UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

Vojko ADAMIČ

Mentor:
doc. dr. Iztok Prezelj

Obveščevalna dejavnost, nadzor prostora, določanje ciljev in izvidništvo (ISTAR) v Slovenski vojski

SPECIALISTIČNO DELO

Ljubljana, 2010

Obveščevalna dejavnost, nadzor prostora, določanje ciljev in izvidništvo (ISTAR) v Slovenski vojski

POVZETEK

Obveščevalna dejavnost navadno države izvajajo zato, da bi si pridobile podatke o dogajanjih v interesnih območjih, ki bi lahko vplivala na varnost, nemoten razvoj in druge pogoje delovanja in obstoja teh držav. Opisali smo značilnosti obveščevalne dejavnosti nasploh in se bolj podrobno posvetili vojaški obveščevalni dejavnosti. V tej nalogi predstavljamo ISTAR kot najsodobnejši sistem vojaške obveščevalne dejavnosti; najprej z nekaj teoretičnimi izhodišči, v nadaljevanju pa še z opisom ISTAR sistemov NATO in EU ter medsebojno primerjavo ISTAR sistemov v Kanadi, Nizozemski, Veliki Britaniji. Sistemi vseh treh držav so v analizi dobili pozitivne ocene, ugotovili pa smo, da ima Kanada slabši sistem od Nizozemske, ta pa od Velike Britanije.

V nalogi je poleg tega podrobno predstavljen sedanji vojaški obveščevalni sistem v Slovenski vojski, ki ga primerjamo s sistemi prej omenjenih držav. V tej primerjavi ugotovimo, da daleč zaostaja za zahtevami sodobnih obveščevalnih sistemov.

Na koncu predstavimo predlog variante novega obveščevalnega sistema SV po principih delovanja ISTAR sistema. V primerjalni analizi s sistemi omenjenih je predlog dobil pozitivno oceno in pokazal, da je pomanjkljivosti sedanjega obveščevalnega sistema SV možno z nakupom opreme in spremembo načina delovanja relativno hitro odpraviti in se približati zahtevam sodobnega obveščevalnega dela.

KLJUČNE BESEDE

Vojaška obveščevalna dejavnost, obveščevalni podatek, vojaška obveščevalna služba, obveščevalni krog, ISTAR.

Intelligence, Surveillance, Target Acquisistion and Recconnaissance (ISTAR) in the Slovenian armed forces

ABSTRACT

States use intelligence to gain or collect information about issues in their area of interest that might influence security, further development or other interest of acting country. We described intelligence in general in this thesis and focused afterword on the military intelligence, ISTAR is such intelligence system, and we described it in this thesis first in theory and than in sequel also with detailed look into the Canadian, Dutch, Britanian, NATO and EU ISTAR concepts. NATO and EU ISTAR concepts were our guidance when we analysed and compared the Canadian, Dutch, and Britanian ISTAR systems. They all fulfil requirements in the comparison and gain positive grade although we found more faultiness in the Canadian system than in the Dutch one and they were both less developed than ISTAR in the Great Britain.

We also presented the current Slovenian military intelligence system and compared it with the three mentioned countries. The current Slovenian system turned out as far behind mostly due to technical inferiority, undeveloped connection and planning failures.

Thesis is concluded with a proposal for the future Slovenian ISTAR system. It is compared with above-mentioned countries under the same criteria with positive grade. It became evident that current deficiencies in the Slovenian military intelligence system could be rectified in a relatively short time procuring new, contemporary equipment and changing philosophy, culture and practise within the intelligence community.

KEYWORDS

Intelligence activity, intelligence data, military intelligence service, intelligence circle, ISTAR.

KAZALO SLIK

1 UVOD

Strateško varnostno okolje Republike Slovenije se zaradi procesa globalizacije, razvoja informacijske družbe, hitrega razvoja azijskih trgov, katastrofalnih življenjskih razmer v mnogih državah tretjega sveta, okoljskih sprememb in drugih vzrokov spreminja. Nestabilnost, grožnje in tveganja, ki iz tega izhajajo, predstavljajo glavni izziv globalne varnosti. Pomen klasičnih vojaških groženj se sicer zmanjšuje, čeprav jih dolgoročno ni moč izključiti. Nadomeščajo jih "sodobne" oblike ogrožanja varnosti, med katere najpogosteje uvrščamo mednarodni terorizem, ilegalne migracije, organizirani kriminal, trgovino z mamili in belim blagom, ekstremizem, različna etnična gibanja, verski fanatizem, okoljske probleme, proizvodnjo in promet z nevarnimi biološkimi, kemičnimi in jedrskimi snovmi ter zlorabo interneta. Glavne značilnosti naštetih groženj so asimetričnost delovanja, kompleksnost, transnacionalni značaj, raznovrstnost in nedoločljivost struktur.

Obveščevalna dejavnost na obrambnem področju predstavlja pomembno mesto v vodenju vodilnih političnih struktur in vojaških oseb. Njen osnovni namen je zagotoviti pomembne informacije politikom in vojaškim poveljnikom za nemoteno in uspešno izvajanje nalog.

Pravočasna in pravilna uporaba (upoštevajoč politiko proaktivnega odzivanja) obveščevalnih informacij lahko prepreči nova konfliktna stanja, jih omili ali omeji ter prepreči teroristične napade.

Spremenjeno strateško in varnostno okolje, vstop Slovenije v NATO in EU, spremenjena poslanstva in naloge obrambnega podsistema nacionalne varnosti ter sprejeti cilji sil terjajo prilagoditve (spremembo organiziranosti) obveščevalne dejavnosti na obrambnem področju. V obeh organizacijah in delu njunih članic je ISTAR[1] prepoznan kot zmogljivost, ki bo sposobna pravočasno usmerjati in povezovati obveščevalne vire, sistematično urejati in vsestransko analizirati pridobljene in shranjene informacije ter jih varno in pravočasno posredovati uporabnikom v obliki ocen, opozoril, celovitih informacij itd.

V Sloveniji je obveščevalno-varnostna dejavnost na obrambnem področju opredeljena v Zakonu o Obrambi in dopolnilih, ki opredeljujejo Obveščevalno varnostno službo (OVS) Ministrstva za obrambo kot nosilko te dejavnosti tako za potrebe Ministra za obrambo kot

[1] ISTAR – angleška kratica za Intelligence, Surveillance, Target Acquisition, Recconnaissance oziroma prevedeno v slovenščino: Obveščevalna dejavnost, nadzor, določanje ciljev in izvidništvo.

tudi SV. Prav tako določa, da ima SV lastno obveščevalno strukturo, ki je organizirana kot štabni organ na vseh nivojih poveljevanja do bataljona. Formacija SV opredeljuje organiziranost in poslanstvo specializiranih enot, ki zbirajo različne obveščevalne podatke doma in v tujini, vendar v SV ni enote, poveljstva ali zavoda, ki bi načrtno zbiral, urejal in analiziral te podatke. Načeloma bi to morali izvajati analitični odseki štabnih obveščevalnih organov na ravni Poveljstva sil in GŠSV[2], vendar sistem ni zaživel.

Povezanost OVS in obveščevalnih organov SV je sicer načelno določena, v praksi pa ni zaživela, kljub temu da operativce OVS pošilja na misije SV v operacijah kriznega odzivanja v vlogi obveščevalnih častnikov.

Na nek način ta element poveljevanja pri delu poveljnikov ni prisoten; deloma zato, ker v Sloveniji ni občutiti neposredne nevarnosti vojaškega spopada; deloma zato, ker v tujini to vlogo prevzemajo pripadniki OVS, deloma pa zato, ker v SV ni sistematičnega pristopa k obveščevalni dejavnosti in ustrezne kadrovske popolnjenosti.

Po uspešno opravljeni nalogi v času osamosvojitvene vojne v Sloveniji leta 1991 smo vodilni častniki manevrske strukture narodne zaščite izdelali analizo celotnega projekta z vojaškega stališča. Pri tem smo izpostavili štiri dejavnike, ki so odločilno vplivali na vojaško izvedbo osamosvojitve. Med njimi je bila na prvem mestu naša odlična obveščevalna organiziranost, ki je uspela načrtno pokriti vse nivoje organiziranosti, življenja in dejavnosti nasprotnika. Na žalost je ta uspeh danes zanikan, in ne navdihuje novih rodov poveljnikov niti obveščevalcev, mene pa ta izkušnja spremlja še vedno in v uveljavitvi ter zgraditvi ISTAR sistema vidim vrnitev obveščevalne dejavnosti SV nazaj v mednarodno priznane okvire stroke.

V sklopu tega nas zanimajo oborožene sile (struktura, oborožitev, doktrina ipd.), biografije pomembnih osebnosti, ekonomija, geografija (predvsem vojaški aspekti terena, kot so prehodnost, kanaliziranost zemljišča, rastlinstvo, sestava tal, naseljenost, ipd.), klima, zunanja in notranja politika tujih držav, znanstveno-tehnično področje, populacijski dejavniki, transportne zmožnosti in zdravstvo (Purg 2002, 15–16). Obveščevalna služba (agencija) je tudi institucija, v katero pripadniki vstopajo prostovoljno, pri čemer gre praviloma za visoko motivirane posameznike.

