Obavještajna analiza i donošenje odluka

Matić, Mateo

Sveučilište u Zagrebu

Fakultet političkih znanosti

Diplomski studij politologije

MATEO MATIĆ

OBAVJEŠTAJNA ANALIZA I DONOŠENJE ODLUKA

DIPLOMSKI RAD

Zagreb, 2024.

Sveučilište u Zagrebu

Fakultet političkih znanosti

Diplomski studij politologije

OBAVJEŠTAJNA ANALIZA I DONOŠENJE ODLUKA

DIPLOMSKI RAD

Mentor: doc. dr. sc. Robert Barić

Student: Mateo Matić

Zagreb

lipanj 2024.

Izjavljujem da sam diplomski rad „**Obavještajna analiza i donošenje odluka**“, koji sam predao na ocjenu mentoru **doc. dr. sc. Robertu Bariću**, napisao samostalno i da je u potpunosti riječ o mojem autorskom radu. Također, izjavljujem da dotični rad nije objavljen ni korišten u svrhe ispunjenja nastavnih obaveza na ovom ili nekom drugom učilištu, te da na temelju njega nisam stekao ECTS bodove.

Nadalje, izjavljujem da sam u radu poštivao etička pravila znanstvenog i akademskog rada, a posebno članke 16-19. Etičkoga kodeksa Sveučilišta u Zagrebu.

Popis slika

Popis kratica

HUMINT	Prikupljanje obavještajnih podataka iz ljudskih izvora
OSINT	Prikupljanje obavještajnih podataka iz otvorenih izvora
SIGINT	Prikupljanje obavještajnih podataka presretanjem signala
GEOINT	Prikupljanje obavj. podataka iz zračnih snimaka, karti i sl.
PDVO	Proces donošenja vojnih odluka
CCIR	Zapovjednikovi zahtjevi za kritičnim informacijama
SOA	Sigurnosno-obavještajna agencija
VSOA	Vojna sigurnosno-obavještajna agencija
EOB	Elektronički bojni poredak
AKH	Analiza konkurentskih hipoteza
COP	Zajednička operativna slika
DARPA	Agencija za napredne borbene istraživačke projekte

Sadržaj

1. Uvod

Tema ovog diplomskog rada je utvrđivanje utjecaja obavještajne analize na proces donošenja odluka. Fokus rada je analiza odnosa između obavještajne analize i donošenja odluka u vojnom kontekstu, što je detaljno prikazano kroz tri razine – taktičku, operativnu te stratešku. Ipak, rad također kroz dva poglavlja obuhvaća i utjecaj razvoja moderne tehnologije na obavještajnu analizu te na utjecaj obavještajne analize u donošenju odluka u kontekstu kreatora politike. Dok jedan dio stručne literature na tu temu ističe važnost i sve veću ulogu obavještajne procjene pri donošenju odluka, posebice onih od strateškog značaja, drugi autori tvrde da obavještajna procjena često završi u sjeni. Takvi autori ističu nepromjenjivu ljudsku prirodu, urođene predrasude, sklonost grupnom razmišljanju i nekolicinu drugih nedostataka kao pogonsku silu koja često nadvladava svaki oblik analitičke prosudbe. Iz ove podijeljenosti proizlazi i teza samog rada – unatoč navedenom skepticizmu, obavještajna analiza postala je neizostavan dio svakog ozbiljnijeg procesa donošenja odluka, te u modernom dobu koje je preplavljeno informacijama iz niza izvora, igra rastuću ulogu pri hvatanju ukoštac s trenutnim sigurnosnim problemima, ali i pri predviđanju onih problema koji tek dolaze.

Iz navedene teze proizlaze i istraživačka pitanja:

1. Koliku ulogu ima obavještajna analiza u procesu donošenja odluka, posebice onih od strateškog značaja?
2. Kako je neprestani razvoj tehnologije utjecao na obavještajnu analizu, ali i obavještajni sektor u cjelini?
3. Koje su sličnosti, a koje razlike između vojnog i političkog sektora kada je u pitanju sinergija obavještajnog i donositelja odluka?
4. Koji su izazovi s kojima se obavještajni analitičari svakodnevno susreću, koji je njihov potencijalni utjecaj na završni obavještajni produkt te mogu li se ti izazovi uopće izbjeći?

Sam pojam obavještajne djelatnosti u širem smislu star je gotovo koliko i prve stalne i organizirane ljudske zajednice. Tako je, primjerice, već i drevni Egipat, par tisućljeća prije Krista imao vrlo razvijen sustav prikupljanja obavještajnih podataka, koristeći se kako sada već ustaljenim metodama poput prikrivenog špijuniranja, tako i prvim (poprilično uspješnim) pokušajima špijuniranja pomoću diplomatskih izaslanika. Špijuniranje se također opsežno koristilo i u Grčkom i Rimskom Carstvu. Špijuniranje nije samo europski fenomen - feudalni Japan često je koristio *shinobije* za prikupljanje obavještajnih podataka, dok su južnoamerički Asteci koristili *pochtecase*, ljude koji su istovremeno služili za špijuniranje, diplomatske misije

te trgovinu, te su imali tadašnji oblik diplomatskog imuniteta. Ipak, najveći razvoj obavještajnog sektora odvio se u 20. stoljeću – gdje su dva svjetska rata i konstantni, paralelni razvoj tehnologije i tehnike rezultirali stvaranjem niza novih metoda i izvora prikupljanja podataka. U okviru ovog diplomskog rada upravo će od najveće koristi, dakako, biti saznanja, tehnike i procedure obavještajnog djelovanja proizašla iz tog dugotrajnog razvoja.

Glede strukture samog rada, glavni dio teksta podijeljen je u pet cjelina. Prva cjelina postavlja temelje samog rada, te razmatra pojedinosti obavještajnog ciklusa kao osnovice obavještajnog djelovanja. Svaki korak ciklusa, od planiranja i usmjeravanja, prikupljanja, procesuiranja i eksploatacije, te naposljetku analize i proizvodnje obavještajnog produkta bit će detaljno opisan, posebice u kontekstu uloge svakog od navedenih koraka u procesu donošenja važnih vojnih i političkih odluka. Sljedeća cjelina bavi se obavještajnim disciplinama kao temeljnoj podjeli obavještajne djelatnosti. Sami obavještajni produkti dijele se s obzirom na njihove izvore, pa ćemo tako za potrebe ovog rada spomenuti prikupljanje podataka iz ljudskih izvora (u nastavku: HUMINT), prikupljanje podataka iz otvorenih izvora (u nastavku: OSINT), prikupljanje podataka iz presretanja i interpretacije signala (u nastavku: SIGINT), te prikupljanje podataka iz satelitskih i zračnih snimaka ili kartografskih podataka (u nastavku: GEOINT). Svaka od ovih obavještajnih disciplina posjeduje određene prednosti i nedostatke kada je riječ o davanju potpore procesu donošenja odluka, o čemu će i biti riječ u poglavlju.

Treća cjelina fokus prebacuje na samu obavještajnu analizu koja je već spomenuta kao dio obavještajnog ciklusa. Upravo je i glavna teza ovog rada značaj utjecaja obavještajne analize u procesu donošenja odluka, tako da se ovo poglavlje ponajviše bavi tehnikama koje se koriste u analizi obavještajnih podataka, te njihov doprinos potpori procesu donošenja odluka. Neke od tehnika koje će biti spomenute su strukturirane analitičke tehnike, testiranje hipoteza i analiza crvenog tima (eng. *red-team analysis*), među ostalim.

Nadalje, sljedeća cjelina bavi se obavještajnom potporom vojnim operacijama, te u užem smislu, utjecaju obavještajne analize i ostalih alata u procesu donošenja vojnih odluka (u nastavku: PDVO) na taktičkoj, operativnoj i strateškoj razini, što uključuje procjenu rizika i prijetnji, operativno planiranje, zaštitu vlastitih snaga, ISTAR sustav i sl. U potpoglavlju gdje će biti analizirana strateška razina, paralelno će se objasniti i sinteza obavještajnog djelovanja i oblikovanja politika. Iako se na prvu možda čini da je navedena uloga u kreiranju politike potpuno zasebna u odnosu na vojne operacije i oružane snage u širem smislu, zapravo se radi o srodnim, a često i identičnim alatima, prednostima i nedostatcima. Samim time se potvrđuje teza pruskog generala i vojnog teoretičara Carla von Clausewitza da je rat jednostavno nastavak političkog odnosa uz dodatak drugih sredstava. Namjerno koristimo frazu 's dodatkom drugih

sredstava' jer je glavna misao da rat sam po sebi ne obustavlja politički odnos niti ga mijenja u nešto sasvim drugo. U suštini, odnos između dvaju ili više država se nastavlja, bez obzira na sredstva koja se koriste - glavne crte duž kojih se odvijaju vojni događaji zapravo su političke, koje se nakon rata nastavljaju i u mir.

Predzadnje poglavlje služi kao kratki osvrt na sve veću uporabu napredne tehnologije u obavještajnom procesu. Konstantni razvoj tehnologije koji je krenuo početkom 20. stoljeća, te ne usporava ni 120 godina kasnije, uzrokovao je rađanje cijelog niza novih obavještajnih disciplina, tehnika i alata. Iako je praktičnih primjera u tom kontekstu bezbroj, poglavlje će se fokusirati na dvije sfere: tzv. analitiku velikih podataka (eng. *big data analytics*), te na uporabu umjetne inteligencije u obavještajnom radu.

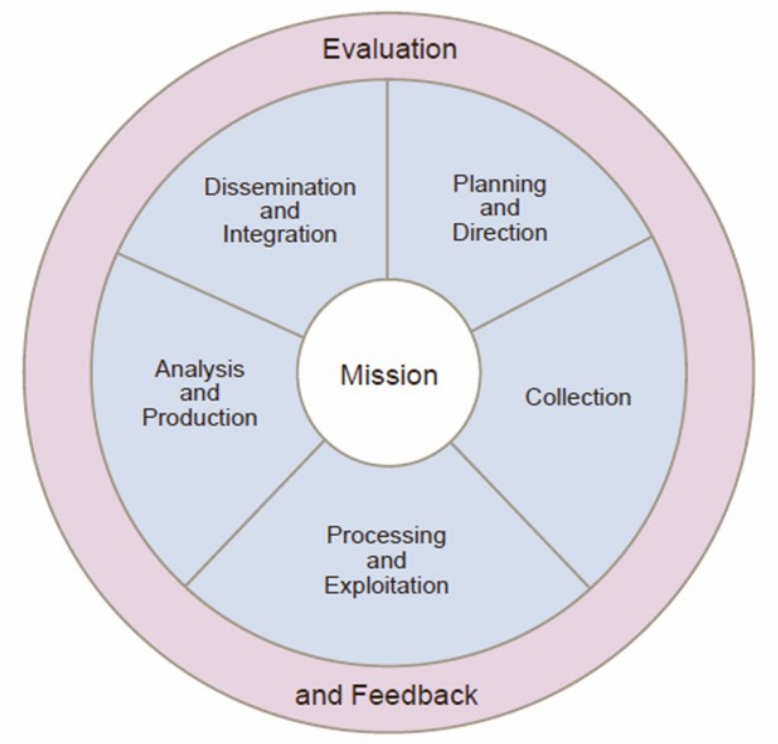
Naposljetku, zadnje poglavlje fokusira se na utjecaj obavještajne analize na donošenje odluka od strane kreatora politike. Iako postoje mnoge sličnosti u prednostima i nedostatcima ovog odnosa s onim u vojnom kontekstu, postoje i ključne razlike koji taj odnos čine još izazovnijim, posebice jer je često riječ o odlukama koji imaju strateški, pa i geostrateški značaj za određenu državu.

Pri kraju samog diplomskog rada nalazi se i zaključak koji objedinjuje sve iznesene argumente u koherentnu završnu misao, te ponovno daje svojevrstan povijesni presjek, uključujući i predviđanja za budućnost odnosa obavještajne analize i procesa donošenja vojnih i političkih odluka. U završnom dijelu rada nalazi se i popis stručne literature koja je korištena pri izradi diplomskog rada. Zbog specifičnosti teme, velika većina literature je na engleskom jeziku, s obzirom da je u Republici Hrvatskoj akademska zajednica koja proučava obavještajne procese, kako domaće tako i globalne, relativno mala u usporedbi s većim zemljama (posebice SAD-om), pa je i brojnost potencijalnih akademskih izvora također ograničena.

2. Obavještajni ciklus

Obavještajni ciklus idealizirani je model koji vizualizira način na koji se obavještajni podaci obrađuju u civilnim i vojnim obavještajnim agencijama te srodnim organizacijama (policiji i sl.). To je zatvorena petlja, sastavljena od koraka koji se neprekidno ponavljaju, koji će, ako se ispune svi preduvjeti, rezultirati gotovim obavještajnim produktom. Značaj obavještajnog ciklusa najviše se očituje u donošenju strateških odluka. Na strateškoj razini, najveći izazov s kojima se donositelji odluka suočavaju je nedostatak vremena za detaljnu prosudbu određenog problema, posebice kada se radi o velikim silama čija vanjska politika ima snažan geopolitički utjecaj, poput SAD-a. Obavještajni analitičari u takvom slučaju imaju jako malo vremena da

ključnim donositeljima odluka na stol donesu obavještajne prosudbe od kojih se, naravno, očekuje da budu što preciznije i točnije moguće. Obavještajni ciklus u tom kontekstu upravo osigurava neprestano, cikličko obavještajno djelovanje koje je preduvjet za stvaranje obavještajnog produkta koji će biti od koristi donositelju odluka u uvjetima s vrlo kratkim vremenskim rokovima za reakciju (Hedley, 2007, 211-214).



Slika 1. Faze obavještajnog ciklusa.
Izvor: https://web.archive.org/web/20160613010839/http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf (Pristupljeno 30.12.2023.)

Gledajući sliku 1, možemo uočiti 6 faza obavještajnog ciklusa. Sam broj faza, kao i njihovi nazivi, nisu isti u svim oblicima stručne literature. Za potrebe ovog rada, koristit ćemo verziju koja se nalazi u *Joint Publication 2-0 – Joint Intelligence* (u nastavku: JP 2-0) priručniku Oružanih snaga SAD-a.

