Operativna upotreba OSINT-a u istraživanju organiziranih kriminalnih grupa

Emir Muhić, MA[1]

SAŽETAK

Organizirane kriminalne grupe (OKG) predstavljaju značajnu prijetnju nacionalnoj i međunarodnoj sigurnosti, zahtijevajući prilagodljive i inovativne pristupe u njihovom istraživanju. U ovom radu istražuje se uloga OSINT-a (Open Source Intelligence) kao ključne metode prikupljanja i analize podataka iz javno dostupnih izvora u kontekstu borbe protiv navedenih aktera. OSINT omogućava efikasno prikupljanje informacija o članovima OKG-a, njihovim aktivnostima i mrežama bez fizičkog izlaska na teren, čime se minimiziraju operativni rizici. Korištenjem društvenih mreža, digitalnih forenzičkih podataka i drugih otvorenih izvora, istražitelji mogu pratiti komunikacije, geolocirati aktere i analizirati obrasce ponašanja kriminalnih grupa. Kroz hipotetički primjer rad ukazuje na važnost OSINT-a u bržem donošenju operativnih odluka i razvoju strategija za neutralizaciju kriminalnih aktivnosti. Cilj istraživanja je razviti operativni model primjene OSINT-a u slučajevima organiziranog kriminala, uz isticanje njegovih prednosti i izazova. Zaključak naglašava važnost unapređenja vještina istražitelja u korištenju OSINT alata, kao i potrebu za jasnim okvirom za upotrebu.

Ključne riječi: *OSINT, organizovane kriminalne grupe, digitalna forenzika, operativni modeli.*

[1] Doktorant, Fakultet za kriminalistiku, kriminologiju i sigurnosne studije.

UVOD

Istraživanje organiziranih kriminalnih grupa[2] je oduvijek predstavljalo značajan izazov i problematiku za državne agencije i službe za provedbu zakona. Evolucija i prilagodba organiziranih kriminalnih grupa (u nastavku teksta OKG) je uslovila i prilagodbu prethodno navedenih agencija i službi koje se u značajnoj mjeri oslanjaju na obavještajni rad. Također, značaj i uloga modernih tehnologija, kao i društvenih mreža koje su neizostavni dio čovjekovog života, omogućavaju efikasnije prikupljanje operativnih podataka koji služe kao podrška istragama. U tom kontekstu, OSINT (Open Source Intelligence) – prikupljanje obavještajnih informacija iz otvorenih, javno dostupnih izvora – postaje sve značajnije sredstvo. OSINT se ističe kao ključni segment savremenog obavještajnog rada zbog mogućnosti brzog, jeftinog i širokog pristupa informacijama koje su od kritične važnosti za identifikaciju i analizu bezbjednosno interesantnih aktera. Uloga OSINT-a u rješavanju cyber kriminala i organiziranog kriminala sve je više prepoznata u novijim istraživanjima (Kao, Chao, Tsai, & Huang, 2018). Na primjer, OSINT bi mogao povećati tačnost krivičnog gonjenja i hapšenja krivaca pomoću okvira poput onog koji su predložili Quick i Choo (Quick & Choo, 2018). Takvi okviri osiguravaju ne samo strukturiran pristup analizi, već i integraciju podataka koji dolaze iz različitih izvora, čime se omogućava sveobuhvatan pregled kriminalnih aktivnosti i povezivanje naizgled nepovezanih informacija. Konkretno, autori primjenjuju OSINT na digitalne forenzičke podatke raznih uređaja kako bi poboljšali analizu kriminalističko-obavještajnih podataka (J. Pastor-Galindo, 2020). Kako bi se riješile dileme u razumijevanju i prevođenju termina *intelligence* na B/H/S jezike, u ovom radu će on imati kontekst *obavještajne informacije* koju čini analitički obrađen podatak[3] i informacija[4] kako bi se osigurala precizna terminološka jasnoća. OSINT ima dugu historiju i njegov početak se veže za Drugi svjetski rat i evidentiranje

[2] OKG u ovom radu prate definiciju UNDOC-a koja glasi: „*strukturirana grupa od tri ili više osoba koja postoji u određenom vremenskom periodu, čiji članovi zajednički djeluju u cilju izvršenja jednog ili više teških zločina ili krivičnih djela, u cilju sticanja direktne ili posredne finansijske ili druge materijalne koristi*."

[3] Podatak je činjenica predočena u određenom formatu – riječ, slika, broj, znak, slovo i tako dalje.

[4] Informacija je logički povezana skupina podataka koja ima određeno značenje.

protivničke propagande koja je dolazila iz tradicionalnih medija. Danas, OSINT ima značajnu primjenu u obavještajnom radu (vojnom, civilnom, cyber) i služi kao bitan element dolaska do informacija o stanju i procesima bitnih za nacionalnu sigurnost (DHS, 2022). Kompleksnost istraživanja i procesuiranja OKG nalaže i upotrebu adekvatnih obavještajnih metoda kao što su OSINT, HUMINT, SIGINT i tako dalje. OSINT za razliku od ostalih metoda omogućava dublju analizu digitalnog i društvenog okruženja bez nužnog oslanjanja na terenski rad i izlaganju opasnosti. Osim toga, OSINT kao metoda omogućava objektivno istraživanje bezbjednosno interesantnih aktera bez izlaska na teren jer se zasniva na verifikaciji i analizi podataka iz javno dostupnih izvora. U istraživanju OKG i njihovih članova koriste se otvoreni izvori kao što su društvene mreže na kojima akteri mogu ostaviti značajan broj podataka i informacija, kao što su fotografije, video snimke, objave i tako dalje. Predmet ovog istraživanja je analiza upotrebe OSINT-a kao obavještajne discipline u otkrivanju, identificiranju, praćenju i dokumentovanju aktivnosti organiziranih kriminalnih grupa. Kao osnovni cilj rada se nameće razvoj operativnog modela plana primjene OSINT aktivnosti u slučajevima istraživanja organiziranih kriminalnih grupa i pojedinačnih bezbjednosno interesantnih aktera. Svrha ovog istraživanja se ogleda u nedovoljnoj istraženosti i marginalizaciji operativne primjene OSINT-a u istraživanju organiziranih kriminalnih grupa, jer su se dosadašnja istraživanja usmjeralvala samo na definisanje pojma.

1. Teorijski i praktični koncept OSINT-a

Širenjem i razvojem cyber prostora kao nove domene ljudskog života, omogućeno je obavještajno djelovanje i prikupljanje podataka i informacija. Kada se govori o otvorenim izvorima, oni u tradicionalnom smislu obuhvataju bilo kojeg nosača informacije – audio, video, foto ili tekstualni zapis. Cyber prostor kao domena je omogućila jednostavniji pristup podacima i informacijama, pri čemu je provođenje istrage pojednostavljeno i olakšano. Definisanje OSINT-a se zasniva dolasku do traženih informacija iz javno dostupnih izvora, te s obzirom na mnoštvo definicija različitih državnih i nedržavnih aktera, kao osnova će se koristiti ona koju je dao Ured direktora nacionalne obavještajne službe (ODNI) Sjedinjenih Američkih Država. ODNI (2011) OSINT definiše kao *obavještajne podatke proizvedene iz javno dostupnih informacija koje se prikupljaju, iskorištavaju i blagovremeno distribuiraju odgovarajućoj publici u svrhu ispunjavanja specifičnih obavještajnih zahtjeva*. Kako navodi Baker (2023), javno dostupne informacije su bilo koji podatak koji je dostupan javnosti bez upotrebe tajne dozvole ili upada u sistem; međutim, može uključivati i podatke koji stoje iza paywall-a kao što je pretplata na novine. Ovi podaci se mogu prikupiti s interneta, društvenih medija, mainstream medija, publikacija i pretplata, audio zapisa, slika, video zapisa i geoprostornih/satelitskih informacija i tako dalje (Baker, 2023). Pored navedenog, ODNI (2011) navodi i

takozvanu „sivu literaturu[5]“ - materijal otvorenog izvora koji je obično dostupan putem kontroliranog pristupa za određenu publikukao i promatranje i izvještavanje[6]. S obzirom na neke ulazne podatke, zajedno sa primjenom naprednih tehnika prikupljanja i analize, OSINT kontinuirano proširuje znanje o meti (J. Pastor-Galindo, 2020). Na taj način pronađene informacije ponovo hrane proces prikupljanja kako bi se približili konačnom cilju (Williams & Blum, 2018).

Osnovni princip OSINT-a je doći do podatka ili informacije iz već postojećeg sadržaja koji se nalazi u cyber ili fizičkom domenu bez nedozvoljenog ulaska u štićene sisteme i mreže. Dakle, OSINT je čisto pasivna metoda koja ne koristi penetraciju i aktivno izviđanje (Baker, 2023). Svaki drugi ulazak u sistem ili mrežu se smatra penetracijom u štićeni sistem i ne spada u OSINT metode. Iako se alati za OSINT prikupljanje razvijaju gotovo svakodnevno, metode koje koriste sami alati mijenjaju se manje dramatično. Većina alata koristi leksičku analizu, analizu mreže, geoprostornu analizu ili kombinaciju ovih metoda za izolaciju, opisivanje i analizu podataka (Williams & Blum, 2018). Sve tri metode postojale su mnogo prije njihove primjene na sadržaje zasnovane na Internetu, ali ogromna proliferacija platformi društvenih medija i sve veća lakoća s kojom pojedinci mogu pristupiti Internetu čine to okruženje bogatim za prikupljanje obavještajnih podataka (Williams & Blum, 2018). S obzirom na digitalizaciju materijalnog svijeta, izvori su najčešće na Internetu i zahtjevaju aktivno traganje, evidentiranje i obrađivanje. U navedenom koriste se različiti elementi nosioca tražene obavještajne informacije kao što su društvene mreže, blogovi, portali, web stranice i tako dalje, na kojima se primjenjuju metode, tehnike i alati pogodni za dolazak do traženog. OSINT nije striktno upotreba alata – softvera i hardvera, već se ogleda i u logičkom povezivanju podataka i informacija, kako bi se odgovorilo na obavještajni zahjev nadređenog. Određene istrage ne zahtjevaju tehnička znanja, već samo niz logičkih i intutitivnih koraka, dok s druge strane postoje istrage koje nalažu poznavanje mrežnih i računarskih sistema, softvera, hardvera i tako dalje kako bi se ispunili obavještajni zahtjevi. Na primjer, nadređeni može dati zadatak da se prikupe osnovne informacije o bezbjednosno interesantnom licu za koje postoji osnovana sumnja da je pripadnik OKG. Pretragom društvenih mreža kao što su Facebook, Instagram ili TikTok, može se doći do osnovnih informacija – interesi (muzika, filmovi, video igre, sportovi i tako dalje), fizički izgled kroz duži vremenski period (može se koristiti za

[5] Kao sivu literaturu ODNI (2011) navodi: izvještaji o istraživanju, tehnički izvještaji, ekonomski izvještaji, izvještaji o putovanjima, radni dokumenti, dokumenti za diskusiju, nezvanični vladini dokumenti, zbornici, preprinti, studije, disertacije i teze, trgovačka literatura, istraživanja tržišta i bilteni. Građa u sivoj literaturi pokriva naučne, političke, socioekonomske i vojne discipline.

[6] Informacije od značaja, koje inače nisu dostupne, a koje daju, na primjer, amaterski posmatrači aviona, radio monitori i satelitski posmatrači (ODNI, 2011).

crossreferencing sa drugim slučajevima), informacije o putovanjima, način i stil života (luksuzan, umjeren, asketski) i tako dalje. Analizom naloga na društvenim mrežama mogu da se saznaju informacije o predmetnom licu. Ukoliko je obavještajni zahtjev izazovniji – određivanje *modus operandi* grupe, potrebne su određene vještine i znanja. Na primjer, identifikacija rute kretanja krijumčara zahtjeva prethodna saznjanja o kretanjima grupe ili lica, geolokaciju podataka (javno dostupne fotografije ili video sadržaja) i potvrđivanje / odbacivanje prethodne rute kretanja, vrijeme i datum kretanja, interakcije drugih naloga sa sadržajem (like, share, comment) i tako dalje. Navedeni proces je zahtjevan, haotičan i nalaže kretavino i kritičko razmišljanje.

2. OSINT i obavještajni ciklus – usmjeravajuća poveznica

Prilikom obavljanja istraga, bilo onih od nacionalnih policijskih agencija, civilnih ili vojnih obavještajnih službi ili čak privatnih istražitelja, proces spoznaje se zasniva na obavještajnom ciklusu. Navedeni ciklus originalno potječe iz Obavještajne zajednice SAD-a i ima ulogu smjernice i upute za pouzdano i ponavljajuće prikupljanje i obradu informacija kako bi se ispunili obavještajni zahtjevi nadređenog aktera. Koraci obavještajnog ciklusa su najosnovnije radnje od početnog planiranja operacije do odgovaranja na obavještajni zahtjev[7] i osiguravanja da je odgovor integriran u operaciju (Headquarters, Department of The Army, 2023). Kao što se aktivnosti operativnog procesa preklapaju i ponavljaju kako misija zahtijeva, tako se događaju i koraci obavještajnog procesa.

Ovaj ciklus je aktivnost razvoja sirovih informacija u gotove obavještajne podatke za korištenje od strane kreatora politike, vojnih zapovjednika i drugih korisnika u donošenju odluka (ODNI, 2011). On je vrlo dinamičan, kontinuiran i beskrajan, a sastoji se od sljedećih elemenata:

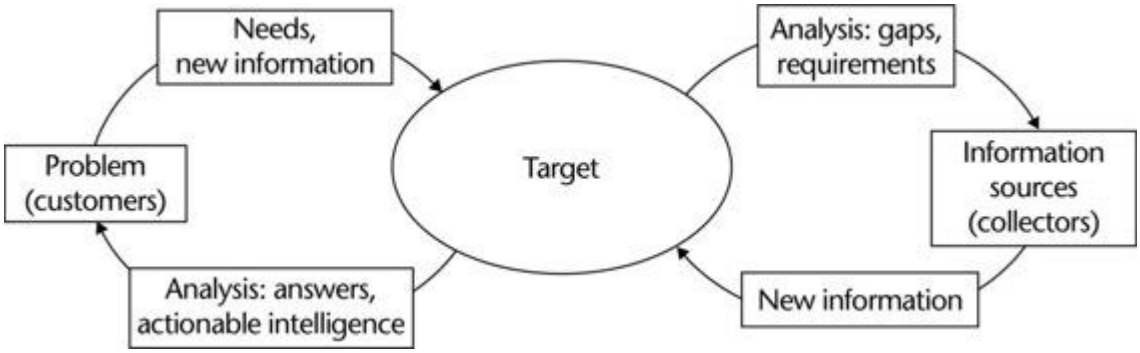
- Planiranje i usmjeravanje;
- Prikupljanje;
- Obrada i iskorištavanja;
- Analize i produkcije;
- Diseminacije;
- Evaluacije i povratne informacije.