[2] Generalštab Slovenske vojske

Temeljno poslanstvo vojaške obveščevalne službe je obveščevalna podpora oboroženim silam. Naravo vojaške obveščevalne dejavnosti lahko pojasnimo s pomočjo definicije obveščevalnega sistema, kot jo navaja ameriško obrambno ministrstvo:

"Obveščevalni sistem je vsak formalni ali neformalni sistem, ki se ukvarja s pridobivanjem, obdelavo in interpretacijo podatkov in ki odločevalcem zagotavlja razumno presojo za delovanje. Termin ni omejen le na obveščevalne organizacije ali službe, ampak opisuje tudi katerikoli drug sistem v vseh njegovih delih, ki izpolnjuje zgoraj navedene naloge" (Dictionary of Military and Associated terms, 2009).

Tudi Đorđević (Đorđević v Purg 2002, 19) v tem smislu pravi, da "sintagma obveščevalni sistem pomeni funkcije, organizacije, njihov stroj, medsebojne odnose in načela, ki predstavljajo zaokroženo celoto".

V zvezi z vojaško obveščevalno dejavnostjo SV lahko slišimo dvome, ali gre v tem primeru sploh za obveščevalno dejavnost (Kolenc 2006). Zakonsko namreč v Republiki Sloveniji ni urejena, ni organizirana kot služba in nima nobenih pooblastil za uporabo posebnih metod in sredstev za pridobivanje podatkov. (Kolenc 2006) kljub vsemu trdi, da gre za zvrst vojaške obveščevalne dejavnosti. Zadnjo trditev sem s proučevanjem problematike sprejel kot veljavno in jo uporabil v tej nalogi.

Vedno hitrejši pretok informacij, kompleksnost odnosov med različnimi državami in združbami v svetu, večplastnost bojevanja v sodobnih, pogosto asimetričnih pogojih vojne in pojavljanje novih, še nepoznanih oblik ogrožanja varnosti za obveščevalne službe predstavlja velik izziv. Nujnost boljše povezanosti, hitrega posodabljanja ocen na osnovi informacij, pridobljenih s sodobnimi obveščevalnimi tehnikami in sredstvi ter učinkovite, varne in neposredne komunikacije med odločevalci in obveščevalci, je vedno bolj očitna. Sistem ISTAR je sodoben odgovor na te izzive.

Obveščevalna dejavnost, nadzor, določanje ciljev in izvidništvo oziroma ISTAR je okrajšava, uporabljena za opis »sistema sistemov«, ki vključuje izdelke v stopnjah zbiranja, usmerjanja in obdelave v obveščevalnem ciklusu ter procesa določanja ciljev. Zagotavlja informacije in obveščevalne podatke za realizacijo CCIR[3] in PIR[4] ter podpira manevrirne in napadalne

[3] Poveljnikove zahteve po kritičnih informacijah predstavljajo osnovo za načrtovanje obveščevalnih dejavnosti
[4] Prioritetni zahtevki za informacije nastajajo v teku vojaških dejavnosti za naknadno usmerjanje obveščevalne dejavnosti

udarne sisteme.

Sistem ISTAR zagotavlja uresničitev vedno večjih potreb, ki jih pred obveščevalni proces postavlja manevrsko bojevanje. Večnacionalne operacije od sistema ISTAR zahtevajo tudi njegovo maksimalno interoperabilnost.

Učinkovito delovanje sistema ISTAR zahteva, da vse njegove komponente delujejo na skupnih standardih ter da celotna operacija ISTAR temelji na skupni doktrini. Kadar morajo biti operacije ISTAR opravljene na večnacionalni podlagi, je prej navedena zahteva bistvena za uspeh. Osnovni princip delovanja je centralizirano vodenje in decentralizirano izvajanje nalog.

V nalogi želimo proučiti izkušnje pri graditvi sistema ISTAR v tujini in predlagati take rešitve pri nadaljnji graditvi obveščevalnih zmogljivosti SV, ki bodo povezljive s tujimi in istočasno prilagojene posebnostim Slovenske vojske. Pri tem bomo izhajali iz domneve, da ima trenutno SV zelo razdrobljeno obveščevalno dejavnost in slabo povezano v celovit sitem vodenja in poveljevanj. Vedno bolj zahtevne operacije, v katere se vključuje SV, pa že zaradi vedno bolj zahtevne zaščite lastnih sil narekujejo potrebo po bolj zmogljivih in lažje povezljivih obveščevalni zmogljivosti že v bližnji prihodnosti.

Naloga bo sledila naslednjim ciljem:

1. **Izpostavitev teoretična izhodišča za posodobitev obveščevalne dejavnosti.**
2. **Predstavitev koncepta obveščevalne dejavnosti v Slovenski vojski.**
3. **Predstavitev koncepta ISTAR v zvezi NATO, EU in na vzorcu izbranih držav.**
4. **Ocenitev možnosti uveljavitve koncepta ISTAR v Slovenski vojski.**

2 UTEMELJITEV RELEVANTNOSTI

(Bajagić 2008) v svojem uvodu ugotavlja, da so varnostne vede in iz njih izvedene raziskave (nacionalna varnost, mednarodna varnost, teorija obveščevalne aktivnosti, sodobni obveščevalno varnostni sistemi, metode obveščevalnega delovanja itd.) relativno mlada področja, ki so šele ob koncu XX. stoletja z razvojem samostojnih kateder varnostnih ved na fakultetah dobile akademski status.

Globoke spremembe mednarodne in globalne varnostne stvarnosti, ki so se dogajale konec prejšnjega in v začetku tega stoletja, so usodno vplivale na mesto, vlogo, cilje, delokrog in metode dela obveščevalnih služb. Glede na to in glede na naloge, ki jih te službe v novem varnostnem okolju dobivajo, se je v demokratičnih družbah za razpravo o umestitvi, organiziranosti, vlogi ter nadzoru nad delovanjem obveščevalno varnostnih sistemov v družbi zelo povečal interes akademske, strokovne in splošne javnosti.

Tudi (Scott in Jackson 2004) k temu dodajata, da je razumevanje obveščevalne dejavnosti v 21. stoletju pogojeno s pogledi znanstvenikov, novinarjev in praktikov na naravo obveščevalne dejavnosti in njene vedno bolj pomembne vloge v nacionalnem in mednarodnem dogajanju. Ob tem še navajata, da lahko pristope raziskovalcev obveščevalne dejavnosti razvrstimo na tri načine.

V prvem raziskovalci izhajajo predvsem iz organizacijskih posebnosti obveščevalnih služb in jih razumejo predvsem kot orodje za zbiranje informacij, ki so potrebne domačim odločevalcem za razumevanje odločitev ali dogajanj v tujini.

V drugem raziskovalci skušajo razumeti ali ponazoriti modele obveščevalnih procesov. Cilj jim je prepoznati in analizirati osebna, politična in organizacijska nasprotja, značilna za obveščevalne organizacije, in njihov vpliv na proces odločanja.

V tretjem raziskujejo predvsem vpliv obveščevalnih služb na politiko in vodenje države. Veliko snovi za raziskave dajejo nedavno odprti arhivi nekdanjih diktatorskih režimov kakor tudi primerjave z vplivom obveščevalnih služb na državno politiko Velike Britanije v času imperializma ali ZDA v 20. stoletju.

(Bajagić 2008) navaja tudi, da analize obveščevalno-varnostnih služb posamezne države v primerjavi s podobnimi službami drugih držav prikažejo številne podobnosti pa tudi razlike.

Področja interesa in končni cilji posameznih služb so različni in odražajo interese njihovih držav. Po drugi strani pa imajo obveščevalne službe s stališča teorije in metodologije delovanja veliko skupnih značilnosti. Na to kaže tudi nekoliko bolj podrobna analiza obveščevalnih sistemov oboroženih sil izbranih držav v tej nalogi.

V zadnjih letih je SV vedno bolj vpeta v mednarodno vojaško dejavnost s članstvom v NATU in EU ter z udeležbo njenih pripadnikov na mirovnih misijah po svetu. Razumevanje pomembnosti obveščevalnih podatkov in poti, po katerih poveljniki zahtevajo in pridobivajo informacije je torej pomembno za uspešno vključevanje v večnacionalne sestave.

(Ferris 2004) v svojem prispevku razmišlja o sodobnih izzivih pri zbiranju in obdelavi vedno večjega števila informacij v kratkem časovnem obdobju. Poudarja vedno večjo vključenost informacijske tehnologije v obvladovanje bojišča s ciljem prehiteti nasprotnika in mu zadati usodne udarce, še preden uspe razviti svoje sile in uresničiti svoje načrte. Ponujeno možnost imenuje po ameriškem vzoru »Netcentric Warfare ali kratko C4ISR[5]«. Pri tem navaja vodilne ustvarjalce tega modela, ki so prepričani, da se bodo s tem pristopom uspešno premaknili iz situacije, v kateri so odločevalci preobremenjeni z zamegljenimi pogledi na bojišče in z oblikovanjem odločitev brez pravih informacij v situacijo, v kateri bodo preobremenjeni z optimiziranjem delovanja v okolju z neštetimi pravimi in pravočasnimi informacijami. Premaknili se bodo torej iz časa odločanja brez pravih ali samo delnih informacij v obdobje, kjer bo odločitev temeljila na skoraj perfektnih informacijah. V NATU in EU so ta sistem poimenovali C4ISTAR ali kratko ISTAR

Od SV je pričakovati, da bo sposobna prispevati tudi svoj doprinos k zbiranju, analiziranju in posredovanju obveščevalnih podatkov za mednarodne potrebe. V ta namen je SV sprejela nekaj obvez in med njimi se je tudi obvezala, da bo v naslednjih nekaj letih organizirala, opremila in usposobila ISTAR enoto za taktično uporabo in več ISTAR elementov za delo v višjih večnacionalnih sestavih. Predpogoj za uspešno mednarodno uveljavitev pa je uvedba podobnega sistema v domače okolje.