Kao što smo nagovijestili u samom uvodu, obavještajni ciklus, kako u cjelini, tako i u svojim fazama, usko je vezan za donošenje odluka i one koje takve odluke donose. Tako je prva faza obavještajnog ciklusa je planiranje i usmjeravanje (na slici: *Planning and Direction*), tj. izdavanje zahtjeva od strane donositelja odluka. Donositelji odluka, koji su zapravo različiti akteri na različitim razinama, obavještajnoj agenciji/sustavu predstavljaju svoje zahtjeve koji služe kao potpora u donošenju odluka, tj. ispunjenju određenih ciljeva. Primjerice, gledano s najveće moguće - nacionalne razine – u vladi Sjedinjenih Država obavještajne zahtjeve ili

prioritete može izdati Bijela kuća, dok Kongres nadzire djelovanje obavještajnih službi. S druge strane, gledajući najmanju moguću razinu u ovom kontekstu - taktičku razinu neke vojne postrojbe - zapovjednik postrojbe prije i tijekom planiranja vojne operacije izdaje zahtjeve za ključnim informacijama (eng. *Commander's Critical Information Request* – u daljnjem tekstu: *CCIR*) koje su od velikog značaja za pravilno i pravovremeno donošenje odluka (JP 2-0, 2013, I-7).

Na nacionalnoj razini, takvi zahtjevi često su dugotrajne prirode, tj. ponavljaju se, često na godišnjoj bazi. Najbolji primjer je godišnje izvješće Sigurnosno-obavještajne agencije (u nastavku: SOA) Republike Hrvatske. Rad SOA-e te srodne agencije koja se bavi vojno-obrambenim dijelom nacionalne sigurnosti, Vojno-sigurnosne obavještajne agencije (u nastavku: VSOA), nadgledaju i usmjeravaju Predsjednik i Vlada Republike Hrvatske. Zahtjevi na ovoj razini često su vrlo slični svake godine, te sadržavaju generalne smjernice poput pronalaženja aktivnih i pasivnih prijetnji nacionalnoj sigurnosti države od strane drugih država, terorističkih organizacija ili sl., procjeni statusa ugroze i rizika kako same države, tako i u kontekstu saveznih organizacija (NATO), itd. (SOA, 2022, 4).

U vojnom kontekstu, te kroz tri razine – stratešku, operativnu i taktičku, obavještajni zahtjevi od strane zapovjednika ovise o razini o kojoj se radi te o samoj operaciji. Ipak, to često uključuje razmještaj i brojčanu snagu protivnika, informacije o naoružanju i tehnici koje neprijatelj posjeduje, analizu zemljišta, meteorološke uvjete i sl. O sintezi obavještajnog djelovanja/analize te vojnih operacija podrobnije ćemo u jednom od narednih poglavlja.

Sljedeći korak u obavještajnom ciklusu je prikupljanje (na slici: *Collection*). Kao odgovor na zahtjeve, obavještajne službe razvijaju plan prikupljanja obavještajnih podataka primjenom dostupnih izvora i metoda, ali i traženjem obavještajnih podataka od drugih agencija, bile one u istoj državi ili pak u savezničkoj[1]. U trećem poglavlju će upravo biti riječ o obavještajnim disciplinama, tj. izvorima podataka. Naravno, evaluacija i povratno izvještavanje od strane donositelja odluka, upravo kako je prikazano i na slici 1, prožeto je kroz sve korake obavještajnog ciklusa, te ne predstavlja zaseban, konačni korak. Tako donositelji odluka direktno i indirektno upravljaju i prikupljanjem podataka, te mogu favorizirati podatke dobivene iz ljudskih izvora, ili pak one dobivene presretanjem elektronskih signala itd. Često je za potpunu obavještajnu sliku, i samim time, donošenje ispravne odluke, potrebno kombinirati podatke dobivene iz različitih izvora (Lowenthal, 2019, 249-251).

Treći korak u obavještajnom ciklusu je procesuiranje i iskorištavanje (na slici:

[1] Ponajbolji primjer obavještajne suradnje između više država je savez *Five Eyes*, koji uključuje SAD, Ujedinjeno Kraljevstvo, Kanadu, Australiju te Novi Zeland.

Processing and Exploitation). Nakon što se plan prikupljanja izvrši te se podaci prikupe iz svih planiranih izvora, oni se obrađuju za iskorištavanje, tj. pripremaju se za analizu. Neke od aktivnosti koje spadaju u ovu fazu su prvotna klasifikacija podataka, zatim dešifriranje (po potrebi) ili pak prevođenje podatka s izvornog jezika na materinji, pretvaranje podataka i informacija iz izvornog oblika u onaj kojeg je lakše koristiti, pogotovo u kontekstu softverskih programa i sl. Korištenjem navedenih procesa od sirovog podatka (eng. *data*) dobivamo informaciju, svojevrstan međukorak između sirovog podatka te gotovog obavještajnog produkta. Valja napomenuti kako se već u ovom koraku uključuju obavještajni analitičari – stručne, visoko specijalizirane osobe koje imaju značajnu ulogu u cijelom procesu, jer upravo od njih i njihovog rada ovisi kvaliteta i uporabljivost konačnog produkta. Samim time, u ovom koraku se isključuju donositelji odluka, kako zbog njihovog nedostatka stručnosti, tako i zbog očuvanja objektivnosti podataka, tako da donositelji odluka ne mogu utjecati na filtraciju i obradu podataka kako bi dobili ono što možda žele čuti ili vidjeti na temelju ranijih pretpostavki (Lowenthal, 2019, 255-256).

Vezujući se na prethodni odlomak, zbog objektivnije, ali i puno brže obrade sirovih podataka, u svim razvijenim državama koriste se softverski alati. U tom kontekstu možemo govoriti o alatima kao što su rudarenje podataka (eng. *data mining*) te uporaba umjetne inteligencije (u nastavku: AI), među ostalim. Mišljenje većine stručnjaka iz tog područja je da je AI sve sposobniji te sa sve većom točnošću i pouzdanošću može obraditi enorman broj podataka te iz njih izvući skrivene indikacije, uzorke i sl. (Mitchell i dr., 2020). O navedenoj temi više ćemo govoriti u posljednjem poglavlju rada.

Četvrti korak je analiza i produkcija, tj. proizvodnja gotovog obavještajnog produkta (na slici: *Analysis and Production*). Ovaj korak je usko vezan s prethodnim te ga provode iste osobe. U procesu analize koristi se nekolicina analitičkih i operativnih postupaka procjene istinitosti koja se provodi na osnovu dostupnih informacija dobivenih u prethodnom koraku. Slikovito prikazano, zapravo se obavlja slaganje svojevrsnog mozaika iz niza navedenih obavještajnih informacija kako bi se proizveo gotov obavještajni proizvod, koji tek u tom potpunom i konciznom obliku može biti potpora donositelju odluke (Lowenthal, 2019). S obzirom na važnost ovog koraka i obavještajne analize općenito za ovaj rad, ova tema bit će u detalje razrađena u trećem poglavlju.

Peti korak je distribucija i integracija gotovog obavještajnog proizvoda (na slici: *Dissemination and Integration*). U ovom se koraku fokus ponovno vraća na donositelje odluka. Važno je napomenuti da obavještajna služba/agencija koja je stvorila proizvod u pravilu izbjegava imenovati izvore informacija i korištene metode, što dodatno štiti objektivnost

sustava i anonimnost obavještajnih djelatnika. Ovisno o osjetljivosti obavještajnog produkta, njegova se distribucija vrši na razne oblike. Manje osjetljive informacije mogu se dijeliti i elektronskim putem uz uporabu zaštitnih mjera poput kriptiranja, zaštićenih telefonskih linija i sl., dok se visokorizične i osjetljive informacije dijele usmenim brifiranjem na sigurnim lokacijama (Lowenthal, 2019).

Zadnji korak u obavještajnom ciklusu, kako smo već napomenuli, paralelno se odrađuje tijekom svih ostalih koraka, ali je njegova uloga najopipljivija na kraju jednog ciklusa – što ujedno predstavlja i početak novog. Taj korak je evaluacija i povratna informacija. Ovaj korak je od najveće koristi upravo obavještajnom osoblju koje je i proizvelo gotov obavještajni produkt, jer dobra povratna informacija naglašava prednosti i mane produkta koji je distribuiran donositeljima odluka, što znači da se naredni ciklusi mogu optimizirati tako da bolje ispune određena očekivanja od krajnjih korisnika – donositelja odluka. Ako izuzmemo sa strane korisnost ili nekorisnost obavještajnog proizvoda, povratna informacija svakako bi trebala dati odgovore na ono što se u stručnoj literaturi naziva ključnim obavještajnim pitanjima (eng. *Key Intelligence Questions*), koja se bave upotrebljivošću i pravovremenošću[2] produkta, činjenicama koje su korištene pri njegovoj izradi te način korištenja, te ispunjenje očekivanja od strane donositelja odluka – ako očekivanja nisu ispunjena, treba dati argumentirane razloge zašto je to tako. Naposljetku, povratna informacija daje i odgovor na pitanje: koji je sljedeći korak? – tj. na što se obavještajne službe trebaju fokusirati u sljedećem obavještajnom ciklusu (Lowenthal, 2019).

Ovo poglavlje daje nam solidne temelje za daljnju analizu povezanosti obavještajnog sustava i donositelja odluka. Naglasak je, kao što smo mogli uvidjeti, na neprekidnost procesa obavještajnog ciklusa. Kao konačnu misao ovog poglavlja valja napomenuti da je u moderno doba obavještajni ciklus nemoguće zamisliti kao linearnu petlju koja se odvija u vakuumu. Značajno obilježje 21. stoljeća je konstantno bombardiranje ogromnom količinom informacija, pa i samim time raste broj stručnjaka koji favoriziraju imenicu „mreža“ umjesto „ciklus“, jer sakupljači podataka rade paralelno s analitičarima, a potrošači koriste i konzumiraju više informacija nego ikad. Postavlja se pitanje koliko je pojam obavještajnog ciklusa relevantan i što bi ga u budućnosti moglo zamijeniti (Nolan, 2015).

[2] Pravovremenost je ključan pojam u obavještajnom svijetu. Obavještajni produkt gotovo svake sekunde gubi na relevantnosti i točnosti - od iznimne je važnosti da on bude dostavljen donositeljima odluka u što kraćem roku.

3. Obavještajne discipline

Obavještajne discipline predstavljaju glavnu podjelu u kontekstu izvora prikupljanja obavještajnih podataka. Nagli razvoj tehnologije kroz 20. i 21. stoljeće rezultirao je stvaranjem novih potencijalnih izvora podataka, a samim time i novim metodama njihovog otvorenog i prikrivenog prikupljanja. Tako se HUMINT-u, koji u jednom ili drugom obliku postoji već tisućama godina, pridružio i SIGINT, OSINT, MASINT, CYBINT, GEOINT itd. Za potrebe ovog rada detaljnije ćemo obraditi 4 glavne discipline[3]: HUMINT, OSINT, SIGINT te GEOINT.

3.1. HUMINT

Prikupljanje podataka iz ljudskih izvora, skraćeno HUMINT (skraćenica potječe od eng. naziva - Human Intelligence) fokusira se na međuljudski kontakt, te se po tome razlikuje od tehničkih sredstava prikupljanja obavještajnih podataka kao što su presretanje signala, operacije u kibernetičkom prostoru i sl. HUMINT se može provoditi na razne načine – tradicionalni oblici HUMINT-a uključuju špijunažu, izviđanje (više vrsta i oblika), ispitivanje i razgovore sa svjedocima i općenito osobama koje imaju pristup određenim informacijama. Kao što smo već napomenuli, HUMINT u jednom ili drugom obliku, posebice u kontekstu špijuniranja, postoji već tisućama godina. Sama riječ „špijuniranje“ često se uzima kao sinonim za obavještajno djelovanje općenito, a obavještajne djelatnike se izjednačava sa špijunima (Lowenthal, 2019).

Potencijalni izvori informacija koji spadaju pod HUMINT su mnogobrojni. Na međudržavnoj razini, tu ubrajamo diplomatske radnje i izvještavanje od strane akreditiranih diplomata, konzulata, vojnih atašea i sl. Javna je tajna da države koriste svoje diplomatsko osoblje i infrastrukturu za špijuniranje drugih država. Jedan od najpoznatijih incidenata u tom kontekstu dogodio se nakon što je Edward Snowden, bivši suradnik američke Agencije za nacionalnu sigurnost (u nastavku: NSA), 2013. godine u javnost iznio nevjerojatnu količinu visoko klasificiranih američkih obavještajnih podataka te procedura obavještajnih agencija. Sjedinjene Države gotovo su se preko noći našle u vrlo nezgodnoj poziciji. Osim što su dotični podaci govorili da je NSA, uz još nekolicinu agencija, imala pristup praktički svim mobilnim i drugim elektroničkim uređajima stanovnika SAD-a te provodila opsežno špijuniranje nad

[3] Valja napomenuti kako se MASINT i CYBINT također smatraju glavnim disciplinama, no izostavljeni su zbog nužno ograničenog opsega ovog rada.

vlastitim građanima, SAD su optužene i za praćenje komunikacija drugih zemalja, među kojima su se našli i jaki saveznici. Posebnu medijsku pozornost je pridobio slučaj Savezne Republike Njemačke, gdje se ispostavilo da je NSA prikupljala podatke o komunikaciji milijuna njemačkih građana, dužnosnika na najvišim razinama vlasti u Berlinu, te su špijunirali i samu kancelarku Angelu Merkel. Ova su otkrića uzdrmala američko-njemačke odnose (reuters.com, 2021).

Na nižim razinama, a unutar civilnih obavještajnih agencija, HUMINT se provodi koristeći specijalizirano osoblje koje vrši prikriveni nadzor, dogovara i vrši tajne sastanke s doušnicima, provodi ispitivanja svjedoka i sl. Unutar oružanih snaga neke države HUMINT se može provoditi na taktičkoj, operativnoj i strateškoj vojnoj razini. Obično na višim razinama HUMINT provodi zasebna obavještajna agencija, tj. jedan od njenih podsektora (u Republici Hrvatskoj bi to bila VSOA) za stvari od posebnog značaja za oružane snage u cjelini, dok se za niže razine, ovisno o situaciji, koristi i vojno i civilno osoblje koje je obučeno za prikupljanje podataka iz ljudskih izvora općenito, ili specijalizirano za određenu metodu/tehniku prikupljanja. Ogledan primjer HUMINT-a na taktičkoj razini je komunikacija s autohtonim stanovništvom tijekom provođenja operacija potpore miru. U tu svrhu, svaki vojnik je svojevrstan „senzor“ koji konstantno prikuplja informacije iz okoline, što uključuje i održavanje dobrih odnosa s domaćim stanovništvom. Stjecanje njihove blagonaklonosti uvijek je pri vrhu prioriteta u svakoj mirovnoj operaciji. U ovu kategoriju, među ostalom, također spada ispitivanje ratnih zarobljenika, te razne vrste patrola i izviđanja - od konvencionalnog, kojeg mogu provoditi regularne (primjerice pješačke) postrojbe do specijalnog[4] kojeg provode visoko specijalizirane postrojbe (Steele, 2010).