Gotovo svi autori koji se bave obavještajnim studijama navode četiri ili više koraka, pri čemu dolazi do minornih razlika, i podkategroija u svakom koraku. Sagledavajući literaturu svaki ciklus započinje planiranjem i okončava se

[7] Zahtjev za obavještajnim podacima je 1. Svaki predmet, opći ili specifičan, za koji postoji potreba za prikupljanjem informacija ili proizvodnjom obavještajnih podataka. 2. Zahtjev za obavještajnim podacima kako bi se popunila praznina u znanju ili razumijevanju komande o operativnom okruženju ili snagama prijetnje (JP 2-0).

diseminacijom ili povratnom informacijom u zavisnosti od autora. Na primjer obavještajni ciklus CIA-e opisuje ovaj proces kao planiranje i usmjeravanje, prikupljanje, obradu, analizu i proizvodnju i diseminaciju (CIA, 2024), dok Johnsonov Priručnik za obavještajne studije (Loch, 2006) opisuje ove faze kao prikupljanje, obradu, analizu i proizvodnju, klasifikaciju i diseminaciju. RAND također daje svoj obavještajni ciklus te ga definiše kroz 1. prikupljanje – akvizicija i zadržavanje, 2. obradu – prijevod i agregaciju, 3. iskorištavanje – autentifikaciju i kontekstualizaciju, i 4. produkciju – klasifikaciju i diseminaciju (Williams & Blum, 2018). Navedene stavke koreliraju sa pet glavnih procesa (identifikacija, prikupljanje, ispitivanje, analizu i prezentaciju, dati apstrakt) u digitalnoj forenzici koja je ključna u istraživanju organiziranih kriminalnih grupa (Kao, Chao, Tsai, & Huang, 2018).

Prilikom upotrebe OSINT-a za istraživanje specifičnog bezbjednosno interesantnog lica, potrebno je razviti model obavještajnog ciklusa koji u prvom planu ima metu – bezbjednosno intresantno lice. Obavještajna zajednica Sjedinjenih Američkih Država implementirala je koncept sličan pristupu usmjerenom na cilj. Taj koncept, nazvan "proizvodnja zasnovana na objektima" (engl. *object-based production* ili OBP), podrazumijeva organiziranje obavještajnih aktivnosti oko "objekata" (ciljeva) koji su od obavještajnog interesa (Clark, 2016). Ključna karakteristika ovog pristupa je dijeljenje ažuriranih saznanja o obavještajnom cilju putem platformi zasnovanih na oblaku. Clark (2016) je ponudio navedeni model (Ilustracija 1), pri čemu se kao osnovni elementi pojavljuju: meta, Potrebe, nove informacije, analiza: praznine, zahtjevi, izvori informacija (prikupljači), nove informacije, analiza: odgovori, upotrebljive obavještajne informacije, problem (korisnici).



Ilustracija 1 - Obavještajni ciklus fokusiran na metu (Clark, 2016)

Dijagram osigurava struktuiran i direktno orjentiran proces prikupljanja i analize informacija u vezi sa metom. Kontinuirano se daju zahtjevi, vrši provjera, verifikuje podatak / informacija. Na taj način se omogućava brzo odlučivanje na

osnovu direktnih promjena u materijalnom svijetu, kao i odgovaranje na obavještajne zahtjeve koji dolaze od donosioca odluka.

Obavještajni ciklus je bitan za aktivnosti koje se poduzimaju u OSINT-u zbog određivanja onoga šta je bitno za davatelja obavještajnog zahtjeva - subjekta koji traži informacije, te kreiranja produkta koji zadovoljava njegovu potrebu. Istraživanje organiziranih kriminalnih grupa započinje obavještajnim zahtjevom o relevantnim informacijama – kretanjima, imovini, aktivnostima, prostornoj lokaciji djelovanja, suradnicima i tako dalje. Kroz obavještajnih zahtjev postavljaju se okviri koji služe za fokusiranje istrage na određene relevantne informacije, što onemogućava besciljno lutanje ili proizvoljnost istražitelja koje kao posljedicu može imati prikupljanje podataka i informacija koje nisu od operativne važnosti. Dakle, obavještajni zahtjev će služiti istražitelju za definiranje onoga šta se treba saznati, dok obavještajni ciklus ukazuje na proces dolaska do informacija.

3. Operativna upotreba OSINT-a u istraživanju OKG

OSINT ima značajnu upotrebu u istraživanju OKG i drugih modaliteta koji ugrožavaju nacionalnu sigurnost. Iako je dugo vladalo mišljenje da OSINT nije posebna obavještajna disciplina kao što su HUMINT, SIGINT, ELITN i tako dalje, njegova primjena u istragama govori suprotono. Koncept obavještajnih podataka otvorenog koda (OSINT) je relativno nov za agencije za provođenje zakona i labavo je definiran kao obavještajni podaci prikupljeni iz javno dostupnih izvora koji ne zahtijevaju prikrivene ili tajne metode prikupljanja (Brunet & Claudon, 2015). Ovaj modalitet ima značajne operativne mogućnosti koje zavise od njegovog korisnika i aktera koji traži informaciju. Kako bi se adekvatnije razumjela operativna upotreba OSINT-a, neophodno je razumjeti upotrebne mogućnosti u različitim situacijama. Na primjer, svaka operacija u kojoj se nadzire bezbjednosno interesantno lice započinje prikupljanjem podataka o njemu, analizom navedenih podataka, te kreiranjem izvještaja. S ozbirom na dinamičnost i promjenjivost stiuacije, javljaju se situacioni problemi i izazovi, čije je rješavanje prepušteno istražitelju. Shodno tome, upotreba OSINT-a u istraživanju OKG je dinamičan proces koji primarno zavisi od kreativnosti, sposobnosti i vještina analitičara, kao i njegovog fokusa na ispunjavaje obavještajnog zahtjeva.

3.1. Prikupljanje, kategorisanje i primarna obrada podataka bezbjednosno interesantnog lica

Društvene mreže u modernom vremenu su postale vrijedan izvor informacija i imaju operativnu primjenu u istragama OKG, naročito onih grupa koje posjeduju

veoma nisku ili nepostojeću OPSEC[8] kulturu. Kao primjeri i vrste društvenih mreža mogu se navesti sljedeće: kolaborativni projekti (npr. Wikipedia); blogovi i mikroblogovi (npr. Twitter /X); zajednice sadržaja (npr. YouTube); stranice društvenih mreža (npr. Facebook); virtualni svijetovi igara (npr. World of Warcraft); i virtuelni društveni svjetovi (npr. Second Life) (Kaplan & Haenlein, 2010). Određivanje koja će društvena mreža biti određena za prikupljanje podataka zavisi od lica koje ima otvoren nalog na navedenoj društvenoj mreži. Za neka krivična djela (kao što su prijetnje ili uvredljivi komentari,10 ili prijevara) materijal 'otvorenog koda' kao što je Twitter (druga vrsta društvenih medija (Kaplan & Haenlein, 2010)) može sam po sebi biti prima facie dokaz krivičnog djela (Sampson, 2016). Za druga krivična djela kao što je krijumčarenje ljudi, mogu se koristiti druge društvene mreže poput TikToka na kojima je evidentan broj krijumčara afro-azijskog porijekla koji promoviraju svoje usluge[9]. Druge društvene mreže, kao što je Instagram, mogu poslužiti za evidentiranje života – kretanja, boravka i drugih aktivnosti pripadnika organiziranih kriminalnih grupa koji često objavljuju sadržaj o svom luksuznom i raskošnom životu, što predstavlja važan izvor podataka i informacija.

Aktivnosti identifikacije bezbjednosno interesantnih lica započinje obavještajnim zahtjevom za identifikaciju i eventualno lociranje. U određenim slučajevima mogu postojati generalijski podaci lica, kao i njegova fotografija što značajno ubrzava istragu. U slučajevima kada postoji fotografija lica i indicije koje ukazuju na njegovo kretanje i geolokaciju, web pretraživači poput Google i Yandex-a, kao i mnogobrojni alati (Tabela 1) predstavljaju značajnu pomoć.

Tabela 1 - Lista alata za pretragu fotografija

Alat	Opis
Berify	Reverse image pretraga za pronalazak ukradenih slika i videozapisa.
Bing Image Search	Bingova stranica za reverse image pretragu.
Eagle Eye	Pregledava društvene mreže za postavljenu sliku.
Geospy	Pokušava locirati gdje je slika snimljena koristeći AI.
Google Image Search	Googleova stranica za reverse image pretragu.

[8] Operativna sigurnost (OPSEC) predstavlja koncept zaštite vlastitih aktivnosti od protivnika. Nekada to označava neobjavljivanje sadržaja koji se može dovesti u vezu sa licem, dok u drugim slučajevima isto nalaže upotrebu kompleksnih sistema koji skrivaju identitet aktera i omogućavaju da aktivnosti, procesi i akteri ostanu neprimjećeni i neidentifikovani.

[9] Navedeno je evidentno pretraživanjem društvenih mreže korištenjem različitih tagova kao što su migration, western balkan, refugees i tako dalje. Postoje i određene chat grupe na sms servisima poput WhatsAppa, Telegrama, Discorda, Vibera i ostalih. Razlozi za veliki influks migranata a-a porijekla je destabilizacija Bliskog istoka, naročito Levanta i Afganistana, što je povezano sa političkim previranjima u navedenom regionu.

Osint Combine	Alat za poboljšanu reverse image pretragu s tabelarnim rezultatima iz Googlea i Yandexa.
Tineye	Reverse image pretraga za pronalazak gdje se slike pojavljuju na internetu.
Yandex Image Search	Yandexova stranicaza reverse image pretragu.

Navedeni alati nisu jedini i postoji mnoštvo drugih koji se koriste, neki su besplati, a neki ne. Proces pretrage može započeti i na nalogu suradnika i fotografije na kojoj se nalazi lice od interesa. Daljim pretragama i dolaskom do profila lica od našeg interesa, započinje se proces prikupljanja podataka. Navedeni podaci se mogu svrstati u kategorije pogodne za daljnju analizu (Tabela 2).

Tabela 2 Kategorije podataka potrebnih za analizu – operativni karton

Kategorija	Detalji	Značaj
Podaci o korisniku	- Zvanično ime i prezime - Korisničko ime na društvenoj mreži (@username) - URL profila - Datum rođenja - Mjesto rođenja - Obrazovanje - Zaposlenje/pozicija - Mjesta boravka - Kontakt informacije - Porodica/odnosi - Životni događaji - Biografija - Profilna fotografija - Ostale fotografije korisnika	Fokusira se na osnovne podatke dostupne na profilu potrebne za poduzimanje daljih radnji. Iz navedenog se kreira dosije lica te pronalaze elementi pogodni iskorištavanju.
Profilna slika	- Opis profilne slike (lica, simbol, objekt) - Identifikacija fizičkih karakteristika (boja kose, tetovaže, itd.) - Provjera autentičnosti (AI alati za analizu slika)	Analizira profilnu sliku za identifikaciju ili verifikaciju prethodno dobijenih podataka.
Veze korisnika	- Prijatelji - Porodica - Kolege - Članstva/grupe	Omogućavaju mapiranje društvene mreže subjekta, identifikaciju bliskih kontakata i potencijalnih saradnika ili članova OKG-a.

Interakcije korisnika	- Sviđanja - Emojiji - Komentari - Lista prijatelja/pratitelja - Članstva u grupama ili stranicama - Često komentirani ili spominjani profili	Pruža uvid u društvenu mrežu i povezane osobe kako bi se razvila socijalna mapa.
Sadržaj objava	- Kontekst (posao, zabava, itd.) - Vrste sadržaja (tekst, slike, video) - Lokacije - Prijatelji/porodica - Lični podaci - Navike (pušenje, konzumacija alkohola, upotreba droga, fitness, video igre, sportovi) - Hobiji	Identificira teme interesa i moguće veze s određenim aktivnostima za dalje iskorištavanje i razvijanje toka akcije.
Medijski sadržaj	- Fotografije korisnika - Identifikacione karakteristike (boja kose, tetovaže) - Fotografije s identifikatorima lokacije - Navike (pušenje, konzumacija alkohola, upotreba droga) - Lokacija - Prijatelji/porodica - Hobiji	Pruža vizualne i geolokacijske informacije za fizičku identifikaciju, praćenje aktivnosti i analiza ponašanja subjekta.
Meta podaci	- Lokacije - Vrijeme - Datumi - Korištene platforme -Korišteni uređaji	Pomaže u praćenju vremena, lokacija i korištenja društvenih mreža.
Analiza tijela	-Rane na tijelu -Ožiljci -Tetovaže -Invaliditet -Bolesti -Promjene na koži	Navdene stavke pomažu u mogućem identificiranju lica ukoliko je učestvovalo u nekom za istražitelja intresantnom događaju. Rane na rukama mogu ukazivati na fizički sukob ili povredu nastalu udarcem u staklo i tako dalje. Specifične rane ili invaliditeti mogu ukazati na nestručno rukovanje priručnim sredstvima (detonatori, eksplozivi i tako dalje).

Nakon prikupljanja navedenih stavki, započinje se sa analiziranjem podataka i utvrđivanjem određenih veza koje ispunjavaju obavještajni zahtjev poput kretanja bezbjednosno interesantnog lica, uvida u suradničku mrežu, utvrđivanja imovine koju posjeduje, te informacija koje su potrebne za izvršenje određenih operativno – taktičkih radnji. Prema učestalosti posjećivanja određenih lokacija (metapodaci o lokaciji, vremenu i datumima), mogu se kreirati obrasci ponašanja i dati okviri za vođenje posebnih istražnih radnji. Zbog velikog broja podataka koji se nalaze na društvenim mrežama (pratitelji, prijatelji, lajkovi i tako dalje), poželjno je koristiti takozvane *data scrapere*[10], naročito one razvijene u vlastitoj agenciji / službi.