Sistem ISTAR v oborožene sile po svetu uvajajo predvsem na osnovi izkušenj iz vojn v Afganistanu in Iraku s ciljem bolj uspešnega boja z vedno bolje organiziranimi nasprotniki Zahoda kot vodilne sile v svetu.

[5] Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance

Pri iskanju virov o ISTAR do sedaj v Sloveniji nisem zasledil domačih del in virov. Obstoječi viri na obveščevalnem področju se osredotočajo predvsem na naslednje vsebine:

- Sistemska urejenost in umeščenost obveščevalne dejavnosti: (Anžič 1996 in 1997; Balant in Čaleta 2006; Buzan 1991; Črncec 2009; Đorđevič 1985; Grizold 1992 in 1994; Kolenc 2006a in b; Prezelj 2005; Purg 2002; Stopar 1997.
- Pravni okvir: Holsti in Kolevi 1991; Purg 1995.
- Uporaba posebnih in tajnih metod delovanja: Lapušina 2004; Vovk 2006; Šaponja 1999.
- Izkukšnje tujih vojska pri obveščevalnem delu: Armor 2003, 2004 in 2006; Finer 1989; Hitl 1959; Holsti, Kalevi 1995; Segal 1993; Žunec, Ozren, Tus A. 1999.

V nalogi bom proučil tuje izkušnje in načrte na področju uveljavljanja sistema ISTAR ter predlagal oblike organiziranosti in opremljenosti domačih ISTAR zmogljivosti. Z izdelavo specialistične naloge na to tematiko želim osvetliti do sedaj neraziskane ali manj proučene vidike delovanja SV.

V nalogi bom o tem razmišljal s stališča poveljnika bataljona ali brigade, ki ta sistem potrebuje za izvedbo svoje naloge. Tak pristop po mojem mnenju omogoča kreativno iskanje za naše potrebe sprejemljivih rešitev in ne le slepo kopiranje rešitev veliko večjih vojaških sistemov.

Sistem ISTAR si lahko predstavljamo kot s sodobnimi komunikacijskimi kanali povezano mrežo zbiralcev, urejevalcev, analitikov in uporabnikov obveščevalnih podatkov, organiziranih v podsisteme dejavnosti. Najbolj običajni so SIGINT[6], IMINT[7], MASINT[8], GEOINT[9], HUMINT[10], WEAPON LOCATING[11] , OSINT [12] in ZAŠČITA SIL[13].

[6] Signal Intelligence – pridobivanje informacij s spremljanjem telekomunikacijskih povezav. Razdeljeno je na COMINT – Communications Intelligence – nadzor radijskega prometa, in ELINT – Electronic Intelligence, kjer gre za nadzor računalniških povezav.

[7] Zbiranje podatkov s pomočjo posnetkov. Ločimo fotografije v vidnem spektru (EO – Electro-Optical), infra rdečem spektru (IR – Infra Red Thermal) in v radarski tehniki (SAR – Synthetic Aperture Radar), ki v slabem vremenu ali skozi oblake lahko da odlično kvaliteto fotografije.

[8] Measurement and Signal Intelligence pomeni pravzaprav odkrivanje sprememb v okolju, ki temeljijo na sledeh, ki jih puščajo živa bitja, oprema ali aktivnosti na površju. Te spremembe so običajno opazne in merljive na različne načine.

[9] Geospital Intelligence je enostavno povedano analiza geografskih podatkov s pomočjo kart ali drugega geografskega materiala. Analizira spremembe zemeljskega površja ali tik pod površino zemlje, ki so lahko posledica naravnih procesov ali človeškega dela.

[10] Human Intelligence pokriva vse oblike pridobivanja informacij od ljudi.

[11] Določanje položaja orožij. Tu gre predvsem za radarske in senzorske sisteme, ki lahko odkrijejo lokacijo minometnih in artilerijskih orožij, ko delujejo, v določenih primerih pa tudi drugo težje orožje in enote.

Ker imajo tudi ti podsistemi svoj notranji ustroj, baze podatkov, analitike in načrtovalce, je glavna naloga ISTAR urejeno in načrtno usmerjanje delovanja podsistemov s ciljem zagotoviti odgovore na naročnikove obveščevalne zahteve.

(Omand 2009) v svojem prispevku opozarja na pasti, v katere lahko zaide obveščevalna organizacija, ki deluje brez jasnih omejitev in jasnih navodil. Ponuja šest usmeritev za delo obveščevalnih zmogljivosti. Te so:

a. Naloga mora temeljiti na zadostnem, dlje trajajočem vzroku.
b. Pri izvedbi naloge mora integriteta obveščevalne zmogljivosti ostati nedotaknjena.
c. Metode in način delovanja morajo biti proporcionalni nevarnosti.
d. Aktivnosti mora odobriti in nadzirati ustrezna avtoriteta.
e. Pri izvedbi naloge mora obstajati realna ocena možnosti za uspeh.
f. Kadarkoli je možno informacije zbrati na javen in odprt način, se je potrebno izogibati uporabi tajnih ali prikritih načinov delovanja.

Iz tega sledi, da si sistem ISTAR ne sme sam postavljati nalog in zahtev in da je nujno potrebno zagotoviti tako transparentnost delovanja, ki onemogoča zlorabe. Zato je pomembno izpostaviti nedeljivo odgovornost poveljnikov za pravilno delovanje takega sistema. Ob tem je potrebno poudariti nujnost visoke usposobljenosti poveljnikov za uporabo tako zmogljivega sistema, ker se nam v nasprotnem primeru lahko izrodi v neobvladljiv stroj ali pa v popolnoma neuporaben kup sodobne tehnologije in razočaranih pripadnikov.

V nalogi bi rad poudaril nedeljivo odgovornost poveljnikov za učinkovito delovanje in uporabo sistema, česar po mojih izkušnjah v SV do sedaj nismo dovolj poudarjali in kar se kaže tudi v precej omejenih zmogljivostih obveščevalne dejavnosti SV.

Predlagano specialistično delo je odraz moje lastne strokovne potrebe po proučevanju delovanja obveščevalnih sistemov doma in v svetu, poleg tega pa znotraj strokovne javnosti v SV in MORS že dlje časa poteka razprava o načinih in oblikah izvajanja obveščevalne dejavnosti SV.

---

[12] Open Sources Intellegence je pridobivanje podatkov iz odprtih virov, kot so internet, tisk in televizija, tiskane publikacije, izjave in drugi uradni ali javno dostopni viri informacij o vseh vidikih dela in življenja določene populacije ali območja.

[13] Force Protection. Pod tem pojmom razumemo serijo različnih senzorjev, ki na temelju zvočnih signalov, IR slike, tresenja tal ali zračnih valov in radarske slike odkrijejo potencialno nevarnost in sprožijo ustrezno reakcijo lastnih sil.

3 HIPOTEZE

Pri izdelavi naloge bomo preverili naslednje hipoteze:

Hipoteza 1:

Slovenska vojska ima sistem varnostno-obveščevalne zagotovitve, ki pa ne dosega standardov NATO in EU.

Hipoteza 2:

Tuje vojske v tej nalogi primerjanih držav članic NATO imajo obveščevalno dejavnost organizirano po načelih sistema ISTAR.

Hipoteza 3:

Sistem vojaške obveščevalne zagotovitve v SV je že danes zgrajen do te mere, da ga lahko z relativno enostavnimi organizacijskimi posegi in tehničnimi posodobitvami hitro približamo sodobnim zahtevam sistema ISTAR.

4 METODE DELA

Pri proučevanju ISTAR bom uporabil naslednje metode:

1. Metoda zbiranja, analize in interpretacije virov.
2. Metoda študije primerov.
3. Primerjalna metoda s programom DEXI.03.
4. Deskriptivna metoda.
5. Opazovanje z udeležbo.

4.1 UPORABA IN ANALIZA PISNIH IN ELEKTRONSKIH VIROV

Metoda analize pisnih virov bo uporabljena pri proučevanju že uveljavljenih teorij, spoznanj in ugotovitev. Vanjo bom vključil različna znanstveno-teoretična in strokovna dela, pa tudi poljubna dela s področja proučevanja tematike specialistične naloge. Mediji bodo knjige, strokovni in poljudnoznanstveni članki, različni statistični podatki, internetne strani znanstvenih, strokovnih in drugih civilnih in vojaških institucij v Sloveniji in tujini. Najpomembnejši vir naloge bodo slovenski normativni dokumenti in sprejeti NATO standardi.