Kada govorimo o prednostima i manama HUMINT-a u odnosu s donositeljima odluka, jedna od jedinstvenih prednosti HUMINT-a je njegova sposobnost davanja odgovora na kompleksna pitanja, tj. probleme, koji mogu biti puni nijansi i dvosmislenosti. Steele (2010, 41) ističe: „Dok se tehničkim disciplinama prikupljanja mora reći "što, kada i gdje", u slučaju HUMINT-a moramo ispravno shvatiti samo tri stvari: 1. Razumjeti pitanje, 2. Znati tko zna odgovor na to pitanje (ljudski izvor će otkriti potrebne nijanse), 3. Povezati izvor s klijentom (krajnjim korisnikom) ili ispitati izvor.“ Prema istom autoru, glavne prepreke uspjehu HUMINT-a su upravo krajnji korisnici, zastarjele sigurnosne smjernice i neadekvatna pravna potpora njegovom korištenju. Gledano iz financijskog aspekta, HUMINT košta manje, zahtijeva manje vremena i mnogo je responsivniji od tehničkog prikupljanja, djelomično zato

[4] U Oružanim snagama Republike Hrvatske aktivnosti specijalnog (dubinskog) izviđanja provode dubinski izvidnici koji su u sastavu Obavještajne pukovnije.

što je s HUMINT-om obrada ugrađena duž cijelog ljudskog lanca, od izvora do sakupljača, preko analitičara do potrošača (Steele, 2010).

S druge strane, potencijalne mane HUMINT-a fokusiraju se upravo na esencijalan ljudski faktor koji je u samoj srži discipline. Ljudska prosudba, iako je za razliku od tehničkih i softverskih alata sposobna razaznati fine detalje i kontekst u hrpi informacija, također može biti narušena neobjektivnošću. Zbog neizbježne ljudske prirode ponekad je nemoguće izbjeći utjecaj osobnih uvjerenja te pribjegavanju porocima, čak i kod najprofesionalnijih obavještajnih djelatnika. Također, HUMINT agenti, s obzirom da su najčešće povezivani s opipljivim, terenskim poslom, najpodložniji su otkrivanju od strane protuobavještajnih djelatnika države ili organizacije koju špijuniraju, pa tako mogu postati dvostruki agenti, što može predstavljati ozbiljnu sigurnosnu ugrozu za državu iz koje agent potječe (Steele, 2010).

3.2. OSINT

Kada govorimo o prikupljanju podataka iz otvorenih izvora – OSINT, prilikom definiranja samog pojma stručnjaci često nailaze na probleme. Ako bi uzeli preširoku definiciju, u OSINT bi mogli uvrstiti i banalne stvari poput čitanja stranih novina od strane vladara, diplomata i drugih državnih službenika kako bi bili u tijeku zbivanja u svijetu. Iz ovoga proizlazi da ležerno promatranje svijeta – što svi stalno činimo – treba razlikovati od svrhovito organiziranog pristupa prikupljanju i iskorištavanju informacija što bismo očekivali u obavještajnom kontekstu. Stoga ćemo za potrebe ovog rada OSINT definirati kao metodično prikupljanje i iskorištavanje informacija iz javno dostupnih izvora radi ispunjavanja obavještajnih zahtjeva. Shodno tome, prikupljanje i iskorištavanje treba biti metodično prije nego što se nešto kvalificira kao OSINT, drugim riječima, ponavljajući i strukturirani (birokratski) napori trebaju biti vidljivi. Također, treba razlikovati prikupljanje OSINT-a od znanstvenog istraživanja. Iako se koriste slične, ponekad i iste metode, OSINT se razlikuje od istraživanja prvenstveno po tome što je namijenjen za stvaranje prilagođenog znanja koje pomaže donositeljima odluka (Block, 2023).

Iako se u stručnoj literaturi na temu može naći više vrsta podjela, OSINT izvori generalno se dijele u šest glavnih kategorija. Prva kategorija su javno dostupni mediji, što uključuje fizičke novine i časopise, televizijske te radio prijenose. Druga kategorija, koja je nedvojbeno preuzela primat u posljednjih nekoliko desetljeća, jest Internet. U ovu kategoriju uključeno je mnoštvo sadržaja – od najvećeg značaja su društvene mreže, blogovi i forumi. Sljedeća kategorija su javno dostupni državni podatci, što također uključuje širok spektar

pojmova kao što su medijske konferencije, izvještaji, proračuni, saslušanja i vijećanja, javni govori i dr. Četvrta kategorija uključuje akademske i profesionalne publikacije - od akademskih članaka, časopisa i konferencija do disertacija i sl. Peta kategorija objedinjuje sav materijal komercijalne prirode – baze podataka, industrijske i financijske procjene i izračune itd. Zadnja kategorija se bavi tzv. „sivim tiskom“, u koju su svrstani izvori informacija poput patenata, poslovnih dokumenata, tehničkih izvješća, biltena i sl. (Block, 2023).

Eksponencijalnim rastom Interneta od njegovog osnutka 1983. godine paralelno je rasla i uporaba OSINT-a u obavještajnim zajednicama diljem svijeta. Prema svim relevantnim izvorima, minimalno tri četvrtine podataka od ukupnog broja koju prosječna NATO članica „proguta“ tijekom jedne godine se klasificira kao OSINT. Citirajući umirovljenog vrhovnog zapovjednika američkog CENTCOM-a, generala Zinnija, Steele (2010, 15) govori o ulozi OSINT-a kao glavnom izvoru obavještajnih produkata koji su mu bili servirani dok je obnašao navedenu dužnost:“ 80 posto onoga što sam trebao znati kao vrhovni zapovjednik Središnjeg zapovjedništva SAD-a dobio sam iz otvorenih izvora. U otvorenim izvorima bih mogao pronaći još 16 posto, ako bi znao što treba tražiti. Na kraju svega, klasificirani obavještajni podaci iz drugih izvora činili su, u najboljem slučaju, samo 4 posto mog zapovjednog znanja.“

3.3. SIGINT

SIGINT podrazumijeva prikupljanje obavještajnih podataka presretanjem signala, bilo da se radi o komunikaciji između ljudi (eng. *communications intelligence* - COMINT) ili iz elektroničkih signala koji se ne koriste izravno u komunikaciji (eng. *electronic intelligence* - ELINT). Povijest SIGINT-a kao obavještajne discipline, iako mnogostruko kraća od povijesti HUMINT-a, daje odličan uvid u brzinu razvoja tehnologije i znanosti. Dvadeseto stoljeće obilježila su dva svjetska rata, koja su još uvijek do danas dva najveća sukoba u ljudskoj povijesti, ali je stoljeće obilježila i činjenica da je upravo vojni sektor imao primat nad korištenjem i razvojem najnovije tehnologije. U tom kontekstu posebice treba istaknuti 1. svjetski rat, gdje je SIGINT doživio procvat. Britanci su u tom periodu zasigurno imali značajnu prednost u korištenju SIGINT-a. Nakon objave rata Velika Britanija je presjekla sve njemačke podmorske kabele, što je prisililo Nijemce da za komunikaciju koriste ili radio, čiji su promet Britanci već tada mogli presresti i prisluškivati, ili pak telegrafsku liniju koja se spajala preko britanske mreže i također se mogla prisluškivati. Nastala je i specijalizirana služba za presretanje poznata kao „Y služba“ , koja se vrlo brzo razvila do te mjere da su Britanci mogli presresti gotovo sve službene njemačke poruke. Nažalost, cijena svega navedenog često je bila

izražena u ljudskim životima (Winkler, 2009).

S obzirom da su povjerljive i osjetljive informacije obično šifrirane, SIGINT također obuhvaća alate, tehnike i procedure kao što su kripto-analiza - za dešifriranje poruka, analiza prometa – koja proučava tko kome signalizira i u kojoj količini, presretanje glasovne i tekstualne komunikacije, stvaranje tzv. elektroničkog bojnog poretka (eng. *electronic order of battle* – EOB). EOB detaljno opisuje sve poznate kombinacije odašiljača (izvora signala) i komunikacijskih platformi u određenom području odgovornosti, kako za prijateljske, tako i za protivničke podatke. Na današnjem modernom, asimetričnom bojištu, EOB je jedan od najsloženijih procesa pri stvaranju kompletne slike bojišnice (Horne, 2002).

U kontekstu stvaranja obavještajnih podataka koji olakšavaju donošenje odluka, nedvojbeno je da je SIGINT postao nezamjenjiv od svog razvoja početkom 20. stoljeća. Presretanje signala nemoguće je nadomjestiti ili zamijeniti nekom drugom obavještajnom disciplinom. Samim time, SIGINT je od iznimnog značaja za donošenje odluka, posebice kroz sve tri vojne razine – taktičku, operativnu i stratešku. S druge strane, uporaba SIGINT-a u civilnom sektoru često nailazi na moralne i pravne dvojbe i probleme. Tako je već spomenuti zviždač, Edward Snowden, iznošenjem američkih klasificiranih obavještajnih podataka u javnost izazvao lavinu reakcija na špijuniranje gotovo cijelog stanovništva i stranih zemalja od strane američkih obavještajnih službi.

Povezano s tim, donositelji odluka često se vode tzv. matricom rizika i nagrade. Ako pogledamo sliku 2., donositelji odluka zasigurno izbjegavaju (ili bi trebali izbjegavati) radnje koje su visokog rizika, a zauzvrat ne predstavljaju veliku potencijalnu nagradu (gornji lijevi kvadrant) – u ovom kontekstu to bi bilo izravno prisluškivanje visokih dužnosnika strane države, kao što je bio slučaj s američkim prisluškivanjem njemačke kancelarke Angele Merkel. Otkrivanje takvog djelovanja u prijateljskoj državi moglo bi ozbiljno narušiti odnose dvaju država, a u neprijateljskoj državi bi moglo rezultirati neželjenom odmazdom poput terorističkih napada i sl. Visoki dužnosnici vrlo često prolaze kroz rigorozne sigurnosne provjere te su educirani u polju informacijske i komunikacijske sigurnosti te protuobavještajnog djelovanja, što ograničava potencijalno izvlačenje korisnih informacija od njih samih (reuters.com, 2021).

S druge strane, radnje niskog rizika, ali i niske potencijalne nagrade (vidi sliku 2. - donji lijevi kvadrant) u kontekstu SIGINT-a u nevojne svrhe uključuje operacije presretanja signala i elektroničkog špijuniranja širokih razmjera, poput špijuniranja stanovnika SAD-a od strane NSA-a. Ovakve radnje, ako se otkriju, od strane obavještajnih agencija koje su provodile špijuniranje uglavnom se fokusiraju na jedan argument – da je to sve u interesu sigurnosti građana, te da se dobronamjerni građanin ne treba pribojavati takvih radnji, s obzirom da ne

skriva ništa ilegalno. Međutim, paralelno se postavlja pitanje – je li to zaista opravdan, ispravan način?

Slika 2. Matrica rizika i nagrada.

Izvor: https://www.limegreenconsulting.co.uk/uploads/2/8/9/8/28986239/image-36-risk-reward-matrix_orig.jpg (Pristupljeno 06.01.2024.)

3.4. GEOINT

Sam pojam GEOINT-a predstavlja prikupljanje obavještajnih podataka iz niza geoprostornih vještina i disciplina – što, među ostalima, uključuje fotogrametriju[5], kartografiju, analizu slika, daljinsko očitavanje i analizu terena. Prvotno se smatralo da je GEOINT samo novi izraz koji se koristi za objedinjavanje širokog raspona gore navedenih vještina i disciplina. Međutim, ubrzo je prihvaćeno mišljenje da je GEOINT više od samog zbroja ovih dijelova. Prostorno razmišljanje koje je srž GEOINT-a može sintetizirati bilo koje podatke koji se mogu konceptualizirati u geografskom prostornom kontekstu. Također, GEOINT može biti potpuno neovisan o satelitskim ili zračnim slikama, pa se samim time može jasno razlikovati od IMINT-a (USGIF, 2016).

Kontekst prostora od iznimne je važnosti pri donošenju odluka. To se posebice očituje u PDVO, gdje zapovjednici od najmanjih do najvećih razina moraju imati kontinuiran uvid u kvalitetne geoprostorne informacije. Te informacije trebale bi odgovarati na neka ključna pitanja (NGA, 2016, 6): „Gdje se ja nalazim? Gdje se nalaze moji suborci? Gdje se nalaze protivničke snage? Kad bi mogli očekivati njihov pokret? Gdje se nalaze civili? Koje se prepreke (prirodne i umjetne) nalaze u području operacije, i kako ih zaobići? Koji je utjecaj

[5] Fotogrametrija je znanstvena disciplina koja se bavi dobivanjem pouzdanih informacija o fizičkim objektima i okolišu kroz proces snimanja, mjerenja i tumačenja fotografskih slika, uzoraka slika elektromagnetskog zračenja i drugih pojava (ASPRS, 2024).

svega navedenog na moje snage i provođenje operacije?“

S druge strane, GEOINT je od velikog značaja i u nevojnom sektoru, ali i dalje u kontekstu nacionalne sigurnosti i strategije iste. Primjera radi, GEOINT može biti esencijalan dio sustava ranog upozoravanja na potencijalne prijetnje nacionalnoj sigurnosti. Praćenjem promjena u fizičkom okruženju, poput kretanja postrojbi ili razvoja infrastrukture, donositelji odluka mogu identificirati potencijalne vojne i nevojne prijetnje prije nego što se one manifestiraju. Nadalje, GEOINT uvelike podiže razinu situacijske svjesnosti s obzirom da pruža geoprostorne informacije u stvarnom vremenu. Takve su informacije od vitalnog značaja tijekom kriza i izvanrednih situacija (ekološko-tehnološke katastrofe, poplave, požari i sl.), jer pomažu donositeljima politika da brzo reagiraju i ublaže potencijalnu štetu. Naposljetku, GEOINT-om se služe i policijske snage za poboljšanje granične sigurnosti pružanjem ključnih informacija o graničnim prijelazima, otprije poznatim i novonastalim krijumčarskim rutama i potencijalnim prijetnjama, što u produžetku pomaže i donositeljima politika da razviju strategije za osiguranje granica i sprječavanje nezakonitih aktivnosti (USGIF, 2016).