Kada je obavljeno prikupljanje podataka, započinje se sa njihovom obradom i kreiranjem analize. U ovoj fazi, sirovi podaci poput generalijskih informacija, metapodataka, lokacija i drugog, dobijaju svoj značaj. Obrada se može promatrati kroz sljedeće stavke:

- verifikacija već dobijenih podataka (generalijski podaci, fizički izgled, lokacije, suradnici i tako dalje),
- kategorizacija podataka po njihovom značenju i operativnoj upotrebljivosti (generalijski podaci *versus* podaci o suradničkoj mreži),
- struktuiranje podataka kroz kreiranje veza, identifikacija učestalih obrazaca ponašanja (posjećene lokacije, vrijeme obavljanja aktivnosti, prisustvo događajima, osobe sa kojima se najčešće komunicira i tako dalje),
- razumijevanje konteksta (povezanost sa kriminogenim licima i događajima,
- svrha objave (šta želi da se postigne – prezentiranje luksuznog života, zastrašivanje, pronalazak saradnika),
- mjesta djelovanja i sastajanja sa drugim bezbjednosno interesantnim licima),
- identifikacija ključnih aktera – saradnici i ostali članovi,
- kreiranje izvještaja (odgovori na obavještajni zahtjev i usmjeravanje donosioca odluka prema novim tačakama interesa),
- poduzimanje operativno – taktičkih mjera i radnji (racija, nadzor telekomunikacija, praćenje, lišenje slobode i tako dalje).

Navedena obrada je potrebna zbog povezivanja nasumičnih podataka u jednu koherentnu cjelinu. Fotografija lica ne daje mnogo informacija, međutim, njeno povezivanje sa mjestom, datumom i vremenom fotografisanja, kontekstom i

[10] Navedeno su programi i skripte koje izdvajaju određenu vrstu podataka sa web izvora.

mogućim predmetima /osobama na njoj, usmjerava istragu. U toku navedenog postupka, potreban je fokus na detalje koji mogu ukazati na naizgled nepostojeće veze i odnose.

3.2. Analiza naloga na društvenim mrežama članova OKG i izvođenje zaključaka

Nakon što su prikupljeni i kategorisani podaci, te obavljena primarna obrada podataka u koherentnu cjelinu, potrebno je započeti sa analizom naloga. Društvene mreže su značajan pokazatelj života određene osobe i kao takve se trebaju u potpunosti iskoristiti. Poslednjih godina, sa napretkom velikih podataka i tehnika rudarenja podataka, istraživačka zajednica je primetila da otvoreni podaci predstavljaju moćan izvor analize društvenog ponašanja i dobijanja relevantnih informacija (Chen, Chiang, & Storey, 2012). Uvid u naloge na društvenim mrežama istražitelju može dati značajne informacije o predmetnom licu koje se mogu koristiti za dalje planiranje aktivnosti. Naravno, postoje izuzeci i outlieri koji navedenu tezu mogu osporiti, ali prosjek nalaže upotrebu analitičke matrice i zaključivanja. Također, varijable kao što su godine, spol, kulturološki i etnički faktor, hijerarhijski status u grupi, prethodno iskustvo, kognitivne sposobnosti, duševne bolesti i psihofizičko stanje mogu utjecati na prikupljanje informacija. Različiti tipovi ličnosti mogu utjecati na jednostavnost i brzinu prikupljanja podataka i informacija, te kreiranju analiza. Navedni tipovi nisu predmet razmatranja, te se u korist argumenta daje jednostavan primjer operativnog postupanja. Kao hipotetički primjer se može koristiti visokopozicionirani mladi pripadnik OKG koji na društvenim mrežama često prezentira svoj luksuzni život. Uvidom njegovog naloga na društvenoj mreži kao što je Instagram koju češće koriste milenijalci[11] i Gen Z[12] za razliku od generacije X ili baby boomera, mogu da se identificiraju sljedeće varijable:

a) Način života – luksuzan, umjeren, asketski;
b) Socijalna povezanost – velika, srednja, niska;
c) Aktivnost na društvenoj mreži – velika, srednja, niska;
d) Interesi i sviđanja;
e) Direktne veze sa drugim bezbjednosno interesantnim licima;
f) Mentalno stanje;

Navedeno predstavlja pojednostavljen proces prikupljanja informacija iz otvorenih izvora što služi za dubinsku analizu. Uvidom u stavke kao što je na

[11] Demografska skupina rođena od 1981. do 1996. godine, nasljedila demografsku skupinu Gen X.Nekada se naziva i Gen Y.
[12] Demografska skupina rođena od 1997. do 2012. godine, naslijedila demografsku skupinu Gen Z.

primjer lukszan način života i značajna socijalna povezanost, mogu da se traže indicije o djelovanju grupe i uloge pojedinca u njoj.

a) Način života – različiti tipovi ličnosti nastoje da prezentiraju svoj relani život širem auditorijumu putem društvenih mreža. Za navedeno su najadekvatniji Instagram, TikTok i Facebook koji su zasnovani na upotrebi fotografija i video snimaka kao medijuma prenošenja informacija. Pripadnici OKG, odnosno općenito kriminogene osobe, često zbog potrebe za validacijom (Reid, 2023) nastoje da prikažu svoj raskošan i luksuzan život, kao i pristup resursima (novcu) ili kroz prezentaciju resursa nastoje da ostvare socijalne veze. Prikupljanjem i analizom fotografija sa društvenih mreža, primarno Instagrama koji je popularan kod Gen Y i Z, mogu da se uvide sljedeće stavke koje život mogu klasificirati kao luksuzan, umjeren ili asketski:

- Odjeća – da li su u fokusu skupi brendovi ili odjeća nove mode. Pažnja se treba usmjeriti i prema specifično namjenjenoj odjeći – odjeća za planinarenje, taktička odjeća, sportska odjeća;
- Uređaji – da li lice koristi najnoviji model telefona prilikom slikanja (selfie pred ogledalom) ili je u pitanju stariji ili flagship model. Fotografiranje igraćih konzola, *high spec* računara i slično ukazuje i na mogućnost ulaganja novca u sisteme za zabavu i njihov značaj kao sredstva zabave;
- Nakit – može ukazati na pristup resursima ili nedostatak isti ukoliko se koriste replike ili plagijati luksuznih brendova.
- Prevozna sredstva – da li se lice slika u automobilima visoke vrijednosti, ima li pristup drugim prevoznim sredstvima koja signaliziraju pristup resursima– avioni, helikopteri, jahte;
- Putovanja – da li lice često putuje, na koje destinacije, koliko dugo i gdje tačno boravi – hoteli i drugi smještaji. Zaključuje se na osnovu tagova i datuma objave. Može da se koristi za crossreferencing za određene događaje – nesupješne atentate, sastanke sa drugim bezbjednosno interesantnim licima i tako dalje;

Uvidom u navedene stavke, moguće je doći do zaključka da li je način života predmetnog lica luksuzan ili ne. Ukoliko lice prezentuje luksuzan život, istraga se usmjerava u legalne izvore primanja, što može ukazati na povezanost sa OKG i činjenje krivičnih djela.

b) Socijalna povezanost predmetnog lica ukazuje na njegovo mjesto u hijerarhiji i i široj zajednici. Uvid u odnos naloga koje lice prati i koji njega prate ukazuje na popularnost ili prezentnost, kao i težnje koje lice ima, na primjer privlačenje pažnje suprotnog pola. Fotografije sa drugim osobama – porodica, prijatelji, druga bezbjednosno interesantna lica mogu da posluže za usmjeravanje istrage i

povezivanje sa drugim događajima, procesima, stanjima i dešavanjima. Velika socijalna povezanost ili njeno fiktivno prezenotovanje može da se iskoristi za operacije infiltracije i evidencije ključnih tačaka u kriminalnoj mreži.

c) Aktivnost na društvenoj mreži kao što je kontinuirano objavljivanje sadržaja ili komunikacija sa *sockpuppet* nalozima, može ukazati na dostupnost lica, njegov hijerarhijski status, način života, povezanost sa drugim bezbjednosno interesantnim licima. Također, periodi bez objavljivanja sadržaja i komunikacije se mogu interpretirati kao faze planiranja ili izvođenja krivičnih djela, ili skrivanja nakon izvršenja. Upotrebom određenih alata prilikom komunikacije, moguće je odrediti geolokaciju preko IP-a[13]. Različiti nivoi aktivnosti se mogu interpretirati u skladu sa prethodno dobijenim saznanjima ili razvojem novih verzija.

d) Interesi i sviđanja ukazuju na interene osobnosti lica. Uvidom u *following/followers* listu i *lajkovane* i komentirane objave, mogu se kreirati modeli ličnosti. Pa tako, praćenje ili lajkovanje velikog broja sadržaja o određenom modelu automobila, nakita, odjeće ukazuje na preference lica o lukszu ili težnji ka luksuzu. Također, praćenje *softcore* porongrafskih sadržaja na drušvenim mrežama (OnlyFans modeli i tako dalje), ukazuje na mogući promiskuitet lica ili njegova interna stanja.

e) Veze sa drugim bezbjednosno interesansnim licima ukazuju na njegovu socijalnu povezanost, hijerarhiju u grupi, popularnost, veze i tako dalje. Podaci se mogu koristiti za identifikaciju suradničke mreže i povezivanje sa prethodnim krivičnim djelima ili pretpostavke na zajedničku suradnju u budućim kriminalnih aktivnostima.

f) Određivanje mentalnog stanja i intelektualnih kapaciteta se zasniva se na analizi sadržaja koji se objavljuje i tekstu – opisu sadržaja. Na primjer, velika količina ljubavnih objava može ukazati na to da lice pati ili je u sretnoj ljubavnoj vezi. Objave o lojalnosti, motivaciji i pripadnosti grupi mogu ukazati na unutargrupne probleme. Vulgarne i provokativne objave ukazuju na određene interne procese kroz koje lice prolazi. Potrebno je obratiti pažnju i na stil pisanja koji ukazuje na nivo obrazovanja i školovanja, što može poslužiti za planiranje i izvođenje drugih operativnih radnji.

Nakon izvršene analize naloga bezbjednosno interesantnog lica, potrebno je kreirati izvještaj kojim se odgovara na prvobitno dobijeni obavještajni zahtjev koji je započeo istragu. Odgovori mogu biti pozitivni - daju odgovor, negativni – ne daju traženu informaciju i neutralini - ostavljaju mogućnost za dalje istraživanje. Nakon što naručitelj obavještajnog zahtjeva dobije odgovor

[13] Internet protokol – mrežni protokol koji koriste uređaji za prenos podataka putem interenta.

(pozitivan, negativan, neutralan), on u skladu sa daje novi zahtjev, redefiniše ili precizira prethodni. Iako je istražitelj dostavio traženo, potrebna je kontinuirana verifikacija i ukazivanje na novitete – suradnici, aktivnosti, lokacije.

3.3. Operativni problemi i nemogućnost pristupa podacima

Prilikom aktivnosti prikupljanja podataka, značajan problem za istražitelja je sami početak. Pitanje *od čega početi* zavisi od obavještajnog zahtjeva, međutim u većini slučajeva, korištenje *search* opcije na društvenim mrežama predstavlja početni korak. Značajan problem za istragu jeste privatan nalog bezbjednosno interesantnog lica, koje ima srednji ili visok OPSEC. Navedeno zaustavlja istragu i zahtjeva kreativnost u rješavanju ovog izazova. Jedan od načina jeste upotreba *sockpuppet* naloga koji je prethodno kreiran, kultiviran i održavan za slučajeve nadzora, infiltrace, ostvarivanja kontakta i sličnog. Nalog treba da se održava kontinuirano i izgleda organski. Ukoliko je nalog zapostavljen i nije adekvatno kultivisan, predmetno lice može posumnjati u novog *pratitelja,* te ukloniti sadržaje koji ga kompromitiraju ili daju dovoljno informacija o njemu, te ukloniti novog *pratitelja*. Značajan problem je i nedostatak kreativnosti istražitelja kao i nepoznavanje određenih tehnika ili metoda dolaska do traženih podataka i informacija, kao i nepoznavanje upotrebe alata. Tehnička i kreativna nesposobnost ograničava istragu, te neadekvatno korištenje *sockpuppet* naloga može da upozori lice od intresa da je predmet istrage. Samokompromitacija može uzbuniti cijelu mrežu, koja će se povući i uspostaviti rigorozni OPSEC. U tom slučaju, istraživanje lica od intresa, saradnika i drugih bezbjednosno intresantnih subjekata se okončava, te je potrebno koristiti druge adekvatne i upotrebljive obavještajne metode osim OSINT-a (HUMINT, SIGINT, ELINT).

Naredni problem može biti nejasan i neadekvatan obavještajni zahtjev koji se može tumačiti na različite načine, ili je loše definiran. Široko definiran obavještajni zahtjev će onemogućiti istražitelju fokusiranje na ono što je bitno, te će nastojati da pribavi, obradi i analizira sve podatke i informacije, što zahtjeva mnogo vremena i može biti kontraproduktivno zbog dinamičnosti radnji koje poduzima lice od intresa. Na taj način će se izgubiti bitne informacije i istraga se može usmjeriti u krivi tok. Isto se može prevazići traženjem novog obavještajnog zahtjeva ili zahtjevom za redefiniranje ili preciziranje već dobijenog. Na primjer, nadređeni može zahtjevati da se prikupe podaci o bezbjednosno interesantnom licu, pri čemu nije precizirano sa koje mreže, koji podaci (foto, audio, video, tekst), suradničke veze, hijerarhijske veze i tako dalje. S druge strane, precizan i jasan obavještajni zahtjev bi glasio: „*Prikupiti informacije po bezbjednosno interesantnom licu Z kako bi se utvrdili identitet, posljednja lokacija, kretanje u zadnjih 60 dana na osnovu metapodataka, aktivnosti, kontakti i moguća povezanost sa organiziranim kriminalnim grupama. Istragu započeti obradom naloga na društvenoj mreži Instagram, gdje lice ima otvoren i javan profil*

@usernameZ.“ Na ovaj način se omogućava istražitelju da se fokusira na ispunjavanje zahtjeva, a ne na razmišljanje šta je potrebno donosiocu odluka. U određenim slučajevima, poželjno je da istražitelj nasluti šta je donositelj odluke želio, te da samostalno razvije istragu, međutim, ponekad navedeno može biti kontraproduktivno i bespotrebno.

