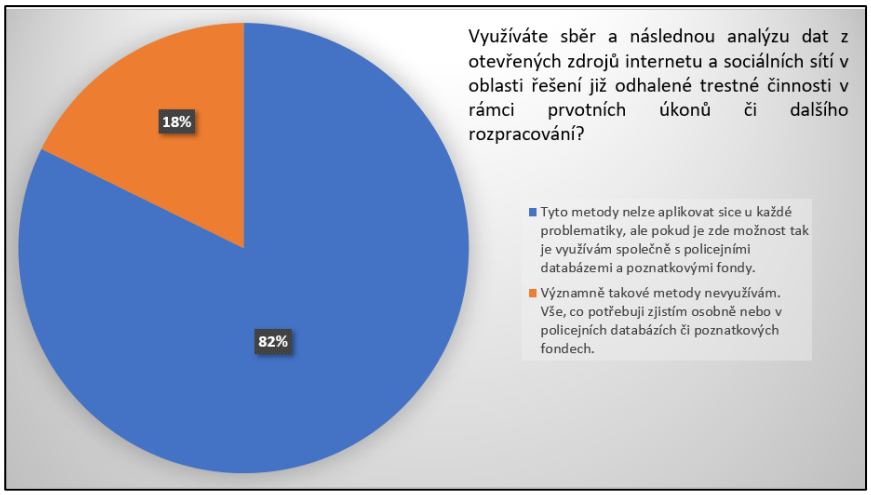
Obr. č. 37 – Graf s procentuálním vyjádřením znalosti SOCMINT metody.

Na otázku ohledně absolvování vzdělávacích aktivit k danému tématu byla odpověď u policistů s převahou negativní odpovědí, což se opět dalo očekávat z hlediska nedostatečných kapacit vzdělávacích zařízení či příležitostí zahraničního charakteru a nízkému počtu lektorů v těchto tématech s praktickými zkušenostmi. Data respondentů jsou rovnoměrně zastoupena a je zcela evidentní, že vzdělání, či biologický nebo služební věk nemá na tuto otázku žádný vliv. I když bylo u tohoto dotazu předpoklad vlivného faktoru, jako je služební zařazení, kde je zcela zjevně větší možnosti účasti na vzdělávacích aktivitách i v mezinárodním měřítku u útvarů s celostátní působností, zde byla data zcela diametrální od očekávání. Jen 9 z 30 respondentů zařezaných na ÚCP absolvovalo vzdělávací aktivitu v tomto směru. Grafické vyobrazení odpovědí obr. č. 38



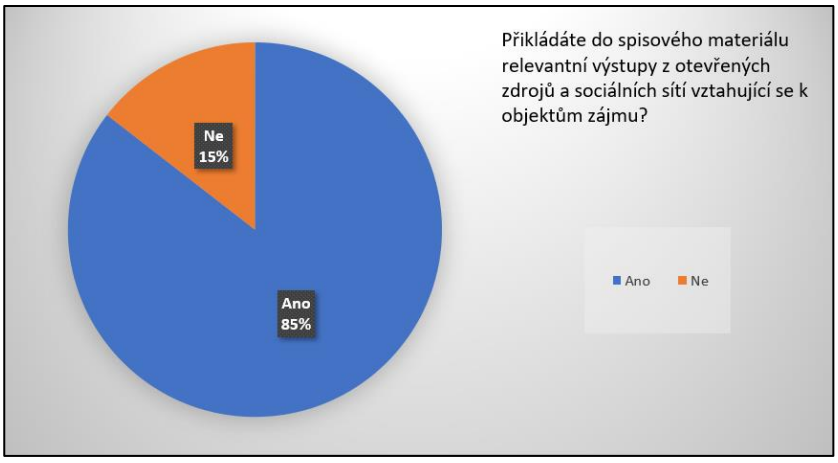
Obr. č. 38 – Graf s procentuálním vyjádřením absolvovaných OSINT kurzů.