4. Značaj obavještajne analize u procesu donošenja odluka

Ne postoji segment obavještajnog djelovanja koji je važniji od pravilnog odnosa između same obavještajne zajednice i ljudi koji koriste njezine proizvode. Ovaj odnos, za koji bi se očekivalo da će se uspostaviti automatski, uspostavlja se tek kao rezultat značajnog i svjesnog truda. Obavještajni analitičari zaslužni su za veći dio tog truda. Svrha analize obavještajnih podataka je otkriti određenom donositelju odluka temeljni značaj odabranih informacija. Analitičari bi u svom radu trebali započeti s potvrđenim činjenicama, primijeniti stručno znanje kako bi proizveli uvjerljive, ali manje sigurne zaključke (nalaze), pa čak i prognozirati, kada je prognoza odgovarajuće kvalificirana. Međutim, analitičari se ne bi trebali baviti proricanjem sudbine koje nema temelja u činjenicama.[6]

Ovo poglavlje dat će uvid u kompleksnost obavještajne analize i njezinih raznih dimenzija, a samim time paralelno objasniti njen odnos s donositeljima odluka. Prvo potpoglavlje pobliže opisuje neke od metoda rasuđivanja kojima se analitičari koriste pri obavještajnoj analizi, što predstavlja svojevrsni temelj cijelog procesa. Nadalje, drugo potpoglavlje bavi se metodama analize. U tom kontekstu spomenut ćemo analizu konkurentskih hipoteza, „linchpin“ analizu, te analizu crvenog tima kao jedne od najčešće korištenih metoda analiza.

[6] Ovaj tok misli se u stručnoj literaturi veže i za mnemotehniku „*Four F's Minus One*“ – od eng. *Fact – Finding – Forecast – Fortune*. Obavještajni analitičar može tijekom analize ići do 3. razine – *Forecast*, ali ne i preko nje.

4.1. Vrste rasuđivanja

Objektivnost je 'zvijezda vodilja' koja bi trebala prožimati kompletan proces obavještajne analize. Da bi objektivno proizveo obavještajne podatke, analitičar mora primijeniti proces prilagođen prirodi problema. Stručna literatura razlikuje približno desetak različitih vrsta rasuđivanja, a za potrebe ovog rada obradit ćemo četiri: induktivno rasuđivanje, deduktivno rasuđivanje, abduktivno rasuđivanje te istreniranu intuiciju.

Proces indukcije podrazumijeva, u svojoj srži, razotkrivanje raznih veza koje povezuju proučavane pojave, tj. fenomene. Dok indukcija obično nije na potpuno racionalnoj razini, i dalje se suptilno razlikuje od intuicije po tome što obično postoji obrazac koji indukcija prepoznaje, a taj se obrazac može primijeniti i na druge situacije. Samim time, ljudska sposobnost prepoznavanja uzoraka u naizgled nasumičnom skupu događaja jedna je od ključnih vrijednosti indukcije, te je zbog toga u suprotnosti s dedukcijom, s obzirom da se ne kreće od već dokazane opće teorije (Krizan, 1999).

U praksi, primjer induktivnog razmišljanja bi primjerice bila provedba intervjua s vojnicima koji su došli iz područja operacije gdje su konstantnu prijetnju predstavljale improvizirane eksplozivne naprave (u nastavku: IEN). Vojnici tijekom takvog intervjua (ili sigurnosnog debrifinga) spomenu da je tijekom operacije često svježe iskopano tlo upućivalo na novopostavljenu IEN, ili je pak civilno stanovništvo bilo osobito loše raspoloženo dan prije nego što su naišli na IEN. Uzimajući u obzir niz ovakvih naočigled nepovezanih specifičnosti, obavještajni djelatnici kroz proces indukcije mogu sastaviti *modus operandi* protivnika te u sljedećim obavještajnim pripremama vojnog osoblja uključiti te informacije kako bi povećali sigurnost prijateljskih snaga.

Na suprotnoj strani od indukcije imamo dedukciju - logičan proces kojim se zaključak donosi na temelju niza pretpostavki za koje se pretpostavlja njihova istinitost. Tu već možemo uočiti suprotnost indukciji s obzirom da počinje od općeg te ide prema specifičnoj situaciji. Mnoga znanstvena područja se temelje na deduktivnom rasuđivanju, od kojih možemo istaknuti matematiku i logiku. Zaključci dobiveni dedukcijom, ako su utemeljeni u istinitim pretpostavkama, ne mogu biti opovrgnuti. Tu se upravo može prepoznati i glavna opasnost dedukcije – osjetljiva je na kognitivne pristranosti. Obavještajni analitičari prilikom korištenja dedukcije trebaju promatrati i teže dostupne varijable – primjerice, osobnosti određenog zapovjednika - kako bi saznali je li obrazac kojeg smo prepoznali doista opća doktrina ili vrijedi samo u kontekstu određene osobe ili grupe (Krizan, 1999).

Praktični primjer dedukcije možemo pronaći u bilo kakvom planiranju gotovo bilo čega. Primjera radi, prilikom vremenskog planiranja operacije, zapovjednik mora svo raspoloživo vrijeme podijeliti na najsvrhovitiji mogući način. Ako od višeg zapovjedništva dobije zadaću da mora doći do određene kontrolne točke ne kasnije od 09:00 (što predstavlja prvu činjenicu), te zna da vozila koja njegova postrojba koristi za transport imaju prosječnu brzinu od 60 km/h (što predstavlja drugu činjenicu), te je od kontrolne točke trenutno udaljen 60 km (treća činjenica), može iz te 3 činjenice deducirati da s trenutnog položaja prema kontrolnoj točci mora krenuti najkasnije u 08:00 kako bi stigao na vrijeme.

Dolazimo i do abduktivnog rasuđivanja. Abdukcija se često koristi pri rješavanju problema gdje nam nisu dostupni svi podaci, pa je stoga korištenje indukcije i dedukcije onemogućeno. Ova vrsta logičkog zaključivanja započinje promatranjem ili skupom opažanja, a sljedeći korak je pronalazak najvjerojatnijeg (često ujedno i najjednostavnijeg) objašnjenja za navedena opažanja. Ovakav postupak rezultira uvjerljivim zaključcima koji se ne mogu provjeriti, što razlikuje abdukciju od dedukcije. Zbog toga što ne možemo provjeriti zaključke, oni su otvoreni za preispitivanje ili mijenjanje s boljim objašnjenjem (Krizan, 1999).

S obzirom da nam u stvarnom životu često nisu dostupne sve informacije pri rješavanju problema, abdukciju također možemo naći u nizu praktičnih primjera. Recimo, primjera radi, da prvi vojnik u koloni tijekom patrole nekog područja uoči pješačku minu nasred ceste koja je loše skrivena i poprilično ju je lako uočiti. S obzirom da raspolaže samo jednom činjenicom - da je mina ispred njega, indukcija i dedukcija su u ovom slučaju onemogućene. Vojnik mora iz šireg konteksta izvući moguće hipoteze: je li nešto omelo neprijatelja dok je postavljao minu, pa ju nije stigao primjereno zamaskirati, ili je pak ona namjerno postavljena tako da se ju lako uoči, kako bi skrenula pozornost na sebe i prikrila neku drugu radnju, primjerice zasjedu? U ovom slučaju vojnik bi korištenjem abduktivnog rasuđivanja pretpostavio da je najvjerojatnija opcija da mina služi kao distrakcija, jer je malo vjerojatno da bi neprijatelj postavio minu nasred ceste gdje ju je lako uočiti, a pogotovo da ju ne zamaskira.

Za kraj ovog potpoglavlja spomenut ćemo i intuiciju, tj. njen istrenirani oblik kao dodatnu vrstu rasuđivanja. Intuicija u svom izvornom obliku podrazumijeva da je određena osoba do rješenja došla unutarnjim promišljanjem, a ne fokusirajući se striktno na činjenice i dokaze. Sama intuicija se može na određen način i u određenoj mjeri izvježbati s iskustvom i primjenjivanjem zdrave i samokritične unutarnje logike. Iskusni analitičari, a ponekad i oni manje iskusni, često će se prilikom rješavanja nekog problema za kojeg ne postoji mnogo informacija osloniti na vlastitu intuiciju. Koraci koji vode do zaključka tijekom intuitivnog rasuđivanja možda nisu vidljivi, te je svakako važno potvrditi intuiciju koliko je god moguće s

dostupnim činjenicama i alatima. U ovom kontekstu obavještajni djelatnici na menadžerskim pozicijama, kao što su voditelji analitičkih timova, igraju ključnu ulogu, jer upravo oni određuju koliko će slobode dopustiti svojim analitičarima u korištenju vlastite intuicije (Krizan, 1999).

Iako povijest zasigurno pamti mnogo slučajeva gdje se intuicija pokazala vrlo uspješnom i krucijalnom za postizanje nekog velikog pothvata (a i mnogo slučajeva gdje se ispostavila pogrešnom), za naš primjer uzet ćemo probijanje japanskog stroja za šifriranje u 2. svjetskom ratu koji je nosio kodni naziv „PURPLE“, te se koristio za enkripciju najosjetljivijih japanskih diplomatskih poruka. Američki kriptoanalitičari do 1940-te uspjeli su razbiti nekoliko jednostavnijih japanskih šifri, ali su se i dalje mučili s PURPLE-om, iako je sam stroj bio mehanički jednostavniji od njemačke Enigme. Streloviti napredak u razbijanju šifre dogodio se kad je jedan od kriptoanalitičara koji je radio za američki *Signal Intelligence Service – SIS*[7]*,* Leo Rosen, svojim kolegama prezentirao naočigled neobjašnjivu tezu koja se temeljila isključivo na njegovoj intuiciji. Naime, Rosen, bez da je ikada vidio PURPLE, došao je do zaključka da stroj ne koristi rotor kao ključni mehanizam za enkripciju, kao što je bio slučaj kod Enigme, nego koristi koračnu sklopku koja se tada upotrebljavala u telefonima. Ta hipoteza se kasnijim pokusima ispostavila istinitom te su saveznici imali ključ za PURPLE u svojim rukama, a Rosen je svoje iznenadno otkriće pravdao s istreniranom intuicijom koja se temeljila ponajviše na činjenici da je po struci bio komunikacijski inženjer i imao mnogo iskustva u toj sferi (Freeman i dr., 2003).

4.2. Metode obavještajne analize

U prošlom potpoglavlju obradili smo neke od najčešćih vrsta rasuđivanja, koje analitičar koristi kako bi sastavio obavještajni proizvod. Ovo potpoglavlje će se fokusirati na metode obavještajne analize, koje služe za potvrdu ili osporavanje rezultata prošlog koraka. Strukturirane metode analize svoju primjenu nalaze, osim za potvrdu i osporavanje, i u identifikaciji mentalnih sklopova, prevladavanju osobnih predrasuda analitičara ili šire cjeline, upravljanju rizikom i neizvjesnošću te poticanju kreativnosti. U ovom potpoglavlju detaljnije ćemo opisati tri metode: analizu konkurentskih hipoteza, „linchpin“ analizu, te analizu crvenog tima.

[7] *Signals Intelligence Service* – odjel vojske SAD-a za razbijanje šifri tijekom 2.svj. rata. Kasnijim preustrojem početkom 1950-ih postaje Agencija za nacionalnu sigurnost (eng. *National Security Agency*), koja je danas jedna od najbitnijih američkih obavještajnih agencija.

Analiza konkurentskih hipoteza (u nastavku: AKH) jedna je od vrsta procjene više konkurentskih hipoteza za određeni skup podataka. Sama analiza razvijena je 70-ih godina prošlog stoljeća od strane iskusnog američkog CIA-inog obavještajca, Richardsa Heuera, upravo za potrebe same agencije. Krajnji cilj ove analize je proizvesti najbolju inačicu djelovanja iz nesigurnih podataka, te je usko povezana s abduktivnim zaključivanjem, kojeg smo već spomenuli. U tu svrhu AKH ima za cilj pomoći analitičaru i da minimizira utjecaj kognitivnih pristranosti i ograničenja koja predstavljaju jednu od najvećih prepreka pri proizvodnji ispravnih obavještajnih proizvoda (Heuer, 2007).

Tipičan ciklus AKH sastoji se od sedam koraka. Prvi korak je pronalazak svih potencijalnih hipoteza – za tu svrhu se često koristi više analitičara koji do hipoteza dolaze „olujom mozgova“ (eng. *brainstorming*). Drugi korak je vezivanje dostupnih opipljivih dokaza, ali i logičkih argumenata za svaku navedenu hipotezu. Sljedeći korak, koji je prema Heueru i najvažniji, je stvaranje matrice. Matrica je sastavljena od svih hipoteza, teorija, argumenata i dokaza, te se uporabom jednog po jednog dokaza ili teorije pokušava opovrgnuti što veći broj hipoteza. Nakon što se početni broj hipoteza značajno smanjio u trećem koraku, četvrti korak dodatno rafinira dobiveno te prikupljanjem dodatnih dokaza i prepoznavanjem nelogičnosti i praznina isključuje još jedan broj hipoteza. Peti korak je najskloniji pogreškama, s obzirom da ovdje analitičari nastoje donijeti provizorne zaključke o relativnoj vjerojatnosti svake hipoteze. U ovom koraku se svakoj hipotezi dodjeljuje i razina dosljednosti, gdje manja dosljednost implicira manju vjerojatnost da je ona ispravna. Najmanje konzistentne hipoteze se eliminiraju. Dok ovaj i prethodni korak generiraju određeni postotak vjerojatnosti za svaku hipotezu, analitičar ipak mora upotrijebiti vlastitu prosudbu kako bi donio konačni zaključak. Analitičari u sljedećem koraku testiraju i provjeravaju dobivene zaključke pomoću analize osjetljivosti, čija je svrha pokazati kako bi na zaključke utjecalo da su ključni dokazi ili argumenti pogrešni, podložni različitim tumačenjima i sl. Valjanost i dosljednost ključnih dokaza i argumenata dvaput se provjeravaju kako bi se osigurala ispravnost. Na kraju AKH analitičari prezentiraju svoje zaključke donositeljima odluka, što uključuje i sažetak odbačenih alternativa skupa s razlogom njihovog odbačaja. Također se identificiraju prekretnice u procesu kako bi iste poslužile u narednim analizama (Heuer, 2007).

Dolazimo i do druge metode – linchpin analize. Linchpin analiza kao polaznu točku uzima provjerene, sigurne informacije, ili u najmanju ruku one s velikom vjerojatnošću sigurnosti. Polazeći od poznanica, analitičari korištenjem linchpin analize pokazuju potrošačima, kolegama i menadžerima da je problem temeljito proučen i u vezi sa stvarnošću. Drugim riječima, ova metoda je svojevrstan alat za usidrenje koji nastoji smanjiti opasnost od

samo-prouzročene obavještajne pogreške, kao i pogrešnog tumačenja od strane donositelja odluka ili kreatora politike. Sama analiza stvorena je 1990-ih godina kao jedna od odgovora na rastuću potrebu za proaktivnim pristupom analizi u obavještajnim krugovima, s obzirom da su se do početka tog desetljeća pretežito uporabljivale tzv. „post-mortem“ metode analize, koje su se fokusirale na obavještajne propuste koji su se već dogodili (Heuer, 1999).