S obzirom da društvene mreže često mogu biti sredstvo dezinformiranja i obmanjivanja šire publike, tako i istražitelji mogu da budu indirektna meta obmane. Clark (2016) navodi da su poricanje i obmana glavno oružje u kontraobavještajnom arsenalu jedne zemlje ili organizacije, pri čemu se navedeno može prenijeti i na pripadnike organiziranih kriminalnih grupa. Obmanjivanje, dezifnromiranje i laganje zavisi od psihološkog profila i mentalnog stanja lica od interesa koje zbog internih procesa može da prikaže vlastiti život u superlativu. Dezinformisanje i obmana mogu biti i rezultat kompromitacije istražitelja koji su vlastitim nesmotrenim postupcima ukazali na aktivnosti prikupljanja podataka. Lice od intresa u tom trenutku može da započne sa vlastitim kontraobavještajnim postupcima, navodeći na krivi trag – na primjer objavljujući fotografije nakon nekoliko dana, označavanje na lokacijama na kojima nije i tako dalje. Nemogućnost brze verifikacije će značajno ugroziti istragu i omogućiti bezbjednosno interesantnom licu da sakrije prethodne tragove.

4. Hipotetički primjer istrage bezbjednosno interesantnog lica koje pripada OKG

U svrhu boljeg razumjevanja tematike upotrebe OSINT-a koja u određenim sutacijama može biti nejasna i apstraktna, u nastavku će se dati hipotetički slučaj djelovanja bezbjednosno interesantnog lica koje je član organizirane kriminalne grupe. Ovaj hipotetički slučaj ima za cilj da ukaže na primjenu obavještajnog ciklusa koje usmjeravaju istragu nakon zaprimanja obavještajnog zahtjeva nadređenog / donosioca odluka, te poduzimanja radnja kojim se daje odgovor na njega. Kako bi se pojednostavile aktivnosti i problematika, koristiti će se trenutačna migrantska kriza kojom je država Bosna i Hercegovina značajno ugrožena. Metodologija koja je korištena u primjeru je općenita i pojednostavljena, bez preciznih detalja poput vrste alata i njihove upotrebe. Različite sigurnosne službe i agencije imaju vlastite metodologije istraživanja, te one nisu predmet ovog rada. Primjer će biti prikazan kroz narativ kojim se omogućava korištenje OSINT-a, obavještajni zahtjev kojim se jasno definiše šta je potrebno saznati i razradu aktivnosti kojim će odgovoriti na obavještajni zahtjev. Svaka sličnost sa stvarnim situacijama je slučajna i služi za ilustrativni prikaz.

4.1. Narativ i hipotetičko činjenično stanje

Operativni podaci dobijeni od zapadnih strateških partnera ukazuju na djelovanje organizovane kriminalne grupe pod nazivom KLL. Navedena grupa broji oko 15 članova, koji su državljana Afganistana. Grupa kao glavnu djelatnost i izvor zarade ima krijumčarenjem migranata iz Turske prema zapadnoj Evropi. Glavni operativac koji djeluje na teritoriji Bosne i Hercegovine je Tom Sawyer, čija je uloga ključna u završnoj fazi krijumčarskog lanca. Prema dostupnim informacijama, Tom Sawyer ima vodeću ulogu u uspostavljanju kontakta s migrantima po njihovom dolasku u BiH i osiguravanju nesmetanog tranzita ka zapadnoj granici. Trenutna saznanja ukazuju na to da migranti započinju svoj put u Turskoj u nekom od migrantskih kampova, zatim prolaze kroz Bugarsku i Srbiju. Po dolasku do zapadne granice Srbije ulaze u slabo nadzirane šumske predjele, te ilegalno ulaze na teritorij Bosne i Hercegovine, aktivno izbjegavajući patrole Granične policije BiH. U Višegradu ih preuzima Tom Sawyer, koji dalje organizuje njihov transport do krajnje destinacije –Bihaća. Na osnovu prikupljenih podataka, utvrđeno je da migranti za ovu uslugu plaćaju značajne novčane iznose, što ukazuje na visok stepen finansijske koristi za grupu KLL.

Partneri su proslijedili informaciju da Tom Sawyer koristi društvene mreže Instagram i TikTok kao primarni kanal za promociju svojih ilegalnih aktivnosti. Njegova digitalna prisutnost omogućava ne samo oglašavanje „usluga“ već i povezivanje s potencijalnim klijentima, čime se zaobilaze klasični posrednici i osigurava cjelokupan novčani iznos koji se ne dijeli sa posrednikom. Na objavama jasno se mogu vidjeti:

- Izgled Tom Sawyera (fotografije i video sadržaji),
- Prepoznatljivi pejzaži i lokacije u BiH, kao što su most u Višegradu, kafići i nargilane u Sarajevu i putokazne table na kojima je jasno naznačen smjer i udaljenost prema Bihaću (npr. „Bihać 15 kilometara“).
- Interakcije u komentarima i lajkovima, koje pružaju dodatne tragove o njegovim vezama i saradnicima.

Dodatno, informacije dobijene putem HUMINT-a potvrđuju da Tom Sawyer trenutno boravi u Sarajevu, te da je čest gost u jednom kafiću na Baščaršiji. Njegov identitet je dodatno verifikovan putem broja telefona, koji je dostavljen službama. Pregledom aplikacije WhatsApp, koja je često korištena za komunikaciju među migrantima iz Afganistana, utvrđeno je da broj pripada Tomu Sawyeru, budući da isti koristi svoju profilnu sliku na aplikaciji. Navedeno služi da se poveže lice imena Tom Sawyer koji se oglašava na društvenim mrežama sa telefonskim brojem koji koristi za komunikaciju. Dalja analiza poruka ukazuje na mogućnost postojanja šifrovanih termina i fraza koje se koriste za koordinaciju aktivnosti. Učestale su poruke o lubenicama, cvjetovima i kuglanju. Do sada se nije uspjelo razjasniti šta navedeno označava.

Aktivnosti grupe KLL predstavljaju ozbiljnu prijetnju nacionalnoj sigurnosti, s obzirom na to da ilegalne migracije mogu biti povezane sa sekundarnim sigurnosnim rizicima, uključujući:

- Potencijalne veze sa drugim oblicima organizovanog kriminala (trgovina ljudima, drogom ili oružjem).
- Rizik od radikalizacije ili infiltracije ekstremističkih elemenata među migrantima uzrokovane nemirima na Bliskom istoku.
- Destabilizaciju lokalnih zajednica kroz povećani pritisak na resurse i sigurnosne kapacitete.

Tom Sawyer, kao ključni akter, trenutno predstavlja prioritet u zaustavljanju rada KLL grupe. Njegova digitalna prisutnost otvara prostor za OSINT operaciju, kojom bi se prikupile dodatne informacije o njegovim aktivnostima, vezama i metodama rada. Operativne praznine trenutno uključuju: detaljne podatke o njegovim saradnicima, precizne vremenske okvire krijumčarskih operacija i rute koje koristi u urbanim područjima. Cilj je stvoriti cjelovit profil Tom Sawyera i njegove kriminalne mreže, koristeći informacije iz digitalnih izvora, HUMINT-a i drugih obavještajnih disciplina, kako bi se olakšalo njihovo neutralisanje.

4.2. Obavještajni zahtjev nadređenog

Kako bi istražitelji mogli da započnu operaciju istrage, nadređeni im dostavlja obavještajni zahtjev. Obavještajni zahtjev treba da usmjeri istragu kroz definisanje nepoznanica.

U nastavku se nalazi hipotetički obavještajni zahtjev koji se se odnosi na djelovanje jednog od aktera iz organizirane kriminalne grupe. Hipotetički obavještajni zahtjev sadrži sljedeće pojedinosti

Predmet: Praćenje aktivnosti Toma Sawyera i grupe KLL na društvenim mrežama radi identifikacije krijumčarskih ruta i saradnika.

Cilj zahtjeva: Prikupiti i analizirati otvorene izvore informacija (OSINT).

Navedeno je potrebno za ostvarivanje sljedećeg:

- Utvrdio identitet, pravac kretanja i mjesta boravišta Toma Sawyera i ostalih članova kriminalne grupe KLL.
- Identifikovale tajne krijumčarske rute koje koriste migranati na teritoriji BiH.
- Prikupile informacije o potencijalnim saradnicima i kontaktima koji pružaju podršku OKG na ruti Turska-Bugarska-Srbija-BiH.
- Analizirao sadržaj sa društvenih mreža (Instagram, TikTok, WhatsApp) u svrhu mapiranja aktivnosti, geolociranja ruta i eventualnog otkrivanja šifrovanih poruka ili ključnih informacija.

Specifični zadaci:

- Detaljna analiza profila Toma Sawyera na Instagramu i TikToku (objave, komentari, lajkovi).
- Identifikacija osoba koje komuniciraju ili sarađuju sa Tomom Sawyerom (analiza interakcija na društvenim mrežama).
- Prikupljanje i geolociranje vizuelnih informacija sa objavljenih sadržaja (pejzaži, putokazi, lokacije).
- Proučavanje komunikacija na aplikaciji WhatsApp i analiza dostavljenog broja telefona kako bi se potvrdio identitet i aktivnosti.
- Mapiranje ruta kretanja (ceste, šumski i planinski putevi) migranata na osnovu prikupljenih podataka i HUMINT informacija.
- Utvrđivanje lokacije boravišta Toma Sawyera u Sarajevu i analiziranje njegovih dnevnih rutina, kretanja i navika.

Očekivani rezultati:

- Kompletan profil Toma Sawyera sa potvrđenim podacima o identitetu, lokaciji i aktivnostima.
- Detaljna mapa krijumčarskih ruta kroz teritoriju BiH, sa identifikovanim tačkama prelaska i lokacijama okupljanja migranata (Višegrad, Sarajevo, Bihać).
- Popis saradnika i lica koja učestvuju u krijumčarenju migranata.
- Prikupljeni dokazi sa društvenih mreža koji potvrđuju aktivnosti krijumčarenja i povezanost sa OKG KLL.

Rok za dostavu rezultata: 10 radnih dana od dana pokretanja zahtjeva.

4.3. Razrada aktivnosti koje se poduzimaju u svrhu odgovora na obavještajni zahtjev

Nakon što je dobijen obavještajni zahtjev, započinje se sa jasnim utvrđivanjem poznatih i nepoznatih informacija. Njihovim utvrđivanjem planiraju se i usmjeravaju aktivnosti istražitelja /tima, kako bi se izbjeglo traganje za informacijama koje već postije i verifikovane su. Utvrđivanjem nepoznanica započinje se istraga jer upravo nepoznanice predstavljaju usmjeravajući faktor. Nakon usmjeravanja, započinje se sa aktivnostima kao što su prikupljanje osnovnih podataka, Analiza društvenih mreža i digitalna forenzika sadržaja, saradnja sa jedinicama na terenu i kreiranje izvještaja na osnovu sprovodenih aktivnosti. Navedeni koraci se mogu prikazati na sljedeći način:

1. Jasno utvrđivanje poznatih informacija

Instražitelj ili tim kojem je dodjeljen navedeni obavještajni zadatak prvenstveno ima cilj da utvrdi šta posjeduju od podataka i informacija. Na osnovu prethodnog narativnog teksta, uviđa se sljedeće:

- Identitet lica: Lice koristi fiktivno ime Tom Sawyer, ali profilna slika i drugi sadržaji na društvenim mrežama ukazuju da je riječ o licu azijskog porijekla, koje odgovara fizičkim konstitucijama afganistanaca.
- Organizirana kriminalna grupa: Utvrđeno je da se grupa zove LLK, što može biti određena skraćenica ili kod koji je povezan sa kulturuom i jezikom Afganistana. Taokđer je utvrđen i broj lica – 15, ali nije utvrđena hijerarhijska struktura i vođa.
- Kriminalne aktivnosti: Krijumčarenje migranata od Turske, preko Bugarske i Srbije (nejasne rute kretanja), nakon čega ulaze na teritorij BiH i kreću se nepoznatim rutama od Višegrada do Bihaća.
- Sredstva komunikacije: WhatsApp broj sa profilnom slikom koji služi za ugovaranje krijumčarenja. Ne postoje informacije da li se broj koristi i za međugrupnu komunikaciju.
- Iskoristivi tragovi:
    - Instagram i TikTok nalog na kojim je vidljiv sadržaj o uslugama krijumčarenja.
    - Geolokacijski pejzaži u objavama – most u Višegradu, kafići u Sarajevu, putokaz „Bihać 15 kilometara“.
    - Interakcije sa na objavama kao što su lajkovi, komentari i dijeljenja.
- Operativni HUMINT podaci:
    - Lokacija spavanja u Sarajevu.
    - Specifičnost korištenja aplikacije WhatsApp za komunikaciju.
    - Kretanje kroz šumske puteve.

2. Utvrđivanje nepoznatih informacija

Istražitelji navode informacije koje su im nejasne ili ih nemaju na raspolaganju. Odgovori na njih su potrebeni kako bi se kompletirala cjelokupna „slika“ o predmetnom licu i njegovom *modus operandi*. Nepoznanice su sljedeće:

- Identifikacija svih članova LLK grupe
    - Imena članova grupe,
    - Hijerarhija grupa,
    - Njihovi nalozi na društvenim mrežama,
    - Brojevi telefona,
    - Zaduženja i specijalizacije (finansiranje, transport, regrutovanje i tako dalje).
- Preciznija analiza digitalnih tragova

    - Dodatni profili Tom Sawyera na Facebooku, Telegramu, Viberu, Discordu ili drugoj aplikaciji.
    - IP adrese uređaja i geolokacije sa kojih se prijavljuje.
    - Ko su korisnici koji komentarišu i lajkuju sadržaje. Kojoj grupi pripadaju: migranti, pomagači ili potencijalni klijenit.
- Logistika krijumčarenja
    - Precizne rute kretanja nakon ulaska u BiH i na kojim mjestima prelaze na teritoriju BiH.
    - Na kojim lokacijama prelaze u Višegradu ili njegovoj okolini.
    - Gdje borave kada pređu u Višegrad, da li postoji neko zborno mjesto za odmor.
    - Gdje borave u Bihaću poslije transporta, da li postoje jasno određene lokacije ili su *ad hoc*.
- Da li imaju kontakta sa drugim grupama koje djeluju na teritoriji Turske, Bugarske i Srbije.
- Na koji nači se vrši plaćanje – gotivna, kritpovalute ili hawala sistem.
- Na osnovu čega se određuje ruta kretanja.