4.2 METODA ŠTUDIJE PRIMEROV

Metoda študija primerov bo temeljila na vsebinskih sklopih (indikatorjih) in bo uporabljena z namenom iz vzorca prikazati trenutno stanje na obravnavanem področju v posameznih državah. Posebnost pri obravnavi tematike s to metodo bo predstavljalo pomanjkanje javno-dostopnih virov o stanju v enotah in državah iz vzorca, zato bo ta del vseboval tudi moja lastna opažanja in ocene.

Obravnavali bomo naslednje primere:

- Koncept ISTAR v EU in NATU, ki sta si podobna. Ta dva koncepta sta za Slovensko vojsko pomembna zato, ker sodelujemo v celi vrsti skupnih operacij kriznega odzivanja po svetu in ker smo se s sprejemom mednarodnih standardov delovanja zavezali k spoštovanju in vgrajevanju opreme, postopkov in organizacijskih oblik, kot jih ti standardi predvidevajo ali predpisujejo.

- ISTAR kopenske vojske Kanade. Zanimivost tega sistema je, da je grajen v relativno veliki oboroženi sili, ki svoje izkušnje nabira na misijah po svetu in je istočasno

članica NATA. Kljub svoji velikosti pa kanadska kopenska vojska ostaja precej klasično organizirana. Kljub temu da je kanadska vojska tehnološko mnogo bolj napredno opremljena, ostaja obveščevalna dejavnost na taktični ravni še vedno v zaostanku za nasprotnikom. To skušajo Kanadčani rešiti z uvedbo ISTAR zmogljivosti in so nam na tem področju podobni. Njihove izkušnje in načrte je zato koristno proučiti in jih uporabiti pri graditvi lastnih zmogljivosti.

- ISTAR zmogljivosti kopenske vojske Velike Britanije (VB). Obveščevalni sistem kopenske vojske VB je zanimiv za proučevanje predvsem zato, ker skrbno kombinira izkušnje iz tekočih operacij po svetu in izkušnje, ki si jih je britanska vojska nabrala v boju z irskimi uporniki na severnem delu otoka. Pri tem na eni strani pospešeno uvaja tehnološko zelo zahtevne opazovalne, analitične in komunikacijske sisteme, na drugi strani pa na taktični ravni še vedno od obveščevalnih organov zahteva klasičen pristop za zbiranje novih obveščevalnih informacij in za njihovo analiziranje na osnovi preteklih izkušenj s Severne Irske in iz okolja, v katerem izvajajo operacije. Kljub temu da je britanska vojska neprimerno večja od slovenske, pa so njene izkušnje in načrti pri graditvi ISTAR zanimivi tudi za nas.

- ISTAR zmogljivosti Nizozemske so za nas zanimive tudi zato, ker je nizozemska vojska med manj številčnimi, vendar aktivno in uspešno vključena v operacije NATA. Obveščevalno dejavnost so razvijali na osnovi izkušenj in jo neprestano preverjali ali dopolnjevali na teh operacijah. Njihov sistem je zgrajen tako, da se modularno vključuje v domače operativne bojne skupine in je istočasno tudi mednarodno povezljiv.

4.3 PRIMERJALNA METODA

S primerjalno metodo organiziranosti vojaške obveščevalne dejavnosti tujih OS bom poskušal ugotoviti primerno organiziranost obravnavanega področja za SV. V nalogi bom uporabil podatke, ki so v izvirniku brez stopnje tajnosti.

Pri tem bom uporabil računalniško orodje DEXI 03. To je računalniško orodje za več-parametrsko odločanje, ki je sposobno medsebojne primerjave več variant rešitev po enakih kriterijih. V orodje vnesemo kriterije, po katerih bomo primerjali različne predloge ali rešitve, jim določimo vrednosti ter medsebojna razmerja. Potem vsak predlog ali rešitev posebej ocenimo glede na vnesene kriterije in vrednosti, orodju pa pustimo, da jih medsebojno

primerja in predlaga optimalno rešitev. Odločitev o najbolj primerni rešitvi je na koncu še vedno prepuščena uporabniku, orodje ponudi le objektivno analizo variant po enakih kriterijih in tehnično najbolj primerno rešitev.

Uporabnost orodja je tudi v tem, da jasno pokaže na pomanjkljivosti rešitev. Posodabljanje rešitev z odpravljanjem pomanjkljivosti je v orodju preprosto in lahko postopek ponavljamo toliko časa, dokler ne najdemo pravega odgovora.

4.4 DESKRIPTIVNA METODA

Deskriptivna metoda bo uporabljena za opis proučevanja in predstavitve dobljenih podatkov in rezultatov.

4.5 OPAZOVANJE Z UDELEŽBO

Pri mojem delu v tujini, posebno pa še pri opravljanju dolžnosti v domovini, sem se srečeval s problematiko sistematičnega usmerjanja obveščevalnega delovanja SV. Dodobra sem spoznal organiziranost, dosežke in omejitve obveščevalnega sistema SV in razlike, ki ga ločijo od podobnih sistemov v vojskah, s katerimi se primerjamo najbolj pogosto.

Tudi v Slovenski vojski smo v zvezi z možnostmi uvajanja ISTAR v uporabo veliko razmišljali, vendar so mnenja in ideje različni. V tej nalogi bom uporabil nekaj razmišljanj in predlogov, do katerih smo prišli pri tem skupnem delu. Kljub temu ti predlogi in mnenja ne odražajo uradnega stališča Slovenske vojske ali Ministrstva za obrambo, temveč le moj osebni pogled na obravnavano tematiko.

V nalogi bom o sodobnem obveščevalnem sistemu razmišljal s stališča poveljnika bataljona ali brigade, ki ta sistem potrebuje za izvedbo svoje naloge. Večina svoje vojaške kariere sem preživel na takih ali podobnih dolžnostih in si nabral kar nekaj izkušenj. Tak pristop po mojem mnenju omogoča kreativno iskanje za naše potrebe sprejemljivih rešitev in ne le slepo kopiranje rešitev veliko večjih vojaških sistemov.

5 OMEJITVE

Pri proučevanju tematike ISTAR se nujno srečamo s problemom tajnosti, saj delovanje obveščevalnih in varnostnih služb, tudi ISTAR , temelji na tajnosti delovanja.

V zvezi s tem je potrebno omeniti problem doktrinarnih obveščevalnih dokumentov, ki so pogosto označeni s stopnjo tajnosti in s tem so javnosti nedosegljivi.

Pri izdelavi specialistične naloge delo otežuje določilo »potrebe po vedenju in potrebe po delitvi podatkov«[14]. Zato v specialistični nalogi uporabljam le javno dostopne vire, ki niso označeni s stopnjo tajnosti. Del virov predstavljajo gradiva delovnih teles NATA za izgradnjo sistema ISTAR in sestavnih delov ter moji zapiski oziroma opažanja. Kot izhodišče za primerjavo ISTAR Velike Britanije, Kanade, Nizozemske bom uporabil koncept Evropske unije in NATA.

[14] Gre za prevod določb »need to know« in »need to share«. Zakon u tajnih podatkih (Ur. list RS št. 135/2003) in akti, sprejeti na njegovi podlagi, govore o možnosti vpogleda in posredovanja tajnega podatka le v primerih, ko sta hkrati združena dva elementa; imetje dovoljenja za dostop do tajnih podatkov in potreba po vedenju (Henigman; 2006: 6).

6 OBVEŠČEVALNA DEJAVNOST

6.1 OBVEŠČEVALNA DEJAVNOST – RADOVEDNOST ALI KAJ VEČ?

Kaj sploh je obveščevalna dejavnost? Kako jo lahko ločimo od vsakodnevnega zbiranja informacij, recimo o tem, v kateri banki ponujajo bolj ugodne kredite ali pri katerem trgovcu lahko kupimo cenejšo zelenjavo? Na ta vprašanja smo v literaturi naleteli na kar nekaj odgovorov in definicij pojma obveščevalne dejavnosti[15]

(Bajagič 2008) ugotavlja, da so skozi zgodovino države vlagale velike napore, da se pravočasno in celovito poučijo o razmerah in stanju v svoji okolici,in pri tem koristile različne možnosti. Na ta način je prišlo do razvoja zunanje politike kot dela državnih aktivnosti, ki so bile namenjene uporabi različnih informacijskih kanalov, predvsem diplomacije, sredstev javnega obveščanja in obveščevalno dejavnost.

Obveščevalno dejavnost Bajagič razume kot specifično in ekskluzivno družbeno in politično dejavnost, ki jo kot osnovno načelo odlikuje tajnost pri delu. Poleg tega se obveščevalna dejavnost v glavnem ukvarja s tajnostmi v družbi, medčloveških odnosih ali znotraj različnih družbenih entitet (država, skupnost držav, organizacije, posamezniki itd.), ki jih skuša odkriti z uporabo posebnih metod dela. Vse to je vplivalo, da se obveščevalna dejavnost razume kot tajna in nezakonita aktivnost, za obveščevalne službe pa se pogosto uporablja naziv »tajne službe«, kar je seveda napačno razumevanje.

