Policejní akademie České republiky

v Praze

Fakulta bezpečnostně právní

Katedra kriminální policie

Využití zpravodajství z otevřených zdrojů (OSINT) v oblasti národní bezpečnosti – metody, nástroje, případové studie

Diplomová práce

Open Source Intelligence (OSINT) in National Security – Methods, Tools and Case Study

Master Thesis

Vedoucí diplomové práce: doc. JUDr. Ladislav Pokorný, Ph.D.

Vypracoval: Bc. Josef Česal

Praha

2023

Čestné prohlášení

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

V Hrochově Týnci, dne 22. 12. 2023 _____

Poděkování

Mé poděkování patří JUDr. Ladislavu Pokornému, za odborné vedení, podnětné připomínky a cenné rady při zpracování mé diplomové práce.

Anotace

Diplomová práce se zabývá představením zpravodajství z otevřených zdrojů jako nástroje zpravodajského zabezpečení Armády České republiky, představuje vybrané klíčové teoretické koncepty, výhody a nevýhody OSINT a zpravodajského zabezpečení a představuje praktickou aplikaci. Výsledkem praktické aplikace na případové studii je závěr o využívání OSINT v rámci AČR, kde autor dospěl k závěru, na základě stanovených hypotéz, že OSINT je aplikovatelný na taktické úrovni velení a řízení, ale v současné době vykazuje fundamentální nedostatky. V samotném závěru diplomové práce představuje autor oblasti, ve kterých je dosahováno pokroku, nebo naopak kam by se měla zaměřit pozornost odpovídajících funkcionářů.

Klíčová slova

Zpravodajství z otevřených zdrojů, národní bezpečnost, zpravodajský cyklus, sociální média, zpravodajské zabezpečení AČR.

Annotation

This diploma thesis is focused on description of Open Source Intelligence (OSINT) – as Intelligence support tool, and intelligence support, introduces key selected theoretical concepts, pros and cons of OSINT and provide real case study. Result of real case study analysis is conclusion about level of OSINT implementation in to Czech army – OSINT is capable to be fully implemented into Czech army, but currently occurs really serious shortages. In conclusion of this diploma thesis, author introduce areas of rapid improvement, or offer recommendation which areas of OSINT development should be emphasized.

Key Words

Open Source Intelligence, National Security, Intelligence Cycle, Social Media, Army of Czech republic Intelligence support.

Obsah

1. Úvodní a obecná část diplomové práce

1.1. Úvod

Současná problematika národní bezpečnosti, z pohledu Armády České republiky (AČR), nezahrnuje pouze tradiční vojenské hrozby, ale i ty méně tradiční, reagující na dynamicky měnící se bezpečnostní prostředí.

Mezi relativně nové fenomény, jímž musí AČR čelit, patří vedle terorismu, dezinformacím i kybernetická bezpečnost. Při hodnocení rizik tradičních i méně tradičních, je klíčovým nástrojem orgánů zpravodajského zabezpečení zpravodajství z otevřených zdrojů (OSINT - Open Source Intelligence), zahrnující svůj vlastní zpravodajský cyklus (plánování, shromaždování, analýza a šíření).

V současné digitální éře, kdy je přístup k informacím prakticky neomezený, časově relativně nenáročný a finančně výhodný, hraje OSINT klíčovou úlohu. Digitální éra představuje zároveň zvrat ve zpravodajské činnosti a zpravodajském zabezpečení, kdy již hlavním problémem při odstraňování mlhy války (Fog of War – mentální konstrukt označující nejistotu a informační mezeru) není nedostatek informací, nýbrž jejich správné ohodnocení, analýza a interpretace.

Analytici se musí vyrovnat se značnou mírou klamání a matení zejména na zdrojové straně, kdy jednání protivníka, nepřítele je pouze jednou z možných příčin (ne)úmyslné úpravy reality. Tento fenomén se projevuje zejména při analýze sociálních sítí, ale stále častěji i čerpání z online verzí zavedených informačních zdrojů, vlivem enormního tlaku na rychlost a stručnost dochází k informační devalvaci tradičních zdrojů. Výše uvedené zvyšuje tlak na lidský kapitál, jejich soustavnou přípravu a supervizi výstupů činnosti.

Na taktické úrovni systému velení a řízení prostupuje OSINT prakticky všemi činnostmi zpravodajského zabezpečení, jak v rámci zpravodajské přípravy bojiště (IPB - Intelligence Preparation of Battlefield) tak i v rámci zpracování tematických zpravodajských informací z prostoru zpravodajského zájmu

a odpovědnosti. Jako taková představuje nosnou schopnost zpravodajských štábů.

V další části úvodu bude proveden popis jednotlivých částí diplomové práce. Úvodní část stanovuje cíl práce, výzkumnou otázku a s ní související hypotézy, jež budou následně verifikovány. Práce pokračuje představení použitých metod a rešerší dostupné literatury, zahájené v rámci přípravy analytické části tvorby diplomové práce.

Hlavní část diplomové práce je rozdělena do tří kapitol seznamující čtenáře postupně se zpravodajstvím z lidských zdrojů, zpravodajským zabezpečením v Armády České republiky (ZZ AČR) a následně ohledně využití OSINT prováděného zpravodajským zabezpečením AČR v kontextu národní bezpečnosti.

Závěrečná část je koncipována jako zevšeobecněná analýza případové studie a její reálných analogií. Konkrétní výstupy, nemohly být publikovány z důvodu ochrany „need-to-know“, přesto autor pevně doufá, že generalizované výsledky přispějí k porozumění problematiky této diplomové práce.

1.2. Cíl diplomové práce, omezení a použité metody

Cílem diplomové práce je představení zpravodajství z otevřených zdrojů jako jeden z nástrojů zpravodajského zabezpečení, seznámení s vybranými metodami a nástroji, a to v rámci teoretického kontextu a následně objasnit využití OSINT na konkrétní a reálné situaci. Vychází z předpokladu, že zpravodajské zabezpečení je nedílnou součástí složek moci státu. Součásti je konstatování o přínosech OSINT jako takového.

K dosažení dílčího cíle diplomové práce byla stanovena následující výzkumná otázka:

„*Je OSINT aplikovatelný v rámci zpravodajského zabezpečení na taktickém stupni velení a řízení?*“

Následně byly stanoveny hypotézy, jejichž zamítnutím, případně verifikací, lze zodpovědět výzkumnou otázku,

H1: AČR disponuje adekvátní strukturou zpravodajských orgánů na taktickém stupni.

H2: Zpravodajský obor zpravodajství z otevřených zdrojů poskytuje požadované výstupy aplikovatelné na taktickém stupni velení a řízení AČR.

H3: Nástroje OSINT jsou uplatnitelné v rámci zpravodajského zabezpečení AČR.

Diplomová práce se omezuje na část složky nástrojů moci[1] státu, konkrétně na zpravodajské zabezpečení AČR, v rámci zajištění národní bezpečnosti na taktickém stupni velení a řízení. V rámci ZZ se zaměřuje na využití zpravodajství z otevřených zdrojů. Další omezení vyplývá z citlivosti údajů a ochraně utajovaných informací o struktuře zpravodajských štábů AČR a náplni jejich činnosti, se kterými je autor důvěrně obeznámen, proto v rámci diplomové práce budou použity pouze obecná konstatování a tvrzení.

1.3. Rešerše dostupné literatury

Při tvorbě rešerše dostupné a relevantní literatury bylo postupováno následovnými postupy:

a) Studiem doktrinální struktury Severo Atlantické Aliance (NATO – North Atlantic Treaty Organization), řada AJP-2 a Armády České republiky.
b) Využití vyhledávacích dotazů s použitím klíčových slov: Zpravodajství z otevřených zdrojů, národní bezpečnost, zpravodajský cyklus, sociální média, zpravodajské zabezpečení AČR a jejich anglickými ekvivalenty.

V rámci formulací rešeršních dotazů byly využity operátory. Zpravodajství z otevřených zdrojů, národní bezpečnost, zpravodajský cyklus, sociální média, zpravodajské zabezpečení AČR. Výsledky vyhledávání byly omezeny jazykově (angličtina, čeština), teritoriálně a následně filtrovány dle aktuálnosti.

První kategorii jsou alianční vojenské dokumenty (vojenské doktríny nižších řádů, programy příprav jednotek AČR a slovník pojmů), druhou kategorii pak tvoří monografie a elektronicky dostupné zdroje. Citace informačních zdrojů spadajících do druhé kategorie jsou zapsány podle normy ISO ČSN 690:2011.

[1] DIME – diplomatic, information, military and economic

Doktrinální soustava NATO v oblasti zpravodajství[2]:

1. AJP-2 Spojenecká společná doktrína zpravodajství, kontrazpravodajství a bezpečnosti
2. AJP-2.1 Spojenecká společná doktrína zpravodajských postupů, přejata standardizační dohodou STANAG 2190.
3. AJP-2.7 Spojenecká společná doktrína společného zpravodajství, průzkumu a sledování, přejata standardizační dohodou STANAG 2191.
4. AJP-2.9 Spojenecká společná doktrína zpravodajství z otevřených zdrojů, přejata standardizační dohodou STANAG 6522.

Doktrinální soustava AČR[3]

1. Doktrína zpravodajského zabezpečení v AČR (Pub-20-63-01)
2. Programy přípravy jednotek AČR (Prog-1-3)
3. Programy přípravy jednotek AČR – 1. doplněk platný od 1.1.2020 (Pub-70-01-01)
4. Slovník základních pojmů z oblasti zpravodajského zabezpečení v AČR (Pub-20-00-02)

Bibliografické zdroje

1. AKHBAR, Babak, BAYERL, Saskia, SAMPSON, Fraser (Eds.). Open Source Intelligence Investigation. From Strategy to Implementation. Springer, 2016. ISBN 978-3-319-47671-1.
2. BAZZELL, Michael. *Open Source Intelligence Techniques. Resources for Searching and Analyzing Online Information.* 9. vyd. 2022. ISBN 9798761090064.
3. BORN, H., LEIGH, I. Making Intelligence Accountable – Legal Standards and Best Practice for Oversight of Intelligence Agencies, DCAF Handbook, 2005, ISBN 978-92-9222-017-4.
4. CLARK, R., M. Intelligence Analysis, a target Centric Approach, CQ Press, 2013, ISBN 978-1-4522-0612-7

[2] Struktura obsahuje pouze platné a pro AČR závazné dokumenty, zdrojem dat je vnitřní informační systém ADMIS

[3] Výběr dokumentů ve vztahu ke zpravodajskému zabezpečení, řešící problematiku OSINT.

5. KENT, S. Strategic Intelligence for American World Policy. Pp. xiii, 1949. LOWENTHAL, M. M. Intelligence. From Secrets to Policy. CQ Press, Washington, D.C., 2000.
6. MICHÁLEK, L., POKORNÝ, L., STIERANKO, L. a MARKO, M. Zpravodajství a zpravodajské služby. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2013. ISBN 978-80-7380-428-2.
7. PAPÍK, Richard. *Strategie vyhledávání informací a elektronické informační zdroje*. 1. vyd. Praha: Velryba, 2011. ISBN 978-80-85860-22-1.
8. POKORNÝ, L. Zpravodajské služby. Praha: Auditorium, 2012. ISBN 978-80-87284-21-6.
9. RAMWELL, S., DAY, T., GIBSON, H. Use cases and Best practice for LEAs. In Akhgar, B., Bayerl, P. S. & Sampson, F. (Ed.). Open Source Intelligence Investigation: From strategy to implementation. 2016
10. SCHULSKY, Abram. N., SCHMIDT, Gary. J. Silent Warfere, Understanding the World of secret Intelligence, third edition, Washington D.C., 2002.
11. STEELE, R. D. Open Source Intelligence, Handbook of Intelligence, ed. Loch K. Johnson, New York: Routledge, 2007, ISBN10 0-415-77050-5, s. 129–147.
12. WEHMEIER, S., MC´INTOSH, C., TURNBULL, J. Oxford Advanced Learner´s Dictionary of Current English, 7 edition, Oxford, English 2005. ISBN 0-19-431649-1.

Internetové zdroje

1. BIELSKA, Aleksandra. *Open Source Intelligence Tools and Resources Handbook.*
I-INTELLIGENCE, 2020. [online]. [22. 12. 2023]. Dostupné z: https://documentsn.com/document/158a_open-source-intelligence-tools-and-resources-handbook.html.
2. BURKE, C. Freeing knowledge, telling secrets:Open Source Intelligence and development, CEWCES Research Papers, Paper 11, s. 1-22. [online]. [22. 12. 2023] Dostupné

z: https://pure.bond.edu.au/ws/portalfiles/portal/28737919/Freeing_knowledge_telling_secrets.pdf

3. CASANOVAS, Pompeu Juan ARRAIZA, Felipe MELERO, Jorge GONZÁLEZ – CONEJERO, Gila MOLCHO, Montse CUADROS. *Fighting Organized Crime Through Open Source Intelligence: Regulatory Strategies of the CAPER Project.* [online]. [12. 4. 2021]. Dostupné z: https://core.ac.uk/download/pdf/78532664.pdf.
4. STROUHALOVÁ, J. Vybrané trendy globální bezpečnosti. [online]. [29. 12. 2020]. Dostupné z: https://www.valka.cz/14431-Vybrane-trendyglobalni-bezpecnosti

1.4. Definice a vymezení pojmů

Bezpečnost

Pojem bezpečnost není jednotně ukotven a je úzce spjat i ve vztahu s posuzovanou entitou (člověk, firma, stát, …), V odborné literatuře lze nalézt pozitivní i negativní definici. V případě negativní definice se hovoří o bezpečí jako o stavu absence nebezpečí a ohrožení.

V roce 2002, v rámci České bezpečnostní terminologie, byla bezpečnost definována jako: *„stav, kdy jsou na nejnižší možnou míru eliminovány hrozby pro objekt (zpravidla národní stát, popř. i mezinárodní organizaci) s jeho zájmy a tento objekt je k eliminaci stávajících i potenciálních hrozeb efektivně vybaven a ochoten při ní spolupracovat".*[4]

Bezpečnost je definována Slovníkem základních pojmů z oblasti zpravodajského zabezpečení v AČR[5] jako: „*Stav dosažený v případě, kdy určené informace, materiál, personál, aktivity a zařízení jsou chráněny proti terorismu, špionáži, rozvratným akcím, sabotážím a organizovanému zločinu, stejně jako proti ztrátě a neoprávněnému prozrazení".* Tato definice je tak v souladu s vymezením uvedeném v AJP-2.

Z pohledu taxonomie lze rozlišit celou řadu dopřesňujících pojmů, souvisejících s bezpečností, například vnitřní a vnější, národní, mezinárodní a globální.

Národní bezpečnost

Pojem národní bezpečnost vymezuje obecnější pojem „bezpečnost". V souvislosti z národní bezpečnosti se nejčastěji uplatňuje negativní definování jako *„absence bezpečnostní hrozby a rizika".* Z tohoto vymezení lze tedy odvodit, že stát/národ je bezpečný, pokud nejsou ohroženy jeho základní atributy, hodnoty a myšlenky, na nichž je založen. Takovéto vymezení by bylo, v případě státu, ale nedostatečné vzhledem k výzvám a hrozbám, jímž je na mezinárodním globalizovaném poli vystaven. Proto autoři přichází z do přesněním, kdy je stát

---

[4] ZEMAN, P., a kol. Česká bezpečnostní terminologie: *Výklad základních pojmů*. Masarykova univerzita Brno, Mezinárodní politologický ústav, 2002, 1. vyd., s. 13, ISBN 80-210-3037-2

[5] AČR. Pub-20-00-02, *Slovník základních pojmů z oblasti zpravodajského zabezpečení v AČR*. 2. vyd., s. 10

schopen hrozbu a riziko eliminovat. Rozdílný je dále i konečný stav, kdy se mluví o stupnici od „nepředstavuje existenční ohrožení“, přes „zachování základních funkcí státu“ až po „zajištění běžného života“

V realistickém přístupu mezinárodních vztahů, je národní bezpečnost klíčový prvek k udržení a posílení své moci a obsahuje i ochranu vlastních zájmů, které nutně nemusí být u výše uvedených vymezení obsaženy.

AČR na taktickém stupni velení a řízení využívá OSINT jako nástroj pravidelného monitoringu médií a vyhledávání konkrétních informací. V neposlední řadě je využíván jako prvotním zdrojem získávání údajů a informací a je zároveň doplňujícím zdrojem k informacím.

Za účelem zajištění národní bezpečnosti vytváří stát komplexní bezpečnostní systém, zahrnující koncepční dokumenty (Bezpečnostní strategie ČR, Obranná strategie ČR, etc.) a bezpečnostní entity státu[6].

OSINT

Open Source Intelligence se definuje jako proces shromažďování, zpracování a analýzy informací z veřejně dostupných zdrojů s cílem získat relevantní, aktuální a užitečné informace pro podporu rozhodování a pochopení aktuálního stavu událostí.

Slovník základních pojmů z oblasti zpravodajského zabezpečení v AČR[7] definuje OSINT jako: „*zpravodajská informace získaná z veřejně dostupných informací jakož i z dalších neutajovaných informací, jež jsou omezeně publikovány či zpřístupňovány“.*

OSINT je klíčovým zdrojem vstupů do procesu společné zpravodajské přípravy operačního prostředí (JIPOE – Joint Intelligence Preparation of Operational Environment) nebo zpravodajské přípravy bojiště. OSINT tak například napomáhá k lepšímu porozumění operačního prostředí ze strany velitelů,

[6] Pojem byl použit pro souhrnné označení všech aktérů bezpečnostního systému a zahrnuje i mimo jiné ozbrojené síly, bezpečnostní sbory, zpravodajské služby etc.

[7] AČR. Pub-20-00-02, *Slovník základních pojmů z oblasti zpravodajského zabezpečení v AČR*. 2. vyd., s. 149

odpovědí na požadavky na informace a k podpoře tvorby dalších zpravodajských výstupů.