3. Poduzete aktivnosti za ispunjenje obavještajnog zahtjeva

Prikupljanje osnovnih podataka

Istražitelji započinju operaciju sa verifikacijom identiteta kroz provjere dostavljenog broja (predstavljanje kao potencijalni klijent) na razlučitim SMS servisima kao što je WhatsApp, Telegram, Viber i tako dalje. Downloaduje se fotografija sa WhatsAppa, te se vrši njena analiza i opis. Društvenim mrežama se posvećuje pažnja radi utvrđivanja osnovnih informacija, nakon čega se izvršava popunjavanje operativnog kartona iz tabele 2.

Analiza društvenih mreža i digitalna forenzika sadržaja

Istražitelj započinje pretragu profila i objava na njemu. Sve objave i sadržaji se preuzimaju uz pomoć *data scrapera* i kategorišu u tematske foldere – fotografije, video snimke, komentare, lajkove, pratitelje i praćene. Ukoliko objave imaju geotagove, nastoji se verifikovati njihova tačnost te pružiti precizne koordinate.

Digitalna analiza sadržaja (fotografije, video sadržaji) se vrše upotrebom alata za reverse search kao što su Google, Yandex i TinEye. Uporedo se vrši ekstrakcija EXIF[14] metapodatka kao što su lokacija uređaja u trenutku snimanja, tehničke specifikacije i vrsta uređaja, format i datum /vrijeme snimanja. Ukoliko lice posjeduje tehnička znanja i ima visoku operativnu sigurnost, navedeno neće dati podatke, te se u tom slučaju započinje sa opisivanjem sadržaja – doba dana,

[14] Izmjenjivi format slikovne datoteke je standard koji specificira formate za slike, zvuk i pomoćne oznake koje koriste digitalni fotoaparati (uključujući pametne telefone).

godišnje doba, broj lica i njihov izgled. Navedeno služi za dalje profiliranje i moguće povezivanje sa drugim akterima u krijumčarskoj mreži.

S obzirom da ruta kretanja predstavlja značajnu problematiku, potrebno je mapirati kretanje kroz prošlost na osnovu datuma objave, geolokacije i mogućeg doba dana i sata kada je fotografija / video učinjen. Za utvrđivanje tačne lokacije koristi se Google Earth, Geoguesser ili AI alat koji ima mogućnost geoliciranja. Ova aktivnost služi za kreiranje obrasca ponašanja, odnosno utvrđivanja da li on postoji – objave svaka tri dana ili je raspored objava nasumičan. Postoji mogućnost da lice objavljuje sadržaj nekoliko dana nakon što je isti kreiran, čime se vrši direktna obmana, a isto se utvrđuje sa komparacijom EXIF metapodataka. Također, kroz obradu ovih podataka, dobija se jasnija informacija o korištenju ruta, pri čemu se za isto mogu koristiti Google maps i označiti dvije susekventne lokacije na sadržaju, pri čemu se pokazuje moguća ruta pješke ili prevoznim sredstvom.

Pored ruta kretanja, bitni su i kontakti koji su ostvareni na društvenim mrežama. Interakcije sa drugim nalozima ukazuju na moguće saradnike i klijente. Nalozi koji lajkaju ili komentarišu objavu predstavljaju bitne elemente mreže te se isti trebaju mapirati, pri čemu se za vizuelizaciju koristi Maltego ili neki drugi softver.

Saradnja sa jedinicama na terenu

Na osnovu organizacije službe / agencije i suradnje sa drugim partnerima, potrebno je ukazati na neštićene prelaze na granicama, što će poslužiti jedinicama na terenu da uspostave punktove za nadzor. Također, provjeravaju se baze podataka i utvrđuje da li ima pozitivnih nalaza, odnosno da li je neka od sigurnosnih agencija evidentirala Tom Sawyera – ilegalni prelazak, minorni prekršaj, krivično djelo, smještaj u prihvatnom centru i tako dalje. S obzirom na lokalitet djelovanja bezbjednosno interesantnog lica, utvrđuje se da li postoje informacije o njegovim aktivnostima u Višegradu, Sarajevu ili Bihaću. Potrebno je mapirati kretanja lica na mjestima gdje je često viđen – kafići i prenoćišta. Podaci i informacije o kretanju u Sarajevu se mogu iskoristiti za posebene istražne mjere i radnje kao što su praćenje i nadzor, te u posebnim slučajevima nadzor telekomunikacija zbog jasnog utvrđivanja veze između lica i telefonskog broja koji koristi.

Kreiranje izvještaja i odgovor na obavještajni zahtjev

Po isteku roka od 10 dana, potrebno je dostaviti izvještaj. U navedenom analitičkom izvještaju se jasno i koncizno daju nalazi, te ukazuje na nedostajuće informacije koje zahtjevaju dalje poduzimanje operativnih radnji. S obzirom na značajno veliku kriminalnu grupu i potencijalne klijente, može se predložiti

nastavak OSINT operacije u kojoj se nastoji doći do podataka i informacija o drugim članovima i hijerarhijskim postavkama grupe. Može se preporučiti djelovanje HUMINT elemenata i infiltracije u samu grupu pod legendom klijenta, kao i upotreba SIGINT-a, odnosno nadzora telekomunikacija, praćenje GPS-a uređaja i aktivnog presretanja interent saobraća i komunikacije.

Nakon izvještaja i odgovora, krajnji korisnik informacije može zahtjevati nova saznanja ili dati upute za izvođenje drugih radnji.

ZAKLJUČNA RAZMATRANJA

Upotreba OSINT-a kao obavještajne discipline u istraživanju organiziranih kriminalnih grupa postaje sve više i više zastupljena među agencijama za provedbu zakona. Iako postoje podijeljena mišljenja o navedenoj disciplini, njena oporetivna upotreba je kolosalna. OSINT omogućava efikasno, efektivno i ekonomično prikupljanje podataka koji se odnose na organizirane kriminalne grupe. Također, veliki je značaj smanjenja rizika izlaganju opasnosti na terenu, što je primjetno kod HUMINT-a. Međutim, upotrebom ove metode, postoje i izazovi poput fragmentacije podataka, dezinformacija, anomalija, tehničkih i personalnih ograničenja, što može značajno otežati ili zaustaviti u potpunosti istragu. Ukoliko se osmisle načini za prevazilaženje ograničenja, OSINT značajno može unaprijediti rad agencija za provedbu zakona u borbi protiv OKG, naročito ukoliko se sjedini sa drugim disciplinama poput HUMINT-a, SIGINT-a. Na ovaj način se omogućava potpuni nadzor nad kriminalnim grupama i pojedincima koje su predmet istrage. Kako bi se poboljšale aktivnosti borbe protiv organiziranog kriminaliteta koji značajno narušava nacionalnu sigurnost (ilegalne migracije, trgovina ljudima, krijumčarenje narkotika, proliferacija oružja), potrebno je uložiti sredstva u kreiranje alata i obuku istražitelja. Kroz obuku i razvoj novih alata, omogućava se potpuno iskorištavanje ove obavještajne discipline. Značajna je važnost razvijanja OSINT protokola i njihova aplikacija u istraživanju kriminalnih grupa i krivičnih djela kojima se značajno ugrožava nacionalna sigurnost. Hipotetički primjer je ukazao na kompleksnost istrage i različite varijable koje utječu na istragu. Upotrebom OSINT-a i koordinacijom sa jedinicama na terenu i drugim partnerskim agencijama / službama, omogućava se brzo i efikasno djelovane, razbijanje kriminalnih grupa te njihovo procesuiranje. Veliku važnost treba pridodati kontinuiranom djelovanju i nadzoru na društvenim mrežama koje su pogodne za diseminaciju krijumčarskih ili drugih usluga koje pružaju organizirane kriminalne grupe. Dalja istraživanja na ovu tematiku trebaju biti usmjerena u razvoj metodologija istraživanja različitih kriminogenih grupa, kao i aktera koji ih provode. Na taj način će se obogatiti fond znanja i sredstava koja su državi dostupna u borbi protiv transnacionalnog kriminaliteta i prijetnji.

Bibliography

Baker, R. (2023). *Deep Dive: Exploring the Real-World Value of Open Source Intelligence.* Wiley.

Brunet, J., & Claudon, N. (2015). Military and Big Data Revolution: A Practitioner's Guide to Emerging Technologies. U A. Staniforth, B. Akhgar, P. S. Bayerl, H. Arabnia, G. B. Saathoff, & R. Hill, *Application of Big Data for National Security.* Butterworth-Heinemann.

Chen, H., Chiang, R. H., & Storey, V. C. (2012). Business intelligence and analytics: From big data to big impact",. *MIS Quarterly*, 1165-1188.

CIA. (2024). *The Intelligence Cycle.* CIA. Preuzeto od https://www.cia.gov/spy-kids/static/59d238b4b5f69e0497325e49f0769acf/Briefing-intelligence-cycle.pdf

Clark, R. M. (2016). *Intelligence Analysis: A Target-Centric Approach Fifth Edition.* CQ Press.

DHS. (2022). *Ethical Frameworks in Open-Source Intelligenc.* Public-Private Analytic Exchange Program.

Headquarters, Department of The Army. (2023). *FM-2: Intelligence*. Washington DC.

J. Pastor-Galindo, P. N. (2020). The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends. *IEEE Access*, 10282-10304.

Kao, D.-Y., Chao, Y.-T., Tsai, F., & Huang, C.-Y. (2018). Digital Evidence Analytics Applied in Cybercrime Investigations. *IEEE Conference on Applications, Information and Network Security* (str. 111-116). Langkawi, Malaysia: IEEE.

Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons*, 59-68.

Loch, J. K. (2006). *Handbook for Intelligence Studies.* Routledge.

ODNI. (2011). *US National Intelligence: An Overview.* Washington DC: ODNI.

Quick, D., & Choo, K.-K. R. (2018). Digital forensic intelligence: Data subsets and Open Source Intelligence (DFINT. *Future Generation Computer Systems*, 558-567.

Reid, E. (2023). 'Trap Life': The psychosocial underpinnings of street crime in inner-city London. *The British Journal of Criminology*, 168–183.

Sampson, F. (2016). Intelligent evidence: Using open source intelligence (OSINT) in criminal proceedings. *Police Journal: Theory, Practice and Principles*, 1-15.

Williams, H. J., & Blum, I. (2018). *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise.* RAND Corp.

DODATAK

Operational use of OSINT in the investigation of organized crime groups

Emir Muhić, MA[1]

ABSTRACT

Organized criminal groups (OCGs) represent a significant threat to national and international security, requiring adaptive and innovative approaches in their investigation. This paper examines the role of OSINT (Open Source Intelligence) as a key method of collecting and analyzing data from publicly available sources in the context of the fight against the aforementioned actors. OSINT enables efficient collection of information about OKG members, their activities and networks without physically going out into the field, thereby minimizing operational risks. Using social networks, digital forensics data and other open sources, investigators can monitor communications, geolocate actors and analyze the behavior patterns of criminal groups. Through a hypothetical example, the paper points to the importance of OSINT in making operational decisions faster and developing strategies to neutralize criminal activities. The aim of the research is to develop an operational model for the application of OSINT in cases of organized crime, while highlighting its advantages and challenges. The conclusion emphasizes the importance of improving the skills of investigators in the use of OSINT tools, as well as the need for a clear framework for use .

Keywords : *OSINT, organized criminal groups, digital forensics, operational models.*

[1]Doctoral student, Faculty of Criminology, Criminology and Security Studies.

INTRODUCTION

Investigating organized crime groups [2]has always been a significant challenge and problem for state agencies and law enforcement agencies. The evolution and adaptation of organized criminal groups (in the following text OKG) also conditioned the adaptation of the previously mentioned agencies and services that rely to a significant extent on intelligence work. Also, the importance and role of modern technologies, as well as social networks, which are an indispensable part of human life, enable more efficient collection of operational data that serves to support investigations. In this context, OSINT (Open Source Intelligence) – gathering intelligence from open, publicly available sources – is becoming an increasingly important tool. OSINT stands out as a key segment of modern intelligence work due to the possibility of quick, cheap and broad access to information that is of critical importance for the identification and analysis of actors of security interest. The role of OSINT in solving cybercrime and organized crime is increasingly recognized in recent research (Kao, Chao, Tsai, & Huang, 2018). For example, OSINT could increase the accuracy of criminal prosecutions and arrests of criminals using a framework such as the one proposed by Quick and Choo (Quick & Choo, 2018). Such frameworks provide not only a structured approach to analysis, but also the integration of data coming from different sources, thus enabling a comprehensive overview of criminal activities and connecting seemingly unrelated information. Specifically, the authors apply OSINT to digital forensic data from a variety of devices to improve criminal intelligence analysis (J. Pastor-Galindo, 2020). In order to solve dilemmas in understanding and translating the term *intelligence* into B/H/S languages, in this paper it will have the context of *intelligence information* , which consists of analytically processed data [3]and information [4]in order to ensure precise terminological clarity. OSINT has a long history and its beginnings are linked to the Second World War and the recording of enemy propaganda that came from traditional media. Today, OSINT has a significant application in intelligence work (military, civil, cyber) and serves as an essential element of obtaining information about the state and processes essential for national security (DHS, 2022). The complexity of the investigation and processing of OKG requires the use of adequate intelligence methods such as OSINT, HUMINT, SIGINT and so on. Unlike other methods, OSINT enables a deeper analysis of the digital and social environment without necessarily relying on field work and exposure to danger. In addition, OSINT as a method enables objective research of actors of

[2]OKG in this work follow the definition of UNDOC which reads: " *a structured group of three or more persons that exists for a certain period of time, whose members act together with the aim of committing one or more serious crimes or criminal acts, with the aim of obtaining direct or indirect financial or other material benefits* ."