Obveščevalne službe so legalni organi državne oblasti, katerih delo temelji na ustavi in zakonih, podzakonskih aktih in drugih pravnih predpisih. Drugo seveda je vprašanje, ali se dejavnosti obveščevalnih služb vedno izvajajo v skladu z zakoni.

Glede na potrebe in cilje nosilcev državne oblasti obveščevalna dejavnost obsega zunanjo obveščevalno dejavnost, kontraobveščevalno dejavnost in druge naloge varnosti države (zaščita ustavne ureditve, integriteta, suverenost in ozemeljska celovitost države, terorizem, organizirani kriminal, orožje za masovno uničevanje itd.).

Warner (2009) o obveščevalni dejavnosti razmišlja tako, da v teoriji preizkuša ustreznost definicij, kot so jih opredelili različni ameriški avtorji ali institucije in poskuša poiskati najbolj ustrezno. Poglejmo si nekaj njegovih izhodišč:

[15] Pomen angleške besede »Intelligence« je večplasten, zato bom v tej nalogi za to besedo v slovenskem prevodu uporabljal izraz »obveščevalna dejavnost«.

Tako temeljna listina ameriških obveščevalnih agencij – »The National Security Act of 1947[16]« opredeljuje obveščevalno dejavnost kot informacije, ki se nanašajo na zmogljivosti, namene ali aktivnosti tujih vlad ali tujih elementov, organizacij ali posameznikov (Warner 2009, 6).

»The Hoover Commission[17]« je v poročilu za ameriški Kongres o obveščevalnih dejavnostih leta 1955 opredelila obveščevalno dejavnost kot dejavnost, ki se ukvarja z vsemi stvarmi, ki bi morale biti poznane, preden se sproži določen način delovanja (Warner 2009, 8).

»The Brown-Aspin Report[18]« je v letu 1996 za ameriško vlado ponudil pogled na razvoj ameriških obveščevalnih zmogljivosti in nalog v 21. stoletju in pri tem obveščevalno dejavnost opredelil kot informacije o tujih zadevah – ljudeh, prostoru, dogajanjih in stvareh, ki jih vlada potrebuje za izvajanje njenih funkcij (Warner 2009, 7).

Zadnji »Dictionary of Military and Associated Terms«, ki ga je ameriško obrambno ministrstvo izdalo leta 2009, na strani 208 opredeljuje obveščevalno dejavnost kot:

a) izdelek, ki nastane kot rezultat zbiranja, procesiranja, združevanja, analiziranja, ocenjevanja in razlaganja razpoložljivih informacij, ki se nanašajo na tuje države ali območja;

b) informacijo ali znanje o nasprotniku, ki si ga pridobimo z opazovanjem, preiskavami, analizami in razumevanjem posebnosti.

CIA je leta 1999 v enem od svojih biltenov pri tej debati sodelovala z oceno, da je obveščevalna dejavnost enostavno poznavanje sveta in predvidevanje o bodočnosti sveta okoli nas kot osnova za odločanje in delovanje ameriške vlade. Sherman Kent[19], priznani vodilni analitik v CIA, je obveščevalno dejavnost opredelil kot znanje, ki ga morajo imeti ameriški visoki civilni in vojaški voditelji, da lahko varujejo nacionalne pridobitve (Warner 2009, 4).

[16] The National Security Act of 1947 je dokument, ki ga je sprejel Ameriški kongres 26. julija 1947 kot temeljni usmerjevalni dokument, v katerem je bila jasno opredeljena varnostna politika ZDA in dane usmeritve za organizacijo, način delovanja in koordinacijo obveščevalno-varnostne dejavnosti med zvrstmi znotraj vojske in med vojsko ter drugimi obveščevalnimi ali varnostnimi organi ameriške države.
[17] To je bila ameriška vladna komisija, ki je junija 1955 pripravila poročilo o obveščevalni dejavnosti ZDA za Kongres pod imenom »Intelligence Activities«.
[18] Poročilo je bilo namenjeno usmeritvam za delovanje obveščevalnih služb v 21. stoletju in ga je imenovana komisija izdelala leta 1996.
[19] Citat je iz njegove knjige »Strategic Intelligence for American Foreign Policy«, izdana 1949.

Nekdanji namestnik direktorja CIA Vernon Walters je v svojih spominih – »Silent Missions« iz leta 1978 na strani 621 ponudil definicijo obveščevalne dejavnosti kot informacijo, ki ni vedno na voljo v javnem življenju, o moči, virih, zmogljivostih in namenih tujih dežel, ki lahko vplivajo na življenje in varnost ameriških državljanov (Warner 2009, 5).

Vse naštete obrazložitve so si podobne in izpostavljajo informacijo kot bistven element obveščevalne dejavnosti, vendar (Warner 2009) razmišlja širše in ugotavlja, da je morda informacija za poveljnike ali politike dovolj, vsekakor pa ni dovolj za tiste, ki se ukvarjajo z obveščevalno dejavnostjo. Vzemimo na primer telefonski imenik. Od ogromne količine informacij v imeniku običajno potrebujemo le nekaj telefonskih številk ali naslovov tistih, ki jih poznamo ali želimo poklicati. Prav tako lahko dobimo veliko informacij iz prospektov, časopisov, revij, zemljevidov ipd, pa vendar v običajnem življenju njihove avtorje ne moremo imeti za obveščevalne agente, niti njihova dela niso plod obveščevalne dejavnosti. Torej zbiranje informacij ni dovolj dobra obrazložitev, kaj obveščevalno dejavnost loči od radovednosti.

(Shulsky 2002) v zvezi s tem vprašanjem ugotavlja, da ni enostavno opredeliti značilnosti obveščevalne dejavnosti, ki bi dovolj jasno izražale razlike od vsakodnevne ali znanstvene radovednosti. Ugotavlja, da je ena od skupnih lastnosti obveščevalnih služb ta, da se vse ukvarjajo z zbiranjem ali zanikanjem informacij in se pri tem poslužujejo tajnosti kot ogrinjala, ki drugim preprečuje pogled na metode in rezultate obveščevalnega dela. Povezava med obveščevalno dejavnostjo in tajnostjo je po njegovem bistvena za ločevanje med obveščevalnimi (»intelligence«) in drugimi intelektualnimi (»intellectual«) dejavnostmi.

Vendar tudi v takem razmišljanju lahko najdemo dvom, če skušamo pojasniti, ali so vse prikrite ali tajne aktivnosti v tuji državi res tudi obveščevalna dejavnost. Shulsky je v svojih razmišljanjih zamolčal še eno posebnost obveščevalne dejavnosti in ta je, da je obveščevalna dejavnost vodena z državnega nivoja ali državnih pooblaščencev na osnovi državnih pravnih in drugih aktov.

(Warner 2009, 10) nam na koncu predstavi po njegovem vseobsegajočo definicijo obveščevalne dejavnosti, in sicer obveščevalna dejavnost:

a) je za doseganje polne uporabnosti vezana na uporabo zaupnih virov in metod dela,
b) izvajajo jo državni pooblaščenci in uslužbenci za potrebe države,

c) osredotočena je na tujce, tuje države ter druge tuje subjekte. (če gre za domače subjekte, potem so take aktivnosti del dejavnosti ministrstev za notranje zadeve, pravosodja in drugih državnih inštitucij za notranjo varnost države);
d) vezana je na izdelavo in posredovanje informacij.
e) vključena je v prikrita posredovanje države v tujih entitetah. (če so dejavnosti javne in odprte, potem gre za diplomacijo, oziroma če jih izvajajo uniformirani predstavniki države, potem gre običajno za vojaške akcije).

Kljub temu da se pri iskanju prave definicije obveščevalne dejavnosti zadržujemo že kar nekaj časa, še vedno nisem zadovoljen z zadnjim odgovorom. Verjetno bi bil sprejemljiv pred dogodki v septembru 2001, po tem pa se je narava dela obveščevalnih služb pomembno spremenila.

(Cogan 2004) nam v svojem prispevku pojasni, da so se metode dela obveščevalnih služb po septembru 2001 pomembno spremenile. Metode po novem karakterizira strategija aktivnega, celo napadalnega (»offensive hunt«) lova namesto dotedanjega zbiranja tako ali drugače dostopnih informacij. Ta strategija zahteva toliko virov in aktivnosti, da presega zmogljivosti celo tako velikih služb, kot je CIA. Medagencijsko sodelovanje na nacionalni ravni, mednarodna izmenjava informacij in skupni napori obveščevalnih služb ter specialnih vojaških in policijskih sil so postali nujni in ključni pogoj za doseganje uspeha. Cogan ob tem dodaja, da je še v mirnem času potrebno zagotoviti tudi pravne okvire za tovrstno sodelovanje.

Strategija aktivnega lova vsebuje tudi metode, ki pred 2001 običajno niso bile v naboru klasičnih obveščevalnih služb. Ne zajemajo le lovljenja in potrebe odstranitve vodilnih teroristov, temveč v določenih okoliščinah ignoriranje predpisov, običajnih lokalnih socialnih in vedenjskih navad ter delovanja ali sodelovanja obveščevalnih in varnostnih služb tujih držav.