Veřejně dostupné zdroje

„Informace z otevřených zdrojů, které zahrnují jakýkoliv materiál zveřejněný nebo vysílaný pro použití širokou veřejností; dostupný na vyžádání komukoli ze široké veřejnosti; dostupný veřejnosti online nebo off-line. Jsou tvořeny údaji, které byly shromážděny obvykle s využitím redakčního procesu, který zajišťuje určité filtrování a validaci, ale také řízení prezentace těchto informací“[8]*.*

Sociální média

AJP-2.9 vymezuje sociální média jako *„interakci jednotlivců v rámci které si osoby sdílejí a vyměňují informace v prostředí virtuálních komunit“.*[9]

Tato obšírná definice zahrnuje sociální sítě využívající internet nebo další telekomunikační služby umožňující osobám vytvořit si profil (veřejný, polo veřejný), definovat seznam uživatelů, se kterými sdílí informace a získat přístup k profilu dalších uživatelů. Mezi globálně nejrozšířenější je zajisté Facebook, TikTok a Instagram. Dále do této kategorie spadají blogy, profesní sítě a sdílení audio-vizuálního materiálu.

Pro zpravodajské účely je nezbytné provézt analýzu cílové skupiny těchto sociálních sítí, protože jejich obliba je generačně diferenciovaná.

Analýza sociálních médií je do značné míry zatížena nekontrolovatelnými náhodnými zdroji s prokazatelným pokřivením objektivní reality na základě cíle, postojů, zkušeností a názoru autora. Sociálně sítě jsou vhodným prostředím pro automatizované a záměrné šíření desinformací a propagandy. Jejím cílem je identifikace síťových uzlů a jejich vzájemných vztahů. Při analýze se uplatňují multidisciplinární znalostí analytiků zejména z oblasti sociálních, matematických, antropologických věd, pokročilých znalostí strojového učení a principu fungování sociálních sítí a internetu.

---

[8] NATO. AJP-2.9, *Spojenecká společná doktrína zpravodajství z otevřených zdrojů*. A. Úřad pro standardizaci, 2019., s. 1-2

[9] NATO. AJP-2.9, *Spojenecká společná doktrína zpravodajství z otevřených zdrojů*. A. Úřad pro standardizaci, 2019., s. 1-3

Zdroj

„Ve zpravodajském kontextu člověk nebo věc, od kterých mohou být získány informace. Zdroj je tedy primárním nositelem informace (disponuje jí, nebo se o ní dozvídá v důsledku své činnosti), který ji nezpracovává ani samostatně nepředává“[10]

Práce se zdroji je základním předpokladem pro efektivní zpravodajskou činnost.

Zpravodajský cyklus

Zpravodajský cyklus je myšlenkový konstrukt zaužívaný v teorii zpravodajství. Odborná literatura, definuje zpravodajský cyklus jako:

1. *„Řetězec činností, při nichž jsou informace získávány, shromaždovány, zpracovávány do formy zpravodajské informace a dány k dispozici uživatelům. Tento řetězec je složen ze čtyř fází. Řízení, shromaždování, zpracování a distribuce“.*[11]
2. *„Nepřetržitý sled postupných, vzájemně navazujících a cyklicky se opakujících činností a procesů, při nichž jsou informace získávány, shromažďovány, zpracovávány do formy zpravodajských informací a distribuovány oprávněným uživatelům. Zpravodajský cyklus vyjadřuje proces realizace zpravodajské činnosti. Fázemi zpravodajského cyklu jsou: řízení, shromaždování, zpracování a šíření“-*[12]

Zpravodajský cyklus bývá používán k popisu procesního modelu zpravodajské činnosti a zpravodajského zabezpečení, nicméně moderní trendy přístupu ke zpravodajství, jako například „Target Centric Approach“[13] vnímají zpravodajský cyklus jako popis struktury[14] generického zpravodajského orgánu.

---

[10] AČR. Pub-20-00-02, *Slovník základních pojmů z oblasti zpravodajského zabezpečení v AČR*. 2. vyd., s. 145

[11] NATO. AJP-2.9, *Spojenecká společná doktrína zpravodajství z otevřených zdrojů*. A. Úřad pro standardizaci, 2019., s. 2-1

[12] AČR. Pub-20-00-02, *Slovník základních pojmů z oblasti zpravodajského zabezpečení v AČR*. 2. vyd., s. 151

[13] CLARK, R., M. Intelligence Analysis, a target Centric Approach, CQ Press, 2013, ISBN 978-1-4522-0612-7

[14] CLARK, R., M. Intelligence Analysis, a target Centric Approach, CQ Press, 2013, ISBN 978-1-4522-0612-7

Autor této práce usuzuje, že hlavním přínosem dalšího využívání tohoto přístupu, spočívá v edukativní činnosti a objasnění činnosti zpravodajských orgánů.

Zpravodajské zabezpečení

Pod pojmem zpravodajské zabezpečení v AČR se rozumí: *„Soubor schopností, činností, procesů, systémů, personálu a úkolů za účelem tvorby požadovaných zpravodajských informací pro podporu rozhodovacích procesů velitelů a štábů AČR, které je realizováno v pěti oblastech: zpravodajství, sledování a průzkum, elektronický boj, geografické zabezpečení a hydrometeorologické zabezpečení.“*[15]

Tento pojem byl zaveden v rámci delimitačního procesu s Vojenským zpravodajstvím realizujícím zpravodajskou činnost.

Principy zpravodajského zabezpečení jsou dostupnost, sdílení, utajení, iniciativa, flexibilita, interoperebilita a komplexnost.

[15] AČR. Pub-20-00-02, *Slovník základních pojmů z oblasti zpravodajského zabezpečení v AČR*. 2. vyd., s. 151

2. Hlavní část diplomové práce

2.1. Zpravodajství z otevřených zdrojů

2.1.1. Úvod

Zpravodajství z otevřených zdrojů je zavedeným zdrojem zpravodajských informací s dlouhou tradicí ve zpravodajské činnosti. OSINT poskytuje informace s potenciální zpravodajskou hodnotou, jež jsou dostupné široké veřejnosti.

OSINT je nezávislá disciplína shromažďování zpravodajských informací, přispívající k naplnění zpravodajských požadavků, zejména pak v oblastech doplnění či potvrzení informací z jiných zdrojů, pro doplnění kontextu.

V moderním operačním prostředí jsou nezbytné informace nejen o potenciálních vojenských prostředcích a záměrech protivníka, ale také o společenském prostředí (kultura, vnímání událostí, motivace. Právě na tyto aspekty je nejvhodnější využití OSINT. OSINT je také klíčovým vstupem do procesu společné zpravodajské přípravy operačního prostředí, při hodnocení elementů operačního prostředí: politický, ekonomických, společenský element, infrastruktura a informace.

OSINT využívá úplný zpravodajský cyklus v podobě systematického shromažďování, zpracování, využívání a distribuce (CPED – collect, process, exploit, disseminate). Odlišnost OSINT od průzkumu veřejně dostupných informací spočívá v aplikaci zpravodajského procesu vycvičenými analytiky s cílem naplnit zpravodajské požadavky pro potřeby velitele.

Svojí charakteristikou se řadí mezi zdrojovou část, k jejíž činnosti se využívá mluvený a psaný záznam – tedy nástroje lidské komunikace. Mluví se zde o takzvané „literal intelligence“[16]- LITINT[17]. Zavedení pojmu OSINT nepředstavuje pouhé přejmenování, nýbrž v sobě zahrnuje potenciální zdroje dostupné díky vysoké míře globální informatizace a digitalizace. Hlavním hybatelem bylo bezprecedentní rozšíření internetu, díky čemuž do kategorie

[16] Dále se do této kategorie řadí HUMINT – zpravodajství z lidských zdrojů, COMINT – komunikační zpravodajství a shromažďování informací z kybernetické domény

[17] LITINT je zastaralý pojem zahrnující potenciálně zpravodajsky přínosné zdroje informací z veřejně dostupných a publikovaných zdrojů, jako například noviny, knihy a periodika.

OSINT spadají i fotografie, infografiky, texty, databáze a texty publikované online.

Z pohledu teorie mezinárodních vztahů, zejména v realistickém přístupu[18], představuje OSINT důležitou roli při sledování a shromažďování informací o ostatních státech. OSINT poskytuje státům možnost získat otevřeně dostupné informace, které mohou být klíčové pro hodnocení bezpečnostních hrozeb a rizik, monitorování vojenských aktivit a posilování strategického postavení.

Analýzou otevřených zdrojů může bezpečnostní aktér získat náhled na plány, záměry a aktivity ostatních aktérů na mezinárodní scéně. OSINT může být využíván k posílení informační nadvlády.

Díky relativní snadnosti k přístupu, široké dostupnosti a množství nákladově dostupných informací, se OSINT stal velmi užitečným startovacím nástrojem zpravodajské analýzy. Přesto, či spíše právě proto, je OSINT mnohdy považován za méně vypovídající zdroj informací, než jiné utajované a více nákladné zdroje[19]

Dle Vondrušky[20] existují dva základní rozdílné přístupy k OSINT. Prvním je cílený OSINT a druhý je plošný, které se liší svým určením a zaměřením.

Cílený OSINT se zaměřuje vyhledávání konkrétních relevantních informací. Využití cíleného OSINTU je například tvorba rešerší, vyhledávání informací o osobách nebo úvodní fáze penetračního testování.

Plošný OSINT představuje automatizované vyhledávání a zpracování velmi rozsáhlého objemu dat, která jsou následně analyzována. Tyto informace mohou posloužit například k monitorování vývoje bezpečnostní situace v prostoru

---

[18] Realismus v mezinárodních vztazích zdůrazňuje státní suverenitu, racionální jednání států ve vlastním zájmu a soutěživost mezi nimi v anarchickém mezinárodním systému. Moc je klíčovým prvkem, a státy se snaží maximalizovat svůj prospěch bez ohledu na morální hodnoty

[19] JOHNSTON, Rob. *ANALYTIC CULTURE IN THE US INTELLIGENCE COMMUNITY*. Online. Center for the Study of Intelligence, 2005. Dostupné z: https://www.cia.gov/static/Analytic-Culture-Intelligence-Community.pdf. [cit. 2024-01-11]., s.24

[20] VONDRUŠKA, Petr. Metody a nástroje OSINT. Diplomová práce. Praha: Bankovní institut vysoká škola Praha, 2013., s.12

zájmu. Uplatnění nalezne například pro systémy pro monitoringu médií nebo analýzy sociálních sítí.

V AČR se OSINT využívá v souladu s postupy popsanými v AJP-2.7 a AIntP-14.

2.1.2. OSINT v systému zpravodajského zabezpečení

OSINT je klíčovým přispěvatelem do procesu společné zpravodajské přípravy operačního prostředí, kdy prostřednictvím metodiky hodnocení operačních proměnných (PMESII – political, military, economic, social, infrastructure and information) přispívá k lepšímu porozumění operačnímu prostředí, systematickou činností naplňuje požadavky na informace (IR – Information Requirements) a vytváří tipy a podměty pro další disciplíny shromažďování informací.

V neposlední řadě podporuje:

- Aktuální zpravodajství: zlepšuje povědomí o situaci díky širšímu pokrytí a aktuálnosti informací
- Zpracování výchozích zpravodajských operací: všeobecné informace o vedení, bezpečnosti, vojenských prostředcích, terorismu, případných zbraní hromadného ničení, mezinárodních vztazích, demografii, klimatu aj. týkající se zájmové oblasti ke komplexnímu pochopení operačního prostředí. Právě zde je hlavní uplatnění OSINT v systému ZZ v AČR.
- Podporuje psychologické operace: přispívá informacemi o kultuře, hodnotách, záměrech a možnostech ovlivnění cílových skupin. Příkladem jsou informace a hlášení popisující cílovou skupinu z hlediska relevantních aktérů a jejich vnímání
- Podporuje analýzu trendů a hodnocení měřítek efektivity, pochopením dopadů faktorů PMESII z pohledu vlastních sil i protivníka.
- Podpora tvorby alternativních scénářů.

Na taktické úrovni přináší zpravodajství z otevřených zdrojů největší přínosy v rámci obecných zpravodajských činností.

Hlavní zásady činnosti OSINT jsou uvedeny v dokumentu MC 0647 – POLICY ON OPENSOURCE INTELLIGENCE (OSINT). Dále se řídí následujícími obecně platnými zásadami:

- Zaměření: činnost musí být realizována v souladu s Plánem shromažďování informací, jako součást nezdrojového zpravodajství. Jako takové se zaměřuje na odpovědi na zpravodajské požadavky velitelů.
- Dodržování předpisů: Analytici NATO jsou povinni dodržovat veškerá platná zákonná omezení, autorská a licenční práva a to vždy s přihlédnutím k platné národní legislativě.
- Efektivita: vzhledem k vysokému riziku informačního zahlcení a duplování informací, k jejich objemnosti je nutné, aby OSINT poskytoval nezdrojovým analytikům pouze relevantní informace k zabezpečení efektivní činnosti.
- Hodnocení zdrojů: Nezbytným krokem je ověření pravdivosti a platnosti uvedených informací. Tyto informace musí být pravidelně a průběžně vyhodnocovány v souladu se zavedenými postupy a k přístupu k datům a informacím musí být uplatňován obzvláště kritický přístup.
- Dostupnost: Analytikům by měl být zabezpečen přístup k co nejširšímu spektru materiálů, včetně placených. Omezení zdrojové báze neúměrně zvyšuje riziko využití zaujatých informací.

Zdrojovou část OSINT můžeme, při značné míře zjednodušení, rozdělit na tři základní typy zdrojů, které se následně upřesňují:

a) Online

Nejrychleji se rozšiřující zdroj neutajovaných dat a informací, v široké škále kvality a využitelnosti. Udržování přehledu o relevantních zdrojích dat se stává činností na plný úvazek a bez podpory moderních technologií se jedná takřka o neřešitelný úkol. Moderní technologie jsou uplatnitelné zejména při zpracování a následné prezentaci analyzovaných dat, lidských faktor však zůstává nenahraditelný v oblasti interpretace informací, kde se uplatňují zkušenosti a osobní kvality analytika (empatie, kulturní znalost prostředí, aj.).

Nezbytnou součástí je důsledné hodnocení zdroje, v souladu se zpravodajskými postupy.

b) Tištěné

Některé materiály vhodné pro zpravodajství z otevřených zdrojů, stále nejsou k dispozici na celosvětové síti internet a nalézají se pouze v knihovnách komerčních databázích. Jako hodnotné tištěné zdroje jsou nejčastěji uváděny noviny, monografie, patenty a technická literatura.

c) Šedá literatura

Samostatným druhem je takzvaná „šedá literatura“, jejíž využití v rámci OSINT je předmětem odborných a legislativních diskusí. Pod pojmem šedá literatura se rozumí dokumenty, s omezeným přístupem a vnitřním stupněm utajení, tedy nikoli dle zákona č.219/1999 Sb., o ochraně utajovaných informací a jejích obdobě. Jinými slovy se jedná o neutajované informace, které však nejsou komerčně dostupné. Jedná se zejména o pracovní verze dokumentů, technické zprávy a normativní dokumenty. Z pohledu autorství by se mělo jednat o entity, jejichž hlavní náplní práce není publikační činnost.

Nicméně tyto citlivé materiály se mohou omylem dostat do depozitářů knihoven, být distribuovány v rámci odborných konferencí. Tato literatura se nachází i online, zejména pak na webových stránkách a chatovacích místnostech, zabezpečených heslem. Případné využití je již nutné koordinovat i v rámci shromažďování v kybernetickém prostoru, neboť je nutné překonat překážku (heslo) a tím může dojít k činnosti mimo OSINT.

Zdroje jsou kategorizovány následovně:

- Řízené: zdroje jsou pod kontrolou zpravodajského orgánu a lze jim přímo zadávat úkoly. Z pohledu OSINT se jedná o zdroje, kdy úkolování je dovolenou v rámci limitu smluv nebo podmínek předplatného. Jedná se například o akademické zdroje, think tanky a v jisté podobě i komerční subjekty.
- Neřízené: zdroje nelze přímo řídit a úkolovat. Jedná se o nejčastější typ zdroje v rámci OSINT. Jedná se o zavedená média, webové stránky

a případně zveřejňované dokumenty (například smlouvy, technické specifikace)

- Příležitostné: Nevyžádané informace, představující největší riziko, mimo jiné i z důvodu absence historie zdroje. Někteří teoretici zařazují příležitostné zdroje mezi neřízené zdroje.

Specifickými zdroji dat a informací jsou například zvláštní typy internetových stránek

- Deep web obsah nedostupný prostřednictvím běžných vyhledávacích nástrojů. Jedná se o privátní stránky, vyžadující registraci/přihlášení před získáním přístupu. Zpravidla využívají dynamický obsah, který znesnadňuje pohyb bez znalosti domény, kterou jsou generovány.
- Dark web jsou stránky veřejně viditelně, ale skrývající IP adresu serverů. Jedná se o součást „Deep webu“, která byla úmyslně skryta a není dostupná prostřednictvím většiny webových prohlížečů. Často využívají šifrované sítě, vyžadující specifický software, konfiguraci a oprávnění.
- Sociální média a sociální sítě se staly velmi důležitým a hodnotným zdrojem informací, proto se v poslední době hovoří o zpravodajství ze sociálních médií[21] (SOCMINT – Social Media Intelligence). Prostředí sociálních sítí se vyznačuje pozměněnými společenský akceptovatelnými normami, svébytným jazykem. Jedná se o přínosný zdroj informací ohledně politických, psychologických a sociálních vlivů napříč globálně digitalizovaným světem. Jedná se o vhodný prostor pro výskyt extrémistických a teroristických skupin, kde mohou rychle a relativně snadno propagovat svojí ideologii, verbovat nové příslušníky nebo být nástrojem komunikace.