[3]Data is a fact presented in a certain format - word, image, number, character, letter and so on.

[4]Information is a logically connected group of data that has a specific meaning.

security interest without going out into the field because it is based on the verification and analysis of data from publicly available sources. In the research of OKG and their members, open sources such as social networks are used, where actors can leave a significant amount of data and information, such as photos, videos, publications and so on. The subject of this research is the analysis of the use of OSINT as an intelligence discipline in detecting, identifying, monitoring and documenting the activities of organized criminal groups. The main goal of the work is the development of an operational model of the plan for the application of OSINT activities in cases of investigation of organized criminal groups and individual actors of security interest. The purpose of this research is reflected in the insufficient research and marginalization of the operational application of OSINT in the research of organized criminal groups, because previous research was focused only on defining the term.

1. Theoretical and practical concept of OSINT

With the expansion and development of cyberspace as a new domain of human life, intelligence activities and the collection of data and information have been made possible. When we talk about open sources, in the traditional sense they include any carrier of information - audio, video, photo or text. Cyberspace as a domain has enabled simpler access to data and information, while conducting investigations has been simplified and facilitated. The definition of OSINT is based on obtaining the required information from publicly available sources, and given the multitude of definitions by various state and non-state actors, the one given by the Office of the Director of National Intelligence (ODNI) of the United States of America will be used as a basis. ODNI (2011)OSINT defines it as *intelligence data produced from publicly available information that is collected, exploited and timely distributed to the appropriate audience for the purpose of fulfilling specific intelligence requirements* . According to Baker (2023), publicly available information is any information that is available to the public without the use of a secret permit or breaking into the system; however, it may also include data behind a paywall such as a newspaper subscription. This data can be collected from the internet, social media, mainstream media, publications and subscriptions, audio recordings, images, videos and geospatial/satellite information (Baker, 2023), etc. In addition to the above, the ODNI (2011)also lists so-called "gray literature [5]" - open source material that is usually available through controlled access for a specific audience as well as observation and

[5]ODNI (2011) lists as gray literature: research reports, technical reports, economic reports, travel reports, working documents, discussion documents, unofficial government documents, proceedings, preprints, studies, dissertations and theses, trade literature, market research and newsletters. Gray literature covers scientific, political, socioeconomic and military disciplines.

reporting [6]. Given some input data, together with the application of advanced collection and analysis techniques, OSINT continuously expands knowledge about the target (J. Pastor-Galindo, 2020). In this way, the information found feeds back into the collection process to get closer to the final goal (Williams & Blum, 2018).

The basic principle of OSINT is to obtain data or information from already existing content located in the cyber or physical domain without unauthorized access to protected systems and networks. Therefore, OSINT is a purely passive method that does not use penetration and active reconnaissance (Baker, 2023). Any other entry into the system or network is considered penetration into the protected system and does not belong to OSINT methods. Although tools for OSINT collection evolve almost daily, the methods used by the tools themselves change less dramatically. Most tools use lexical analysis, network analysis, geospatial analysis, or a combination of these methods to isolate, describe, and analyze data (Williams & Blum, 2018). All three methods existed long before their application to Internet-based content, but the massive proliferation of social media platforms and the increasing ease with which individuals can access the Internet make it a rich environment for intelligence gathering (Williams & Blum, 2018). Considering the digitization of the material world, the sources are most often on the Internet and require active searching, recording and processing. In the aforementioned, various elements of the carrier of the requested intelligence information are used, such as social networks, blogs, portals, websites and so on, on which methods, techniques and tools suitable for reaching the requested information are applied. OSINT is not strictly the use of tools - software and hardware, but is also reflected in the logical connection of data and information, in order to respond to the intelligence request of the superior. Certain investigations do not require technical knowledge, but only a series of logical and intuitive steps, while on the other hand there are investigations that require knowledge of network and computer systems, software, hardware and so on to fulfill intelligence requirements. For example, a superior can give a task to collect basic information about a person of security interest who is reasonably suspected to be a member of the OKG. By searching social networks such as Facebook, Instagram or TikTok, basic information can be found - interests (music, movies, video games, sports and so on), physical appearance over a long period of time (can be used for cross-referencing with other cases) , travel information, lifestyle (luxurious, moderate, ascetic) and so on. By analyzing orders on social networks, it is possible to find out information about the person in question. If the intelligence requirement is more challenging - determining the group's *modus operandi* , certain skills and knowledge are required. For example, the

[6]Information of importance, which is not otherwise available, and which is provided by, for example, amateur plane spotters, radio monitors and satellite observers (ODNI, 2011).

identification of a smuggler's movement route requires prior knowledge of the movements of a group or person, geolocation of data (publicly available photos or video content) and confirmation / rejection of the previous movement route, time and date of movement, interactions of other accounts with the content (like, share, comment) and so on. The mentioned process is demanding, chaotic and requires movement and critical thinking.

2. OSINT and the intelligence cycle – a guiding link

When conducting investigations, whether by national police agencies, civilian or military intelligence services, or even private investigators, the process of knowing is based on the intelligence cycle. The stated cycle originally originates from the US Intelligence Community and serves as guidelines and instructions for the reliable and repeatable collection and processing of information to meet the intelligence requirements of a superior actor. The steps of the intelligence cycle are the most basic actions from initial planning of an operation to responding to an intelligence request [7]and ensuring that the response is integrated into the operation (Headquarters, Department of The Army, 2023). Just as the activities of the operations process overlap and repeat as the mission requires, so do the steps of the intelligence process.

This cycle is the activity of developing raw information into finished intelligence for use by policymakers, military commanders, and other decision-making users (ODNI, 2011). It is highly dynamic, continuous, and never-ending, and consists of the following elements:

- Planning and directing;
- Gathering;
- Processing and exploitation;
- Analyses and productions;
- Disseminations;
- Evaluations and feedback.

Almost all intelligence studies authors list four or more steps, with minor differences, and subcategories within each step. Looking at the literature, each cycle begins with planning and ends with dissemination or feedback, depending on the author. For example, the CIA's intelligence cycle describes this process as planning and directing, collection, processing, analysis, and production and dissemination (CIA, 2024), while Johnson's Handbook of Intelligence Studies (Loch, 2006)describes these stages as collection, processing, analysis and

[7]An intelligence requirement is 1. Any subject, general or specific, for which there is a need to gather information or produce intelligence. 2. A request for intelligence to fill a gap in the command's knowledge or understanding of the operational environment or threat forces (JP 2-0).

production, classification, and dissemination. RAND also gives its intelligence cycle and defines it through 1. collection - acquisition and retention, 2. processing - translation and aggregation, 3. exploitation - authentication and contextualization, and 4. production - classification and dissemination (Williams & Blum, 2018). The listed items correlate with five main processes (identification, collection, examination, analysis and presentation, give an abstract) in digital forensics, which is crucial in the investigation of organized criminal groups (Kao, Chao, Tsai, & Huang, 2018).

When using OSINT to investigate a specific person of security interest, it is necessary to develop a model of the intelligence cycle that has a target in the foreground - a person of security interest. The United States intelligence community has implemented a concept similar to the target-oriented approach. This concept, called "object-based production" (English: *object-based production* or OBP), implies organizing intelligence activities around "objects" (targets) that are of intelligence interest (Clark, 2016). A key feature of this approach is the sharing of up-to-date knowledge of an intelligence target via cloud-based platforms. Clark (2016) offered the above model (Illustration 1), where the basic elements appear: target, Needs, new information, analysis: gaps, requirements, sources of information (collectors), new information, analysis: answers, usable intelligence , problem (users).

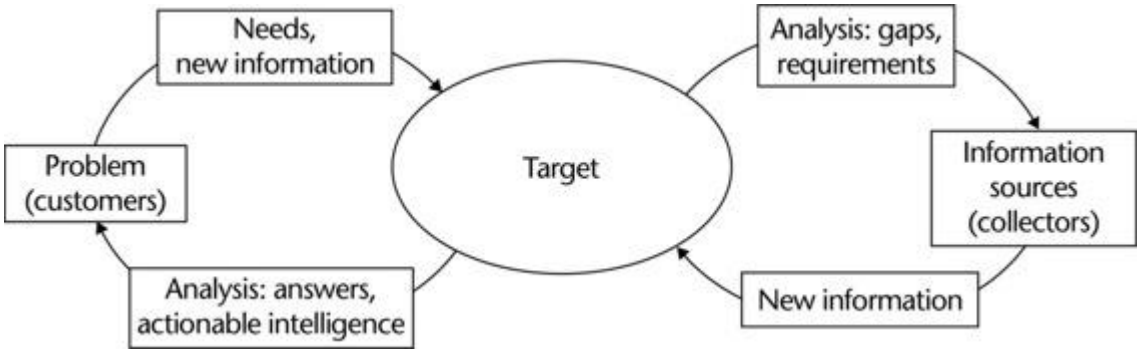


Illustration 1- Target Focused Intelligence Cycle (Clark, 2016)

The diagram ensures a structured and directly oriented process of gathering and analyzing information related to the target. Requests are continuously given, checks are made, data / information is verified. In this way, it is possible to make quick decisions based on direct changes in the material world, as well as to respond to intelligence requests coming from decision makers.

The intelligence cycle is essential for the activities undertaken in OSINT because it determines what is important for the provider of the intelligence request - the entity seeking information, and creates a product that meets their needs. The investigation of organized crime groups begins with an intelligence request on

relevant information - movements, assets, activities, spatial location of operations, associates, and so on. Through the intelligence request, frameworks are set that serve to focus the investigation on certain relevant information, which prevents aimless wandering or arbitrariness of the investigator, which can result in the collection of data and information that is not of operational importance. Therefore, the intelligence request will serve the investigator to define what needs to be found out, while the intelligence cycle indicates the process of obtaining information.

3. Operational use of OSINT in OKG research

OSINT has significant use in the investigation of OCG and other modalities that threaten national security. Although it has long been thought that OSINT is not a separate intelligence discipline like HUMINT, SIGINT, ELITN and so on, its application in investigations speaks to the contrary. The concept of open source intelligence (OSINT) is relatively new to law enforcement agencies and is loosely defined as intelligence gathered from publicly available sources that do not require covert or covert collection methods (Brunet & Claudon, 2015). This modality has significant operational possibilities that depend on its user and the actor seeking the information. In order to more adequately understand the operational use of OSINT, it is necessary to understand the possibilities of use in different situations. For example, every operation in which a security interested person is monitored begins with the collection of data about him, the analysis of said data, and the creation of a report. Considering the dynamism and variability of the situation, situational problems and challenges arise, the resolution of which is left to the investigator. Accordingly, the use of OSINT in the investigation of the OCG is a dynamic process that primarily depends on the creativity, abilities and skills of the analyst, as well as his focus on fulfilling the intelligence requirement.

3.1 . Collection, categorization and primary processing of data of a person of security interest

Social networks in modern times have become a valuable source of information and have an operational application in OKG investigations, especially those groups that have a very low or non-existent OPSEC [8]culture. Examples and types of social networks include the following: collaborative projects (eg Wikipedia); blogs and microblogs (eg Twitter /X); content communities (eg YouTube); social networking sites (eg Facebook); virtual game worlds (eg World of Warcraft); and virtual social worlds (eg Second Life) (Kaplan & Haenlein, 2010). The

[8]Operational security (OPSEC) represents the concept of protecting one's own activities from adversaries. Sometimes this means not publishing content that can be linked to a person, while in other cases it also requires the use of complex systems that hide the identity of actors and enable activities, processes and actors to remain unnoticed and unidentified.

determination of which social network will be designated for data collection depends on the person who has an open account on the specified social network. For some crimes (such as threats or offensive comments,10 or fraud) 'open source' material such as Twitter (another type of social media (Kaplan & Haenlein, 2010)) can itself be prima facie evidence of a crime (Sampson, 2016). For other crimes such as human trafficking, other social networks such as TikTok can be used, where there is an evident number of smugglers of Afro-Asian origin promoting their services [9]. Other social networks, such as Instagram, can be used to record the life - movements, whereabouts and other activities of members of organized criminal groups who often publish content about their luxurious and opulent lives, which represents an important source of data and information.

Identification activities of persons of security interest begin with an intelligence request for identification and possible location. In certain cases, there may be general information about the person, as well as his photo, which significantly speeds up the investigation. In cases where there is a photo of a face and clues indicating its movement and geolocation, web browsers such as Google and Yandex, as well as numerous tools (Table 1), are a significant help.

Table 1- List of photo search tools

Tools	Description
Beify	Reverse image search to find stolen images and videos.
Bing Image Search	Bing's reverse image search page.
Eagle Eye	He scans social media for the uploaded image.
Geospy	It tries to locate where the image was taken using AI.
Google Image Search	Google's reverse image search page.
Osint Combine	Tool for improved reverse image search with tabular results from Google and Yandex.
Tineye	Reverse image search to find where images appear on the internet.
Yandex Image Search	Yandex reverse image search page.

The above tools are not the only ones and there are many others that are used, some are free and some are not. The search process can also start on the associate's account and the photo of the person of interest. With further searches and reaching the profile of the person of our interest, the data collection process

[9]This is evident by searching social networks using different tags such as migration, western Balkans, refugees and so on. There are also certain chat groups on sms services such as WhatsApp, Telegram, Discord, Viber and others. The reasons for the large influx of migrants of AA origin is the destabilization of the Middle East, especially the Levant and Afghanistan, which is connected with the political turmoil in the said region.

begins. The above data can be classified into categories suitable for further analysis (Table 2).