Linchpin analiza nema striktne korake u provedbi, no ipak posjeduje određene kontrolne uvjete koje se moraju ispoštovati prilikom njenog korištenja. Kao i kod mnogih drugih metoda analize, najprije se identificiraju glavni neizvjesni čimbenici i varijable za koje se procjenjuje da će vjerojatno utjecati na ishod problema, dok paralelno obraćamo pozornost na raspon i odnose među čimbenicima u igri. Nakon toga, analitičari razvijaju prosudbe i hipoteze o odluci. Sljedeći korak je izdvajanje jedne ključne pretpostavke (upravo je to i srž samog *linchpina* – pravi smisao te riječi) te se ona ili potpuno eliminira ili se preokreće. Zatim je potrebna ponovna procjena dostupnih dokaza u svjetlu ove promijenjene ili eliminirane ključne pretpostavke, te se stvara novi skup hipoteza i prosudbi. Na kraju, ponovno vraćamo eliminiranu/promijenjenu pretpostavku te utvrdimo jesu li nove prosudbe i dalje točne. Ako jesu, onda eliminirana pretpostavka nije ključna za naš problem, a ako su nakon njenog vraćanja u igru nove pretpostavke postale neistinite ili nelogične, pronašli smo ključnu pretpostavku (Heuer, 1999).

Linchpin analiza može biti od značajne korisnosti u obavještajnom kontekstu. Međutim, postoje i određeni nedostaci koji se trebaju izbjeći. Prvi nedostatak je što ovaj pristup može uzeti u obzir samo pretpostavke koje su svjesno napravljene. Postoje skrivene pretpostavke koje ljudi stvaraju svaki dan, od kojih se neke mogu pokazati vrlo rizičnima. Nadalje, ovaj linchpin analiza ima tendenciju identificirati samo 'neugodne' rizike, tj. prijetnje da bi se pretpostavka mogla pokazati lažnom i postati problem za projekt. Samim time, linchpin analiza nije najbolji izbor kada se radi o identificiranju prilika (Heuer, 1999).

Naposljetku, fokus prebacujemo na analizu crvenog tima. Analiza crvenog tima je kreativna analitička tehnika koja pokušava replicirati misli i postupke protivnika. Glavni cilj u ovoj metodi analize je ispitati planove, procese i unutarnje djelovanje druge grupe ili organizacije, obično protivnika. Kao i mnoge druge vrste analize, analiza crvenog tima svoje korijene vuče iz vojnih krugova, ali je s vremenom postala uobičajena praksa i u sigurnosno-obavještajnim sustavima. Težište ove analize je promjena perspektive - obično je gledište analitičara fokusirano na njihove vlastite, prijateljske snage, dok je kod analize crvenog u fokusu protivnički, „crveni“ tim. Samim time, analitičari nisu više samo promatrači, nego svoju ulogu prebacuju u glumce (Mateski, 2009).

Ova metoda je osobito korisna kada se donositelji odluka suočavaju s osobom, skupom osoba, organizacijom itd. koja ima drugačiju kulturu, skup vrijednosti, uvjerenja, način razmišljanja i sl. U konstantnom izbjegavanju kognitivnih zamki u kontekstu valjane obavještajne analize, jedna od temeljnih ideja, a na kojoj se upravo bazira ova analiza, je da ne smijete pretpostaviti da će vaš protivnik djelovati ili odgovoriti onako kako biste vi. Ipak, uroniti u svijet svog protivnika je zahtjevan pothvat. Jedan od najvećih izazova i preduvjeta kvalitetne analize crvenog tima je stvaranje kompetentnog tima. Ako nam uvjeti i raspoloživa sredstva dozvoljavaju, crveni tim bi se trebao sastojati od ljudi koji imaju kulturno znanje o entitetu kojeg pokušavamo oponašati. U idealnom slučaju, ovo znači da bi bilo poželjno sastaviti analitičare koji govore određeni strani jezik, odrasli su u ciljanoj zemlji i sl. Ako se analizira određena poslovna organizacija, njen bivši (ili sadašnji) zaposlenik također može biti od velike pomoći. U isto vrijeme, stručni analitičar bez ikakvog znanja o predmetu može na stol donijeti neutralnu perspektivu. Cilj je imati uravnotežen tim koji se može istinski uvući u ulogu protivnika, a da ne zaglavi u unaprijed stvorenim predodžbama (Mateski, 2009).

S druge strane, pored svih navedenih prednosti analize crvenog tima, ona donosi i određene rizike. Jedan od glavnih rizika analize crvenog tima je pretjerano povjerenje u rezultate. Što je krajnji proizvod autentičniji, to će djelovati uvjerljivije, iako rezultati gotovo nikad ne mogu projicirati sve moguće smjerove djelovanja protivnika. Također, analize crvenog tima obično su dugotrajne i troše mnogo resursa. Tim koji je osposobljen za imitiranje protivnika trebao bi biti što dugotrajniji kako bi se postigao željeni efekt legitimnosti, što pak znači da te iste analitičare ne možemo angažirati na drugim projektima (Mateski, 2009).

5. Obavještajna potpora u vojnim operacijama

U kontekstu oružanih snaga i njihovih raznovrsnih aktivnosti, obavještajna potpora je od iznimne koristi i esencijalan je dio kako mirnodopskih, tako i ratnih zadaća. Kao što smo već napomenuli, u današnjem dobu gotovo sve moderne, demokratske zapadne zemlje imaju zasebna tijela koja se bave obavještajnim djelovanjem i izvan oružanih snaga, najčešće u obliku raznih agencija. Ipak, ovo poglavlje pobliže će pojasniti obavještajnu potporu oružanim snagama u kontekstu provođenja vojnih operacija. Kroz tri potpoglavlja, od kojih će se svako baviti slijedno-rastućom razinom – taktičkom, operativnom i strateškom – bit će obuhvaćena sama srž odnosa obavještajnog i vojnog, posebice kroz vizualizaciju s praktičnim primjerima.

5.1. Taktička razina

Taktička razina u vojnom kontekstu uključuje planiranje i provedbu bitaka i sukoba „uređenim rasporedom i manevriranjem borbenih elemenata u odnosu jednih na druge, te u odnosu na neprijatelja radi postizanja borbenih ciljeva“ (JP 1, 2013, I-8). Na početku je bitno napomenuti da ne postoje kruta ograničenja ili granice između tri razine koje će biti promatrane u ovom poglavlju, ali ova razgraničenja uvelike pomažu zapovjednicima kroz sve tri razine u planiranju i sinkronizaciji operacija, adekvatnom dodjeljivanju resursa i dodjeljivanju zadataka odgovarajućoj postrojbi.

Obavještajna potpora na taktičkoj razini u većini slučajeva podrazumijeva potporu koju provode ili snage koje organski pripadaju toj ustrojbenoj cjelini, ili pak specijalizirani, pridodani elementi, ako je riječ o namjenskoj organizaciji snaga. Ako uzmemo Oružane snage Republike Hrvatske (u nastavku: OSRH) kao primjer, razina bojne ili njen ekvivalent (eskadrila u Hrvatskom ratnom zrakoplovstvu) je najniža razina koja posjeduje vlastite obavještajne kapacitete. Primjerice, u kontekstu mehanizirane pješačke bojne, kakvih je u OSRH tri[8] s identičnim ustrojem, obavještajnu potporu tijekom svakodnevnih zadaća i u mirnodopskim uvjetima pruža obavještajni pododsjek (S-2). Više razine (brigada, kopnena vojska, glavni stožer) također imaju obavještajne pododsjeke te se njihovi kapaciteti povećavaju sukladno razini (Fabijančić, 2017).

Generalno govoreći, obavještajni pododsjek obnaša djelatnosti u potpori zapovjedniku. U borbenim uvjetima, bilo da se radi o vježbi ili stvarnoj situaciji, preuzimaju niz dodatnih

[8] 1. mehanizirana bojna „Tigrovi“ te 2. mehanizirana bojna „Gromovi“ se nalaze u Petrinji, dok se 3. mehanizirana bojna „Pauci“ nalazi u Kninu.

zadaća, kao što je analiza protivničke doktrine, njihovih kapaciteta, prednosti i slabosti[9] – gdje možemo povući paralelu s analizom crvenog tima. Također izrađuju obavještajnu pripremu bojnog polja, pružaju podršku postrojbama za izviđanje, kreiraju zajedničku operativnu sliku itd. Zajednička operativna slika (u stručnoj literaturi često opisana skraćenicom COP – od eng. *Common Operating Picture*) je taktički prikaz informacija koji omogućuje osoblju u zapovjednim ulogama (donositelji odluka) da donose učinkovite odluke na temelju konstantnog ažuriranja razumijevanja trenutne situacije. COP se stvara prikupljanjem podataka iz više izvora i njihovim spajanjem u jedan kohezivni prikaz (Fabijančić, 2017).

Osim već navedenog, obavještajni pododsjek, u suradnji sa zapovjednicima, analizira i određuje niz zahtjeva za kritičnim informacijama, u koje spadaju prioritetni obavještajni zahtjevi, zahtjevi za informacije o vlastitim snagama itd. Valja napomenuti da, kada govorimo o nižim taktičkim postrojbama (kao što je bojna), njihov kapacitet proizvodnje samostalnih obavještajnih proizvoda uvelike ograničen, s obzirom da su navedeni pododsjeci znatno ograničeni ljudstvom (timovi do 5 ljudi, koji su sastavljeni od djelatnih časnika i dočasnika) te resursima, te se u svom radu oslanjaju na obavještajne pododsjeke viših razina (brigada i više), koji po potrebi spuštaju relevantne informacije na niže razine (Fabijančić, 2017).

Osim S-2, u postrojbama taktičke razine često se može naći i izvidnički element. U kontekstu OSRH, svaka mehanizirana bojna posjeduje i izvidnički vod. Izvidnica predstavlja specijaliziranu postrojbu koja je osposobljena da uporabom specifičnih taktika, tehnika i procedura provodi misije neposrednog identificiranja, promatranja i prikupljanja podataka koji će kasnije biti dostavljeni donositeljima odluka - zapovjednicima. Na taktičkoj razini, izvidnica raspolaže primarno sa sredstvima HUMINT-a i IMINT-a. Izvidničke patrole su savršen primjer aktivnosti gdje je naglasak na obavještajnom djelovanju, jer izvidnici neposrednim izviđanjem i sve češćom uporabom bespilotnih letjelica mogu neopaženo prikupiti krucijalne podatke o terenu (kroz OAKOC čimbenike[10]) i neprijatelju (kroz SALUTE čimbenike[11]). Te se informacije zatim čim prije dostavljaju zapovjednicima onih postrojbi koje su u fokusu operacije. Za kraj, valja istaknuti da odluke na taktičkoj razini mogu imati dalekosežne posljedice, što ih ponekad usko veže za strateške obavještajne agende. Ovo je kritičan koncept

[9] Najčešće se za ovu svrhu koristi tzv. SWOT analiza – snage/prednosti (*strengths*), slabosti (*weaknesses*), mogućnosti (*opportunities*) te prijetnje (*threats*).

[10] OAKOC – mnemotehnika za analizu zemljišta koja obuhvaća promatranje i polja vatre (*Observation and Fields of Fire*), avenije prilaza (*Avenues of Approach*), ključno zemljište (*Key terrain*), prepreke – prirodne i umjetne (*Obstacles*) te zaklon i prikrivanje (*Cover and Concealment*).

[11] SALUTE – mnemotehnika za opisivanje karakteristika uočenog protivnika koja obuhvaća veličinu (*Size*), aktivnost (*Activity*), lokaciju i smjer kretanja (*Location and Direction*), obilježja uniforme/odjeće (*Uniform*), vrijeme i datum opservacije (*Time and Date*) te uočenu opremu i naoružanje (*Equipment and Weapons*).

koji je pojavom asimetričnog, modernog ratovanja postao još i važniji, te može biti presudan za planove koje postavljaju nacionalne države i njihove vojne i obavještajne zajednice (Garlauskas, 2003).

5.2. Operativna razina

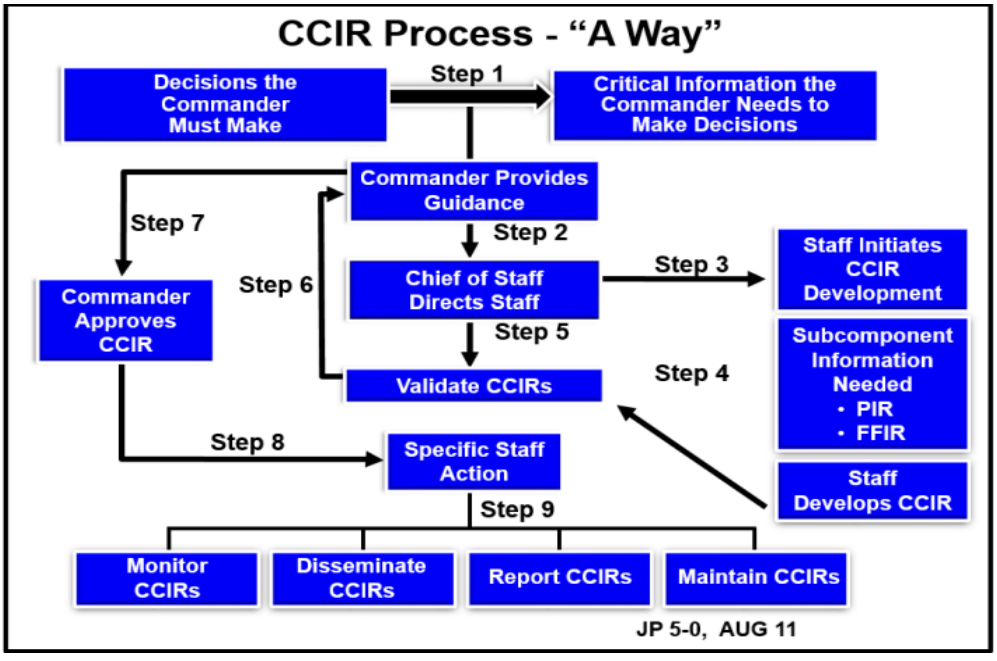
Aleksandr Svečin, časnik u sovjetskoj Crvenoj armiji 1920-ih, prvi je predložio koncept operativne razine rata kao esencijalan dio ruske novonastale vojne teorije „dubokih operacija" (ruski: *glubokaya operatsiya*). Koncept dubokih operacija naglašavao je uništavanje, potiskivanje ili ometanje neprijateljskih snaga ne samo na crti dodira, nego i po cijeloj dubini bojnog polja. S druge strane, američka vojska nije usvojila operativnu razinu rata kao doktrinu sve do 1982. gdje se prvi put spominje u *FM-u 100-5, Operacije*. U kontekstu moderne vojne teorije, operativno umijeće predstavlja razinu zapovijedanja koja povezuje detalje taktike s ciljevima strategije, te služi kao svojevrsna premosnica između te dvije razine. Za razliku od taktičke razine, ovdje je fokus na zajedničkim kognitivnim naporima viših zapovjednika i njihovih stožera, što obuhvaća njihova znanja i vještine, kreativnost, iskustvo i fleksibilnost pri donošenju važnih odluka. Drugim riječima, operativna razina razvija strategije, kampanje i operacije za organiziranje i korištenje vojnih snaga integracijom ciljeva, načina i sredstava - povezuje političke potrebe s vojnom moći (ADP 5-0, 2019).