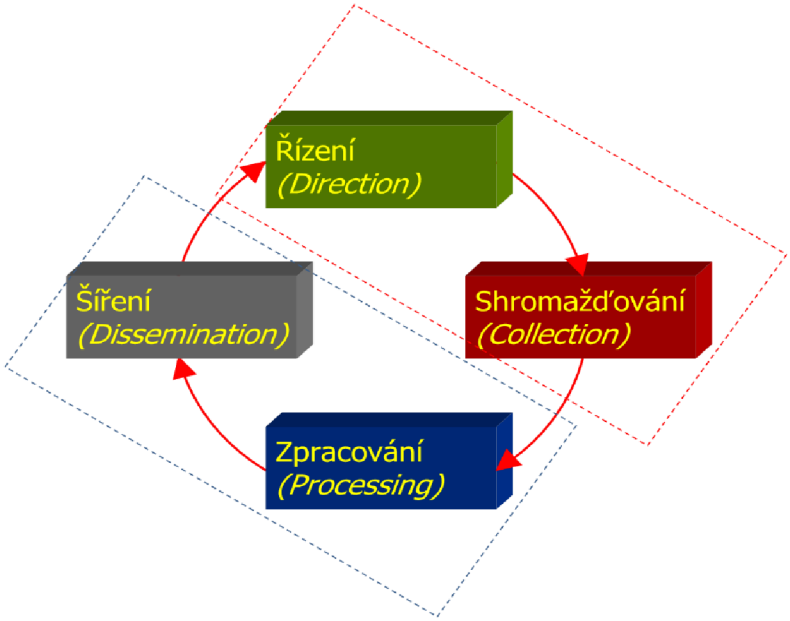
Z pohledu formy lze OSINT rozlišit na aktivní a pasivní. Pasivní forma OSINTU zjednodušeně představuje studium informací největších zpravodajských portálů a stanic, sledování populárních uživatelů na sociálních sítích.

[21] Charakter spadá do shromažďování, nicméně v AČR není považována za zpravodajský obor. Je vnímána jako podoblast zpravodajství z otevřených zdrojů.

Na druhé straně aktivní přístup k OSINT zahrnuje nejen aktivní přístup k hledání a zajišťování dostupných zdrojů dat a informací, aktivně využívá zdrojů s omezeným přístupem (nutná registrace, z důvodu bezpečnosti však nejsou použité soukromé účty, zjištěná data jsou katalogizována a následně archivována.

OSINT a zpravodajský cyklus

Zpravodajský proces je myšlenkový konstrukt hojně používaný v AČR

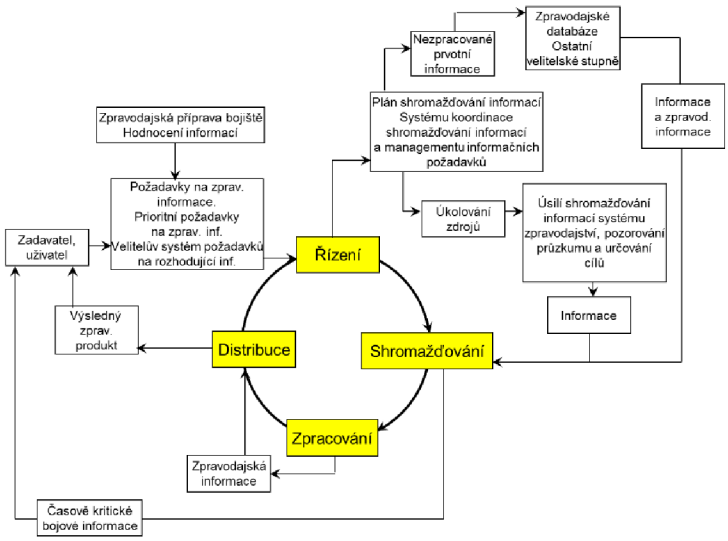


Obrázek 1: Zpravodajský cyklus

k procesnímu popisu a vizualizaci zpravodajského zabezpečení. Skládá se ze 4 hlavních, vzájemně ovlivněných, fází. Jednotlivými fázemi je plánování, shromaždování, zpracování a šíření. Tyto fáze jsou založeny na managementu zpravodajských požadavků (IRM – Intelligence Requirements Management) a managementu shromažďování informací (CM – Collection Management). IRM a CM tak zabezpečí včasné a efektivní fungování zpravodajského cyklu.

Mnohdy se pojem „Zpravodajský cyklus“, pro zjednodušení, znázorňuje kružnicí o 4 částech ve vnitřním kruhu, vnější kruh je pak tvořen zpětnou vazbou. Toto znázornění je pak využíváno jako charakteristika zpravodajského zabezpečení, což evokuje mylnou představu o cykličnosti celého procesu.

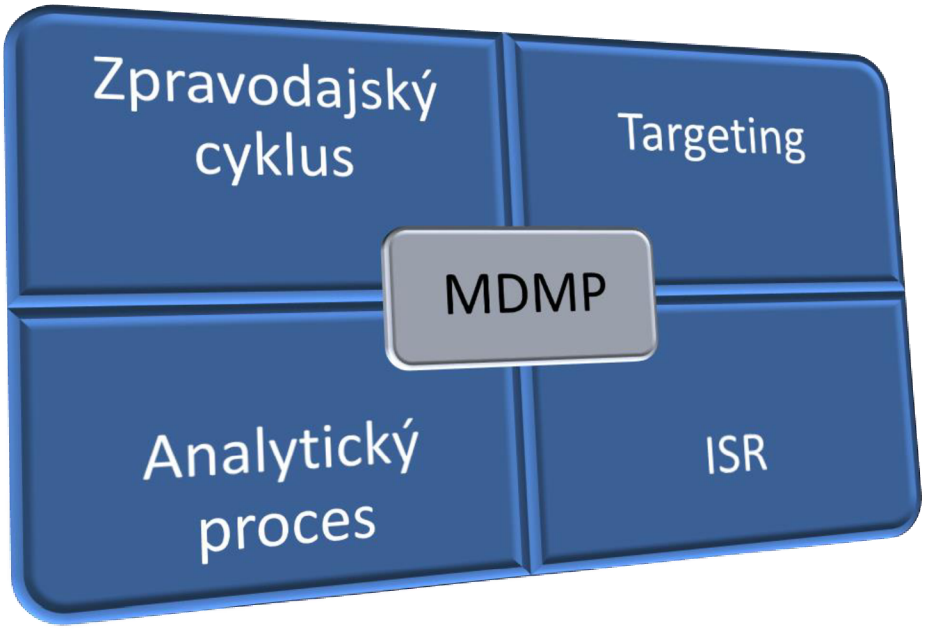
Označení zpravodajský cyklus je matoucí. Procesy, jež zpravodajský cyklus popisuje, nemají jednoduché vztahy, jak je zobrazeno na obrázku, naopak vzájemná provázanost, zpětnovazební vztahy, souběžnost i několika fází, nepřetržitá aktualizace a zároveň striktní oddělení. Takováto charakteristika by byla pro lidský mozek velmi obtížně pochopitelná, neboť popisuje zpravodajský cyklus jako lineární procesy, nicméně lidský mozek a zpravodajská realita nejsou v žádném případě lineární, proto se využívá myšlenkového konstruktu „Zpravodajské cyklu“, který umožňuje snazší interpretaci a představu o obecném a komplikovaném pojmu.



Obrázek 2: Zpravodajský proces dle zpravodajského cyklu

Realitu nadále komplikuje skutečnost, kdy zpravodajský cyklus je zasazen do procesu plánování velitele (plánování ale i vedení bojové přípravy, nezřídka kdy, však předchází těmto fázím), ale i zákazníka a v rámci něhož probíhá řada vnitřních procesů a cyklů (analytický, targeting, zpravodajství, sledování a průzkum …).

Přestože zpravodajský cyklus je definován procesním způsobem, stále více zpravodajských praktiků se přiklání ke strukturálnímu výkladu, tedy tvrdí, že zpravodajský cyklus spíše popisuje strukturu zpravodajských orgánů a štábů.



Obrázek 3: Provázanost cyklů

Kritikové takovéhoto vnímání zpravodajského cyklu nejčastěji poukazují na následující „nedostatky“:

Silně formalizovaný proces, snadno předvídatelný tím pádem snadno zranitelný pro protiopatření.

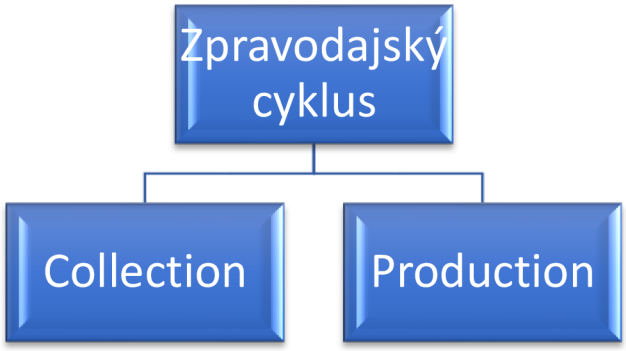
- Minimální zatažení zákazníka do zpravodajského procesu,
  - striktní oddělení zdrojů, analytiků a klienta,
  - malý prostor pro zpětnou vazbu, obzvláště mezi šířenými produkty a potřebami klienta.
- Odosobněná zodpovědnost za informační výstupy.

Hlavními aktéry celého zpravodajského cyklus jsou:

a) Producenti – zpravodajské štáby, organizace
b) Zákazníci – příjemci informace, velitelé, zainteresované strany

Řízení

Řízení je definováno jako: *„Fáze zpravodajského cyklu pro stanovení shromažďovacích požadavků, plánování úsilí pro shromažďování, vydání rozkazů a žádostí zpravodajským štábům pro shromažďování a zabezpečení nepřetržité kontroly produktivity těchto štábů.“*[22]



Obrázek 4: Členění zpravodajského cyklu dle povahy

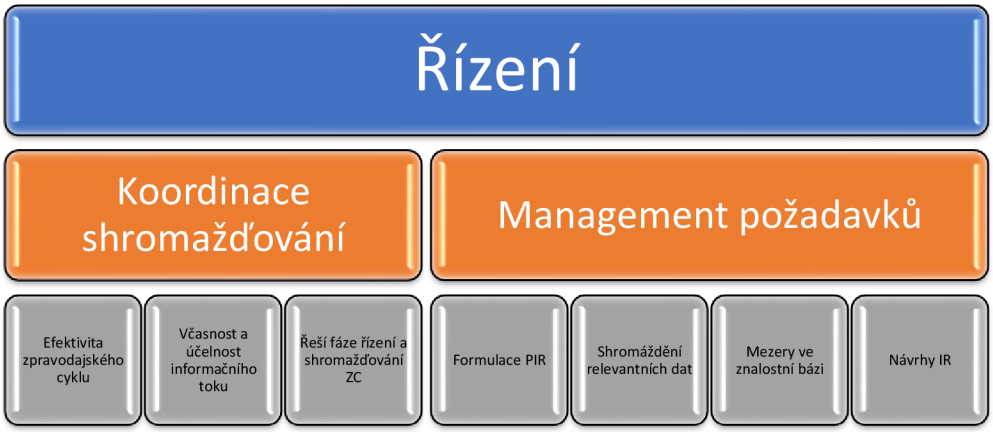
Fáze „Řízení a shromažďování“ zpravodajského cyklu se zpravidla realizují ještě před zahájením operace, v průběhu operace pak probíhá kontrola, zda shromažďované informace odpovídají plánu shromažďování informací (Collection Plan, CP). V nejobecnější rovině lze konstatovat, že fáze řízení se zabývá:

- stanovením zpravodajských požadavků (CCIR[23], PIR[24], IR[25], RFI[26]),
- plánování úsilí shromažďování (CP[27]),
- vydání rozkazů a požadavků, průběžná kontrola výslednosti zdrojů a agentur shromažďování

[22] AČR. Pub-20-00-02, *Slovník základních pojmů z oblasti zpravodajského zabezpečení v AČR*. 2. vyd., s. 106

[23] Požadavky velitele na důležité informace (Commander’s Critical Information Requirements)
[24] Prioritní zpravodajské požadavky (Priority Intelligence Requirements)
[25] Požadavky na informace (Information Requirements)
[26] Žádost o informace (Request for Information)
[27] Plán shromažďování informací (Collection Plan)

Přirozenou součástí fáze řízení je porozumění problému a jeho následný rozklad (problem breakdown), tvorba strategií shromažďování a finálně tvorba plánu shromažďování informací.



O

Obrázek 5: Členění fáze "Řízení"

V případě pochopení úkolu je analytik vystaven celé řadě omezení, jako například množství proměných nebo omezení lidské mysli a podobně. Aby došlo k minimalizaci vzniklých chyb lze využít, v obecné rovině, dvou přístupů:

Dekompozice[28] a vizualizace[29]. Mnoho (polo)strukturovaných analytických technik obsahuje obě výše uvedené vlastnosti. Jako příklad možných použitelných technik lze uvézt Checklisty, AIMS, Matice, Síťovou analýzu či myšlenkové mapy. Každá metoda má své výhody i nevýhody a uplatní se při rozličných situacích. Výčet není ani zdaleka úplný.

Fáze řízení je iniciována požadavky či identifikovanými mezerami, což je možné pouze při správném definování a popisu. Nejčastějším problémem je vágní a příliš obecné definování problému a požadavku.

Zadávání úkolů zahrnuje mimo jiné:

a) Zhodnocení, zda lze na požadavky zodpovědět s využitím stávajících informací, případně pokračuje koordinování shromažďováním chybějících informací a dat.

[28] Rozklad řešeného (úkolu, analytický problém) na základní části tak, aby každá složka mohla být hodnocena samostatně.

[29] Grafické zobrazení problematiky, slouží ke snazšímu pochopení vzájemných vazeb a vztahů.

b) Monitorování procesu shromažďování, zpracování, využívání a distribucí (CPED) zpravodajských informací.
c) Zajištění včasného provádění činností OSINT, případně distribuce dle stanovených priorit.
d) Zajištění zákonitosti činnosti OSINT a respektování pravidel pro sdílení OSINT.

Shromažďování

V rámci této fáze dochází ke shromažďování dat a informací a následné zpracování do použitelného formátu k dalšímu použití. Shromažďování je determinováno zejména časem, tématy, rozsahem a disponibilních zdrojů. Zároveň je naplánován způsob shromažďování požadovaných informací.

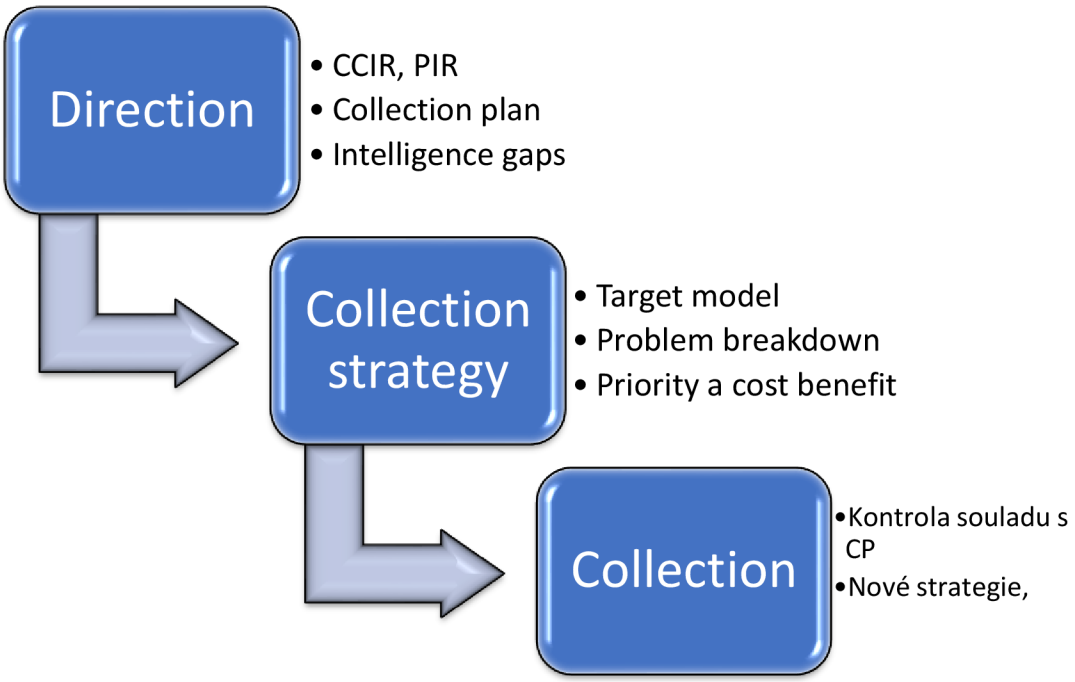
Druhá fáze zpravodajského cyklu, ve které zpravodajské štáby, v souladu s plánem shromažďování informací vytěží své zdroje, odeberou data a informace od agentur, které následně předá příslušným a oprávněným příjemcům ke zpracování. Hlavním přínosem je vytvoření obrazu bojiště pro zákazníka (velitele, štáb) prostřednictvím odpovědí na požadavky velitele, obdržených během první fáze zpravodajského cyklu. Integrální součástí je kontrola získaných poznatků, dat a informací, zda jsou v souladu s plánem shromažďování informací.

Shromažďování informací, vzhledem ke komplexnosti prostředí a řešených úkolů, probíhá s časovým předstihem před samotným plánováním operace, tak aby identifikované mezery ve znalostech (*intelligence gaps*) byly odstraněny a mohlo tak dojít k včasnému zpracování a využití.

Proces tvorby/výběru/hodnocení strategie shromažďování, svojí podstatou tvoří most mezi první a druhou fází zpravodajského cyklu, a je založen na sdílení „Modelu cíle – *Target Model*“ a „Rozpadu problému – *Problem breakdown*“ mezi zdroji a agenturami (*collectors)* a analytickou částí. Díky tomuto sdílení zdroje/agentury schopny naplno využít svůj potenciál a jedinečné znalosti a dovednosti (*know how*). Při tvorbě strategie je nesmírně důležitým krokem určování priorit a neustálé porovnávání poměru cena/výkon a zaměřit se na obsahovou kvalitu než na formální úpravu.

Další faktory ovlivňující plán shromažďování informací z otevřených zdrojů jsou:

a) Plánování a alokace zdrojů ve spolupráci s vše zdrojovými zpravodajskými analytiky.
b) Hodnocení rizik zaujatosti, dezinformací a sledování protivníkem naší aktivity OSINT.
c) Přístup datových vědců ke zdrojovým souborům dat.
d) Zvážení disponibilního času a požadovaného typu informací pro určení šířky, hloubky, strategií a technik shromažďování.
e) Legislativní aspekty.
f) Utajení operace.
g) Koordinace shromažďování s ostáními činnostmi vlastních sil.