Sodobni obveščevalci bodo v 21. stoletju iz zbiralcev postali lovci. Ne bodo več pasivno zbirali informacij, jih analizirali in se potem odločali, kaj z njimi, temveč bo večina njihovega dela na lovu za obveščevalnimi sledmi, ki jih bodo pripeljale do ujetja in morda tudi odstranitve teroristov kot trenutno največje grožnje varnosti.

Pri tem bo zaradi obsega in narave aktivnosti vedno bolj vključena vojska, predvsem specialne sile, artilerija, zračne sile in vrhunska tehnologija. Tehnično in organizacijsko je

taka rešitev v celoti sprejemljiva, težava pa nastane pri vprašanju nadzora nad delovanjem obveščevalnih služb in oboroženih sil. Omenjene operacije se namreč izvajajo prikrito ter z ali brez vedenja ali povabila države, v kateri se taka operacija izvaja. V kolikor operacije izvaja vojska, različne nadzorne inštitucije nad delom obveščevalnih služb niso pristojne za nadzor, ker pa gre za tajne operacije v interesu obveščevalnih dejavnosti ali služb, se lahko zgodi, da tudi inštitucije za nadzor nad oboroženimi silami ne morejo v celoti uresničevati svojih nalog.

V ZDA so sprejeli odločitev, da take operacije načrtuje nacionalni varnostni svet, in ki zagotovi nadzor in koordinacijo pri izvedbi. Ne glede na razlike ali podobnosti v rešitvah tega vprašanja v različnih državah, smo se s tem dotaknili etike in zakonitosti pri izvajanju obveščevalne in povezanih dejavnosti.

6.2 ETIKA OBVEŠČEVALNE DEJAVNOSTI

V prejšnjem poglavju smo ugotovili, da je obveščevalna dejavnost tesno povezana s tajnostjo, ki zakriva pogled na metode in rezultate dela. V sodobni, demokratični družbi si težko predstavljamo, da bi država kot inštitucija sama kršila splošne človeške in pravne norme z dejavnostmi, ki temeljito posegajo v integriteto posameznika, združbe ali države. Dilema, kako ohraniti spoštovanje človekovih pravic in istočasno zagotoviti delovanje učinkovitega obveščevalnega sistema, ki se je sposoben zoperstaviti sodobnim grožnjam, je vedno bolj prisotna tako v krogih raziskovalcev obveščevalne dejavnosti kot tudi vlad, parlamentov, politikov, praktikov, civilne družbe in drugih.

(Scott, 2004) ugotavlja, da so tajne akcije zahodnih obveščevalnih služb v času hladne vojne spodkopale legitimnost obveščevalnih služb Zahoda (predvsem ameriških), če ne celo zunanje politike. Kritiki tajnih posegov v času hladne vojne take aktivnosti razumejo bolj kot inštrumentarij za zadovoljevanje lastnih političnih ali ekonomskih interesov ter v cilju nove hegemonije in imperializma.

Dogodki septembra 2001, zadnji poseg v Iraku ter iranska nuklearna kriza so sprožilci novega odnosa javnosti do vprašanja legitimnosti tajnega delovanja obveščevalnih služb. Čutiti je možno manj glasno nasprotovanje družbe do tovrstnih aktivnosti. Pa vendar se Scott sprašuje, ali ne obstaja nevarnost, da bi tiho pristajanje na tajne operacije v tujih okoljih oslabilo legitimnost aktivnosti mednarodnih inštitucij.

(Herman 2004) se sprašuje, ali je sploh potrebno govoriti o obveščevalni dejavnosti in etiki. V Veliki Britaniji nekateri (npr. The Times) razmišljajo, da narodi rutinsko vohunijo drug za drugim, in nekatera uradna razmišljanja[20] British Security Service sporočajo, da se je vohunjenje dogajalo že stoletja prej in bo tako tudi v naprej. Obveščevalna dejavnost je zbiranje informacij, ki direktno ne škodujejo posamezniku. Nekatere službe res izvajajo tajne operacije, ki morebiti lahko zbudijo etične dvome, toda to so njihove dodatne in nikakor glavne dejavnosti.

Pri proučevanju odnosa med etiko in obveščevalno dejavnostjo lahko ugotovimo, da gre pravzaprav za dvoje ločenih razumevanj etike. Eno se ukvarja z moralnimi dilemami družbe v zvezi z uporabo obveščevalnih metod in posledičnimi zakonskimi omejitvami, drugo pa za osebno in kolektivno etiko pripadnikov obveščevalnih služb ter notranja zapisana in nezapisana pravila delovanja.

(Shpiro 2007) zatrjuje, da se etične dileme pojavijo šele, ko se obveščevalec pri delu sreča s svojimi notranjimi dilemami. Etična pravila obnašanja pri delu zagotavljajo set navodil, ki temeljijo na določenih pogledih in opredelitvah vloge obveščevalne dejavnosti v družbi. Ugotavlja, da se etika začne tam, kjer se zakonska ali druga pisna regulativa neha, etičnost delovanja posameznika ali skupine obveščevalcev pa je v mnogočem odvisna od pripravljenosti teh posameznikov za spoštovanje predpisov.

V svojem razmišljanju je dr. Shpiro prišel do zaključka, da etiko obveščevalcev opredeljuje pet kriterijev:

- vztrajanje pri resnici,
- zavarovanje virov tako pred notranjo kot tudi zunanjo javnostjo,
- odklanjanje prikrivanja notranjih napak,
- spoštovanje veroizpovedi
- osebnostni moralni karakter obveščevalca.

Ugotovimo lahko, da je etika obveščevalnega dela kombinacija družbenih norm, opredeljenih v zakonskih in drugih splošnoveljavnih družbenih predpisih, osebnostnih značilnosti obveščevalcev ter notranjih zapisanih in nezapisanih pravil delovanja obveščevalnih služb.

(Omand 2009) raziskuje vpliv sodobnega, agresivnega terorizma na spreminjanje odnosa javnosti do delovanja obveščevalnih služb. Zaradi občutka ogroženosti postajajo tajne in bolj

[20] M15: The Security Service 4th eddition (London: The Stationery Office, 2002), str. 15.

agresivne operacije obveščevalnih služb bolj sprejemljive za ljudi, ki celo sprejemajo omejitve že doseženih lastnih svoboščin v cilju preprečevati delovanje akterjev ogrožanja družbene varnosti. Pri tem izpostavlja, da je vprašanje, koliko časa bo družba še odobravala omejevanje lastnih svoboščin in izvajanje nasilnih oblik delovanja tajnih služb. V ta namen ponuja rešitev v poglobljeni družbeni debati o tej temi ob istočasnem nenehnem dvigovanju ugleda obveščevalnih služb v družbi prav s poudarjenim spoštovanjem družbenih norm.

Pri tem predlaga šest usmeritev za tajno delovanje obveščevalnih služb. Te so po njegovem:

1. Obstajati mora dlje časa trajajoč in zadosten razlog.
2. Zagotovljena mora biti integriteta službe, njenih pripadnikov in virov.
3. Uporabiti je potrebno proporcionalne metode dela.
4. Jasno morajo biti opredeljeni odgovornost in pooblastila.
5. Obstajati mora sprejemljiva možnost uspeha.
6. Tajno delovanje je metoda, ki jo izberemo zadnjo, potem ko vse druge odpovedo.

Prva usmeritev zahteva, da oblikovanje in delovanje določenih obveščevalnih zmogljivosti opredelimo na osnovi ustrezno odobrenega spiska obveščevalnih zahtev. Te pa ne nastanejo same po sebi, temveč v zahtevnem procesu analize situacije in ocene ogroženosti.

Druga usmeritev govori o tem, da je v družbi neprestano potrebno skrbeti za ugled in spoštovanje službe ter ustvarjati zaupanje družbe v delovanje služb. To je dolgotrajen proces, ki ga lahko onemogoči že ena, nestrokovno, neetično ali neodobreno izvedena operacija.

Tretja usmeritev opozarja na ustreznost uporabljenih metod glede na zahtevnost operacije, stopnjo grožnje in načina delovanja nasprotnika. Uporaba nesorazmerno agresivnih metod pri pridobivanju podatkov ali drugih aktivnostih tajnih služb v družbi zbuja dvom o upravičenosti izvajanja operacij in ruši integriteto službe.

Četrta usmeritev zahteva jasno opredeljene odgovornosti za načrtovanje, odobravanje in izvajanje tajnih operacij in delo obveščevalnih služb nasploh ter njihov nadzor. Zunanji nadzor nad delom obveščevalnih služb mora zagotavljati, da kljub varovanju skrivnosti, družbeni mehanizmi lahko uspešno odpirajo še tako občutljiva vprašanja delovanja služb.

Peta usmeritev zahteva, da odločevalci resno pretehtajo rizike, ki jih izvedba neke operacije lahko povzroči za ugled službe, bodoče podobne operacije, mednarodno sodelovanje, politično stabilnost v družbi in podobno. Čeprav je na prvi pogled uspeh operacije

zagotovljen, pa poglobljena analiza možnih posledic za širše družbene interese lahko pokaže več škode kot koristi. V takem primeru operacij v predvideni obliki ne smemo izvajati.