Kada govorimo o obavještajnoj potpori u kontekstu operativne razine, bitna razlika u odnosu na taktičku razinu je fokus na stvaranje zajedničkog okvira koji donositeljima odluka i njihovim stožerima služi za usmjeravanje i koordinaciju njihovih misli, rasprava, planova i procjena. Učinkovito izvršenje obavještajnog procesa ovisi o uključenosti zapovjednika i stožera, a s druge strane i o učinkovitom prikupljanju informacija. Zapovjednici iniciraju obavještajni proces izdavanjem smjernica za planiranje, utvrđivanjem prioriteta te određivanjem CCIR-a (ADP 5-0, 2019). Tako se na operativnoj razini mogu razaznati svi elementi koje smo dosad spomenuli u radu – od kompletnog obavještajnog ciklusa, do raznih metoda obavještajne analize (s obzirom da operativna razina uključuje i profesionalne obavještajne analitičare, što je rijetkost na taktičkoj razini), te raznih metoda prikupljanja obavještajnih podataka.

Koncept zapovjednikovih zahtjeva za ključnim informacijama (CCIR) jedan je od dva koncepta koje ćemo detaljnije proučiti u ovom potpoglavlju. Na samom početku valja napomenuti da CCIR nije nepromjenjiv skup zahtjeva za izvješćivanje ograničen na određene radnje ili događaje, već više filozofija zapovijedanja i sustav povratnog informiranja i

izvještavanja koja može stvoriti prilike i prostor za odlučivanje. Ako pogledamo sliku 3., možemo vidjeti da je prvi korak u CCIR procesu prepoznavanje odluka koje zapovjednik mora donijeti, nakon čega slijedi njegovo usmjeravanje dostupnih resursa stožera u tom smjeru. Stožer zatim inicira razvoj CCIR-a, što možemo smatrati svojevrsnim obavještajnim ciklusom. U tom trenutku se prikupljaju sve dostupne informacije kako o prijateljskim snagama, tako i neprijateljskim, koristeći sve raspoložive resurse, te se prateći daljnje korake obavještajnog ciklusa dolazi do gotovog obavještajnog produkta – u ovom kontekstu, CCIR-a. Zapovjednik zatim donosi odluku odobrava li dobiveni CCIR ili ne – ako ne, ciklus kreće iznova, a ako da, zapovjednik je spreman za donošenje odluka pod uvjetom da stožer kontinuirano prati i održava CCIR sukladno stanju na terenu, te po potrebi izvještava zapovjednika o novonastalim promjenama - što predstavlja 9. korak na slici (ADP 5-0, 2019).

Za kraj, bitno je istaknuti da se kroz sustav naučenih lekcija uočilo da zapovjednici na višim razinama smatraju da je tradicionalni, taktički pogled na CCIR-ove koji podržavaju zahtjeve vremenski osjetljivih, unaprijed dogovorenih odluka, često preuzak da bi bio učinkovit na višim razinama. Ovaj taktički pogled ne obuhvaća nužnost boljeg razumijevanja okruženja niti ključnu ulogu procjene na operativnoj razini. Nadalje, operativni CCIR-ovi, ako su usmjereni na specifične događaje na "taktičkoj razini", mogu spriječiti donošenje odluka i agilnost podređenih (ADP 5-0, 2019).



Slika 3. Koraci u procesu CCIR-a.

Izvor: https://grugq.github.io/resources/jp5_0.pdf (Pristupljeno 18.01.2024.)

Drugi koncept koji će biti detaljnije analiziran u ovom potpoglavlju je ISTAR[12]. ISTAR, kao i upravo opisan CCIR, koncept je koji uključuje radnje koje se mogu provoditi na sve tri razine, a ne samo na operativnoj. U širem smislu, ISTAR je koncept koji objedinjuje nekoliko funkcija bojnog polja kako bi se pružila obavještajna podrška borbenim snagama kroz korištenje svojih raspoloživih senzora (izvora prikupljanja informacija) te upravljanje tim prikupljenim informacijama. Kao što smo već objasnili, informacije se na bojnom polju prikupljaju paralelno iz više izvora i na više načina. Informacije se potom prosljeđuju obavještajnom osoblju na analizu, a potom zapovjedniku i stožeru radi lakšeg planiranja, povećanja situacijske svjesnosti i efektivnijeg donošenja odluka (Davies, 2021).

U praksi, primjeri ISTAR sustava su raznovrsni, te uključuju zračne, pomorske i kopnene sustave nadzora i izviđanja. Zračni (i svemirski) sustavi su posebice pogodni jer omogućuju odličan nadzor nad velikim područjima, te uključuju satelite, specijalno opremljene izvidničke zrakoplove s posadom kao što je američki Lockheed U-2, te besposadne letjelice, kao što je izraelski Elbit Hermes 900. Od kraja Hladnog rata veći dio uloge strateškog izviđanja je sa zrakoplova s posadom prešao na satelite, a na taktičkoj razini je sve češća uporaba bespilotnih letjelica, koje su postale jedne od ključnih obilježja modernog ratovanja (Davies, 2021). Povećana uporaba autonomnih sustava i umjetne inteligencije nije samo ograničena na zračne sustave, pa je tako krajem 2021. godine američka mornarica započela testiranje besposadnih plovila, u cilju očuvanja svojih interesa na otvorenom moru (Ziezulewicz, 2021).

5.3. Strateška razina

Izveden iz grčke riječi *strategos*, pojam strategija, kada je prvi put ušao u uporabu krajem 18. stoljeća, smatran je u užem smislu kao umijeće raspoređivanja trupa. Nešto kasnija definicija britanskog vojnog povjesničara i teoretičara sir Basila Henryja Liddella Harta (1895. - 1970.), stavila je manji naglasak na bitke, definirajući strategiju kao "umijeće raspodjele i primjene vojnih sredstava za postizanje ciljeva politike" (Hart, 1991, 321). U potonjoj se definiciji razaznaje i glavna ideja strategije – strateški potezi uvijek su vezani za političke, te često imaju dalekosežne nacionalne (a ponekad i međunarodne) posljedice.

Kada govorimo o obavještajnoj potpori na strateškoj razini, možemo govoriti o njoj kao pokretaču strategije. Kvalitetna obavještajna potpora ne samo da pruža temeljne informacije na temelju kojih se mogu izrađivati planovi, već također projicira potencijalne reakcije drugih –

[12] ISTAR – vojni koncept koji uključuje obavještajno djelovanje (*Intelligence*), motrenje (*Surveillance*), odabir ciljeva (*Target Acquisition*) te izviđanje (*Reconnaisance*).

kako protivnika, tako i onih neutralnih – na te planove, pomažući donositeljima odluka na strateškoj razini (u vojnom kontekstu su to najčešće generali) da procjene izvedivost predloženih smjerova djelovanja. Osim toga, budući da je strategija po definiciji proaktivna, obavještajni podaci pomažu donositeljima odluka da prepoznaju prilike i prijetnje, posebice u širem kontekstu nacionalne sigurnosti, kako bi mogli razviti odgovarajuće planove. Valja napomenuti da navedeni koncept obavještajnog djelovanja kao predviđajućeg pokretača strategije nije ništa novo – još je drevni kineski filozof Sun Tzu (2022, 84) vidio pravovremenu i točnu informaciju kao temeljno oruđe stratega, rekavši: "Upoznaj neprijatelja i upoznaj sebe; ni u stotinu bitaka nećeš biti u opasnosti."

U kontekstu odnosa između obavještajnog i strateškog, postoje dvije glavne škole mišljenja o ispravnom postupanju. Prvo mišljenje ističe važnost odvajanja analitičkog procesa, tj. samih analitičara od političke ili strateške zajednice kako bi se izbjeglo ometanje. U praksi, ovakvo se mišljenje moglo pronaći u američkoj obavještajnoj zajednici kroz 20. stoljeće. Temeljno mišljenje je bilo da se održavanjem distance između obavještajnog i strateškog sektora štiti analitičare od nepotrebnog pritiska i omogućuje im se adekvatna sloboda za formiranje vlastitih procjena koje nisu iskvarene vanjskim utjecajima. Tako je obavještajna zajednica odgovarala na pitanja kada je to od nje zatražila strateška zajednica, te je davala adekvatna upozorenja o prilikama i prijetnjama za nacionalnu sigurnost kad bi se oni otkrili (George i Bruce, 2008).

S druge strane, jedan dio stručnjaka vjeruje da je bliska koordinacija između analitičara i stratega/političara neophodna kako bi se osiguralo da su obavještajne procjene relevantne za postavljena strateška pitanja. Sherman Kent (1903. – 1986.), američki profesor povijesti te dugogodišnji obavještajac unutar američke CIA-e, kojeg se često naziva i ocem obavještajne analize, ističe problem u odvajanju analitičara od stratega. Iako ova filozofija može zaštititi objektivnost obavještajne zajednice, do problema dolazi kada donositelji odluka na strateškoj razini formuliraju nešto novo u npr. vanjskoj politici te oni sami moraju inicirati dostavljanje obavještajnih podataka za određeni potez. U tom slučaju, obavještajna zajednica riskira da je se uopće ne konzultira, te time brzo može izgubiti korak s razvojem strategije. To za posljedicu može imati pojavu da analitičari ne razumiju kontekst ili pozadinu zahtjeva od strane donositelja odluka, pa su samim time i njihovi odgovori brzi i relativno precizni, ali u široj slici nevažni zbog nedostatka konteksta. Posljedično, strateg će imati nepotpuno ili možda čak i pogrešno razumijevanje operativnog okruženja (George i Bruce, 2008).

Nadalje, premošćivanje jaza između obavještajnog djelovanja i strategije može donijeti dodatni niz prednosti. Prvo, razumijevanjem prioriteta i izazova s kojima se stratezi suočavaju, analitičari mogu raditi kako bi osigurali da se stalni analitički napori, kao i napori prikupljanja sirovih informacija, usredotoče na strateške probleme (koji su često i političke prirode) koji se trenutno rješavaju. Možda još važnije, ako analitičari sudjeluju u razmatranju različitih inačica djelovanja, veća je vjerojatnost da će na licu mjesta iznijeti relevantne informacije, tako informirajući raspravu i pomažući donositelju odluka da razmisli o izborima i mogućim ishodima. Takve razmjene informacija omogućuju donositelju odluka ne samo procjenu onoga što analitičar zna i misli, već i razumijevanje temeljnih pretpostavki i stupnja neizvjesnosti u prosudbi. Uvažavanje ograničenja obavještajnih prosudbi pomaže strategu da razvije prijedloge koji priznaju i uzimaju u obzir neizvjesnost – koja je neizbježna u strateškom planiranju. Ako obavještajni kadar ne može uvijek prodrijeti kroz maglu neizvjesnosti, može pomoći barem u definiranju njene veličine i značaja (George i Bruce, 2008).

Ipak, integracija obavještajnih analitičara u strateški tim nosi i određene rizike. Iako bi analitičari trebali nastojati utjecati na promišljanje strategije pružanjem relevantnih informacija o aktualnim problemima, oni ne bi smjeli zagovarati određenu politiku. Analitičari mogu ponuditi vlastita informirana mišljenja ako se to od njih zatraži, ali općenito bi se trebali ograničiti na identifikaciju prilika ili procjene vjerojatnih reakcija na predloženi tijek djelovanja. Ako obavještajni analitičari počnu podržavati određenu političku opciju, njihove procjene mogu postati pristrane, lišavajući njihov rad objektivnosti koja je, kao što smo već zaključili, u samom središtu obavještajnih analiza. Također, mogu postati žrtve pristranosti potvrde, tražeći podatke koji su u skladu s njihovim unaprijed stvorenim idejama i ignorirati informacije koje se ne podudaraju s preferiranom opcijom politike. Iako ti rizici postoje čak i kada analitičari nisu integrirani u strateški tim, potencijal za analitičku pristranost se povećava kada su obavještajni službenici uključeni u rasprave o politici (George i Bruce, 2008).

6. Sinergija napredne tehnologije i obavještajne djelatnosti

Iako će u bliskoj budućnosti vojni sukobi najvjerojatnije i dalje biti vođeni istim čimbenicima koji su povijesno poticali ratove –od vjerskih, ideoloških, ekonomskih razlika i zaštite resursa, do težnje za moći i utjecajem – načini na koje se rat vodi će se promijeniti, posebice ako se nezaustavan trend razvoja tehnologije nastavi. Razvojem novih tehnologija paralelno će se razvijati i nove taktike, tehnike i doktrine, te je moguće da će novi akteri ući u sam vrh utjecajnih sila na geopolitičkoj sceni ako dobiju i iskoriste pristup tim sposobnostima. Kombinacija poboljšanih senzora, automatizacije i umjetne inteligencije (u nastavku: AI) s drugim naprednim tehnologijama proizvest će točnije, bolje povezano, brže i razornije oružje sve većeg dometa, primarno dostupno najnaprednijim vojskama, ali zbog globalizacije nadohvat ruke i manjim državnim i nedržavnim akterima. Međutim, bez kvalitetne obavještajne potpore i najbolje opremljena vojska ne može daleko. Kako smo već natuknuli u prethodnim poglavljima, obavještajni sektor itekako je iskoristio val razvoja tehnologije. Dvadeset prvo stoljeće, iako još ni četvrtinu iza nas, možemo sa sigurnošću nazvati stoljećem informacija. Ovo poglavlje se upravo fokusira na taj aspekt naše sadašnjosti. Koliki je utjecaj tehnologije na obavještajnu djelatnost? Kroz dva potpoglavlja, gdje se prvo osvrće na analitiku velikih podataka, a drugo na umjetnu inteligenciju, pokušat ćemo dati dio odgovora na to pitanje.