Table 2Categories of data required for analysis - operational record

Category	Details	Importance
User data	- Official name and surname - Username on the social network (@username) - Profile URL - Date of birth - Place of birth - Education - Employment/position - Places of residence - Contact information - Family/relationships - Life events - Biography - Profile photo - Other user photos	It focuses on the basic information available on the profile needed to take further actions. From the above, a file of persons is created and elements suitable for exploitation are found.
Profile picture	- Profile picture description (face, symbol, object) - Identification of physical characteristics (hair color, tattoos, etc.) - Authentication (AI image analysis tools)	Analyzes profile picture for identification or verification of previously obtained data.
User connections	- Friends - Family - Colleagues - Memberships/groups	They enable mapping of the subject's social network, identification of close contacts and potential collaborators or members of OKG.
User interactions	- Likes - Emojis - Comments - Friends/followers list - Memberships in groups or pages - Frequently commented or mentioned profiles	It provides insight into the social network and connected people to develop a social map.
Post content	- Context (work, entertainment, etc.) - Content types (text, images, video) - Locations - Friends/family	Identifies topics of interest and possible links to specific activities for further exploitation and

	- Personal data - Habits (smoking, alcohol consumption, drug use, fitness, video games, sports) - Hobbies	development of the course of action.
Media content	- User photos - Identification characteristics (hair color, tattoos) - Photos with location identifiers - Habits (smoking, alcohol consumption, drug use) - Location - Friends/family - Hobbies	Provides visual and geolocation information for physical identification, activity tracking and subject behavior analysis.
Metadata	- Locations - Weather - Dates - Platforms used -Used devices	It helps track time, locations and social media usage.
Body analysis	-Wounds on the body -Scars -Tattoos -Disability -Diseases -Skin changes	The listed items help in the possible identification of a person if he participated in an event of interest to the investigator. Wounds on the hands may indicate a physical conflict or an injury caused by hitting glass and so on. Specific wounds or disabilities may indicate unprofessional handling of improvised means (detonators, explosives, and so on).

After the collection of the mentioned items, the analysis of the data and the determination of certain connections that meet the intelligence requirement, such as the movement of a person of security interest, an insight into the network of associates, the determination of the assets he owns, and the information necessary for the execution of certain operational-tactical actions, are started. According to the frequency of visits to certain locations (metadata about location, time and dates), patterns of behavior can be created and frameworks for conducting special investigative actions can be provided. Due to the large amount of data found on

social networks (followers, friends, likes and so on), it is advisable to use so-called *data scrapers* [10], especially those developed in your own agency/service.

When the data collection is done, they start processing and creating an analysis. In this phase, raw data such as general information, metadata, locations and others gain their importance. The processing can be observed through the following items:

- verification of already obtained data (general data, physical appearance, locations, co-workers and so on),
- categorization of data according to their meaning and operational usability (general data *versus* data on the collaborative network),
- structuring data through creating connections, identifying frequent behavior patterns (locations visited, time of activity, attendance at events, people most frequently communicated with, and so on),
- understanding the context (connection with criminogenic persons and events,
- the purpose of the post (what it wants to achieve – presenting a luxurious life, intimidation, finding collaborators),
- places of activity and meeting with other persons of security interest),
- identification of key actors - associates and other members,
- creation of reports (answers to intelligence requests and directing decision-makers towards new points of interest),
- undertaking operational-tactical measures and actions (raids, surveillance of telecommunications, monitoring, deprivation of liberty and so on).

The mentioned processing is necessary due to the connection of random data into one coherent whole. A photograph of a face does not provide much information, however, its association with the place, date and time of photographing, context and possible objects/persons on it directs the investigation. In the course of the mentioned procedure, it is necessary to focus on details that may point to seemingly non-existent connections and relationships.

3.2. Analysis of OKG members' social media accounts and drawing conclusions

After the data has been collected and categorized, and the primary processing of the data into a coherent whole has been carried out, it is necessary to start with the analysis of the order. Social networks are a significant indicator of a certain person's life and as such should be fully utilized. In recent years, with the advancement of big data and data mining techniques, the research community has noticed that open data represents a powerful source of analyzing social behavior

[10]Listed are programs and scripts that extract a certain type of data from web sources.

and obtaining relevant information (Chen, Chiang, & Storey, 2012). Insight into social media accounts can provide the investigator with significant information about the subject that can be used to further plan activities. Of course, there are exceptions and outliers that can challenge the stated thesis, but the average dictates the use of an analytical matrix and conclusions. Also, variables such as age, gender, cultural and ethnic factors, hierarchical status in the group, previous experience, cognitive abilities, mental illness and psychophysical condition can affect the collection of information. Different personality types can affect the ease and speed of collecting data and information, as well as the creation of analyses. The mentioned types are not considered, so a simple example of operational procedure is given for the benefit of the argument. A high-ranking young member of OKG who often presents his luxurious life on social networks can be used as a hypothetical example. By looking at his account on a social network such as Instagram, which is more often used by millennials [11]and Gen Z [12]as opposed to Gen X or baby boomers, the following variables can be identified:

a) Lifestyle – luxurious, moderate, ascetic;
b) Social connectedness – high, medium, low;
c) Social network activity – high, medium, low;
d) Interests and likes;
e) Direct connections with other persons of security interest;
f) Mental state;

The above represents a simplified process of collecting information from open sources, which serves for in-depth analysis. By looking at items such as, for example, a luxurious lifestyle and significant social connection, clues can be sought about the group's activities and the individual's role in it.

a) Lifestyle - different types of personalities try to present their real life to a wider audience through social networks. For the above, Instagram, TikTok and Facebook are the most adequate, which are based on the use of photos and videos as a medium for transmitting information. OKG members, or generally criminogenic persons, often due to the need for validation, (Reid, 2023)try to show their lavish and luxurious life, as well as access to resources (money) or through the presentation of resources, they try to achieve social ties. By collecting and analyzing photos from social networks, primarily Instagram, which is popular with Gen Y and Z, the following items can be seen that can classify life as luxurious, moderate or ascetic:

[11]The demographic group born from 1981 to 1996, succeeding the Gen X demographic. Sometimes called Gen Y.
[12]The demographic group born from 1997 to 2012, succeeded the Gen Z demographic.

- Clothing – whether the focus is on expensive brands or new fashion clothing. Attention should also be paid to specifically intended clothing – hiking clothing, tactical clothing, sportswear;
- Devices - is the person using the latest phone model when taking pictures (selfie in front of the mirror) or is it an older or flagship model. Photographing game consoles, *high-spec* computers and the like indicates the possibility of investing money in entertainment systems and their importance as a means of entertainment;
- Jewelry – can indicate access to resources or lack thereof if replicas or plagiarisms of luxury brands are used.
- Means of transportation – is the person photographed in high-value cars, does he have access to other means of transportation that signal access to resources – planes, helicopters, yachts;
- Travels - does the person travel often, to which destinations, for how long and where exactly does he stay - hotels and other accommodations. It is concluded based on tags and publication date. It can be used for cross-referencing for certain events - unsuccessful assassinations, meetings with other persons of security interest and so on;

By looking at the mentioned items, it is possible to come to the conclusion whether the lifestyle of the person in question is luxurious or not. If the person presents a luxurious life, the investigation is focused on legal sources of income, which may indicate a connection with OKG and the commission of criminal acts.

b) The social connection of the person in question indicates his place in the hierarchy and in the wider community. An insight into the relationship between the accounts that a person follows and those who follow him indicates popularity or presence, as well as aspirations that the person has, for example attracting the attention of the opposite sex. Photos with other people - family, friends, other persons of security interest can serve to direct the investigation and connect it with other events, processes, situations and happenings. A large social connection or its fictitious representation can be used for infiltration operations and records of key points in a criminal network.

c) Activity on a social network, such as continuous publication of content or communication with *sockpuppet* accounts, may indicate the availability of a person, his hierarchical status, lifestyle, connection with other persons of security interest. Also, periods without publication of content and communication can be interpreted as phases of planning or execution of criminal acts, or hiding after execution. Using certain tools during communication, it is possible to determine

geolocation via IP [13]. Different levels of activity can be interpreted in accordance with previously acquired knowledge or the development of new versions.

d) Interests and likes indicate the internal personality of the person. By looking at *the following/followers* list and *liked* and commented posts, personality models can be created. So, following or liking a large amount of content about a certain model of car, jewelry, or clothing indicates a person's preferences for luxury or the pursuit of luxury. Also, monitoring *of softcore* pornographic content on social networks (OnlyFans models and so on) indicates possible promiscuity of the person or his internal conditions.

e) Connections with other persons of security interest indicate his social connection, hierarchy in the group, popularity, connections and so on. The data can be used to identify a collaborative network and link it to previous criminal acts or presumption of joint cooperation in future criminal activities.

f) The determination of mental state and intellectual capacity is based on the analysis of the published content and the text - description of the content. For example, a large amount of love posts may indicate that the person is suffering or is in a happy love relationship. Posts about loyalty, motivation and group affiliation can indicate intragroup problems. Vulgar and provocative posts indicate certain internal processes that a person is going through. It is also necessary to pay attention to the writing style that indicates the level of education and schooling, which can be used for planning and performing other operational actions.

After the analysis of the order of the person of security interest, it is necessary to create a report responding to the initially received intelligence request that started the investigation. The answers can be positive - they provide an answer, negative - they do not provide the requested information, and neutral - they leave the possibility for further research. After the client of the intelligence request receives a response (positive, negative, neutral), he accordingly makes a new request, redefines or specifies the previous one. Although the investigator has submitted what was requested, continuous verification and pointing out of novelties is necessary - collaborators, activities, locations.

3.3. Operational problems and inability to access data

During data collection activities, a significant problem for the researcher is the very beginning. The question *of where to start* depends on the intelligence request, however, in most cases, using *the search* option on social networks is the initial step. A significant problem for the investigation is the private order of a person of security interest, who has medium or high OPSEC. The aforementioned

[13]Internet protocol - network protocol used by devices for data transmission via the Internet.

stops the investigation and requires creativity in solving this challenge. One of the ways is to use a *sockpuppet* account that was previously created, cultivated and maintained for cases of surveillance, infiltration, making contact and the like. The account should be maintained continuously and look organic. If the account is neglected and not adequately cultivated, the person in question may suspect a new *follower* , and remove contents that compromise him or provide enough information about him, and remove the new *follower* . A significant problem is the lack of creativity of the investigators, as well as the lack of knowledge of certain techniques or methods of reaching the required data and information, as well as the lack of knowledge of the use of tools. Technical and creative incompetence limits the investigation, and inadequate use of *sockpuppet* accounts can alert a person of interest that he is the subject of an investigation. Self-compromise can alert the entire network, which will step back and institute rigorous OPSEC. In this case, the investigation of persons of interest, collaborators and other security-interested subjects ends, and it is necessary to use other adequate and usable intelligence methods besides OSINT (HUMINT, SIGINT, ELINT).

A further problem can be a vague and inadequate intelligence requirement that can be interpreted in different ways, or is poorly defined. A broadly defined intelligence requirement will make it impossible for the investigator to focus on what is important, and will try to obtain, process and analyze all data and information, which requires a lot of time and can be counterproductive due to the dynamic nature of the actions taken by the person of interest. In this way, important information will be lost and the investigation can be directed in the wrong direction. The same can be overcome by requesting a new intelligence request or a request to redefine or refine the one already received. For example, a superior may request that data be collected about a person of security interest, where it is not specified from which network, which data (photo, audio, video, text), collaborative links, hierarchical links and so on. On the other hand, a precise and clear intelligence request would read: " *Collect information on a person of security interest Z in order to determine the identity, last location, movement in the last 60 days based on metadata, activities, contacts and possible connection with organized criminal groups." Start the investigation by processing an order on the social network Instagram, where the person has an open and public profile @usernameZ* ." This way, the investigator is enabled to focus on fulfilling the request, and not on thinking about what the decision maker needs. In certain cases, it is desirable for the investigator to guess what the decision-maker wanted, and to independently develop the investigation, however, sometimes this can be counterproductive and unnecessary.

Given that social networks can often be a means of misinforming and deceiving a wider audience, investigators can also be an indirect target of deception. Clark

(2016) states that denial and deception are the main weapons in the counterintelligence arsenal of a country or organization, and the aforementioned can also be transferred to members of organized crime groups. Deceiving, deciphering and lying depends on the psychological profile and mental state of the person of interest who, due to internal processes, can present his own life in a superlative. Disinformation and deception can also be the result of the compromise of investigators who, through their own reckless actions, pointed to data collection activities. A person of interest can then start their own counterintelligence procedures, leading to false leads - for example, posting photos after a few days, tagging in locations where they are not, and so on. The impossibility of quick verification will significantly jeopardize the investigation and enable the security of the person of interest to hide previous traces.

4. Hypothetical example of an investigation of a person of security interest belonging to OKG

In order to better understand the topic of the use of OSINT, which in certain situations can be vague and abstract, below will be given a hypothetical case of the actions of a person of security interest who is a member of an organized criminal group. This hypothetical case is intended to demonstrate the application of the intelligence cycle that guides the investigation after receiving an intelligence request from a superior/decision maker, and taking action to respond to it. In order to simplify the activities and problems, the current migrant crisis, which significantly threatens the state of Bosnia and Herzegovina, will be used. The methodology used in the example is general and simplified, without precise details such as the type of tools and their use. Different security services and agencies have their own research methodologies, and they are not the subject of this paper. An example will be presented through a narrative that enables the use of OSINT, an intelligence request that clearly defines what needs to be found out, and the elaboration of activities that will respond to the intelligence request. Any resemblance to real situations is coincidental and serves for illustrative purposes only.

4.1. Narrative and hypothetical factual situation

Operational data obtained from Western strategic partners indicate the activities of an organized criminal group called KLL. The aforementioned group has about 15 members, who are citizens of Afghanistan. The group's main activity and source of income is the smuggling of migrants from Turkey to Western Europe. The main operative operating on the territory of Bosnia and Herzegovina is Tom Sawyer, whose role is crucial in the final stage of the smuggling chain. According to available information, Tom Sawyer plays a leading role in establishing contact with migrants upon their arrival in BiH and ensuring smooth transit to the western

border. Current knowledge indicates that migrants start their journey in Turkey in one of the migrant camps, then pass through Bulgaria and Serbia. After reaching the western border of Serbia, they enter poorly monitored forest areas, and illegally enter the territory of Bosnia and Herzegovina, actively avoiding the patrols of the Border Police of BiH. Tom Sawyer picks them up in Visegrad, who further organizes their transport to the final destination - Bihać. Based on the collected data, it was determined that migrants pay significant sums of money for this service, which indicates a high degree of financial benefit for the KLL group.