Obrázek 6: Vazba fází zpravodajského cyklu na strategii shromažďování

Shromažďování zpravodajských informací může být realizováno následujícími metodami:

- Systematicky pro trvalé, dlouhodobé nebo specifické požadavky a využívá zejména delší časový úsek.
- Ad-hoc neboli dynamické je určeno zejména pro urgentní krátkodobé požadavky.

Zpracování

Třetí fáze zpravodajského cyklu představuje konverzi dat a informací pocházejících z otevřených zdrojů na zpravodajské informace. Zpravodajská informace je definována jako: *„Produkt vycházející z řízeného shromažďování a zpracování informací vztahujících se k prostředí, schopnostem a záměrům aktérů s cílem identifikovat hrozby a navrhnout možnosti využití funkcionáři s rozhodovací pravomocí“*[30]

Proces konverze je strukturovanou sérií sekvenčních činností, kdy dochází například i k identifikaci informačních mezer, jako vstupu do kroku řízení, a k definování požadavků na další shromažďování. Konverze je realizována prostřednictvím srovnávání, hodnocení, analýzy, sjednocení a interpretace.

Jednotlivé subprocesy budou blíže popsány v následujících části textu.

Subproces srovnávání obnáší příjem, seskupování, záznam a archivaci všech zpráv a shromážděných informací, registrace přijetí jednotlivých informací/zpravodajských informací do databází a zařazení do příslušných kategorií a skupin s následnou archivací. Jednotlivé kategorie a skupiny přímo souvisí s požadavky velitele na zpravodajské informace a prostorem odpovědnosti. Nedílnou činností je doplnění metadat a příznaků, umožňující následné vyhledávání a selekci.

Hlavním přínosem je eliminace hrozby „kruhového reportingu“ způsobeného opakovaným výskytem hlášené události jedním zdrojem více zpravodajskými orgány, čímž dochází k iluzi potvrzené informace z více zdrojů, díky čemuž získá vyšší stupeň věrohodnosti. Souvisejícím negativem je nadbytečné zatěžování distribučních kanálů.

Na subproces „Srovnání“ navazuje „Hodnocení“. Dochází k hodnocení věrohodnosti informací a spolehlivosti zdrojů jako dvě zcela oddělené a nezávislé činnosti. Na základě hodnocení je zdroji a informaci přidělen alfa numerický znak, nabývající hodnot 1-6, A- F.

---

[30] AČR. Pub-20-00-02, *Slovník základních pojmů z oblasti zpravodajského zabezpečení v AČR*. 2. vyd., s. 147

Spolehlivost zdroje společně s věrohodností informace udávají indikátor „správnosti“ a míry odstranění nejistoty zákazníkovi. Tento klíčový proces vyžaduje oddělené hodnocení. Patří však k nejsložitěji hodnoceným kritériím vůbec. V případě hodnocení spolehlivosti zdroje se pak zohledňují:

a) Poskytovatel informace
    a. Osobnost zdroje
        i. Pozice,
        ii. příslušnost (kmenová, náboženská, politická, …),
        iii. přístup k informaci
            1. přímý
            2. nepřímý,
        iv. kvalifikace a kognitivní omezení,
        v. minulost a spolehlivost.
    b. Zájem zdroje
        i. Účel poskytnutí informace,
            1. Souhlasné,
            2. protichůdné zájmy.
    c. Způsob předání informace
        i. Přímý
        ii. Zprostředkovaný
b) Poskytované informace,
    a. aktuálnost,
    b. přesnost,
    c. forma

Teprve odděleným zhodnocením výše uvedeného lze získat celkový obraz spolehlivosti zdroje.

Věrohodnost informace odkazuje na přesnost poskytnutých informací. Věrohodnost informace je výsledkem zkoumání logiky, trendů, pravdivosti informace, ale také alternativních hodnocení, schopností prostředků shromáždění pozorovat, hodnotit, zpracovávat a reportovat informace. Odtud vyplývá potřeba koordinované zpravodajské činnosti pro efektivní

shromažďování, na základě důsledné znalosti možností a omezení prostředků shromažďování. Analytici musí mít neustále na paměti možnost klamání, které je v případě OSINT velmi snadné.

Věrohodnost informace		**Kritéria stanovení**
1	Potvrzená	• Velmi cenná, • nová nebo potvrzující analytické závěry, • naléhavá s vysokým dopadem při prodlení, • aktuální, komplexní, • potvrzena z více nezávislých zdrojů, • plně koresponduje s dlouhodobými poznatky a vývojem či od zdrojů s dlouhodobou spolehlivostí hodnověrností, • závažné posuny v úrovni poznání

Věrohodnost informace		Kritéria stanovení
	Pravděpodobná	• Přínosná, • nově podstatným způsobem doplňuje dílčí analytické závěry, • potvrzuje a rozšiřuje známé skutečnosti, • aktualizuje analytické hodnocení jevu, • dlouhodobě aktuální, přínosná, • získaná vlastní činností nebo analýza s komentářem, • potvrzen z více zdrojů.
3	Možná	• Využitelná, • převážně potvrzuje a částečně doplňuje známé skutečnosti (dopřesněni již zaslané) • aktuální od zdroje s dlouhodobou spolehlivostí a hodnověrností, která navíc koresponduje s dlouhodobými poznatky a vývojem • jednozdrojová, vyžadující další ověření či doporučení • získaná vlastní analýzou OSINT či vlastní činností s vlastním komentářem.
4	Pochybná	• Informativní, • dílčí popis jednotlivých skutečností, jevů a událostí, • může být neaktuální či vyvolávat pochybnosti, • částečně potvrzuje / nepodstatně doplňuje známé skutečnosti, • jednozdrojová, dostupná v rámci OSINT • mimo působnost.

Věrohodnost informace		Kritéria stanovení
5	Nepravděpodobná	• Informace je téměř nevyužitelná, • zastaralá, nepravděpodobná, bez informačního přínosu, • není předmětem zpravodajského zájmu, • dezinformace, • nesprávné vyhodnocení zpracovatelem (nemohl vyhodnotit na základě jemu dostupných informací).
6	Věrohodnost nelze určit	• Nehodnocena, • nelze objektivně posoudit s ohledem na schopnosti zdroje, aktuálnímu stavu poznání, • při změně dojde k přehodnocení.

Tabulka 1: Věrohodnost informací

S ohledem na velké množství zdrojů a informací je hodnocení mimořádně důsledné a průběžné.

Cílem analýzy je identifikace významných skutečností pro následnou interpretaci. Informace jsou analyzovány nezávisle na sobě, aby se dosáhlo identifikace všech významných skutečností obsažených v hlášeních a získaných materiálech.

Během sjednocení dochází ke zvážení a kombinování zjištěných faktorů s dalšími zjištěnými a známými skutečnosti do podoby vzorců odpovídající na požadavky velitele na zpravodajské informace. Nedílnou součástí je zvážení relevantnosti informací ve vztahu k řešenému požadavku na zpravodajské informace.

Interpretace představuje závěrečný krok, kdy je posuzován význam informací se známými informacemi. Interpretace je objektivní duševní proces porovnávání a dedukce založených na odborných znalostech a zkušenostech o silách protivníka i vlastních silách. Interpretace dopřesňuje zjištěné skutečnosti pomocí 4 okruhů dotazů, dle typu zjištěných informací.

Při znalosti aktéra se posuzují důsledky jeho přítomnosti v daném místě. Znalost aktivity je porovnána s informacemi o předchozích nebo očekávaných aktivitách, aby bylo možné odhalit případné změny. Význam informace se zaměřuje na kritické posouzení každé dedukce za účelem dodržení relevantnosti a využitelnosti výsledného produktu. Základním principem je snaha o potvrzení a ověření i těch nejvěrohodnotnějších informací.

Kvalitní produkt vyžaduje pouze minimální potřebu interpretace příslušníkem provádějícím srovnávání při zařazování a kategorizace do databází. Každá dodatečná interpretace významným způsobem zvyšuje riziko desinterpretace a ztráty dat.

Na operačních stupních velení a řízení by skutečně každý subproces měl být prováděn jiným příslušníkem zpravodajského štábu, na taktickém stupni velení a řízení AČR lze ale předpokládat, s ohledem na personální obsazenost a počty systemizovaných míst, že se bude jednat o jednu, maximálně dvě osoby, pro které se navíc nebude jednat o hlavní pracovní náplň.

Distribuce

Poslední fáze zpravodajského cyklu, kdy dochází k doručení požadovaných produktů v požadovaném formátu a termínu. Obecné požadavky na formátu jsou často vydefinovány již ve fázi řízení. Pokud tomu tak není, musí zabezpečit maximální využitelnost produktů, při současném minimálním zatížení distribučních kanálů.

Distribuční kanály rozdělujeme na dva základní druhy, dle principu řízení. Princip „push“ (tlačení) umožňuje nadřízeným stupňům velení a řízení, zpravidla komponentní velitelství, případně operačnímu stupni předávat zpravodajské informace na nižším stupni, případně ekvivalentnímu stupni u sousedních jednotek. V rámci OSINT se tak jedná zpravidla o předávání varování zainteresovaným aktérům okamžitě po přijetí takové informace. Jako příklad lze uvést systém distribuce vyžádaných satelitních snímků původem od SATCEN ČR[31].

[31] Satelitní centrum České republiky

Naproti tomu princip „pull“ (stahování) umožňuje oprávněným uživatelům přímý přístup k databázím a dalším úložištím zpravodajských informací. Typickým příkladem tohoto principu jsou webové stránky OSINT určené pro síly NATO a odkazující na shromážděné te matické zpravodajské informace.

Cyklus zpravodajství z otevřených zdrojů

Jistou analogií se zpravodajským cyklem je cyklus zpravodajství z otevřených zdrojů, ze kterého vychází a drobně jej modifikuje. Svojí strukturou se blíží procesu ISR[32], kdy se skládá z pěti kroků s cílem popisu procesu transformace shromážděných dat a informací na zpravodajské informace. Kombinací cyklu zpravodajství z otevřených zdrojů se znalostí nástrojů a strategií shromažďování, při zachování bezpečnostních opatření, získává analytik potřebnou sadu k úspěšnému plnění zadaných úkolů.

Kroky cyklu zpravodajství z otevřených zdrojů jsou:

1. Plánování a řízení
2. Shromažďování
3. Zpracování a vytěžení
4. Analýza a produkce
5. Šíření a integrace

Plánování a řízení

První krok cyklu zahrnuje plánování priorit a požadavků mise. Před zahájením shromažďování by příslušníci ZZ měli mít naprosto jasno o potřebných informacích, jak najít potřebné zdroje a zamýšlený přínos takto nalezených informací. Nedílnou součástí je stanovení strategie shromažďování.

Shromažďování

Během shromažďování jsou využívány stanovené postupy a nástroje v souladu se zvolenou strategií a dle určených priorit a plánu shromažďování.

[32] Proces ISR: Koordinační proces zabezpečující poskytování dat, informací a jednozdrojových informací. Skládá se z pěti kroků (shromáždit, zpracovat, využít, šířit)

Zpracování a vytěžení

Po shromáždění dat a informací, například uplynutím stanovené lhůty, je zahájena fáze zpracování informací, vzájemného prvotního ověřování, kombinování, ukládání, zpracování hlášení a produkce další výstupů. V podstatě se jedná o zestručnění a transformaci shromážděných podkladových materiálů pro efektivnější analýzu v následujícím kroku.

Analýza a produkce

V tomto kritickém kroku dochází k hloubkové analýze shromážděných dat a informací, která následně umožní využití a interpretaci získaných poznatků. Formát výstupu této fáze je dán požadavky zákazníka nebo nastavenými pravidly.

Šíření a integrace

Poslední krok cyklu zahrnující distribuci finálních výstupů oprávněným uživatelům.

2.1.3. Přínosy a slabiny OSINT

V této části textu, autor představí některé hlavní přednosti a slabiny OSINT. Vedle samotného výčtu je přiložen i krátký komentář. Tuto část považuje autor za nezbytnou pro plné pochopení problematiky, nicméně je nezbytné podotknout, že se nejedná o úplný výčet.

Přednosti:

- Rychlost: OSINT umožňuje rychlý přístup k aktuálním informacím z celého světa, a to od textu obrazovým i video materiálům, ale i digitálním otiskům činnosti, uplatnitelné zejména pro skenování a monitorování bezpečnostního prostředí.
- Široký záběr: OSINT umožňuje využívat široké spektrum zdrojových dat, informací a zpracovaných (a interpretovaných studií) při dodržování geografické a zdrojové diverzifikace při zachování vynikající nákladové efektivity. Data zahrnují i textová, audiovizuální i grafická data. Díky tomu lze získat komplexní pohled na události a situace.

- Podpora rozhodování: OSINT je integrován do všech stupňů velení a řízení AČR, jakožto zdrojová součást plánovacího a rozhodovacího procesu odpovědných funkcionářů.
- Identifikace trendů: aplikací podpůrných softwarových aplikací, vlastním skenováním a monitorováním v čase, včetně využití přístupu k již zdánlivě smazaným informací, analytici provádí identifikaci a zhodnocení trendů, Za využití automatizace, nastupujících a přelomových technologií (EDT-(Emerging and Disruptive Technologies): jako například umělé inteligence, neuronových a kvantových technologií) se celý proces výrazně urychluje.
- Spolupráce a sdílení informací: OSINT může být efektivním prostředkem pro spolupráci mezi různými aktéry. Z povahy věci data a informace získané z OSINT zpravidla nepodléhají utajení. Citlivost získaných dat spočívá zejména v dosazení do kontextu či odhalením využívaných postupů a nástrojů. A jako takové, mohou být rychle šířeny a nedochází tak k časovému prodlení, jako tomu je u utajovaných zpravodajských produktů.

Přes všechny tyto benefity, představuje používání OSINT i několik omezení a rizik, jichž si musí být analytici i příjemci produktů vědomi. Tato rizika se dají eliminovat vhodným kombinováním s dalšími zpravodajskými produkty z jiných zdrojů a kritickým přístupem (včetně hodnocení zdrojů a informací).

Rizika:

- Omezená důvěryhodnost: Informace získané z otevřených zdrojů nemusí vždy být důvěryhodné a ověřené. Bez přímého přístupu k pramenům není vždy snadné potvrdit spolehlivost informací. Toto riziko je nejvýznamnější zejména u online dat, kdy nemusí docházet k redakčním zásahům, validaci dat. Je úzce spjatou s dezinformacemi a informačním přehlcením. Dalším problémem, s narůstající naléhavostí pak je informační přehlcení analytiků OSINT, kteří nejsou schopni využívat všech dostupných zdrojů. Proto je v OSINT klíčová správa zdrojů a jejich klasifikace.

- Nedostatečná aktualita: Otevřené zdroje nemusí vždy poskytovat aktuální informace. V některých případech může dojít k zpoždění mezi událostí a zveřejněním informací. Dalším vyplývajícím nebezpečím je recyklace textů, zde je nezbytné, aby analytici nejen důsledně ověřovali informace, ale i zkoumali metadata a zajistili přístup k informacím o publikaci textu. Mnohdy se ve vyhledávání zobrazují na prvních místech starší texty, mírně upravené a tvářící se jako aktuální.
- Chybějící kontext: Informace z otevřených zdrojů může chybět kontext, což může vést k nesprávné interpretaci. Bez širšího porozumění okolnostem může být obtížné plně pochopit situaci.
- Omezená dostupnost: Některé klíčové informace mohou být citlivé nebo omezené a nejsou volně dostupné. To může způsobit nedostatek úplnosti při vytváření celkového obrazu. Proto se doporučuje kombinovat OSINT s dalšími zdroji informacemi, byť na konkrétní části.
- Manipulace a dezinformace: Otevřené zdroje mohou být náchylné k manipulaci a dezinformacím. Informace mohou být záměrně zkreslovány nebo šířeny s cílem ovlivnit vnímání.
- Odhalení vlastních zpravodajských zájmů protivníkovi.

2.1.4. Rozvoj v posledních 10 letech

S pokračující globální informatizací a digitalizací, vývoj bezpečnostního prostředí jsou hlavními hybateli dynamických změn v oblasti zpravodajství z otevřených zdrojů. Některé z hlavních trendů zahrnují:

S nárůstem digitálních technologií a obavami o soukromí došlo ke změnám v legislativě týkající se shromažďování a využívání otevřených dat. Některé země aktualizovaly své zákony a regulace v oblasti kybernetické bezpečnosti a ochrany soukromí. Evropská unie je v tomto směru velmi aktivní, což vedle ochrany obyvatelstva přináší a značný seberegulující prvek pro zpravodajské zabezpečení v AČR. Na jedné straně se jedná o snížení přístupných dat povolenými prostředky, na straně druhé tyto regulace představují nevýhodu v porovnání s protivníky/nepřáteli, jež tato seberugulující pravidla neuplatňují.

Rozvoj technologií strojového učení a umělé inteligence umožnil zefektivnění nástrojů pro automatizované zpracování a analýzu OSINT. To umožňuje rychlejší a efektivnější získávání informací, jejich validaci, hodnocení zdrojů a informací a aktuálnost dat. Rozvoj těchto schopností je nezbytný z důvodu rostoucího množstvím informací dostupných online, včetně sociálních médií, satelitních snímků a veřejně dostupných dat, se rozšířily i zdroje, které lze v rámci OSINT využít. To vše v prostředí, kdy je důraz položen na co nejkratší časový úsek zpravodajského cyklu.

V důsledku mezinárodních hrozeb a globální povahy informací se zvýšila potřeba mezinárodní spolupráce v oblasti OSINT. Země často spolupracují na sdílení informací a zlepšení kybernetické bezpečnosti.

2.1.5. Techniky a nástroje OSINT

V oblasti OSINT existuje široká škála nástrojů a technik, které vedou ke shromažďování a analýze dat. Tyto nástroje autor rozdělil do několika kategorií. Každá z těchto kategorií má své specifické nástroje a technologie, které mohou být využity. Výběr konkrétních nástrojů vždy závisí na cílech a potřebách analytika.

V současné době existuje celá řada komerčně dostupných řešení, softwarových aplikací, naplňující veškeré požadované funkcionality dle předpokládaného použití. Přestože se tato řešení rychle vyvíjí a stávají se stále více komplexními řešeními, momentálně autorovi není znám nástroj, který by pokryl potřeby celého zpravodajského cyklu a byl schopen využívat všech uplatnitelných technik.