6.1. Analitika velikih podataka

Što označava pojam „velikih podataka“? Definicija termina velikih podataka veže se za tri kriterija – to su prvenstveno podaci koji sadrže veću raznolikost – ne govorimo o samo jednoj vrsti podataka, npr. tekstu. Drugi i treći kriterij nam pak govore da pristižu u sve većim količinama, ali i sve većom brzinom. Drukčije rečeno, veliki podaci su veći, složeniji skupovi podataka, te su toliko opsežni da tradicionalni softveri za obradu podataka ne mogu njima upravljati. Ipak, ove ogromne količine podataka mogu se koristiti za novi pristup rješavanju raznih problema (oracle.com, 2023). U domeni nacionalne sigurnosti, količina podataka se eksponencijalno povećavala s rastom samog Interneta, posebno u područjima koja su intrinzično vezana uz nacionalnu sigurnost, kao što su borba protiv terorizma, sigurnost računalnih mreža i te suzbijanje širenja ilegalnog i nuklearnog oružja. Vrlo brzi priljev nestrukturiranih podataka koji se odnose na pitanja nacionalne sigurnosti kao što je primjerice kibernetička obrana zahtijeva i analizu u stvarnom vremenu i izvan-mrežnu analizu (Kulshrestha, 2016).

Rukovanje ovim podacima, dubinsko ispitivanje velikih podataka te njihova vizualizacija u različitim oblicima kao što su karte, grafikoni i vremenske crte, te analize protoka podataka u stvarnom vremenu (ili što je brže moguće) neki su od bitnih zahtjeva za pitanje nacionalne sigurnosti. Podaci se prikupljaju na neviđenim razinama. Primjerice, u kontekstu oružanih snaga, brz tehnološki napredak u senzorima te u umreženim borbenim sustavima, između ostalog, konstantno primorava moderne vojne sile da usvoje komercijalno dostupne tehnologije u nastajanju i prilagode ih za svoju upotrebu. Pojava velikih podataka potiče oružane snage da prebace integrirane sustave podrške odlučivanju, kao što je primjerice *blue force tracker*[13], na arhitekturu i analitiku velikih podataka. Nadalje, ograničenje budžeta te smanjena zainteresiranost za ulazak u oružane snage zajednički su problemi s kojima se suočavaju vojske u vodećim zemljama. Takva pojava implicira još veću ovisnost o tehnologiji zbog smanjene radne snage, što je zauzvrat navelo druge nacije da usvoje strategiju čekanja i promatranja prema kojoj bi se zauzele za najbolje dostupno rješenje koje su usvojile vodeće vojske (Kulshrestha, 2016).

Međutim, izvlačenje korisnih obavještajnih podataka iz gomile informacija koju predstavlja *big data* vrlo je zahtjevan proces. Glavni problemi s kojima se vojska danas suočava uključuju dostupnost sve većih količina senzorskih podataka iz izvora kao što su bespilotne letjelice i sateliti. Primjerice, najjednostavnija cjelodnevna misija izviđanja i nadzora korištenjem samo jedne bespilotne letjelice može proizvesti više od 10 terabajta podataka od kojih se u prosjeku samo oko 5% analizira, a ostatak se pohranjuje. Analitičari su također ograničeni brzinama preuzimanja podataka ovisno o njihovoj lokaciji. Često se komunikacijske linije dijele ili možda nisu stalno dostupne, što povećava kašnjenja u analizi. Pružanje sveobuhvatne svijesti o situaciji ovisi o točnosti i integraciji podataka primljenih od više vrsta senzora i izvora obavještajnih podataka. Tu dolazimo do sljedećeg problema – razni sofisticirani uređaji i softverski alati za sada uglavnom nemaju interoperabilnost, ponajviše zbog sigurnosnih razloga. ISTAR podaci iz različitih izvora pohranjuju se na različitim lokacijama s različitim razinama pristupa, što dovodi do nepotpune analize. Analitičari u prosjeku troše 20 posto svog vremena na analizu već izdvojenih točnih podataka, dok 80 posto vremena troše na traženje točnih podataka (Kulshrestha, 2016).

[13] Sustavi za praćenje prijateljskih snaga (eng. *Blue Force Tracking*) pružaju zapovjednicima lokacijske informacije o njihovim snagama u stvarnom vremenu koristeći GPS te neki oblik geografskog informacijskog sustava (GIS), često integrirano i s komunikacijskim sustavom.

Koliko je zahtjevno pravilno provesti analitiku velikih podataka možemo vizualizirati praktičnim primjerom iz američke operacije „Enduring Freedom“ (listopad 2001. – prosinac 2014.) u Afganistanu. Početak 2009. godine bio je presudan u širem kontekstu operacije. U siječnju iste godine Barack Obama postao je 44. predsjednik SAD-a, dok je paralelno talibanski pokret u Afganistanu prolazio kroz oživljavanje. Doktrina protupobunjeništva, koja je zadnji put prije Afganistana od SAD-a bila korištena u Vijetnamskom ratu, vrlo brzo se našla u fokusu napora operacije. U napore se isto tako brzo uključila i američka Agencija za napredne obrambene istraživačke projekte (u nastavku: DARPA).

Osnovana 1958. kako bi pomogla Sjedinjenim Državama da pobijede u svemirskoj utrci, DARPA je najpoznatija po svojoj proizvodnji i istraživanju futurističke tehnologije, te se smatra zaslužnom i za kreiranje Interneta, između ostalog. Za DARPA-u je uključivanje u Afganistan predstavljalo povratak korijenima iz Vijetnamske ere, nakon gotovo tri desetljeća izbivanja iz ratnih zona. U Vijetnamu je DARPA pogriješila pokušavajući dobiti rat uporabom napredne tehnologije, što nije urodilo plodom. Još jednom se postavilo pitanje mogu li vrhunska znanost i tehnologija učiniti bolje u Afganistanu (Weinberger, 2017).

Samim time, agencija je 2009. pokrenula ambicioznu inicijativu u rudarenju podataka, te je ubrzo vojnom vrhu SAD-a predstavila vrlo tajnoviti program namijenjen predviđanju napada pobunjenika na temelju analitike velikih podataka koju su tada (a i danas) koristile uspješne tvrtke poput Amazona za predviđanje kupnji potencijalnih kupaca. Projekt je dobio ime Nexus 7, te se u sljedećih godinu dana razvio dovoljno da DARPA pošalje približno stotinu svojih zaposlenika u Kabul. Ubrzo su DARPA i NSA sklopili sporazum o dijeljenju podataka kako bi maksimizirali međusobnu korist, no taj savez je već od samog svog početka naišao na značajne probleme. DARPA-ini zaposlenici koji su poslani u ratnu zonu bili su mladi i nisu imali nikakvog vojnog iskustva, a kulturološki šok ubrzo je postao očit. Vojni dužnosnici u Kabulu oklijevali su dijeliti klasificirane obavještajne podatke s informatičkim znanstvenicima koji su mahom tek završili fakultete te nisu posjedovali zahtijevanu razinu sigurnosne provjere, a obavještajni podaci koje su davali nisu bili od pretjerane koristi (Weinberger, 2017).

Kad su stigli u Afganistan, DARPA-ini analitičari su počeli prikupljati što su mogli više obavještajnih podataka, što je uključivalo telefonske zapise NSA-e, radarske podatke vojske i razna obavještajna izvješća. No, problem je bio u tome što je većina podataka koji su dolazili u Nexus 7 bili kvalitativni, a ne kvantitativni, koje nije bilo lako integrirati u računalni program. Čak i kada su podaci bili kvantitativni, poput radarskih (MASINT), njihova pouzdanost bila je upitna jer su radari rijetko pokrivali točno isto područje kroz duži vremenski period (Weinberger, 2017).

Na kraju, unatoč snažnom financiranju projekta od strane američke vojske i svim naporima, program nije ispunio svoje nade da demonstrira zamišljenu sinergiju analitike velikih podataka i obavještajnog djelovanja. Iako stručnjaci ističu više propusta u cijelom mehanizmu koji su na kraju doveli do takvog rezultata, jedan od vodećih problema se smatra činjenica da je DARPA precijenila sposobnost Afganistanaca da pristupe internetu, kao i doseg usluga mobilne telefonije u Afganistanu. Ubrzo se došlo do saznanja da samo 4 posto stanovništva ima pristup i vještine potrebne za pristup i korištenje interneta. Ugovor s DARPA-om, koji je istekao krajem 2011. godine, nije bio ponovno obnovljen (Weinberger, 2017).

6.2. Umjetna inteligencija

Umjetna inteligencija (AI) u 21. stoljeću je nedvojbeno postala transformacijska sila u raznim sektorima. Vojno i obavještajno područje, naravno, nisu iznimka. Svojom sposobnošću obrade golemih količina podataka, analize složenih obrazaca i donošenja trenutnih odluka, AI je revolucionarizirao vojnu tehnologiju - obrambeni sektor primjenjuje AI na toliko različitih načina da je često teško shvatiti dalekosežnost promjena. Bilo da olakšava razvoj autonomnih vozila ili igra ključnu ulogu u kibernetičkoj sigurnosti, AI podupire mnoge značajne razvoje obrambenog sektora u posljednjih desetak godina.

Jedan od najznačajnijih načina na koji vojske koriste AI, a koji je u vrijeme pisanja ovog diplomskog rada nikad aktualniji s obzirom na rat u Ukrajini te konflikt između Izraela i Palestine, je razvoj autonomnog oružja i sustava vozila. Već spomenute bespilotne letjelice, kao i kopnena vozila te podmornice pokretane umjetnom inteligencijom koriste se za izviđanje, nadzor i borbene operacije te se sa sigurnošću da pretpostaviti da će se trend jačanja njihovog značaja na modernom bojištu neometano nastaviti u bliskoj budućnosti. Također, iako je još uvijek daleko od široke primjene, mnoge vodeće vojske svijeta konstantno ulažu financijske i znanstvene napore u razvoj i usvajanje potpuno autonomnih oružnih sustava, što bi moglo drastično promijeniti način na koji zamišljamo bilo kakav oružani konflikt, dodatno udaljavajući ljudske sudionike od često pogubnih posljedica bojnog polja (National Intelligence Council (NIC), 2021).

Nadalje, AI transformira sustave zapovijedanja i nadzora omogućujući analizu podataka u stvarnom vremenu, što rezultira olakšanom donošenju ispravnih i pravovremenih odluka i povećava sve bitniju situacijsku svijest. Ovdje treba napomenuti da krajnji cilj nije potpuna zamjena ljudskih intelektualnih kapaciteta, nego pravilna sinergija umjetne i ljudske inteligencije, gdje bi AI trebao preuzeti obavljanje jednostavnih, repetitivnih zadataka.

U kontekstu kibernetičke sigurnosti, koja se sve češće u stručnoj literaturi redovno uvrštava kao dio nacionalne sigurnosti modernih zemalja, AI također preuzima sve veći dio kolača u otkrivanju i ublažavanju kibernetičkih prijetnji. Algoritmi strojnog učenja efektivno analiziraju mrežni promet, identificirajući potencijalne ranjivosti i reagirajući na kibernetičke napade u stvarnom vremenu. Takvi sustavi također uče iz prethodnih incidenata i stalno se razvijaju, te s vremenom stvaraju agilnu i robusnu infrastrukturu kibernetičke sigurnosti. To je od posebnog značaja jer se kompletni vladini sektori zapadnih zemalja sve više oslanjaju na međusobno povezane digitalne sustave i mreže. Iako to omogućuje olakšano korištenje raznih alata kako državnim službenicima, tako i građanima, to je također potencijalna slabost. Ako neprijateljski akter ugrozi sigurnost takvih sustava, posljedice bi mogle biti ozbiljne (NIC, 2021). Najbolji primjer iz bliske prošlosti je ruski kibernetički napad na Ukrajinu 23. prosinca 2015., kad je hakirana električna mreža u dvije zapadne oblasti Ukrajine, što je rezultiralo nestankom struje za otprilike 230 tisuća potrošača u Ukrajini u trajanju od par sati. Napad se pripisuje *Sandwormu*, ruskoj skupini za kibernetičko ratovanje koja je pod okriljem GRU-a[14], te predstavlja prvi globalno priznat uspješan kibernetički napad na električnu mrežu (Kostyuk i Zhukov, 2019).

Na kraju valja istaknuti i sve veću ulogu umjetne inteligencije u kontekstu simulacija i virtualnih okruženja za obuku vojnog osoblja u realističnim scenarijima. Mnoge su potencijalne prednosti ovakvog načina učenja i razvijanja vještina - inteligentni virtualni protivnici imaju potpuno prilagodljivo ponašanje, napredne inačice omogućuju i strojno učenje koje služi za poboljšanje realističnosti obuke i same interakcije. Također, potencijal za individualiziranu obuku je mnogostruko veći od konvencionalne vojne obuke, pa se prilagodljiva priroda ovakvih simulatora može iskoristiti za prilagođene režime obučavanja koji za cilj imaju otklanjanje osobnih slabosti. Primjerice, OSRH od ožujka 2017. godine posjeduje upravo jedan od takvih sustava – virtualno strelište SATTS (eng. *Small Arms Tactical Training Simulation*). Ovo strelište, koje je donacija od Oružanih snaga SAD-a, omogućuje vojnicima uvježbavanje radnji pri gađanju iz raznih tipova naoružanja – od pištolja i jurišnih pušaka, do snajpera i automatskog bacača granata (hrvatski-vojnik.hr, 2017).

Na višim razinama, sustavi obuke koji se pogonjeni umjetnom inteligencijom pomažu u razvoju ključnih zapovjednih vještina, sposobnosti donošenja odluke pri raznim okolnostima te razvoj i održavanje situacijske svijesti, pripremajući vojno osoblje za složena i dinamična operativna okruženja. Osim što je ovakva vrsta obuke puno sigurnija od konvencionalne vojne

[14] GRU – vojno-obavještajna agencija Glavnog stožera Oružanih snaga Ruske Federacije koja se fokusira na obavještajne djelatnosti izvan Rusije. GRU također posjeduje i vlastite specijalne snage – Spetznaz GRU.

obuke u terenskim uvjetima, ona je često i daleko manji financijski teret za često već opterećene vojne budžete modernih zemalja (NIC, 2021). Ipak, kao što smo već napomenuli na početku potpoglavlja, obuka potpomognuta umjetnom inteligencijom ne bi trebala potpuno zamijeniti konvencionalnu, nego joj pružati potporu.