Na datech otázky „Využíváte sběr a následnou analýzu dat z otevřených zdrojů internetu a sociálních sítí v oblasti řešení již odhalené trestné činnosti v rámci prvotních úkonů či dalšího rozpracování?“ je zcela evidentní dominance pozitivního využití OSINT metod i když v otázkách, zda respondenti ví, co znamenají OSINT a SOCMINT metoda, bylo u OSINT metod balancující hranice odpovědi ANO v 60 % a u SOCMINT metod NE 69 %. Zde je evidentní absence elementárních základů ve výrazech v odborné oblasti, za který může opět vzdělávací systém vně PČR v dané oblasti.



Obr. č. 39 – Graf s procentuálním vyjádřením používání OSINT metody.

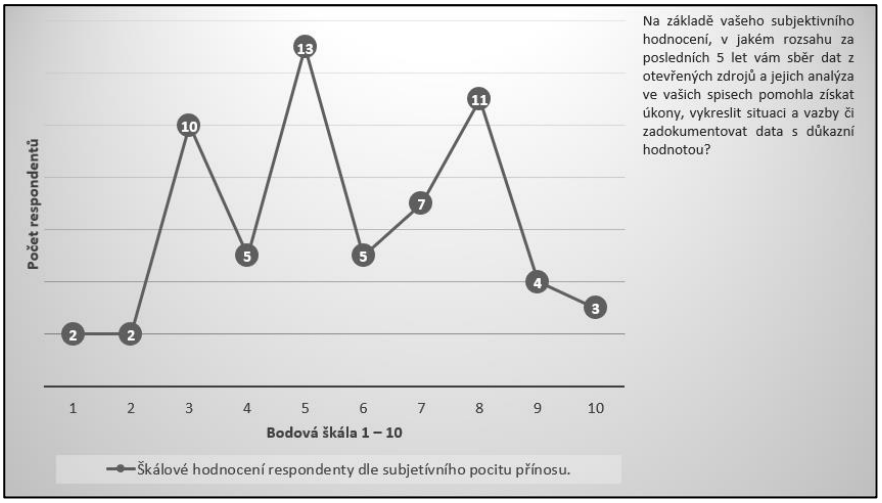
Na otázku „Přikládáte do spisového materiálu relevantní výstupy z otevřených zdrojů a sociálních sítí vztahující se k objektům zájmu?“ bylo většinou odpovězeno ANO, ale u několik respondentů bylo odpovězeno NE zejména 5 respondentů z 21 zařazených na SKPV odvodní nebo územní úrovně a 5 ze 30 respondentů z SKPV celostátní úrovně. Jedná se o respondenty v rozpětí biologického věku 31–45 let, s rovnoměrném zastoupení všech rozpětí služebního věku, s dominantním zastoupením vzdělání magisterského studijního programu.



Obr. č. 40 – Graf s procentuálním vyjádřením využití výstupů OSINT metod.

U bodové škály, subjektivního hodnocení přínosu OSINT metod v ohledu posledních 5 let, kdy u PČR začaly tyto metody získávat stále větší prostor

v kriminálních analýzách a procesních úkonech. Z dat vyplývá, že dominující je v kontextu s počtem respondentů střed škály mezi 3 až 8 bodem pro efektivitu a využitelnost takových to metod v rámci trestního řízení.



Obr. č. 41 – Graf se s škálovým hodnocením respondentů k přínosu OSINT metod.

7.3 Výsledek analýzy

Na základě dat bylo zjištěno, že nejvíce zastoupeným respondentem je osoba biologického věku rozsahu 31-45 let zařazených u SKPV ÚCP, se služebním věkem v rozsahu 11–16 služebního věku, s vysokoškolským vzděláním v magisterském studijním programu, zařezaných na útvarech s celostátní působností. I když v rámci dotazů k OSINT a SOCMINT metodám byly vesměs odpovědi většinou svědčící o neznalosti těchto metod v souhrnném hodnocení bylo výsledkem pravý opak, kde naopak potvrdilo hojné využívaní těchto metod v rámci kriminálních analýz a drtivá většina respondentů uvádí tyto metody jako přínosné v rámci spisového materiálu. Rozdílné odpovědi mezi dotazu uznalosti a užívání OSINT a SOCMINT metod, je prostá neznalost zkratky těchto výrazů, což rovněž reflektuje absenci oficiálních vzdělávacích aktivit vně PČR k těmto tématům. Z odpovědí respondentů je evidentní zájem na využívaní výše zmíněných metod a jejich praktického užívání v rámci TŘ.