V následujícím textu jsou uvedeny vybrané kategorie nástrojů s krátkým představením výhod a nevýhod. K jednotlivým kategoriím je přiřazen i zástupce komerčního softwaru, který svojí povahou nejvíce[33] spadá do uvedené kategorie. Mezi nejpokročilejší spadá software Paterva Maltego, o které bude hovořeno na konci kapitoly.

[33] Mnohé nástroje svým záběrem spadají do více kategorií současně

Analýza obrazu a videa / vizuální analýza dat.

Tato kategorie zahrnuje nástroje pro analýzu vizuálních dat, detekci objektů, tváří, identifikaci vzorů apod. Vizualizace shromážděných dat představuje významný nástroj pro analýzu zkoumaných jevů. Zejména aplikace IBM i2 Analyst's Notebook nabízí široké uplatnění (propojení s dalšími nástroji, příprava podkladů pro prezentaci).

Vizuální zobrazení dat umožňuje analýzu vztahů mezi osobami nebo organizacemi v podobě síťového diagramu, díky čemuž lze snadno identifikovat vzorce v analyzovaných datech.

Analýza sociálních médií

Armáda České republiky vnímá sociální média jako interakci jednotlivců, kde jsou sdíleny a vyměňovány informace v prostředí virtuálních komunit a zahrnují i sociální sítě. Analýza se zaměřuje na identifikaci a porozumění síťových uzlů a jejich vzájemných vztahů. Analýzy vyžadují pokročilé multidisciplinární znalosti analytiků.

Sociální média zahrnují:

- blogy a mikrology,
- sociální sítě (Facebook, VKontkte,4chan, reddit),
- profesní sítě (LinkedIN,Twitter),
- sdílení videa (YouTube, TikTok),
- sdílení audionahrávek (podesty),
- sdílení fotografií (Instagram, Pinterest).

Analýza sociálních médií je nalézá své uplatnění při identifikaci trendů, zjišťování veřejného mínění a monitorování diskuzí za účelem monitorování a sledování (nástroje sledující aktivitu na sociálních médiích, vyhledávání klíčových slov a hashtagů) a k provádění sentiment analýzy[34] (nástroje, které zkoumají sentiment a nálady spojené s určitými tématy na sociálních médiích).

[34] Úspěšnost a spolehlivost sentiment analýzy je stále tématem odborných diskuzí. Obecně je přijímána jako orientační ukazatel, nicméně stále více je uplatňována v rámci AČR. Vedoucí pracovníci k ní mnohdy přistupují příliš nekriticky a nadhodnocují její přínosy a možnosti.

Na základě historických zkušeností z událostí posledních 10 let, lze konstatovat, že sociální média jsou důležitou platformou pro komunikaci a organizaci jak protestních akcí (Libye, Ukrajina), ale také pro činnost disidentu (Čína, Bělorusko) a organizovaného zločinu a teroristických organizací (Islámský stát). Množství sdílených dat exponenciálně roste, vylepšuje se zabezpečení sociálních sítí (end-to-end šifrování) a monitoring se tak stává výzvou pro bezpečnostní složky.

V České republice je stále nejpopulárnější Facebook, kde však průměrný věk uživatele narůstá, mladší generace se přesouvají na platformy s krátkým multimediálním obsahem. Pro potřeby práce, je mezi sociálně sítě řazen i Youtube.com, zejména z důvodu naplnění klíčových atributů pojmu sociální sítě – možnost vytváření profilů, interakce s ostatními uživateli, seskupování se do zájmových skupin a sdílení informací a názorů.

Nástroje a metody monitoringu, a následné analýzy, lze kategorizovat několika kategoriemi:

- Integrované vyhledávání jednotlivých sociálních sítí
- Rozhraní k využití služeb v jiném prostředí (API – Application Programming Interface) rozhraní
- Komerční nástroje monitoringu sociálních sítí
    - Monitorování v reálném čase
    - Kontinuální monitorování
    - Monitorování sociálních médií, extrahování příspěvků, kategorizace
    - Ukládání příspěvků do lokálních databází

Integrovaným vyhledáváním disponují prakticky všechny sociální sítě a platformy. Jedná se o jednoduché vyhledávání, většinou bez možnosti využití operátorů a automatizovaného shromažďování dat. Právě proti automatizovaného shromažďování dat zavedla sociální síť Facebook opatření, kdy je uživateli znemožněno využívat tuto funkcionalitu v případě, že algoritmus vyhodnotí četnost využívání jako nadlimitní, příčemž zohledňuje uživatelskou historii, aktivitu, roční dobu a mnoho dalších kritérií.

Application Programming Interface je označení pro rozhraní, umožňující využití služeb v jiném prostředí, zejména pak pro integraci s dalšími nástroji. Díky API lze využít pokročilého vyhledávání i na sociálních sítích. API využívají prakticky všichni relevantní hráči na poli sociálních sítí a médií obecně. Jako příklad lze uvést: Facebook Open Graph API, Google Custom Search API, Twitter API, Google+ API.

Obecně nástroje pro monitorování sociálních médií pracují na principu agregace uživatelských příspěvků s možností selekce dle vybraných kritérií (téma, geolokace). Aplikace pro monitorování v reálném čase (např. Whos Talkin, Uvrx) jsou schopny provádět monitoring z více zdrojů v jeden okamžik, naproti tomu skýtají nástroje pro kontinuální monitorování i možnost vyhledávání příspěvků zpět v čase a často zahrnují do svého portfolia i jiná média a blogy. Lze v nich využívat i pokročilé dotazování v rámci vyhledávání. Zástupci této kategorie jsou například SiloBreaker a Recorded Future.

Jako příklad nástroje umožňující ukládání do lokálních databází pro následnou detailní analýzu můžeme uvést nástroj Spicy Mango.

Tyto nástroje umožňují široký záběr dat a rychlé odhalování nových událostí. Slabiny vyplývají zejména ze zdrojů čerpaných dat, konkrétně se jedná o potenciálně nízkou kvalitu dat a zranitelnost vůči manipulaci a dezinformacím.

Archivní zobrazení webových stránek

Využití archivního zobrazení webových stránek je silným nástrojem pro analýzu trendů a sledování vývoje určitého fenoménu. Další výhodou je, že díky tomuto nástroji získá analytik přístup i k již neexitujícím stránkám. Slabou stránkou tohoto nástroje jsou dynamické webové stránky a stránky vyžadující autorizované přihlášení. Zástupci této kategorie jsou mimo jiné: Google Cache nebo Wayback MAchine.

Geografické informační systémy (GIS)

Kategorie nástrojů GIS umožňují grafickou analýzu dat na základě geografických informací. Přínosem nástrojů této kategorie je schopnost mapování událostí a zjišťování prostorových vztahů dat prostřednictvím

vizualizace geografických aspektů dat a identifikace geografických vzorů. Pro správnou činnost GIS vyžadují přesná geografická data.

Grafické nástroje

Software umožňující vizualizaci dat v podobě grafů, map a dalších vizuálních reprezentací. Významnou výhodou je vypovídající hodnota výstupu, snadná interpretace a využitelnost pro přípravu verbálních dokladů.

Kopírování webových stránek

V ojedinělých případech je nezbytné či výhodné využít offline použití webových stránek, zachovávající jejich plnou funkčnost, v takovém případě se hovoří o takzvaném „website mirroring".

Tato metoda je vhodná pro práci s metadaty, vyhledávání informací ve zdrojovém kodu stránky.

Zástupci kopírování webových stránek jsou aplikace HTTrack Web Site Copier a Website Ripper Copier.

Metadata

Metadata představují záznamy o vytvoření, zpracování a vlastnostech daného souboru, ať se jedná o webové stránky, dokumenty či multimediální soubory. Dále mohou obsahovat další užitečné informace (geografická poloha, osobní údaje, IP adresy). Metadata mimo jiné mohou být používána k automatizovanému zpracování a kategorizaci dokumentů.

Specifickým případem pouţití metadat je formát Exif (Exchangeable image file format) vkládaný do fotografií při jejich pořízení (digitálním fotoaparátem, mobilním telefonem či jiným zařízením umoţňujícím pořízení fotografií).

Zástupci aplikací pro práci s metadaty: Foca Free, EXIF Tool či Creepy.

Síťová a technická infrastruktura

Za účelem zjištění základních informací a dat o doméně, případně provozovateli nebo DNS záznamů, je nezbytná znalost síťové a technické infrastruktury. Metody zjišťování síťové a technické infrastruktury, jsou výchozím krokem

penetračního testování (tzv. Footprinting), kdy dochází ke shromažďování základních informací o zkoumaném subjektu, jeho síťové a výpočetní (systémové) infrastruktuře nacházející se ve zkoumané síti. Nicméně tento nástroj se již nachází na pomezí kybernetického průzkumu.

Z pohledu OSINT na taktické úrovni nachází široké uplatnění studium údajů o vlastníkovi domény (Whois záznamy[35]) a takzvané websitefootprintinga e-mailfootprinting.

Aplikovatelné nástroje pro vybrané aspekty síťové a technické infrastruktury jsou: Sam Spade, Knock a Shodan.

Údaje o uživatelích

Doplňková metoda, sloužící zejména pro zpřesnění podkladů analýzy vazeb, prostřednictvím nalezení a extrakce kontaktních údajů, ověření existence registrovaných účtů na základě dříve zjištěných uživatelských jmen, e-mailových adres případně i o extrakci určitého obsahu dané stránky (například veškeré informace ve spojitosti s uživatelským jménem/e-mailem etc.). Jedná se o vhodnou metodu zejména pro blogy, aukční a obchodní portály, diskusní fóra a e-mailové služby.

Příklady vhodných nástrojů: Scythe: Account enumerator, The Harvester, NameCheckUp.

Vyhledávače a Meta vyhledávače

Základní nástrojem pro práci v internetu, specificky s world wide web jsou webové vyhledávače (např. Google, Bing, Duck Duck Go) případně Meta vyhledávače, umožňující vyhledávání ve více vyhledávačích zároveň (např. Copernic Agent).

Výsledky vyhledávání se dají dopřesňovat nastavením vyhledávačů, případně za využití speciálních operátorů (booleovské operátory).

---

[35] Whois záznamy obsahují registrační údaje pro každou existující doménu. Whois databáze jsou udržovány v regionálních internetových registrech a obsahují také některé osobní a kontaktní údaje o vlastníkovi domény.

Webové scraperování

Jedná se o nástroje umožňující automatizované shromažďování dat z webových stránek a sociálních médií, novinových portálů, blogů atd.

Velkou předností je automatizace shromažďování dat a rychlý přístup k aktuálním informacím. Díky tomu, analytici ušetří drahocenný čas při skenování a monitoringu a zároveň jsou díky nástrojům provádějící scraperování schopni obsáhnout výrazně větším objem zdrojů v mnohonásobně kratším čase.

Při práci se scraperovacími nástroji je nutné být si vědom jejich omezení. Mezi nejvýznamnější patří omezená schopnost získávat strukturovaná data a nižší citlivost při drobných změnách na webových stránkách (zdrojích dat a informací).

Zpracování přirozeného jazyka / pokročilá analýza textu,

Do kategorie zpracování přirozeného jazyka **(**NLP – Natural Language Processing) zařazujeme software určený pro analýzu a interpretaci textových dat, rozpoznávání entit, kategorizaci textů apod. Jak z popisu vyplývá, jsou určeny pro analýzu textových dat, rozpoznávání klíčových slov a entit, a to především díky schopnosti extrahovat významné informace z textů, automatizace analýzy.

V této kategorii se nachází aplikace s širokou škálou schopností, od prosté automatické sumarizace textu a základní textové analýze (Copernic Summarizer), až po nástroje schopné zasazovat zkoumaný text do kontextu, jeho extrakci s následným grafickým zobrazením (Cogito Semantic technology, Basis Technology).

Relativně rozšířeným nástrojem v rámci AČR je aplikace Tovek Tools české společnosti Tovek, s.r.o. Nástroj je určen pro zpracování velkého objemu nestrukturovaných dat. Vedle shromažďování dat na konkrétní entitu se jedná o vhodný nástroj pro analýzu propojených databází. Rozsah nabízených schopností je odvislý od zvolené varianty, které se standardně nabízí ve dvou provedeních:

- Tovek Tools Search Pack, obsahující funkcionality Index manager a Tovek Agent. Index manager vytváří možnost připojení informačních

zdrojů a jejich následnou indexaci (ruční či automatickou). Funkcionalita Tovek Agent je určena k vyhledávání dokumentů dle zadaného dotazu.

- Tovek Tools Analysts Pack, zahrnuje vedle Tovek Tools Search Pack i následující funkcionality:
    - InfoRating pro kontextovou analýzu dokumentů. Výsledky umožňuje zobrazit pomocí kontextové matice, diagramu vazeb nebo pomocí grafu,
    - Fulltext Plug-in pro Analyst's Notebook.
    - Query Editor je nástroj k vytváření pokročilých dotazů ve formě hierarchické struktury pro velmi přesnou formulaci vyhledávacího dotazu,
    - Harvester provádí analýzu dokumentů, s výběrem relevantních slov za použití statistických metod.

2.1.6. Výzvy pro OSINT

Kybernetická doména, v níž se převážná část OSINT dnešní doby odehrává[36], je jednou z nejdynamičtěji se rozvíjejících operačních domén přijatých NATO[37]. Analytici jsou na denní bázi nuceni se vyrovnávat s informačním přehlcením, kdy trend neúprosně směřuje ke stále zrychlujícímu nárůstu objemu a množství dostupných dat a informací, s velice proměnlivou věrohodností (data, informace) a spolehlivostí (zdroje).

Klíčovými kompetencemi pak bude schopnost AČR digitalizovaný automatizovaný zpravodajský cyklus, schopnost správného ohodnocení zdroje a informace, ověření předkládaných informací (více zdrojově), neboť OSINT je více než jiné zpravodajské disciplíny zatěžován informačními a psychologickými operacemi protivníka/nepřítele. Analytici jsou nepřetržitě nuceni brát v potaz zásady a principy takzvaného „kognitivního válčení".

Významnou výzvou bude rozvoj personálních zdrojů a disponibilního vybavení (hardware, software, přístupy i do širokého spektra placených databází).

[36] Dochází k přesunu z off-line zdrojů do on-line prostředí, stejně tak jak pokračuje digitální globalizace celosvětové společnosti

[37] Dalšími operačními doménami jsou: země, voda, vzduch, vesmír

S nárůstem zpracování osobních dat se stává důležitým tématem ochrana soukromí a etické zpracování dat. Inovace v oblasti OSINT by měly být prováděny s respektem k etickým zásadám a dodržováním právních norem. I v případě OSINT je nezbytné dbát na ochranu zdroje, aby nedošlo k jeho kompromitaci případně fyzické likvidaci. A to jak nositele informace (platformy, serveru, aj.) tak zejména objektu zpravodajského zájmu, například zájmové osoby.

OSINT analytici jsou vázání dodržováním a zohledňováním platného legislativního rámce, v případě Evropské unie (EU – European union) například Obecné nařízení o ochraně osobních údajů (GDPR – General Data Protection Regulation)

Směry možného se přizpůsobení jsou uvedeny v následující kapitole.

2.1.7. Budoucnost OSINT

Tendence v oblasti OSINT jsou pestré a rychle se měnící. Tyto zmíněné trendy naznačují, že OSINT bude hrát ještě významnější roli v oblasti národní bezpečnosti v budoucnosti. Narůstající úlohu budou představovat ty činnosti, jež minimalizují přístup protivníka/nepřítele k zájmovým datům a informacím, v rámci OSINT.

S rozvojem přelomových technologií a pokračující digitalizací, se na poli OSINT bude nezbytné vyrovnat s úlohou umělé inteligence a její integrace do stávajících procesů. Tato integrace by měla probíhat jak záměrně, tak i nezáměrně. Proces nezáměrné implementace převratných technologií, zejména umělé inteligence již započal. Raná stádia umělé inteligence jsou integrovány do rozličných nástrojů (internetové vyhledávače, software pro shromažďování, zpracování dat a informací, k podpoře analýzy etc.).

Extrémní proměnlivost bude stupňovat svůj tlak na včasnost produktů pocházejících z otevřených zdrojů, proto bude nezbytné v maximálně míře zapojit procesy strojového učení a automatizace zejména do fází zpracování a distribuce zpravodajského cyklu.

Kvantové technologie a rozvoj kvantového šifrování představují přelomovou technologii, mající přímý i nepřímý dopad nejen na OSINT, ale na západní společnost jako takovou. Jejich úspěšný rozvoj a nasazení, bude mít přímý dopad například na:

- Šifrování, jako základ bezpečnosti informací. Se zavedením kvantových technologií by se současné způsoby šifrování staly naprosto bezcennými, naopak jejich zavedením by se enormně zvýšila udržitelnost sil a prostředků.
- Shromažďování. Na příjmové straně nedostupnost relevantních dat i informací, způsobených kvantovým šifrováním, naopak může dojít ke zrychlení celého procesu, množství shromážděných dat a metadat.

V návaznosti na výše uvedené trendy bude nezbytná vysoká míra investic do technického vybavení a personálu. V oblasti technického vybavení se bude jednat minimálně o vybavení všech relevantních zpravodajských orgánů, dle předurčení a úrovně velení a řízení, odpovídajícím hardwarem a softwarovými nástroji.

Obrovskou výzvou bude lidský kapitál. Autor práce se domnívá, že AČR bude nucena, bude-li chtít udržet trend, přehodnotit celou řadu oblastí:

- Úprava systemizovaných míst zpravodajských orgánů
- OSINT jako samostatná vojenská odbornost
- Personální politika
- Vzdělávání
- Technologický vývoj

S ohledem na vývojovou dynamiku, rozsah činností a nároky na vzdělání, výcvik, kompetence, znalosti a dovednosti předurčeného personálu, se autorovi zdá nezbytné[38], aby došlo ke vzniku samostatné odbornosti OSINT a k vytvoření dedikovaných systemizovaných míst od úrovně prapor a jeho ekvivalentu. Na rozdíl od jiných zpravodajských oborů, jako je například obrazové zpravodajství (IMINT – Imagery Intelligence) je práce s otevřenými zdroji rutinní

[38] Tyto poznatky též rezonovali na odborném setkání orgánů zpravodajského zabezpečení AČR na půdě Univerzity obrany (2023)

každodenní činností všech zpravodajských orgánů. Osamostatnění vojenské odbornosti, s tím vzniku doktrinálního a vzdělávacího systému, umožní velitelům a náčelníkům zpravodajských orgánů daných jednotek přistupovat k problematice zpravodajství z otevřených zdrojů plně, interdisciplinárně a zároveň vytvoří předpoklady pro specifický přístup v oblasti personální práce.