Šesta usmeritev ne potrebuje posebne pojasnitve, saj je prikrito obveščevalno delovanje običajno dražje in bolj zahtevno od javnega, poleg tega pa nosi v sebi kal možnih zlorab, moralnih dilem in kršenja zakonodaje.

(Turner 1986), nekdanji direktor CIA, je ponudil svoje navodilo za odobravanje tajnih operacij: »Obstaja univerzalni test etičnosti izvajanja obveščevalnih operacij. Tisti, ki odobravajo izvedbo takih aktivnosti, se morajo vprašati, ali lahko svoje odločitve uspešno zagovarjajo pred javnostjo, v kolikor informacije o njih pridejo v javnost.«

Pri tem ni imel v mislih, da morajo odločevalci pred odobravanjem oceniti ali izmeriti domače javno mnenje. Nasprotno, menil je, da se ne bi smelo dogoditi, da bi nekdo odobril operacijo, ki bi se je sramoval pojasnjevati v javnosti.

Sodobni, demokratični pristop k zagotavljanju etičnosti delovanja obveščevalnih služb je kombinacija strogega nadzora nad načrtovanjem, odobravanjem in izvedo operacij znotraj linije vodenja, političnega odobravanja občutljivih operacij, ki bi lahko povzročile mednarodne zaplete, in ustreznih mehanizmov za preprečevanje zlorab moči in tajnosti delovanja.

6.3 PRAVNA UREDITEV OBVEŠČEVALNE DEJAVNOSTI

V prejšnjem poglavju smo ugotovili, da je etika delovanja obveščevalnih služb in obveščevalcev kombinacija pravne regulative v državi in moralnih vrednost posameznih obveščevalcev in službe. V tem poglavju bi se rad ozrl na pravno ureditev obveščevalnih dejavnosti.

Posebno v državah, ki so konec prejšnjega stoletja na tak ali drugačen način prešle in enopartijskega, nedemokratičnega sistema v krog držav z zahodnim tipom demokracije, se je zelo spremenila pravna ureditev delovanja in organiziranosti obveščevalnih služb. Precejšnje spremembe so bile deležni tudi pravni akti držav z dolgoletnim demokratičnim ustrojem, vendar predvsem zaradi na novo prepoznanih groženj. Najbolj se je pravna ureditev spremenila zaradi ogrožanja s strani mednarodno organiziranega kriminala (trgovina z belim blagom, proizvodnja in prodaja mamil, nelegalni denarni tokovi, možnost uporabe orožij za masovno uničevanje in ekstremni mednarodni terorizem).

(Bajagić 2008) ugotavlja, da je mesto obveščevalnih služb v strukturi državnih organov in političnih oblastnikov odvisno od načina pristopa nosilcev politične oblasti do procesa odločanja in razumevanja vloge obveščevalnih dejavnosti. To se odraža predvsem z načinom vzpostavljanja uspešnega sistema vodenja, koordinacije, nadzora in kontrole nad elementi obveščevalno-varnostnega sistema, pa tudi z neprestanim ocenjevanjem primernosti in kvalitete izvedbe operacij.

To pomeni, da je mesto in vloga obveščevalnih služb v sistemu politične oblasti odvisna predvsem od narave odnosov med političnimi elitami in obveščevalnimi strukturami, ki morajo temeljiti na jasno opredeljenih pravilih igre (zakonih in drugih predpisih). Medsebojne odnose med obveščevalnimi službami in oblastniki ureja zakon in predpisana linija subordinacije v hiarhiji državne oblasti.

Sodobni obveščevalno-varnostni sistemi v skladu z opredeljenimi nacionalnimi varnostnimi in zunanjepolitičnimi prioritetami temeljijo svoje delo načelno na (povzeto po Bajagić, 2008):

- strategiji nacionalne varnosti,
- ustavi,
- zakonih o nacionalni varnosti,
- zakonih o posameznih obveščevalnih službah, ki podrobneje opredeljujejo področje njihovega dela, organizacijo in način delovanja,
- drugih zakonih, ki se dotikajo področja obveščevalne dejavnosti – na primer Zakon o tajnih podatkih, telekomunikacijah, varovanju osebnih podatkov, zakoni o delovanju vlade, parlamenta, inšpekcijskih služb, kazenski zakonik itd;
- sprejetih mednarodnih zakonskih normah,
- morebitnih bilateralnih ali večnacionalnih sporazumih,
- podzakonskih aktih, pravilnikih in predpisih, ki se nanašajo na subjekte sistema nacionalne varnosti.

Obveščevalno varnostni sistemi demokratičnih držav imajo natančno razdeljena področja dela in pristojnosti. Vzpostavljeni so normativno opredeljeni, natančni mehanizmi nadzora nad delom obveščevalnih služb s strani zakonodajne, izvršne in sodne veje oblasti.

V nasprotju s tem v demokratično manj razvitih državah obveščevalno-varnostni sistemi ne temeljijo na nacionalnih strategijah varnosti, spoštovanju človekovih pravic in svoboščin in demokratičnemu nadzoru nad njihovim delom. Načeloma delujejo pod neposrednim vplivom vladajočih političnih elit, pristojnosti obveščevalnih, varnostnih in protiobveščevalnih

komponent sistema niso jasno opredeljene, očitna je zloraba inštrumenta tajnosti, sistemi nadzora so nerazviti ali zlorabljeni.

(Črnčec 2009) opozarja, da se lahko tudi v politično urejenem, demokratičnem okolju zakonodaja začne spreminjati, tako da so človekove pravice vedno bolj omejene v korist državnih organov in na škodo posameznika. Te spremembe se dogajajo v tistih državah, kjer so soočeni z neposredno nevarnostjo. Nekatere ekstremne primere take prakse lahko označimo kot temno plat uvajanja nove obveščevalne paradigme. Pri tem najbolj izstopata ZDA in Velika Britanija.

V ZDA je tako brez odločbe sodišča dovoljeno spremljati promet in izmenjavo elektronske pošte preko interneta, na pobudo posameznikov se lahko ugotavlja izvor napadov na posamezne računalnike, z odločbo posebnega obveščevalnega sodišča je možno spremljati vse telefone posameznika (pred tem je bila potrebna odločba za vsako telefonsko številko posebej), v določenih pogojih pridržanje sumljivih oseb časovno ni omejeno. Zakonodaja dovoljuje, da civilnim osebam, osumljenim za teroristična dejanja, lahko sodi vojaško sodišče itd.

V Veliki Britaniji so s spremembo zakonodaje ločili pravni red za tujce in lastne državljane. Tako so lahko tujci priprti brez sojenja brez časovnih omejitev in ob uporabi imigracijske zakonodaje brez pravega zunanjega nadzora. Dokazi zbrani z obveščevalno dejavnostjo, prisluškovnajem in prisilo so lahko uporabljeni v sodnih procesih, prav tako je omogočen dostop do davčnh in finančnih podatkov. Spiski sodnikov posebnih tribunalov, ki se ukvarjajo s sodnimi procesi proti domnevnim teroristom, so tajni, prav tako so posebej izbrani odvetniki in morajo imeti dostop do tajnih podatkov (Phythian, 2009).

Posebni pravni primer je določba, da mora posameznik sodišču dokazovati svojo nedolžnost, v kolikor je obtožen teroristične aktivnosti ali povezave s takimi organizacijami.

Slovenija se (Črnčec 2009, 237) tako kot večina evropskih držav ni uklonila evforiji spreminjanja predpisov, ki omogočajo pregloboke posege obveščevalnih služb v človekove pravice.

6.4 POJASNITEV POJMOV VARNOSTI IN OBVEŠČEVALNE DEJAVNOSTI

Obveščevalno-varnostne službe na državnem nivoju tvorijo nacionalni obveščevalno varnostni sistem kot integralni del nacionalnega sistema varnosti. Glede na pomen nacionalne

varnosti v sodobni družbi, sodobne nacionalne varnostne sisteme v najširšem pomenu tvorijo najvišji organi zakonodajne in izvršne oblasti, posebne ustanove zakonodajne in izvršne oblasti, ki so zadolžene za usmerjanje, kontrolo, nadzor, vodenje in koordinacijo obveščevalno-varnostnega sistema, ministrstva, nacionalne obveščevalne inštitucije, civilne in vojaške obveščevalno varnostne ustanove in druge specializirane ustanove izvršne oblasti.

Ko govorimo o obveščevalni dejavnosti in zagotavljanju varnosti, moramo najprej opredeliti pojem varnosti.

Pojem varnosti se pojavlja skozi celotno človeško zgodovino in je v osnovnem pomenu predvsem povezan z eksistencialnimi vprašanji (kakovosti življenja in smrt) posameznika ter njegovega odnosa z višjimi ravnmi družbenega organiziranja (država, meddržavna skupnost, svet kot celota). Prav zaradi te povezanosti je nujno celostno razumevanje pojma varnosti, vključujoč vse vidike človekovega obstoja in delovanja v družbi (ekonomsko, socialno, politično, izobraževalno, obrambno …).

Sodobna nacionalna varnost je vpeta v širše mednarodno okolje, kjer je odgovornost za zagotavljanje varnosti poleg držav in njihovih zvez vse bolj tudi domena globalnega mednarodnega sistema.