7. Zaključak

Kroz ovaj diplomski rad pokušali smo pobliže objasniti usku vezanost obavještajnog djelovanja i procesa donošenja odluka, posebice onih u vojnim organizacijama. Prvi dio rada postavio je temelje analizirajući značaj obavještajnog ciklusa kao glavne gradivne jedinice cijelog odnosa. Napomenuli smo da je ciklus apstraktan pojam, te je u stvarnosti fleksibilan – to ne znači samo da su njegovi koraci, kao i njihovi točni nazivi, promjenjivi, nego znači da se često više koraka (ili čak svi) odvijaju istovremeno, što je sve češće slučaj s obzirom da živimo u vremenu gdje smo svake sekunde bombardirani gomilom informacija. Zbog toga jedan dio stručnjaka iz obavještajnog područja već niz godina pokušava naći adekvatnu zamjenu za ovaj koncept – dok jedni vjeruju da struktura mreže možda vjernije opisuje cijeli proces u stvarnosti, drugi ističu da je sasvim nebitno kako obavještajni ciklus izgleda kada ga prikažemo na nekoj slici – bitno je da funkcionira.

Sljedeći dio rada daje nezaobilazan uvid u discipline prikupljanja obavještajnih podataka. Zbog ograničenog opsega rada, fokus je stavljen na ustaljene discipline. Krenuvši od HUMINT-a, koji je u jednom ili drugom obliku star koliko i samo čovječanstvo, prvo potpoglavlje ističe važnost ljudskog faktora koji je, unatoč svim tehnološkim napredcima i sofisticiranim uređajima, i dalje nezamjenjiv. Sljedeće potpoglavlje bavi se OSINT-om, koji je već dugi niz desetljeća konstantno u rastu i u gotovo svim razvijenim obavještajnim zajednicama predstavlja poveći postotak izvora informacija. SIGINT, koji je tema trećeg potpoglavlja, disciplina je za koju često države izdvajaju najveći dio obavještajnog budžeta. Međutim, široka uporaba SIGINT metoda prikupljanja često je vezano za kontroverze – rad spominje samo jedan od najpoznatijih slučajeva u posljednjih nekoliko godina - prisluškivanje njemačke vlade od strane NSA-e. Poglavlje je zaključeno s GEOINT-om te njegovom značaju u današnjem višedimenzionalnom sigurnosnom okruženju, gdje geoprostorne informacije često daju visoko korisni prostorni kontekst drugim informacijama, ali su vrijedne i samostalno.

Nadalje, naredna dva poglavlja predstavljaju okosnicu rada. Treće poglavlje na jezgrovit način predstavlja glavnu ideju rada – obavještajnu analizu. Obavještajna analiza predstavlja glavni napor u proizvodnji obavještajnog proizvoda, te je samim time od neprocjenjivog značaja da su svi preduvjeti za kvalitetnu analizu ispunjeni kako bi donositelj odluke dobio obavještajnu procjenu za određen problem što brže, ali i što kvalitetnije. Ovo poglavlje također daje odgovor na četvrto istraživačko pitanje – koji su svakodnevni izazovi u radu obavještajnih analitičara te potencijalni načini za njihovo savladavanje? Tri opisane metode analize – analiza crvenog tima, analiza konkurentskih hipoteza te linchpin analiza, samo su neke od postojećih,

te sve posjeduju određene prednosti i nedostatke – na analitičaru je da prepozna najadekvatniju metodu za trenutni problem, te da uspješnim kombiniranjem više metoda dođe do nepristranog, pravovremenog i preciznog obavještajnog proizvoda. Upravo je ta kombinacija raznih alata, ali i različitih pogleda na isti problem ključna za pravilnu i kvalitetnu obavještajnu analizu.

Donošenje prave odluke od posebne je važnosti kada o toj odluci ovise ljudski životi – što je uvijek moguć slučaj u kontekstu oružanih snaga. U ovom poglavlju nalazimo odgovore na prvo i treće istraživačko pitanje – kolika je uloga obavještajne analize u procesu donošenja odluka te sličnosti i razlike između tog odnosa u vojnom i političkom sektoru. Vojni zapovjednici na sve tri razine – taktičkoj, operativnoj i strateškoj – često se hvataju ukoštac s kompleksnim situacijama pod pritiskom, te je kvalitetna obavještajna potpora jedan od glavnih alata s kojima se može raspršiti magla neizvjesnosti na bojištu, makar se radilo samo o vježbovnoj situaciji. Povijest nam govori da iza gotovo svake pobijeđene bitke, te u užem smislu, odlične odluke zapovjednika u kritičnom trenutku, stoji obavještajna superiornost nad protivnikom, koji umnogostručuje situacijsku svjesnost te olakšava donošenje zahtjevne odluke. S druge strane, kreatori politika često donose odluke koje utječu na cijelu populaciju jedne države. Samim time je odluka važnija jer utječe na mnogo veći broj ljudi, a obavještajni analitičari koji su pridodani kreatorima politike imaju vrlo zahtjevan zadatak – što bolje analizirati određen problem u što manje vremena.

Naposljetku, valja spomenuti i sve veći utjecaj napredne tehnologije na obavještajni sustav. Predzadnje poglavlje bavi se tom tematikom, te ujedno daje i odgovor na drugo istraživačko pitanje rada – utjecaj razvoja tehnologije na obavještajnu analizu. Napredak tehnologije, koji traje već više od stotinu godina i ne pokazuje tendencije usporavanja, zasigurno je iz temelja promijenio način na koji se vrši obavještajna analiza, te se ocrtava uzorak budućih obavještajnih kapaciteta i napora. Pred obavještajnim zajednicama diljem svijeta je zahtjevan izazov – geopolitička slika 21. stoljeća nikad je zamršenija, a u kontekst nacionalne sigurnosti ulazi i niz nekonvencionalnih prijetnji koje često i nadilaze one konvencionalne.

Na samom kraju, autorovo mišljenje je da je budućnost, nakon kratkog stadija predvidivosti, ponovno ušla u kaotičnu neizvjesnost. U trenutku pisanja ovog rada, politička slika svijeta, narušena ratom u Ukrajini, sukobom Izraela i Palestine te nizom dodatnih oružanih sukoba, neminovno zahtijeva još veću spregu obavještajnog i izvršnog sektora političkih i vojnih tijela. U oceanu informacija koje nas preplavljuju svake sekunde, ponekad je samo jedna kap dovoljna kako bi se donijela ispravna odluka s potencijalno dalekosežnim posljedicama. Obavještajni analitičari, po svemu sudeći, nastavit će ulagati značajan dio napora kako bi se pronašla ta kap.

8. Literatura

Block, Ludo (2023) The long history of OSINT. *Journal of Intelligence History* 22(3). https://www.tandfonline.com/doi/full/10.1080/16161262.2023.2224091 Pristupljeno 16.01.2024.

Davies, Philip H. J. (2021) ISR versus ISTAR: A Conceptual Crisis in British Military Intelligence. *International Journal of Intelligence and Counterintelligence* 35(1): 73-100. https://bura.brunel.ac.uk/bitstream/2438/22272/3/FullText.pdf Pristupljeno 20.01.2024.

Fabijančić, Tomislav (2017) *Vojni stožeri.* Zagreb: Hrvatsko vojno učilište.

Freeman, Wes i dr. (2003) PURPLE Revealed: Simulation and Computer-Aided Cryptanalysis of Angooki Taipu B, *Cryptologia* 27(1): 1-43. https://cryptocellar.org/pubs/purple-revealed.pdf Pristupljeno 18.01.2024.

Garlauskas, Markus V. (2003) Intelligence Support for Military Operations. https://apps.dtic.mil/sti/pdfs/ADA524838.pdf Pristupljeno 19.01.2024.

George, Roger Z. i Bruce, James B. (2008) *Analyzing Intelligence: Origins, Obstacles and Innovations*. Washington D.C.: Georgetown University Press.

Hayes, Joseph (2007) *Analytic Culture in the U.S. Intelligence Community.* https://web.archive.org/web/20070613085543/https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/analytic-culture-in-the-u-s-intelligence-community/index.html Pristupljeno 16.01.2024.

Hart, B. H. Liddell (1991) *Strategy.* https://archive.org/details/strategy-b.-h.-liddell-hart Pristupljeno 21.01.2024.

Headquarters, Department of the Army (2019) The Operations Process (ADP 5-0). https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN18126-ADP_5-0-000-WEB-3.pdf Pristupljeno 19.01.2024.

Heuer, Richards J. (1999) *Psychology of Intelligence Analysis.* https://www.cia.gov/static/Pyschology-of-Intelligence-Analysis.pdf Pristupljeno 16.01.2024.

Horne, Barry (2002) Visualising the Electronic Order of Battle. https://apps.dtic.mil/sti/pdfs/ADP013309.pdf Pristupljeno 15.01.2024.

hrvatski-vojnik.hr (2017) Simulacijski sustav SATTS. https://hrvatski-vojnik.hr/simulacijski-sustav-satts/ Pristupljeno 21.01.2024.

Joint Chiefs of Staff (2013) Joint Intelligence (JP 2-0). https://web.archive.org/web/20160613010839/http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf Pristupljeno 08.01.2024.

Kostyuk, Nadiya i Zhukov, Yuri M. (2017) Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events? *Journal of Conflict Resolution* 63(2): 317-347. https://journals.sagepub.com/doi/10.1177/0022002717737138 Pristupljeno 21.01.2024.

Krizan, Lisa (1999) *Intelligence Essentials for Everyone.* https://web.archive.org/web/20090524045712/http://www.ndic.edu/press/8342.htm# Pristupljeno 17.01.2024.

Kulshrestha, Sanatan (2016) Big Data in Military Information and Intelligence. https://shorturl.at/otIU7 Pristupljeno 20.01.2024.

Lowenthal, Mark M. (2019) *Intelligence: From Secrets to Policy – 8th Editon.* Washington D.C.: CQ Press.

Mateski, Mark (2009) Red Teaming: A Short Introduction. https://archive.ph/20171205132811/https://redteamjournal.com/papers/A%20Short%20Introduction%20to%20Red%20Teaming%20(1dot0).pdf Pristupljeno 17.01.2024.

Mitchell, Kwasi i dr. (2020) The Future of Intelligence Analysis. https://www2.deloitte.com/content/dam/insights/us/articles/6306_future-of-intel-analysis/DI_Future-of-intel-analysis.pdf Pristupljeno 10.01.2024.

National Intelligence Council - NIC (2021) The Future of the Battlefield. https://www.dni.gov/files/images/globalTrends/GT2040/NIC-2021-02493--Future-of-the-Battlefield--Unsourced--14May21.pdf Pristupljeno 20.01.2024.

National Geospatial-Intelligence Agency – NGA (2016) Geospatial Intelligence. https://slideplayer.com/slide/4175372/ Pristupljeno 17.01.2024.

Nolan, Cynthia (2015) Understanding the Intelligence Cycle: A Review. *Journal of Strategic Security* 8(4): 114-116. https://www.jstor.org/stable/pdf/26465219.pdf?refreqid=fastly-default%3A5961506dc292dc20514721347740a972&ab_segments=0%2Fbasic_phrase_search%2Fcontrol&origin=&initiator=search-results&acceptTC=1 Pristupljeno 12.01.2024.

oracle.com (2023) What is Big Data? https://www.oracle.com/big-data/what-is-big-data/ Pristupljeno 20.01.2024.

reuters.com (2021) U.S. spied on Merkel and other Europeans through Danish cables. https://www.reuters.com/world/europe/us-security-agency-spied-merkel-other-top-european-officials-through-danish-2021-05-30/ Pristupljeno 13.01.2024.

Sigurnosno-obavještajna agencija – SOA (2022) Javno izvješće za 2022. godinu. https://www.soa.hr/files/file/Javno-izvjesce-2022.pdf Pristupljeno 09.01.2024.

Steele, Robert D. (2010) Human Intelligence: All Humans, All Minds, All the Time. https://www.jstor.org/stable/pdf/resrep11435.pdf?refreqid=fastly-default%3Aa20146e662f2a5c0aa9011ca44434fa4&ab_segments=&origin=&initiator=&acceptTC=1 Pristupljeno 14.01.2024.

Tzu, Sun (2022) *Umijeće Ratovanja.* Zagreb: Mozaik knjiga.

US Geospatial Intelligence Foundation – USGIF (2016) 2016 State of GEOINT Report. https://web.archive.org/web/20180127172804/http://usgif.org/system/uploads/4510/original/2016_SoG_book.pdf Pristupljeno 16.01.2024.

Ziezulewicz, Geoff (2021) The Navy is Testing This Adorable Sailboat Drone. https://www.defensenews.com/news/your-navy/2021/12/13/the-navy-is-testing-this-adorable-sailboat-drone/ Pristupljeno 20.01.2024.

Weinberger, Sharon (2017) The Graveyard of Empires and Big Data. https://foreignpolicy.com/2017/03/15/the-graveyard-of-empires-and-big-data/ Pristupljeno 20.01.2024.

Winkler, Jonathan R. (2009) Information Warfare in WWI. *The Journal of Military History* 73(3): 845-867. https://muse.jhu.edu/article/270202 Pristupljeno 15.01.2024.

Mateo Matić

OBAVJEŠTAJNA ANALIZA I DONOŠENJE ODLUKA

Sažetak

Cilj ovog rada je pojašnjavanje odnosa između obavještajnog djelovanja, posebice obavještajne analize, te procesa donošenja političkih i vojnih odluka. Rad se temelji na premisi da je kvalitetna i pravovremena obavještajna procjena jedna od najvažnijih alata u rukama donosioca odluka, bili oni zapovjednici na svim razinama vojne strukture ili pak političari i ostali donositelji politike na ključnim pozicijama. Rad najprije polaže temelje približavajući čitateljima važnost obavještajnog ciklusa, te zatim pojašnjava specifičnosti različitih obavještajnih disciplina te metoda obavještajne analize. Glavni dio rada fokusira se na obavještajnu potporu donositeljima odluka (zapovjednicima) na sve tri vojne razine – taktička, operativna i strateška. Posljednji dio rada daje kratki osvrt na važnost neprestanog razvoja tehnologije i utjecaj tog razvoja na obavještajnu djelatnost, kao i vojni sektor.

Ključne riječi: Obavještajna analiza, proces donošenja odluka, vojna strategija, donositelji odluka

Mateo Matić

INTELLIGENCE ANALYSIS AND DECISION-MAKING

Summary

The aim of this thesis is to closely examine the relationship between intelligence activities, especially intelligence analysis, and the process of political and military decision-making. The paper is based on the premise that a high-quality and timely intelligence assessment is one of the most important tools in the hands of decision-makers, be they commanders at all levels of the military structure or politicians and other policy makers in key positions. The paper first lays the foundations by highlighting the importance of the intelligence cycle to the readers, and then explains the specifics of different intelligence gathering disciplines and methods of intelligence analysis. The main part of the thesis focuses on intelligence support for decision makers (commanders) at all three military levels - tactical, operational, and strategic. The last part of the thesis gives a brief overview of the importance of the continuous development of technology and the impact of this development on intelligence, as well as the military sector.

Keywords: Intelligence analysis, decision-making process, military strategy, decision-makers