8 Závěr

Vzhledem k rozsáhlosti tohoto tématu, bylo v teoretické části poukázáno jen na určitý rámec vybraných metod, které jsou zásadní pro OSINT a SOCMINT metody sběru dat včetně jejich analýz, které bylo možné použít na praktické aplikaci v kazuistikách. Na výše vybraných třech kazuistikách ze všech oblastí je zcela evidentní klíčová úloha zmíněných metod. Jejich aplikace poukazuje na různá variabilní užívání takovýchto metod nejen ve sběru dat, ale i jejich analýze. Na těchto případech bylo zcela evidentní, že neexistoval jiný nástroj, jak tato ilegální jednání identifikovat a reagovat na ně. I když je použití výše uvedených metod v některých oblastech trestné činnosti prakticky nevyužitelná a tam, kde je využitelná, nemusí být dostatek digitálních dat pro další expanzi, se jedná pořád o jednu ze základních metod pro sběr dat v rámci TŘ.

V rámci výzkumu je zcela evidentní snaha policistů o implementací OSINT a SOMINT metod v rámci kriminálních analýz, nebo při dokumentaci objektů zájmu v TŘ. I když většina policistů projevuje snahu, pořád se jedná o amatérkou činnost naučenou z externích anebo neoficiálních neschválených metod zevnitř organizace založenou pouze na metodách tzv. pokus omyl a bez znalosti základních premis teoretické úrovně. Policie ČR v oblasti vnitropodnikového vzdělávaní, se není schopna adaptovat na dynamický vývoj ve společnosti v souvislosti s užíváním ICT a virtuálního prostředí internetu. Metody jsou často zastaralé a lektoři pro vzdělávání v této oblasti jsou často bez praxe a či respektovaného vzdělání. Jediným garantem moderních teoretických základů v oblasti kriminálních analýz je stále policejní akademie ČR. I když vysokoškolské vzdělání z této oblasti, není u PČR vnímáno jako klíčové, je to velká chyba. Jelikož společně s výše uvedenými teoretickými základy moderních metod a vzdělávaní s aplikaci této teorie do praxe formou přednášek z oblasti kazuistiky, mohou vytvářet elitní analytickou základnu se zkušenostmi, která se dokáže sama replikovat vně organizace rekrutováním policistů s praxí a doplněným vzděláním právě z policejní akademie ČR.

Seznam použité literatury

PASEMAN, Floyd L. *A spy's journey: a CIA memoir. St. Paul*. MN: Zenith, 2004. ISBN 978-0-7603-2066-2.

CARL, L. D. *The International Dictionary of Intelligence*. USA: University Press of America, 1993. ISBN 978-1878292032.

KUBECKA, Ch. *Hack the World with OSINT*. Netherland: HypaSec, 2019. ISBN 978-0-9956875-9-2.

GEHL, R. W. *Weaving the Dark Web*. London, England: The MIT Press, 2018. ISBN 978-0-262-03826-3.

PHYTHIAN, M. (ed.). *Understanding the Intelligence Cycle.* USA: Routledge, 2013. ISBN 978-0-203-55847-8.

PICOLET, J. *Operator Handbook*. USA: Netmux LLC, 2020. ISBN 9798605493952.

RUSSELL, M. A., et al. *Mining the Social Web*. 3rd ed. Canada: OREILLY, 2019. ISBN 9781491985045.

TAYEBI, M. A., et al. *Open Source Intelligence and Cyber Crime*. Switzerland: Springer, 2019. ISBN 978-3-030-41251-7.

BAZZELL, M. *Open Source Intelligence Techniques*. 6th ed. Poland: Amazon, 2018. ISBN 978-1984201577.

BAZZELL, M. *Hiding from the Internet.* 3rd ed. USA, 2016. ISBN 978-1522914907.

Pallaris, Ch. Open Source Intelligence: A Strategic Enabler of National Security. CSS Analyses in Security Policy 2008, 32 (3), 1–3.