Vzhledem k požadavkům kladených na zpravodajské zabezpečení, zejména nepřetržitá podpora, kdy stávající stav je nevyhovující[39], navrhuje autor přidání systemizovaných míst od stupně prapor jedno, na stupni brigáda dvě až tři a organizačně je začlenit do zpravodajských orgánů s primárním úkolem shromažďování dat a informací. Tímto krokem, přikročí AČR ke standardizaci v rámci NATO, čímž se usnadní mezinárodní spolupráce specialistů OSINT.

Příslušníci OSINT budou nevyhnutelně úzce spolupracovat s dalšími specialisty. Na stupni prapor zejména příslušníky kybernetických sil, od úrovně praporních/brigádních úkolových uskupení a brigád pak budou koordinovat svou činnost jak s kybernetickými, tak psychologickými silami. K dosažení pozitivního synergického efektu bude vhodné vytvoření koordinačního orgánu, kde zároveň bude docházet, vedle plánovací a koordinační činnosti, k fúzování dat a informací, sdílení zkušeností a poznatků.

Vzhledem k přínosu i v rámci kontrarozvědné činnosti, spadající do působnosti Vojenského zpravodajství, bude nutná úzká kooperace s touto složkou Ministerstva obrany, podobně jako tomu je u některých dalších zpravodajských oborů, zpravodajského zabezpečení AČR.

Druhou kategorií je personální práce se specialisty OSINT, kdy širší revize bude nezbytným předpokladem pro obsazování míst specialistů kvalitními lidskými zdroji, k jejich rozvoji a zejména dlouhodobé udržitelnosti. Změny se budou muset dotknout náboru vytipovaných specialistů (zjednodušení a urychlení)[40], ale také formy odměňování (náborový příspěvek, zvýšený stabilizační příplatek, aj.) a způsobu výkonu služby (prodloužená doba rozhodná, individuální přístup

[39] Vztaženo k metodikám CREVAL a TACEVAL pro síly a prostředky určené pro NATO

[40] Zde se jeví jako vhodná cesta rozvoj projektu běžícího projektu Virtuálního náborového střediska

k plnění fyzického přezkoušení v závislosti na předurčení podporované jednotky a míry její nasaditelnosti, možnost pravidelné práce z domu).

Na vyšších stupních a určitých pozicích (zejména pro plnění funkce Reach Back – vzdálené podpory) by zajímavým benefitem byla i flexibilní pracovní doba. Snahou vedení rezortu by měla být maximální atraktivita, aby bylo možné personální doplnění, obzvláště v době, kdy armáda ztrácí svoji konkurenceschopnost na trhu práce, a to i v době hospodářské recese.

K získání znalostí, dovedností a schopností bude třeba vytvořit národní systém vzdělávání, zaměřený na rozvoj „soft" i „hard" „skills" a v neposlední řadě, pro řídící pracovníky i zásady tvorby strategie shromažďování informací. Z pohledu infrastruktury se, v době psaní diplomové práce, jeví nejvhodnější vojenskou vzdělávací institucí Univerzita obrany, která na tvorbě a zabezpečení kurzů[41] bude spolupracovat s veřejným i soukromým vysokým školstvím. Národní systém bude plně provázaný se vzděláváním organizovaným institucemi NATO. Národní příspěvky členských států NATO, případně EU, lze využít jako doplněk, případně jako alternativu.

Logickým vyústěním a zároveň existenční podmínkou bude koordinovaná podpora vědy a výzkumu, cestou stále strukturované spolupráce či vědy, výzkumu a inovací. Například v oblastech kvantového šifrování, automatizovaného shromažďování dat a informací, strojového učení, pokročilých vyhledávacích algoritmů, technologií zpracování přirozeného jazyka nebo kontextuální analýze. Z pohledu monitoringu sociálních sítí bude zajímavé využití chobotů pro monitorování sentimentů a informací s následnou analýzou klíčových událostí a automatizovaná tvorba hlášení, dle předem stanovených pravidel.

S rozvojem schopností shromažďování informací se do popředí bude stále více dostávat nutnost kybernetické ochrany, jak po stránce technické, tak zejména po stránce vzdělávání personálu a nastavení procesů hlášení případných

[41] Z pohledu dosahování schopností v současné době není žádoucí vytvoření samostatného studijního oboru

pokusů o kybernetické působení v neprospěch podporované jednotky odpovědným funkcionářům.

2.2. Zpravodajské zabezpečení v AČR

V souvislosti se zpravodajským zabezpečením mnohdy dochází k záměně se zpravodajskou činností, jíž dle zákona 289/2005 Sb. o Vojenském zpravodajství, a zákonem č.153/1994 Sb, o zpravodajských službách České republiky provádí pouze Vojenské zpravodajství, jako jednotná zpravodajská služba s vnitřní a vnější působností a spadající do resortu obrany. Příslušníci Vojenského zpravodajství jsou však také ve služebním poměru vojáka z povolání dle zákona č. 221/1999 Sb. o vojácích z povolání ve znění pozdějších předpisů.

Výběr vojáků z povolání na pozice zpravodajského zabezpečení je odlišné od výběru osob do Vojenského zpravodajství.

Armáda České republiky postupně přechází zpět ke tří stupňovému systému velení a řízení, přičemž zpravodajské zabezpečení představuje nedílnou součást těchto struktur:

- Taktický stupeň je uvažován od nejnižších jednotek (družstvo, četa) až po komponentní velitelství (vzdušné, pozemní, speciální, kybernetické síly),
- Operační stupeň bude v budoucnu zastoupen Velitelstvím pro operace,
- Strategický stupeň představuje Generální štáb Armády České republiky.

Zpravodajské zabezpečení je centralizovaně řízený proces s decentralizovanou exekutivou. Proces je řízen prostřednictvím vnitřních normativních aktů, takzvaných Nařízení pro zpravodajské zabezpečení, jehož součástí je přidělení prostorů zpravodajské odpovědnosti (AIR – Area of Intelligence Responsibility) a zpravodajského zájmu (AII – Area of Intelligence Interest). Tímto, zpravidla geografickým rozdělením je dosaženo efektivního využití sil a prostředků AČR[42].

Zpravodajské štáby jsou organickou součástí každé jednotky velikosti prapor pozemních sil a jejich ekvivalent vzdušných sil (letka). Příslušníci

[42] Při určování AIR a AII je brán v potaz úkol a bojové předurčení jednotek AČR a dále zpravodajské pokrytí zájmových oblastí.

zpravodajského zabezpečení jsou vnitřně členěny dle vojenských odborností a s tím souvisejícími popisy pracovní náplně, které jsou v souladu s hlavními pilíři zpravodajského zabezpečení, uvedenými výše v tomto textu. V rámci certifikačních hodnocení NATO (TACEVAL, CREVAL) je nejčastější výtkou nemožnost zabezpečení zpravodajského zabezpečení trvale v nepřetržitém režimu 24/7 (24 hodin denně, 7 dní v týdnu). V rámci pozemních sil je situace udržitelná, alespoň v rámci maximálních ambic příspěvků AČR do operací NATO a pro národní potřeby je počítáno s mobilizačním přírůstkem. Výrazně horší situace je v rámci ZZ vzdušných sil.

Zpravodajské zabezpečení na taktické úrovni nevymezuje specializaci OSINT. Úkony OSINT tak vykonávají zpravidla příslušníci se specializací „Analytik".

Po technické stránce jsou zpravodajské orgány vybaveny výpočetní technikou s přístupem k síti internet. S ohledem na specifické potřeby příslušníků zpravodajského zabezpečení mají k dispozici nejen standardní „Internet Ministerstva obrany – IMO" se zvýšenou ochranou proti nežádoucím rizikům z prostředí internet, ale za cenu blokování vybraných webových stránek, případně celých domén a teritoriální filtry, ale i takzvaným „Nefiltrovaným internetem Ministerstva obrany", který lze přirovnat ke klasickému počítači připojenému do globální sítě Internet.

AČR si je vědoma důležitosti OSINT v rámci zpravodajského zabezpečení, díky čemuž v posledních letech dochází k plošnému vybavování jednotlivých zpravodajských orgánů softwarem usnadňující činnost OSINT. Z celé množiny můžeme uvést například přístup do vysoce kvalitních databází Jane's, případně rutinní využívání software TOVEK TOOLS. Tato podpora posouvá kvalitativní úroveň OSINT na zcela novou úroveň.

V rámci vojenského vzdělávacího systému sehrávají nejvýznamnější roli dvě instituce, Univerzita obrany v Brně a Velitelství výcviku – Vojenská akademie, Vyškov. Ani jedna z výše uvedených institucí v současné době však neposkytuje cílený kurz zaměřený na problematiku OSINT určený pro příslušníky zpravodajského zabezpečení. V obecné rovině je problematika zahrnuta do jiných odborných kurzů. Nicméně příslušníci zpravodajského zabezpečení

mají možnost účastnit se zahraničních kurzů OSINT pořádaných buď přímo NATO/EU nebo jednotlivými členskými státy uvedených organizací. Účast na nabízených kurzech třetích stran (zejména států) je teoreticky možná, nicméně z důvodu citlivosti prakticky nevyužívaná.

Dne 1. 7. 2019 vzniklo Velitelství kybernetických sil a informačních operací, jakožto další taktické velitelství AČR, které se tento systémový nedostatek snaží kompenzovat nad rámec svých hlavních úkolů.

Vysoce dynamický vývoj zpravodajského zabezpečení nabízí jednoznačný trend i v oblasti OSINT, kdy se AČR přibližuje nejlepším zkušenostem spojeneckých armád. AČR disponuje strukturami, procesy a částečně i personálem pro realizace hodnotného zpravodajství z otevřených zdrojů.

Zpravodajské zabezpečení AČR představuje centralizovaný systém poskytování zpravodajské podpory velitelům a štábům. Výkon ve své působnosti opírá o 5 základních pilířů. V rámci zpravodajského cyklu, shromažďování, využívá mimo jiné zpravodajský obor OSINT. Nicméně nemá dedikovaná systemizovaná místa specialistů OSINT, ani neexistuje vojenská odbornost OSINT. Výkon obstarávají zpravidla příslušníci analytických částí zpravodajských orgánů, když reálně je využíván, v různé podobě a kvalitě, všemi příslušníky.

V celé sledované oblasti dochází ke zvyšování schopností a jejich následnou praktickou aplikaci do činnosti AČR. Modernizační a adaptační mechanismy však momentálně vykazují problémy zejména v oblasti personálu, které se dají rozdělit do dvou hlavních skupin:

1. Strukturální

Zpravodajské zabezpečení vykazuje akutní nedostatek personálu[43] k pokrytí požadovaných schopností a v oblasti OSINT nejsou vytvořena specializovaná systemizovaná místa.

[43] V tomto smyslu se autor nezaobírá celospolečenským trendem nedostatku kvalifikovaného personálu, ani stížnostmi příslušníků zpravodajského zabezpečení, s nimiž byla diplomová práce konzultována. Jedná se o výsledek hodnocení dle metodik NATO (TACEVAL, CREVAL) jejichž účastníkem autor byl, tak vyjádření jednoho konzultanta – certifikovaného hodnotitele NATO TACEVAL, kdy došlo k porovnání požadavků se skutečným stavem v AČR.

Vzhledem ke vzniku nového taktického velitelství bude v blízké budoucnosti nutné provést dekonflikci a vymezení odpovědností v oblasti zpravodajství z otevřených zdrojů.

2. Kompetenční

Personál zpravodajského zabezpečení vykazuje strukturální kompetenční nedostatky. Pro příslušníky není vytvořena národní vzdělávací soustava, skládající se z odborných kurzů a autorizovaných vzdělávacích materiálů, systematický výcvik a školení – zaměřujících se primárně na osvojení tvrdých dovedností a technických znalostí. Velká část příslušníků dále nesplňuje požadavky na účast v zahraničních odborných kurzech (jazyková vybavenost, nezařazení na systemizovaném místě specialisty OSINT). Třetí problematickou oblastí je nesystematická práce podpory rozvoje nezbytných měkkých kompetencí, přispívajících k efektivnímu výkonu, kdy se jedná zejména o informační gramotnost, rozvoj kritického myšlení a schopnost systematické práce se zdroji.

Na základě provedené analýzy lze konstatovat, že hypotéza**: H1: AČR disponuje adekvátní strukturou zpravodajských orgánů na taktickém stupni. Nebyla potvrzena.**

K nápravě současného stavu je nezbytné učinit celou řadu kroků v oblastech doktrín, organizační struktury, technologické a výpočetní infrastruktury, personálu a výcviku.

2.3. Využití OSINT v oblasti národní bezpečnosti

Cílem této kapitoly představení reálné případové studie, za účelem verifikace aplikovatelnosti zpravodajství z otevřených zdrojů jak na taktickém, stupni velení a řízení a uplatnění dříve popsaných procesů. Kapitola si nadále klade za cíl nastínit možné oblasti využití OSINT v rámci procesu IPB, včetně ukázky možných technik uplatnitelných v dané činnosti. Pouze pro úplnost je představ plánovací a rozhodovacího proces velitele, jako nosný koncept plánování na taktickém stupni.

Zpravodajská příprava bojiště, v rámci vojenského rozhodovacího procesu (MDMP - Military Decision Making Process) MDMP, byla vybrána pro svoji klíčovou roli v plánování vojenských operací na taktické úrovni. Uplatnitelnost a využitelnost OSINT tak bude analyzována v činnosti ryze taktické. Některé činnosti zpravodajského zabezpečení v míru, nelze označit za čistě taktickou úroveň, kdy nutně nemusí splňovat některý z atributů. Typickým příkladem jsou souhrnné zpravodajské informace nebo tematické zpravodajské informace.

Cílem této kapitoly není objasnění tvorby, účelu ani uplatnění zpravodajské přípravy bojiště, ani tvorba úplné plánovací dokumentace v gesci štábu nebo zpravodajského orgánu.

V rámci popisované případové studie bude popsán přínos zpravodajství z otevřených zdrojů do procesu zpravodajské podpory, postup jak zpravodajské podpory bylo dosaženo a provázanost s postupy, metodami a nástroji zpravodajství z otevřených zdrojů. Na úvod je uveden kontext případové studie, následuje popis událostí a způsob přispění OSINT k dané problematice.

Kapitola je strukturována do několika částí:

Teoretická – popisující pojmy a principy nezbytné pro pochopení přínosu OSINT v rámci procesu zpravodajské přípravy bojiště (IPB - Intelligence Preparation of Battlefield) na taktickém stupni (zpravodajská příprava bojiště, plánovací a rozhodovací proces velitele,)

1. Zavedení do případové studie – část seznamující s řešenou problematikou. Tato část je dále strukturována do podoby zjednodušeného bodového bojového rozkazu tak, jak je běžně využíván na taktickém stupni velení a řízení. Bojový rozkaz bude, pouze pro potřeby této práce, koncipován jako rozkaz pro zpravodajské orgány, nikoli pro jednotku jako takovou. Zároveň, s ohledem na charakter práce, autor odstoupil od dodržování některých norem zpracování.
2. Příspěvek OSINT – zde je v konkrétních oblastech ukázána role OSINT, včetně možných technik.

2.3.1. Teoretická východiska

Vojenský plánovací a rozhodovací proces

Je interaktivní plánovací metodologie celého štábu vojenské jednotky, k pochopení situace a úkolu, vytvoření variant činnosti a tvorbu operačního plánu/bojového rozkazu. Skládá se ze sedmi kroků:

1. Přijetí úkolu
2. Analýza úkolu
3. Tvorba variant činnosti
4. Analýza variant činnosti
5. Porovnání variant činnosti
6. Schválení variant činnosti
7. Tvorba bojového rozkazu a jeho distribuce

Zpravodajská příprava bojiště je jedním, z nejvýznamnějších procesů, do něhož přispívá zpravodajské zabezpečení na taktickém stupni. Jeho cílem jsou, vedle podpory plánovacího a rozhodovacího procesu, identifikace relevantních aspektů ovlivňujících úspěšné splnění úkolu.

Zpravodajskou přípravu bojiště lze vnímat jako příspěvek zpravodajských orgánů do procesu MDMP, které významnou měrou slouží jako vstup do plánovacího procesu ostatních složek štábu a zejména k podpoře rozhodování velitele.

IPB je složen ze čtyř kroků:

1. **Definování operačního prostředí**
    1. Identifikace významných charakteristik prostoru operace a zájmového prostoru
        1. Geografie, terén a počasí v prostoru.
        2. Populace (etnické, náboženské a věkové rozložení populace v prostoru operace).
        3. Politické a socio-ekonomické faktory (způsob fungování kmenů, klanů, náboženských organizací, korupce, věku, pohlaví, etnika)
        4. Infrastruktura (dopravní, telekomunikační)
        5. Pravidla použití sil.
        6. Hodnocení bezpečnostních aktérů (vojenské schopnosti,

paramilitantní skupin, kriminální a teroristické skupiny, organizovaný zločin, protivládní skupiny.

2. Nepřítel

Analýza protivníka/nepřítele nezahrnuje pouze analýzu známého protivníka/nepřítele, ale také zhodnocení potenciálních hrozeb a rizik

3. Terén a počasí
4. Civilní prostředí

2. **Popsat vliv prostředí na operaci**
    1. Vliv hrozeb (pravidelné, nepravidelné, hybridní)
    2. vliv terénu
    3. vliv počasí (viditelnost, vítr, srážky, oblačnost, teplota, vlhkost, atmosférický tlak)
    4. vliv civilního prostředí
3. **Hodnocené hrozeb**
    1. charakteristika hrozeb (složení, bojová efektivita, síla, doktrína a taktika, schopnosti a omezení)
    2. generický a doktrinální model (doktríny, minulé zkušenosti)
    3. schopnosti hrozeb
4. **Určení variantu činnosti nepřítele**

Bojový rozkaz velitele

Představuje základní dokument k vedení boje (operace). Jedná se o textový dokument s předepsanými přílohami, které vydává velitel podřízeným velitelům s cílem účinně splnit úkol operace ve vzájemné součinnosti.