Partners have forwarded information that Tom Sawyer uses social media platforms Instagram and TikTok as a primary channel for promoting his illegal activities. His digital presence allows him to not only advertise his “services” but also connect with potential clients, bypassing traditional intermediaries and ensuring that the entire amount of money is not shared with the intermediary. The posts clearly show:

- Tom Sawyer's appearance (photos and video content),
- Recognizable landscapes and locations in BiH, such as the bridge in Višegrad, cafes and hookahs in Sarajevo, and signposts that clearly indicate the direction and distance to Bihać (e.g. "Bihać 15 kilometers").
- Interactions in comments and likes, which provide additional clues about his connections and collaborators.

Additionally, information obtained through HUMINT confirms that Tom Sawyer is currently staying in Sarajevo, and that he is a frequent guest in a cafe in Baščaršija. His identity was additionally verified through a phone number, which was provided to the services. A review of the WhatsApp application, which is often used to communicate among migrants from Afghanistan, revealed that the number belonged to Tom Sawyer, as he uses his profile picture on the application. The aforementioned serves to connect the face of the name Tom Sawyer, which is advertised on social networks, with the phone number he uses for communication. Further analysis of the messages indicates the possibility of the existence of coded terms and phrases used to coordinate activities. There were frequent messages about watermelons, flowers and bowling. So far, it has not been possible to clarify what this means.

The activities of the KLL group pose a serious threat to national security, given that illegal migration can be linked to secondary security risks, including:

- Potential links with other forms of organized crime (trafficking in people, drugs or weapons).
- The risk of radicalization or infiltration of extremist elements among migrants caused by unrest in the Middle East.

- Destabilization of local communities through increased pressure on resources and security capacities.

Tom Sawyer, as a key actor, is currently a priority in stopping the work of the KLL group. His digital presence opens up space for an OSINT operation, which would gather additional information about his activities, connections and working methods. Operational gaps currently include: detailed information on his associates, precise timelines of smuggling operations and the routes he uses in urban areas. The goal is to create a complete profile of Tom Sawyer and his criminal network, using information from digital sources, HUMINT and other intelligence disciplines, to facilitate their neutralization.

4.2. Intelligence request from superior

In order for the investigators to start the investigation operation, the superior sends them an intelligence request. The intelligence request should guide the investigation by defining the unknowns.

Below is a hypothetical intelligence request related to the activities of one of the actors from an organized criminal group. A hypothetical intelligence request contains the following details

Subject: Monitoring the activities of Tom Sawyer and the KLL group on social networks in order to identify smuggling routes and collaborators.

Request Objective: Collect and analyze open source intelligence (OSINT).

The above is necessary to achieve the following:

- Determined the identity, direction of movement and whereabouts of Tom Sawyer and other members of the KLL criminal group.
- Identified secret smuggling routes used by migrants on the territory of Bosnia and Herzegovina.
- Collected information about potential collaborators and contacts who provide support to OKG on the Turkey-Bulgaria-Serbia-BiH route.
- Analyzed content from social networks (Instagram, TikTok, WhatsApp) for the purpose of mapping activities, geolocating routes and possibly revealing encrypted messages or key information.

Specific tasks:

- Detailed analysis of Tom Sawyer's Instagram and TikTok profiles (posts, comments, likes).
- Identification of persons who communicate or cooperate with Tom Sawyer (analysis of interactions on social networks).
- Collection and geolocation of visual information from published content (landscapes, road signs, locations).

- Study of communications on the WhatsApp application and analysis of the provided phone number to confirm identity and activity.
- Mapping of movement routes (roads, forest and mountain roads) of migrants based on collected data and HUMINT information.
- Determining the location of Tom Sawyer's residence in Sarajevo and analyzing his daily routines, movements and habits.

Expected results:

- Complete profile of Tom Sawyer with confirmed identity, location and activities.
- Detailed map of smuggling routes through the territory of Bosnia and Herzegovina, with identified crossing points and migrant gathering locations (Višegrad, Sarajevo, Bihać).
- List of collaborators and persons participating in the smuggling of migrants.
- Collected evidence from social networks confirming smuggling activities and connection with OKG KLL.

Deadline for delivery of results: 10 working days from the date of initiating the request.

4.3. Elaboration of activities undertaken to respond to an intelligence request

After receiving an intelligence request, a clear identification of known and unknown information begins. By identifying them, the activities of the investigator/team are planned and directed, in order to avoid searching for information that already exists and has been verified. By identifying the unknowns, the investigation begins, because it is the unknowns that represent the directing factor. After directing, activities such as collecting basic data, social network analysis and digital forensics of content, cooperation with units in the field, and creating reports based on the activities carried out begin. The above steps can be presented as follows:

1. Clearly identifying known information

The investigator or team assigned to the said intelligence task primarily aims to determine what data and information they have. Based on the previous narrative text, the following can be seen:

- Facial identity: The face uses the fictitious name Tom Sawyer, but the profile picture and other content on social media indicate that the face is of Asian origin, matching the physical constitution of Afghans.

- Organized Crime Group: The group has been identified as LLK, which may be a specific abbreviation or code associated with the culture and language of Afghanistan. The number of people has also been determined - 15, but the hierarchical structure and leader have not been determined.
- Criminal activities: Smuggling of migrants from Turkey, through Bulgaria and Serbia (unclear movement routes), after which they enter the territory of BiH and move along unknown routes from Višegrad to Bihać.
- Means of communication: WhatsApp number with a profile picture used for contracting smuggling. There is no information whether the number is also used for intergroup communication.
- Usable clues:
    - An Instagram and TikTok account displaying content about smuggling services.
    - Geolocation landscapes in announcements - bridge in Višegrad, cafes in Sarajevo, road sign "Bihać 15 kilometers".
    - Interactions with on posts such as likes, comments and shares.
- Operational HUMINT data:
    - Sleeping location in Sarajevo.
    - The specificity of using the WhatsApp application for communication.
    - Moving through forest paths.

2. Determining unknown information

Investigators cite information that is unclear to them or not available. The answers to these are needed to complete the overall "picture" of the person in question and their *modus operandi* . The unknowns are as follows:

- Identification of all members of the LLK group
    - Names of group members,
    - Group hierarchy,
    - Their social media accounts,
    - Phone numbers,
    - Debts and specializations (financing, transport, recruitment and so on).
- More precise analysis of digital traces
    - Additional Tom Sawyer profiles on Facebook, Telegram, Viber, Discord or another app.
    - IP addresses of devices and geolocations from which they are logged in.
    - Who are the users who comment and like content. Which group do they belong to: migrants, helpers or potential clients.
- Smuggling logistics

  - Precise movement routes after entering BiH and at which places they cross into the territory of BiH.
  - At what locations do they cross in Višegrad or its surroundings?
  - Where do they stay when they move to Višegrad, is there a gathering place for rest?
  - Where do they stay in Bihać after transport, are there clearly defined locations or are they *ad hoc* ?
- Do they have contact with other groups operating on the territory of Turkey, Bulgaria and Serbia.
- How is payment made – bitcoin, cryptocurrency or hawala system.
- On the basis of which the movement route is determined.

3. Activities undertaken to fulfill the intelligence request

Basic data collection

Investigators begin the operation with identity verification through verification of the provided number (presentation as a potential client) on different SMS services such as WhatsApp, Telegram, Viber and so on. A photo is downloaded from WhatsApp, and its analysis and description is carried out. Attention is paid to social networks in order to determine basic information, after which the operative card from table 2 is completed.

Social network analysis and digital content forensics

The investigator starts searching the profile and posts on it. All posts and content are downloaded with the help of *a data scraper* and categorized into thematic folders - photos, videos, comments, likes, followers and followed. If the posts have geotags, we try to verify their accuracy and provide precise coordinates.

Digital content analysis (photos, video content) is performed using reverse search tools such as Google, Yandex and TinEye. At the same time, extraction of EXIF metadata is performed, [14]such as the location of the device at the time of recording, technical specifications and type of device, format and date/time of recording. If the person possesses technical knowledge and has a high level of operational security, the aforementioned will not provide data, and in that case it begins with describing the content - time of day, season, number of persons and their appearance. The above serves for further profiling and possible connection with other actors in the smuggling network.

Given that the route of movement represents a significant problem, it is necessary to map the movement through the past based on the date of publication,

[14]The Interchangeable Image File Format is a standard that specifies formats for images, audio, and auxiliary tags used by digital cameras (including smartphones).

geolocation and possible time of day and hour when the photo / video was taken. To determine the exact location, Google Earth, Geoguesser or an AI tool that has the ability to geolocate is used. This activity serves to create a pattern of behavior, that is, to determine whether it exists - posts every three days or the schedule of posts is random. There is a possibility that a person publishes content a few days after it was created, which is a direct deception, and the same is determined by comparing the EXIF metadata. Also, through the processing of this data, clearer information is obtained about the use of routes, whereby Google maps can be used for the same and two consecutive locations can be marked on the content, showing a possible route on foot or by means of transport.

In addition to movement routes, contacts made on social networks are also important. Interactions with other accounts indicate possible collaborators and clients. Accounts that like or comment on a post represent essential elements of the network and should be mapped, whereby Maltego or another software is used for visualization.

Cooperation with units in the field

Based on the organization of the service / agency and cooperation with other partners, it is necessary to point out unprotected border crossings, which will help the units in the field to establish monitoring points. Also, the databases are checked and it is determined whether there are any positive findings, that is, whether any of the security agencies registered Tom Sawyer - illegal crossing, minor offense, criminal offense, accommodation in a reception center and so on. With regard to the locality of activities of a person of security interest, it is determined whether there is information about his activities in Višegrad, Sarajevo or Bihać. It is necessary to map the movements of the face in places where it is often seen - cafes and lodgings. Data and information about movement in Sarajevo can be used for special investigative measures and actions such as monitoring and surveillance, and in special cases telecommunications surveillance due to the clear establishment of the connection between the person and the telephone number he uses.

Creating reports and responding to intelligence requests

At the end of the 10-day period, a report must be submitted. The aforementioned analytical report clearly and concisely presents the findings, and points to missing information that requires further operational actions. In view of the significantly large criminal group and potential clients, it can be suggested to continue the OSINT operation, which seeks to obtain data and information about other members and hierarchical settings of the group. It is possible to recommend the operation of HUMINT elements and infiltration into the group itself under the client's legend, as well as the use of SIGINT, that is, telecommunications

surveillance, GPS tracking of devices and active interception of internet traffic and communications.

After the report and response, the end user of the information can request new information or give instructions for performing other actions.

FINAL CONSIDERATIONS

The use of OSINT as an intelligence discipline in the investigation of organized crime groups is becoming more and more prevalent among law enforcement agencies. Although there are divided opinions about the mentioned discipline, its operative use is colossal. OSINT enables efficient, effective and economical collection of data related to organized criminal groups. Also, the importance of reducing the risk of exposure to dangers in the field is great, which is noticeable in HUMINT. However, using this method, there are also challenges such as data fragmentation, misinformation, anomalies, technical and personal limitations, which can significantly complicate or stop the investigation altogether. If ways to overcome limitations are devised, OSINT can significantly improve the work of law enforcement agencies in the fight against OKG, especially if it is combined with other disciplines such as HUMINT, SIGINT. In this way, it is possible to fully monitor criminal groups and individuals who are the subject of the investigation. In order to improve the activities of the fight against organized crime that significantly undermines national security (illegal migration, human trafficking, drug smuggling, proliferation of weapons), it is necessary to invest funds in the creation of tools and the training of investigators. Through training and the development of new tools, it is possible to fully exploit this intelligence discipline. The importance of developing OSINT protocols and their application in the investigation of criminal groups and crimes that significantly threaten national security is significant. The hypothetical example indicated the complexity of the investigation and the various variables that affect the investigation. The use of OSINT and coordination with units in the field and other partner agencies/services enables quick and efficient action, the breaking up of criminal groups and their prosecution. Great importance should be attached to continuous action and monitoring on social networks that are suitable for the dissemination of smuggling or other services provided by organized criminal groups. Further research on this topic should be focused on the development of research methodologies for different criminogenic groups, as well as the actors who carry them out. In this way, the pool of knowledge and resources available to the state in the fight against transnational crime and threats will be enriched.

Bibliography

Baker, R. (2023). *Deep Dive: Exploring the Real-World Value of Open Source Intelligence.* Wiley.

Brunet, J., & Claudon, N. (2015). Military and Big Data Revolution: A Practitioner's Guide to Emerging Technologies. In A. Staniforth, B. Akhgar, PS Bayerl, H. Arabnia, GB Saathoff, & R. Hill, *Application of Big Data for National Security.* Butterworth-Heinemann.

Chen, H., Chiang, RH, & Storey, VC (2012). Business intelligence and analytics: From big data to big impact". *MIS Quarterly* , 1165-1188.

CIA. (2024). *The Intelligence Cycle.* CIA. Retrieved from https://www.cia.gov/spy-kids/static/59d238b4b5f69e0497325e49f0769acf/Briefing-intelligence-cycle.pdf

Clark, RM (2016). *Intelligence Analysis: A Target-Centric Approach Fifth Edition.* CQ Press.

DHS. (2022). *Ethical Frameworks in Open-Source Intelligence.* Public-Private Analytic Exchange Program.

Headquarters, Department of The Army. (2023). *FM-2: Intelligence.* Washington DC.

J. Pastor-Galindo, PN (2020). The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends. *IEEE Access* , 10282-10304.

Kao, D.-Y., Chao, Y.-T., Tsai, F., & Huang, C.-Y. (2018). Digital Evidence Analytics Applied in Cybercrime Investigations. *IEEE Conference on Applications, Information and Network Security* (pp. 111-116). Langkawi, Malaysia: IEEE.

Kaplan, AM, & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons* , 59-68.

Loch, JK (2006). *Handbook for Intelligence Studies.* Routledge.

TAKE IT AWAY. (2011). *US National Intelligence: An Overview.* Washington DC: ODNI.

Quick, D., & Choo, K.-KR (2018). Digital forensic intelligence: Data subsets and Open Source Intelligence (DFINT. *Future Generation Computer Systems* , 558-567.

Reid, E. (2023). 'Trap Life': The psychosocial underpinnings of street crime in inner-city London. *The British Journal of Criminology* , 168–183.

Sampson, F. (2016). Intelligent evidence: Using open source intelligence (OSINT) in criminal proceedings. *Police Journal: Theory, Practice and Principles* , 1-15.

Williams, HJ, & Blum, I. (2018). *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise.* RAND Corp.

ADDITION