Datareportal.com [online]. [cit.25.2.2022]. Dostupné z: https://datareportal.com/social-media-users

Datareportal.com [online]. [cit.25.2.2022]. Dostupné z: https://datareportal.com/reports/digital-2021-global-overview-report

Interpol.com [online]. [cit.25.2.2022]. Dostupné z: https://www.interpol.int/content/download/7253/file/27_CAS01_05_2014_EN_web.pdf

Exploit-db.com:Google Hacking Database. [online]. [cit.25.2.2022]. Dostupné z: https://www.exploit-db.com/

GitHub.com [online]. [cit.25.2.2022]. Dostupné z: www.github.com/ElevenPaths/FOCA

GitHub.com [online]. [cit.25.2.2022]. Dostupné z: www.github.com/lanmaster53/recon-ng

Nmap.org [online]. [cit.25.2.2022]. Dostupné z: www.nmap.org

GitHub.com [online]. [cit.25.2.2022]. Dostupné z: www.github.com/laramies/theHarvester

Chainalysis.com [online]. [cit.25.2.2022]. Dostupné z: https://www.chainalysis.com/chainalysis-reactor/

Elliptic.co [online]. [cit.25.2.2022]. Dostupné z: https://www.elliptic.co/solutions/crypto-wallet-screening

Web-iq.com [online]. [cit.25.2.2022]. Dostupné z: https://web-iq.com/solutions

Darkowl.com [online]. [cit.25.2.2022]. Dostupné z: https://www.darkowl.com/products/vision-app/

Hyperids.com [online]. [cit.25.2.2022]. Dostupné z: https://www.hyperids.com/products-solutions

Cognyte.com [online]. [cit.25.2.2022]. Dostupné z: https://www.cognyte.com/web-intelligence/web-intelligence-investigations/#

Palantir.com [online]. [cit.25.2.2022]. Dostupné z: https://www.palantir.com/platforms/gotham/

Blackdotsolutions.com [online]. [cit.25.2.2022]. Dostupné z: https://blackdotsolutions.com/industries/government/

Sociallinks.io [online]. [cit.25.2.2022]. Dostupné z: https://sociallinks.io/industries/leas-and-government

Maltego.com [online]. [cit.25.2.2022]. Dostupné z: https://www.maltego.com/product-features/

Webz.io [online]. [cit.25.2.2022]. Dostupné z: https://webz.io/data-apis/archived-web-data

Kali.org [online]. [cit.25.2.2022]. Dostupné z: https://www.kali.org/features/

Null-byte.wonderhowto.com [online]. [cit.25.2.2022]. Dostupné z: https://null-byte.wonderhowto.com/how-to/use-buscador-osint-vm-for-conducting-online-investigations-0186611/

Tracelabs.org [online]. [cit.25.2.2022]. Dostupné z: https://www.tracelabs.org/initiatives/osint-vm

GitHub.com [online]. [cit.25.2.2022]. Dostupné z: https://github.com/lockfale/osint-framework

Cnbc.com [online]. [cit.25.2.2022]. Dostupné z: https://www.cnbc.com/2018/03/27/palantir-worked-with-cambridge-analytica-on-the-facebook-data-whistleblower.html

Fortune.com [online]. [cit.25.2.2022]. Dostupné z: https://fortune.com/2020/03/04/facebook-a-i-fake-accounts-disinformation/

Getfireshot.com [online]. [cit.25.2.2022]. Dostupné z: https://getfireshot.com/

Nimbusweb.me [online]. [cit.25.2.2022]. Dostupné z: https://nimbusweb.me/screenshot.php

Securityboulevard.com [online]. [cit.25.2.2022]. Dostupné z: https://securityboulevard.com/2020/07/hushpuppi-and-mr-woodbery-bec-scammers-welcome-to-chicago/

Justice.gov: U.S. Department of Justice [online]. [cit.25.2.2022]. Dostupné z: https://www.justice.gov/usao-ndil/press-release/file/1292061/download

Interpol.com [online]. [cit.25.2.2022]. Dostupné z: https://www.interpol.int/News-and-Events/News/2020/INTERPOL-warns-of-organized-crime-threat-to-COVID-19-vaccines (accessed Feb 25, 2022).

iRozhlas.cz [online]. [cit.25.2.2022]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/dansko-prodej-drog-atlayocom-darknet-socialni-sit-zbrane-porno_2007310941_jgr

Policie.cz: Policie České republiky [online]. [cit.25.2.2022]. Dostupné z: https://www.policie.cz/clanek/operace-green.aspx