1. Všeobecná situace (situace nepřítele, situace vlastní, úkol nadřízeného, záměr nadřízeného, úkol, cíle a činnost sousedů, posilové prostředky k dispozici, ostatní situace)
2. Úkol
3. Způsob plnění (záměr boje, manévr, úkoly podřízeným jednotkám, palby)
4. Logistika, administrativa (materiál a služby, zdravotnické zabezpečení, civilně-vojenská spolupráce)
5. Velení a spojení

Teoretická východiska představují strukturovaný procesní model zpravodajské přípravy bojiště k zajištění požadovaných informací na výstupu z procesu. Jejich znalost je mandatorní pro zabezpečení základní úlohy zpravodajského zabezpečení. Tato teoretická východiska jsou dostatečně kodifikována a aplikována na všech úrovních velení a řízení AČR.

2.3.2. Praktická aplikace OSINT na taktickém stupni AČR

Níže uvedený bojový rozkaz je uveden z důvodu zasazení analýzy do kontextu a za účelem pochopení provázanosti procesů zpravodajské přípravy bojiště a plánovacího a rozhodovacího procesu.

Analýza byla provedena na základě hodnocení reálných zpravodajských orgánů při obdobném (ceteris paribus) námětu. Dalším zdrojem byly analogická hodnocení a pozorování v rámci vojenských cvičení a zahraničních operací. Výsledky byly následně zevšeobecněny aby, došlo k zajištění dodržení všech platných legislativních norem.

1. Všeobecná situace

Vybudování komunikace představuje kritický prvek ve stabilizačním, modernizačním a demokratizačním úsilím v Afganistánu. Komunikace spojuje dvě významná regionální centra (KANDAHAR, TARIN KOWT) oblastí s nejsilnějšími protivládními postoji, oblast DURRANI a GHILZAI u Afgánsko-Pákistánských hranic. Celková délka budované komunikace čítá 117 kilometrů, v současné době je vybudováno přibližně 47kilometrů za devět měsíců.

Oblast je neobydlená, vyznačujícím suchem a prašným povětřím, doprovázeným meteorologickým jevem zvaným „khabad“ – silným prašným větrem.

1.1. Situace nepřítele

Hnutí TALIBAN v minulosti využívalo silné podpory obyvatelstva oblasti, jak pro přípravnou, tak i realizační fází výpadů proti koaličním silám. Civilní obyvatelstvo historicky silně nakloněno hnutí TALIBAN.

Hlavní zásady *„Pashtunwali"- výběr*
Paštunové odvozují čest od následujících zásad. Respektují pouze čestné válečníky.
Pomstít krev
Bránit svým životem osobu, jíž poskytuji útočiště, bez ohledu na její původ
Bránit svým životem vlastní a svěřený majetek
Být pohostinný a bránit život a majetek hostů
Vyhnout se zabíjení žen a Hindů
Cizoložnictví trestat smrtí
Ušetřit toho kdo žádá v boji o smilování

Tabulka 2: Hlavní zásady Pashtunwali

Obyvatelstvo je převážně Paštunské a sunnitské afilace Islámu, orientující se zejména na zemědělství, dodržující striktní kodex „Pashtunwali", nastavující rozdílné sociální normy. Pashtunwali je budováno na tradicích individuální nezávislosti, kolektivního řešení sporu a sdíleného kodexu cti odrážejících se ve všech aspektech života. Společným jmenovatelem je odmítání vnucování pravidel z vnějšku. Míra dodržování je však odvislá oblast od oblasti, čím izolovanější oblast, tím striktnější dodržování.

Reálnou moc nemá hnutí TALIBAN, jako sympatizující „khanové" – kmenoví vůdci, jejichž zájmy jsou však proměnlivé. TALIBAN dlouhodobě podkopává centrální autoritu vládu, která nemá pod kontrolou venkovské a horské oblasti. TALIBAN je schopen kontrolovat tyto oblasti prostřednictvím sítě khanů, na které je uplatňován silný nátlak, zastrašování a cílené vraždy.

Útoky na koaliční síly jsou prováděny, s ohledem na charakter terénu, především léčkou za využití výbušných zařízení (miny, improvizované výbušné prostředky), střelbou z malých ručních zbraní. Povstalecké jednotky preferují nepřímý způsob vedení bojové činnosti.

1.2. záměr nadřízeného

Komunikace bude financována prostřednictvím US Agency for International Development (USAID) a primárně bude využíváno místních dodavatelů a subdodavatelů. Výstavbou komunikace je pověřen ženijní armádní sbor, konkrétně 528. ženijní prapor, který bude v březnu 2005 vystřídán 864. ženijním praporem.

2. Úkol

Zajistit bezpečnost výstavby komunikace z KANDAHARU do TARIN KOWAT v období následujících 5 měsíců. K tomu nařizuji vlastními silami zpracovat IPB za využití všech dostupných zdrojů.

3. Způsob plnění

Zpravodajskou přípravu bojiště zpracovat v podmínkách „Red team analysis“.

Zpravodajská podpora bude zajištěna v průběhu celého procesu výstavby komunikace (plánování, průzkum, zajištění bezpečnosti, a to včetně bezpečnosti dodávek materiálu a údržby ženijní techniky).

4. logistika, administrativa

Ženijní jednotky primárně využívat organických sil a prostředků. Subdodávky a dodávky materiálu řešit prostřednictvím civilně-vojenské spolupráce s místními firmami, stejně tak najímání pracovní síly na pomocné práce.

Zdravotnické zabezpečení pro spojenecké síly řešeno postupy platnými pro spojenecké operace.

Zdravotnické zabezpečení místního obyvatelstva řešit následovně: První pomoc a neodkladná lékařská pomoc řešit organickými silami, následná péče bude zabezpečena prostřednictvím místního zdravotnického systému.

5. velení a spojení

neřeší se

Po obdržení bojového rozkazu zahájil zpravodajský orgán dotčené jednotky zpracovávání svých příspěvků do MDMP a jednotlivých dokladů veliteli. Práce byla prováděna paralelně ve dvou obecných rovinách (analýza prostoru

operace[44] a hodnocení hrozeb[45]), výstupy jsou následně použity jako vstupy do analýzy vlivu na vedení činnosti vlastních sil a prostředků. Před zahájením testování vybrané varianty (provedení válečné hry), byl sestaven detailní model všech relevantních protivníků a nepřítele zasazeném do kontextu prostoru vedení bojové operace. Poznatky získané ve válečné hře jsou následně využity k úpravě zvolené varianty tak, aby v maximální možné míře naplňovala kritéria hodnocení stanovená velitelem dané jednotky a jeho nadřízeným.

V rámci zpracování analýzy prostoru operace, se zpravodajské orgány AČR opírají o velice kvalitní podkladová geografická data a související informace, nalézající se v interních databázích, případně na sdílených úložištích dostupných ze sítě internet. Tento přístup je omezen nutnou registrací. Čistě otevřených zdrojů bylo využito pro aktualizaci dat a získání podrobnějších informací. Zde převládalo využívání nejznámějších internetových vyhledávačů. Výslednými produkty jsou mapy se zákresem ve vrstvách a textový soubor, obsahující bližší popis. Vedle obecných charakteristik je nezbytné získat i detailní informace například o stavu mostů (výška, únosnost, materiál), půdním složení (mající vliv na následné hodnocení vlivu počasí na průchodnost) apod. Tento materiál je následně předán podřízeným jednotkám jako hlavní vstup k jejich plánovacímu procesu a je poskytována podpora k zajištění podkladů a analýz na geograficky více vymezený prostor.

Analytická část hodnocení vlivu prostředí na vedení činnosti, představuje sérii kroků k posouzení vlivu fyzické domény na vedení bojové činnosti například v nejrůznějších kombinacích faktorů (terén, počasí, protivník/nepřítel a civilního prostředí).

Následující třetí fázi lze charakterizovat shromažďováním identifikovaných znalostních mezer, kombinaci získaných dat a informací a zasazování do kontextu. Zde lze spatřit největší slabinu využití OSINT, kdy stávající stav představuje nezbytné minimum a není využito potenciálu. Využívání sociálních médií a internetových vyhledávačů je vhodným začátkem, nicméně v dnešní době je nezbytné, aby navazoval detailnější výzkum.

---

[44] Zaměřuje se na přírodní podmínky v prostoru vedení operace jako je geografie, terén, počasí, sociální struktura aj.

[45] Provádí se analýza protivníka a nepřítele z pohledu jeho záměru, schopností a odhodlání

Závěrečný krok „Tvorba a schválení variant“ je už dále analytickým a simulačním procesem.

1. Fáze: Definování operačního prostředí

Stávající kombinace technik a dat využívaných pro shromažďování dat z „tvrdých“ oblastí (terén, reliéf, počasí) se zdá vyhovující a vytváří potřebný synergický efekt.

Hodnocení měkkých oblastí (věkové, náboženské, etnické složení atd.) vyžaduje aktivní formu přístupu k OSINT za účelem získání aktuálních a věrohodných dat. Zpravodajské orgány se však omezují pouze na základní vyhledávání prostřednictvím internetových vyhledávačů[46], při čemž jsou ignorovány ostatní metody shromažďování, které OSINT nabízí. Stávající stav je hodnocen jako dostatečný, ale neuspokojivý.

Hodnocení bezpečnostních aktérů představuje kombinaci výše uvedených postup. Lze konstatovat, že stav je uspokojivý s velkým potenciálem pro zlepšení.

2. Fáze: Vliv prostředí na vedení činnosti

Druhý krok procesu představuje analytickou fázi a pro potřeby této práce nepředstavuje významný přínos, proto bylo od jeho zhodnocení

3. Fáze: Hodnocení hrozeb

Hodnocení hrozeb skýtá největší potenciál pro uplatnění OSINT ve spolupráci s ostatním zpravodajskými obory. Jedná se o kombinaci všeobecných a detailních dat a informací, zasazovaných do konkrétního prostředí a porovnávání s interními databázemi. Celková míra uplatnění metod a technik OSINT je dostatečná, ale neuspokojivá.

4. Fáze: Tvorba a schválení variant

Nebylo hodnoceno z důvodu minimální potřeb dodatečného shromažďování.

Zpravodajský obor OSINT zaujímá významné místo v procesu zpravodajské přípravě bojiště, nicméně k plnému využití potenciálu bude nutné učinit řadu opatření, jež bude rozvedena dále v textu. Na základě provedené analýzy

[46] Včetně využívání pokročilého nastavení a operátorů

lze konstatovat, že hypotéza **H3: „Nástroje OSINT jsou uplatnitelné v rámci zpravodajského zabezpečení AČR.“ Byla potvrzena.**

Hypotéza H2: **Zpravodajský obor zpravodajství z otevřených zdrojů poskytuje požadované výstupy aplikovatelné na taktickém stupni velení a řízení AČR. Nebyla potvrzena.**

2.3.3. Příspěvek OSINT

Zpravodajské orgány na taktickém stupni, při zpracování zpravodajské přípravy bojiště vychází zejména z interních dokumentů a zdrojů dat. OSINT je vnímán jako nástroj k odstranění mezer ve vědění, dopřesnění dat a informací a k monitoringu aktuálního dění.

Role OSINT tak ve značné míře závisí na fázi procesu. Úvodním krokem je *„Definování operačního prostředí“,* tedy část, kdy dochází ke shromažďování velkého množství všeobecných poznatků, dat a informací. Zde má OSINT nenahraditelnou úlohu. S přibývajícími kroky se navyšuje podíl analýzy, role jiných zpravodajských oborů a tvrdých znalostí. Role OSINT se tedy s přibývajícími fázemi výrazně snižuje. Již ve druhém kroku je vliv OSINT pouze nepřímý.

Oblast	Podoblast	Analýza sociálních médií	Archivní zobrazení webových stránek	Geografické informační systémy (GIS)	Grafické nástroje	Kopírování webových stránek	Metadata	Síťová a technická infrastruktura	Údaje o uživatelích	Vyhledávače, metavyhledávače	Webové scraperování	Pokročilá analýza textu
Geografie	Sídla											
	Vodstvo											
	Porost											
	Pohoří											
Terén	Reliéf											
	Výškopis											
	Půdní složení											
Počasí	Klimatické podmínky											
	Vlhkost											
	Oblačnost											
	Povětří											
Etnické složení	Etnické rozdělení											
	Geografické zastoupení											
	Zvyky, tradice, hodnoty											
Náboženské složení	Procentuální zastoupení											
	Geografické rozmístění											
	Vazby											
Věkové rozložení	Věkové rozvrstvení											
	Věkové rozvrstvení dle pohlaví											
	Věkové rozvrstvení dle geografického umístění											
Sociální struktura	Vzdělání											
	Zaměstnanost											
	Průměrný výdělek											
Náboženské organizace	Charakteristika											
	Klíčové osobnosti											
Genderová struktura	Věkové rozvrstvení dle pohlaví											
	Geografické rozmístění dle pohlaví											
	Vzdělání dle pohlaví											
	Zaměstnanost dle pohlaví											
	Průměrný příjem dle pohlaví											
Korupce a organizovaný zločin	Míra kriminality											
	Druh kriminality											
	Charakteristika aktérů											
Dopravní infrastruktura	Silnice (vč. mostů, tunelů)											
	Železnice (vč. mostů, tunelů)											
	Letiště											
	Vodní doprava (vč. splavů, průplavů)											
Komunikační infrastruktura	Telefonní spojení											
	Datové spojení											
Hodnocení bezpečnostních aktérů	Přehled bezpečnostních aktérů											
	TTP											
	Profily vůdčích osobností											
	Vazby											
	Mediální prezentace											
	Záměr, schopnosti, odhodlání											

Obrázek 7: Zhodnocení aplikace metod OSINT

Za účelem zpřehlednění používaných metod byla vypracována *„Přehledová tabulka aplikovaných metod OSINT“*, vycházející z jednotlivých bodů zpravodajské přípravy bojiště, kroku *„Definování operačního prostředí*[47]*“,* k nimž jsou vztaženy reálně vyžívané metody a techniky (zelená), u brigádních/praporních úkolových uskupení pozemních sil a jejich ekvivalentu u vzdušných sil. Nicméně uplatnitelných metod je celá řada, nicméně z řady objektivních i subjektivních důvodů nejsou používány. Mezi nejčastější[48] důvody nepoužívání sotisfikovanějších metod jsou:

1. Nekvalifikovaný personál (nezaškolen, neseznámen),
2. absence technických prostředků.

Z tohoto důvodu bylo přistoupeno k uvedení doporučené metody (oranžová). Volba doporučené metody zohledňuje výše uvedené důvody a navrhuje takové, které vykazují nejnižší zdrojovou náročnost, při zachování maximalizace informační výnosnosti.

Při pohledu na grafickou reprezentaci výsledků analýzy vyplývá, že taktické zpravodajské orgány zpravodajského zabezpečení se opírají zejména o činnost (meta)vyhledávačů, případně o geografické informační systémy. Co do palety využívaných metod a technik, představuje nejširší záběr profilování zájmových osob, kde však dochází pouze k pozvolnému rozšiřování znalostí technik a metod zpravodajských orgánů. Trend analýzy sociálních médií, způsobený zejména generační obměnou, je patrný.

Z provedené analýzy vyplývá, že rozmanitost využívaných metod a technik, v rámci zpravodajské přípravy bojiště není široká. Analytici v naprosté většině případu využívají pouze základní techniky, nevyžadující hlubší technické znalosti a dovednosti, zejména pak archivní zobrazení webových stránek a využití vyhledavačů a Meta vyhledávačů. Tyto metody a techniky jsou uzpůsobené možnostem taktického stupně při plánování a vedení bojové činnosti. Činnost

[47] Tato fáze procesu zpravodajské přípravy bojiště byla vybrána úmyslně, vzhledem k podstatnému příspěvku OSINT, který s přibývajícími fázemi klesá na úkor analýzy a jiných zpravodajských oborů. Tento jev je logickým dopadem zaměření OSINT na shromažďování dat a informací. Pozdější fáze již provádí fúzování a kombinování dat a informací.

[48] Jedná se o osobní zkušenost rozšířenou o diskusi s náčelníky zpravodajských orgánů

probíhá zpravidla na dočasných místech velení – hlavní místo velení a záložní místo velení dislokovaných v prostoru vedení bojové činnosti.

Tento výsledek byl předatelný vzhledem k omezujícím podmínkám a zvolenému procesu k analýze. Další příčinou značné omezenosti rozmanitosti využívaných metod je lidský kapitál (vzdělání a zaškolení) a absence technického vybavení, zejména vhodného softwaru. Bez eliminace těchto slabých míst, nelze pokračovat pokročilejšími metodami a tím i většího využití OSINT v rámci zpravodajského zabezpečení v AČR.

O kreativním využití technik OSINT lze hovořit zejména v případě hodnocení hrozeb a jednotlivých aktérů, takzvanému profilování, což z celkového pohledu zpravodajské přípravy bojiště, představuje pouze zlomek objemu dat a informací.

Díky provedené analýze lze konstatovat, že pro zvýšení efektivity OSINT a následného synergického efektu v rámci zpravodajské přípravy bojiště, se skýtají zpravodajskému zabezpečení v této oblasti následující příležitosti:

- Implementace metod a technik webového scraperování,
- zavádění nástroje pokročilé analýzy textu,

Na základě provedené analýzy lze konstatovat, že hypotézy**: H2: Zpravodajský obor zpravodajství z otevřených zdrojů poskytuje požadované výstupy aplikovatelné na taktickém stupni velení a řízení AČR. Nebyla potvrzena.** Analýza zároveň ukázala na mnoho slabých míst ve využití OSINT v rámci zpravodajské přípravy bojiště zpravodajským zabezpečením AČR.

Hypotéza H3: „Nástroje OSINT jsou uplatnitelné v rámci zpravodajského zabezpečení AČR.“ Byla potvrzena.

3. Závěr

Diplomová práce *„Využití zpravodajství z otevřených zdrojů (OSINT) v oblasti národní bezpečnosti – metody, nástroje, případové studie“* analyzuje zpravodajský obor zpravodajství z otevřených zdrojů v rámci systému zajištění národní bezpečnosti, jehož je nedílnou součástí, se zaměřením na taktický stupeň velení a řízení.

Diplomová práce si kladla za cíl:

1. představení zpravodajství z otevřených zdrojů jako jeden z nástrojů zpravodajského zabezpečení,
2. seznámení s vybranými metodami a nástroji,
3. objasnění využití OSINT na konkrétní a reálné situaci,
4. zodpovězení výzkumné otázky: *„Je OSINT aplikovatelný v rámci zpravodajského zabezpečení na taktickém stupni velení a řízení?“*

Zároveň byly stanoveny 3 hypotézy, jejichž verifikace/odmítnutí napomohla k zodpovězení výzkumné otázky.

Cíl číslo 1: *„Představení zpravodajství z otevřených zdrojů jako jeden z nástrojů zpravodajského zabezpečení“* byl naplněn v teoretické části hlavní části diplomové práce, konkrétně v podkapitole 2.1 *„Zpravodajství z otevřených zdrojů“*. Kapitola představuje teoretické ukotvení OSINT, úlohu v rámci systému zpravodajského zabezpečení v AČR, zpravodajského cyklu, který blíže představuje. Dále byla provedena analýza cyklu zpravodajství z otevřených zdrojů. Byly představeny hlavní přednosti (např. rychlost, množství dostupných dat a informací, relativní levnosti) a rizika (manipulace a dezinformace, nedostupnost klíčových informací aj.) použití OSINT. Pro pochopení trendů byl představen vývoj v posledních 10 letech výzvy, jimž musí příslušníci zpravodajského zabezpečení čelit a předpokládaný budoucí vývoj.

K zodpovězení druhého cíle *„Seznámení s vybranými metodami a nástroji“* slouží podkapitola 2.1.5 *„Techniky a nástroje OSINT“,* v rámci, níž byl zpracován seznam nejpoužívanějších oblastí metod a technik OSINT, včetně bližšího

popisu. Ambicí této kapitoly nebyl úplný přehled, ani ukázka práce s konkrétními nástroji.

Cílů číslo 3: „Objasnění využití OSINT na konkrétní a reálné situaci“ a zodpovězení výzkumné otázky, jako cíle číslo 4: Je OSINT aplikovatelný v rámci zpravodajského zabezpečení na taktickém stupni velení a řízení?“ bylo dosaženo v kapitolách 2.2 „Zpravodajské zabezpečení v AČR“ a 2.3 „Využití OSINT v oblasti národní bezpečnosti“.

V rámci kapitoly 2.2 „Zpravodajské zabezpečení v AČR“, byl proveden popis zpravodajského zabezpečení po stránce organizačního členění a technického zabezpečení, byly identifikovány dvě hlavní skupiny slabých míst aplikace OSINT na taktickém stupni. Strukturální (absence dedikovaného personálu OSINT a dekonflikce odpovědností s nově vznikajícím operačním stupněm velení a řízení) a kompetenční (vzdělávací soustava, nedostatek kvalifikovaného personálu aj.). Právě zde došlo k odmítnutí hypotézy **H1: AČR disponuje adekvátní strukturou zpravodajských orgánů na taktickém stupni.**

Odůvodnění zamítnutí H1: V rámci organizační struktury ZZ AČR existují systemizovaná místa napříč všemi stupni velení a řízení využívající pasivní formu OSINT a základní techniky a metody. Úroveň znalostí a dovedností je dána spíše individuálními predispozicemi než systematickou přípravou. Nicméně nastavený systém poskytuje alespoň základní výstupy ze zpravodajství z otevřených zdrojů. Stávající stav však neumožňuje maximální využití všech dostupných možností. I mírná modifikace stávající organizační (navýšení počtů, určení specialistů OSINT) struktury či přípravy (zlepšení systematického vzdělávání, prohloubení doktrinální soustavy na úroveň konkrétních postupů) představuje příležitost pro kvalitativní i kvantitativní pozitivní posun v existujících schopnostech zpravodajství z otevřených zdrojů.

Kapitola 2.3 „Využití OSINT v oblasti národní bezpečnosti“ byla členěna do tří podkapitol (uvedení specifické teorie pro potřeby následného porovnání technik a metod OSINT a uvedení kontextu námětu, v rámci, něhož došlo k porovnávání dostupných a reálně využívaných technik a metod na taktickém stupni zpravodajského zabezpečení). Na základě výsledků provedené analýzy

byla zamítnuta hypotéza **H2: Zpravodajský obor zpravodajství z otevřených zdrojů poskytuje požadované výstupy aplikovatelné na taktickém stupni velení a řízení AČR.** Naopak **H3: Nástroje OSINT jsou uplatnitelné, v rámci zpravodajského zabezpečení AČR** byla potvrzena.

Odůvodnění zamítnutí H2: Pozorované výstupy se opírali převážně o práci s vyhledávači a studiem zpravodajských a odborných serverů. Přístup ke kvalitním placeným databázím zůstává velmi limitovaný a centrálně nesjednocený. Proces zpracování dat a informací neodpovídá standardům NATO dle patřičných kritérií hodnocení. V současném systému zpravodajského zabezpečení na taktické úrovni je současná podoba brána jako norma, ergo není vyvíjen tlak ze strany velitelů na kvalitativní procesní posun. Případný tlak se spíše soustředí na zaměření zpravodajského úsilí.

Odůvodnění verifikace H3: Závěrečné posouzení případové studie a reálných zkušeností zpravodajských orgánů prokázalo, že aplikace pokročilých metod by zvýšila subjektivní relevantnost OSINT a zároveň by objektivně přispělo ke zvýšení kvality výstupů.

Přestože 2 ze 3 hypotéz byly zamítnuty, lze konstatovat že OSINT **je uplatnitelný na taktickém stupni velení a řízení AČR.** OSINT je v AČR zavedeným zpravodajským oborem s vytvořenými základními předpoklady pro plnohodnotné využívání. Nicméně pro plnohodnotné využití tohoto oboru je nezbytně nutný další rozsáhlý rozvoj, vyžadující hluboké strukturální změny, přesahující samotné zpravodajské zabezpečení v AČR.

AČR si je vědoma stoupajícího trendu role OSINT v soudobém bezpečnostním prostředí a postupně rozvíjí své schopnosti, minimálně v technologické oblasti, zaváděním softwarových nástrojů pro automatické shromažďování a kontextuální analýzu. Nicméně tempo a rozsah rozvoje jsou nedostatečné. Další rozvoj je doporučeno směřovat do následujících oblastí:

Doktrinální: vznik doktrinálního sytému a podpůrných studijních materiálů.

Organizační: vytvoření systemizovaných míst pro specialisty OSINT (až na stupeň prapor a jeho ekvivalentů) a obecné navýšení počtu příslušníků

zpravodajského zabezpečení, vznik koordinačního orgánu zahrnující příslušníky OSINT, kybernetických a psychologických sil), na operačním stupni vytvoření schopnosti vzdálené podpory taktické úrovně.

Technologické: urychlení realizace nasazování podpůrného softwarového vybavení, zahájit proces zavádění softwaru pro webové screapování a pokročilou analýzu textu, v oblasti vědy a výzkumu se zaměřit na oblasti kvantového šifrování, automatizovaného shromažďování dat a informací, strojového učení, pokročilých vyhledávacích algoritmů, technologií zpracování přirozeného jazyka nebo kontextuální analýzy.

Personální: změna procesu náboru specialistů (zjednodušení a urychlení), forma odměňování monetárními (příspěvek, zvýšený stabilizační příplatek, aj) a způsobu výkonu služby (prodloužená doba rozhodná, individuální přístup k plnění fyzického přezkoušení v závislosti na předurčení podporované jednotky a míry její nasaditelnosti, možnost pravidelné práce z domu/flexibilní pracovní doba dle zařazení podporované jednotky), vytvoření komplexního národního vzdělávacího systému.

4. Seznam zkratek

AČR	Armáda České republiky
AII	Prostor zpravodajského zájmu (Area of Intelligence Interest)
AIR	Prostor zpravodajské odpovědnosti (Area of Intelligence Responsibility)
API	Rozhraní k využití služeb v jiném prostředí (Application Programming Interface)
CCIR	Požadavky velitele na důležité informace (Commander's Critical Information Requirements)
CM	Management shromažďování (Collection Management)
CP	Plán shromažďování informací (Collection Plan)
CPED	Shromáždit, zpracovat, vytěžit, šířit (collect, process, exploit, disseminate)
DIME	diplomacie, informace, vojenství a ekonomie (diplomatic, information, military and economic)
EDT	Nastupující a přelomové technologie (Emerging and Disruptive Technologies)
EU	Evropská unie (European Union)
GDPR	Obecné nařízení o ochraně osobních údajů (General Data Protection Regulation)
GIS	Geografické informační systémy (Geographic Information Systems)
IMINT	Obrazové zpravodajství (Imagery Intelligence)
IMO	Internet Ministerstva obrany
IPB	Zpravodajská příprava bojiště (Intelligence Preparation of Battlefield)

IR	Požadavky na informace (Information Requirements)
IRM	Management zpravodajských požadavků (Intelligence Requirements Management)
ISR	Zpravodajství, sledování, průzkum (Intelligence, Surveillance, Reconnaissance)
JIPOE	Společná zpravodajská příprava operačního prostředí (Joint Intelligence Preparation of Operational Environment)
LITINT	Potenciálně zpravodajsky přínosné zdroje informací z veřejně dostupných a publikovaných zdrojů (Literal Inteligence)
MDMP	Vojenský rozhodovací proces (Military Decision Making Process)
NATO	Severoatlantická aliance (North Atlantic Treaty Organization)
NLP	Zpracování přirozeného jazyka (Natural Language Processing)
OSINT	Zpravodajství z otevřených zdrojů (Open Source Intelligence)
PIR	Prioritní zpravodajské požadavky (Priority Intelligence Requirements)
PMESII	Politická, vojenská, ekonomická, sociální infrastrukturální a informační operační proměnná (political, military, economic, social, infrastructure and information)
RFI	Žádost o informace (Request for Information)
SATCEN ČR	Satelitní centrum České republiky
SOCMINT	Zpravodajství ze sociálních médií (Social Media Intelligence)
USAID	Agentura pro mezinárodní rozvoj USA (US Agency for International Development)
ZZ AČR	Zpravodajské zabezpečení Armády České republiky

5. Seznam tabulek a obrázků

5.1. Seznam tabulek

5.2. Seznam obrázků

6. Seznam použitých zdrojů

Bibliografické zdroje

1. AKHBAR, Babak, BAYERL, Saskia, SAMPSON, Fraser (Eds.). Open Source Intelligence Investigation. From Strategy to Implementation. Springer, 2016. ISBN 978-3-319-47671-1.
2. BAZZELL, Michael. *Open Source Intelligence Techniques. Resources for Searching and Analyzing Online Information.* 9. vyd. 2022. ISBN 9798761090064.
3. BORN, H., LEIGH, I. Making Intelligence Accountable – Legal Standards and Best Practice for Oversight of Intelligence Agencies, DCAF Handbook, 2005, ISBN 978-92-9222-017-4.
4. CLARK, R., M. Intelligence Analysis, a target Centric Approach, CQ Press, 2013, ISBN 978-1-4522-0612-7
5. KENT, S. Strategic Intelligence for American World Policy. Pp. xiii, 1949. LOWENTHAL, M. M. Intelligence. From Secrets to Policy. CQ Press, Washington, D.C., 2000.
6. MICHÁLEK, L., POKORNÝ, L., STIERANKO, L. a MARKO, M. Zpravodajství a zpravodajské služby. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2013. ISBN 978-80-7380-428-2.
7. PAPÍK, Richard. *Strategie vyhledávání informací a elektronické informační zdroje*. 1. vyd. Praha: Velryba, 2011. ISBN 978-80-85860-22-1.
8. POKORNÝ, L. Zpravodajské služby. Praha: Auditorium, 2012. ISBN 978-80-87284-21-6.
9. RAMWELL, S., DAY, T., GIBSON, H. Use cases and Best practice for LEAs. In Akhgar, B., Bayerl, P. S. & Sampson, F. (Ed.). Open Source Intelligence Investigation: From strategy to implementation. 2016
10. SCHULSKY, Abram. N., SCHMIDT, Gary. J. Silent Warfere, Understanding the World of secret Intelligence, third edition, Washington D.C., 2002.
11. STEELE, R. D. Open Source Intelligence, Handbook of Intelligence, ed. Loch K. Johnson, New York: Routledge, 2007, ISBN10 0-415-77050-5, s. 129 – 147.

12. WEHMEIER, S., MC´INTOSH, C., TURNBULL, J. Oxford Advanced Learner´s Dictionary of Current English, 7 edition, Oxford, English 2005. ISBN 0-19-431649-1.
13. ZEMAN, P., a kol. Česká bezpečnostní terminologie: Výklad základních pojmů. Masarykova univerzita Brno, Mezinárodní politologický ústav, 2002, 1. vyd., ISBN 80-210-3037-2

Diplomové práce

14. PAŘIL, Radek. Zpravodajství z otevřených zdrojů (OSINT) v oblasti národní bezpečnosti – zdroje, metody, postupy a nástroje. Diplomová práce. Praha: POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE, 2022.
15. STEHLÍK, Martin. ZPRAVODAJSKÉ SLUŽBY A JEJICH ÚLOHA V BOJI PROTI ORGANIZOVANÉMU ZLOČINU A TERORISMU. Diplomová práce. Brno: Masarykova univerzita, 2010.
16. SUNARDI, Daniela. Zpravodajství z otevřených zdrojů (OSINT) a jeho aplikace v oblasti národní bezpečnosti. Diplomová práce. Praha: POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE, 2021.
17. TISANČÍN, Jan. Otevřené zdroje dat v síti Internet a možnosti jejich vytěžování. Diplomová práce. Kladno: ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE, 2020.
18. VONDRUŠKA, Petr. Metody a nástroje OSINT. Diplomová práce. Praha: Bankovní institut vysoká škola Praha, 2013.

Dokumenty vojenského výboru

19. MC 0647 – POLICY ON OPENSOURCE INTELLIGENCE (OSINT)
20. MC 0646 zásady NATO pro společné zpravodajství, sledování a průzkum

Doktrinální soustava NATO v oblasti zpravodajství:

21. NATO. *AJP-2 Spojenecká společná doktrína zpravodajství, kontrazpravodajství a bezpečnosti.* B. Úřad pro standardizaci, 2020.
22. NATO. AJP-2.1 *Spojenecká společná doktrína zpravodajských postupů*. B. Úřad pro standardizaci, 2016.

23. NATO. AJP-2.7 *Spojenecká společná doktrína společného zpravodajství, průzkumu a sledování*. A. Úřad pro standardizaci, 2016.
24. NATO. AJP-2.9, *Spojenecká společná doktrína zpravodajství z otevřených zdrojů*. A. Úřad pro standardizaci, 2019.
25. NATO. AIntP-14 *Postupy společného zpravodajství, sledování a průzkumu při zabezpečení operací NATO.* A. Úřad pro standardizaci, 2016.
26. NATO. AAP-06 *Slovník NATO s termíny a definicemi vojenského významu pro použití v NATO.* A. Úřad pro standardizaci, 2023.

Doktrinální soustava AČR

27. AČR. Pub-20-63-01 *Doktrína zpravodajského zabezpečení v AČR*. Centrum doktrín VeV-VA, 2020.
28. AČR. Prog-1-3 *Programy přípravy jednotek AČR*. Centrum doktrín VeV-VA, 2021.
29. AČR. Pub-70-01-01 *Programy přípravy jednotek AČR* – 1. dopl.vyd. Centrum doktrín VeV-VA, 2022.
30. AČR. Pub-20-00-02, *Slovník základních pojmů z oblasti zpravodajského zabezpečení v AČR*. Centrum doktrín VeV-VA, 2. vyd., 2021.

Internetové zdroje

31. BIELSKA, Aleksandra. *Open Source Intelligence Tools and Resources Handbook.* I-INTELLIGENCE, 2020. [online]. [22. 12. 2023]. Dostupné z: https://documentsn.com/document/158a_open-source-intelligence-tools-and-resources-handbook.html.
32. BURKE, C. Freeing knowledge, telling secrets:Open Source Intelligence and development, CEWCES Research Papers, Paper 11, s. 1-22. [online]. [22. 12. 2023] Dostupné z: https://pure.bond.edu.au/ws/portalfiles/portal/28737919/Freeing_knowledge_telling_secrets.pdf
33. CASANOVAS, Pompeu Juan ARRAIZA, Felipe MELERO, Jorge GONZÁLEZ – CONEJERO, Gila MOLCHO, Montse CUADROS. *Fighting*

Organized Crime Through Open Source Intelligence: Regulatory Strategies of the CAPER Project. [online]. [10. 1. 2024]. Dostupné z: https://core.ac.uk/download/pdf/78532664.pdf.

34. JOHNSTON, Rob. *ANALYTIC CULTURE IN THE US INTELLIGENCE COMMUNITY*. Online. Center for the Study of Intelligence, 2005. Dostupné z: https://www.cia.gov/static/Analytic-Culture-Intelligence-Community.pdf. [cit. 2024-01-11].
35. STROUHALOVÁ, J. *Vybrané trendy globální bezpečnosti*. [online]. [29. 12. 2020]. Dostupné z: https://www.valka.cz/14431-Vybrane-trendyglobalni-bezpecnosti
36. ZEMAN, P. *ZPRAVODAJSKÝ CYKLUS – KLIŠÉ NEBO NOSNÝ KONCEPT?* In: OBRANA A STRATEGIE / DEFENCE & STRATEGY [online]. [10.1.2024] Dostupné z: https://www.obranaastrategie.cz/cs/archiv/rocnik-2010/1-2010/clanky/zpravodajsky-cyklus-klise-nebo-nosny-koncept.html