Mednarodna varnost pa ni zgolj seštevek nacionalnih varnosti, temveč je celota ukrepov, norm in vrednot, ki se uresničujejo skozi skupno sprejete mednarodne mehanizme in instrumente, ki zagotavljajo obstoj in razvoj vseh držav na ravni mednarodnega sistema[21] (Grizold 1998, 4).

Inštitut OZN za razorožitvene študije (UNIDIR), s sedežem v Ženevi, je izoblikoval naslednjo celostno opredelitev sodobne varnostne paradigme, ki vključuje individualno, državno in mednarodno raven: »Varnost je stanje, v katerem neka država meni, da ji ne grozi nevarnost vojaškega napada, političnega pritiska in gospodarske prisile, tako da se lahko svobodno razvija. Svoboda posameznikov in skupnosti, iz katerih so posamezne države sestavljene, zagotavlja tako obstoj in učinkovito uresničevanje osebnih svoboščin, političnih, socialnih in gospodarskih pravic, pa tudi ohranitev ali obnovitev življenjskega okolja za sedanje in prihodnje rodove.«

[21] Več o tem: Hinsley. 1963. *Power and Persuit of Peace*: 20–29. Cambridge University Press, Cambridge.

Iz predstavljenih definicij varnosti lahko razberemo skupne značilnosti: da je varnost kompleksen pojem, ki ga moramo obravnavati celostno in vsaj v konceptualnih okvirih individualne, nacionalne in mednarodne varnosti. Sam se v tem delu ukvarjam predvsem z nacionalno in mednarodno varnostjo.

Oborožene sile (oborožena sila, armada, vojska) razumem kot specializirano oboroženo organizacijo države, pripravljeno in organizirano za vodenje oboroženega boja. Kot pomemben del organizacije države so tudi glavni inštrument za ohranitev neodvisnosti, ozemeljske celovitosti, obstoječega družbeno-političnega in ekonomskega sistema oziroma za uresničevanje politike vladajočega razreda. Njihova sestava, velikost in opremljenost so odvisni od družbenopolitične ureditve države, stopnje razvoja materialno proizvodnih sil, geografsko-strateškega položaja države, njenih demografskih zmogljivosti, vojne in vojaške doktrine (Gažević 1973, 448 in Dupuy 1993, 1746). Pojem oborožene sile je v mednarodnem vojnem pravu širši kakor v vojaški terminologiji. Po Haškem pravilniku o zakonih in običajih vojne na kopnem iz leta 1907 in Ženevskih konvencijah o zaščiti žrtev vojne iz leta 1949 oborožene sile zajemajo: kopenske, pomorske in zračne sile ter druge oborožene formacije (policijske enote, enote teritorialne obrambe, nacionalne straže, nacionalne garde in razne prostovoljske oborožene formacije), ki po notranjih predpisih posamezne države nosijo zunanje oznake, ne glede na njihovo velikost in specialnost. Del oboroženih sil so tudi enote organiziranih gibanj odpora, ki pripadajo strani v spopadu, ne glede na to, ali delujejo v svoji ali tuji državi, na okupiranem ali neokupiranem ozemlju, pod pogojem, da so njihovi pripadniki vojaško organizirani, da imajo poseben razpoznavni znak, da odkrito nosijo orožje in se držijo pravil vojnega prava, ter prebivalstvo neokupiranega ozemlja, ki je samoinciativno vzelo orožje, da bi se uprlo nasprotnikovi invaziji, ali se zaradi hitrega prodora nasprotnika ni moglo organizirati kot redna oborožena sila, pod pogojem, da odkrito nosi orožje in spoštuje zakone in običaje vojskovanja (Gažević 1973).

Za **obveščevalno dejavnost** (Šaponja 1999) pravi, da je proces, ki zajema zbiranje in analitično obdelavo surovih podatkov ter izdelavo obveščevalnega izdelka, ki ga uporabnik potrebuje pri oblikovanju in sprejemanju odločitev na različnih področjih. Pri obveščevalni dejavnosti v ožjem smislu gre za organizirani proces zbiranja, obdelave in posredovanja podatkov državnim odločevalcem in oblikovalcem različnih politik, pomeni selekcioniranje in postavljanje podatkov v kontekst časa in prostora ter do takrat znanega védenja (o pojavu, dogodku, predmetu, osebi ipd.). Med njene najpomembnejše naloge sodi predvidevanje

razvoja prihodnjih dogodkov in procesov, ki se nanašajo na uporabnika. Obveščevalna dejavnost poteka v krogu, ki ga imenujemo obveščevalni ciklus, je večdisciplinarna in v svojem bistvu intelektualna dejavnost (Kolenc 2006). Kot dejavnost v ožjem smislu je omejena na državne organizacije, katerih delovanje je urejeno z zakoni ali drugimi predpisi, pri čemer zbirajo podatke in izvajajo aktivnosti, ki so sicer prepovedane. Obveščevalna dejavnost v širšem smislu je zavestno in organizirano pridobivanje novega znanja in informacij o dogodkih, pojavih in procesih v bivalnem okolju, naravi, družbi, ki jih potrebujemo pri vsakodnevnem odločanju. Uporaba te dejavnosti ni omejena zgolj na državne specializirane organizacije, marveč je dostopna vsem. Bistvena razlika med informativno in obveščevalno dejavnostjo je v tem, da je obveščevalna informacija analitično obdelan podatek in s tem širša informacija. Podatki, obdelani v obveščevalnem ciklusu, postanejo obveščevalna informacija. Obveščevalna dejavnost postavi vsak podatek v kontekst prostora in časa, skozi prizmo uporabnika (Šaponja 1999, 9, 14, 19 in 56).

Obveščevalni podatek ali **obveščevalni izdelek** (produkt) (angl.: *Intelligence*) je končen proizvod obdelave informacij, ki zadevajo tuje države, sovražnih ali potencialno sovražnih sil ali drugih elementov (organizacij) oz. področja dejanskih ali potencialnih operacij (AAP-6)[22].

Obrambna (vojaška) obveščevalna služba spremlja in analizira globalne varnostno-politične trende, ter preprečuje strateška presenečenja. Pri tem spremlja različne indikatorje, kot so nakupi nove oborožitvene tehnologije, številčno povečanje sestave tujih oboroženih sil (TOS), večje vojaške vaje, večanje zalog in vojaške proizvodnje, spremlja premike enot v bližini meje, povečanje bojne pripravljenosti TOS ipd. V sklopu tega jo zanimajo oborožene sile (struktura, oborožitev, doktrina ipd.), biografije pomembnih osebnosti, ekonomija, geografija (predvsem vojaški aspekti terena, kot so prehodnost, kanaliziranost zemljišča, rastlinstvo, sestava tal, naseljenost ipd), klima, zunanja in notranja politika tujih držav, znanstveno-tehnično področje, populacijski dejavniki, transportne zmožnosti in zdravstvo (Purg 2002, 15–16).

Temeljno poslanstvo obrambne (vojaške) obveščevalne službe (agencije) je obveščevalna podpora oboroženim silam. Ameriška obrambna obveščevalna agencija DIA in avstralska obrambna obveščevalna služba DIO zagotavljata obveščevalne izdelke za potrebe bojevnikov (angl.: *Warfighters*), obrambnih načrtovalcev ter oblikovalcev politik na obrambnem in

[22] Pri prevajanju izraza Intelligence moramo biti pozorni na kontekst, saj ima tri pomene: kot obveščevalna služba, izdelek ali dejavnost (Kolenc, 2006).

varnostnem področju. Poleg oboroženih sil so uporabniki obveščevalnih njunih izdelkov tudi najvišji izvoljeni in imenovani državni uradniki (predsedniki države, vlade, parlamenta, ministri, državni sekretarji ipd). V razvitih obveščevalnih sistemih[23], kot je ameriški, obstaja centralna obrambna obveščevalna služba (DIA), ki koordinira delo "področnih" vojaških obveščevalnih služb, ki delujejo za podporo posameznih zvrsti vojske.

6.5 VOJAŠKA OBVEŠČEVALNA DEJAVNOST V OBOROŽENIH SILAH

Obveščevalno dejavnost na vojaško - obrambnem področju Šaponja deli na obrambno - strateško in taktično (Šaponja 1999, 196–219). Taktična obveščevalna dejavnost je namenjena podpori odločanja za vodenje vojaških operacij. Podatki se zbirajo med razvojem situacije, za razliko od strateške obrambne dejavnosti, pri kateri se dogodki zlasti predvidevajo. Zbiranje podatkov poteka s specializiranimi izvidniškimi enotami in tehničnimi sredstvi, organizirana pa je praviloma v generalštabu (Purg 2002, 15–16). Nižje od generalštaba se v poveljstvih in enotah piramidalno širi vojaška obveščevalna struktura kot del vojaške organizacije. Ta struktura opravlja poslanstvo, ki ga imenujemo z izrazi obveščevalna *zagotovitev, podpora* ali *dejavnost*.

V zvezi z vojaško obveščevalno dejavnostjo[24] SV lahko slišimo dvome, ali gre v tem primeru sploh za obveščevalno dejavnost (Kolenc 2006). Zakonsko namreč v Republiki Sloveniji ni urejena, ni organizirana kot služba in nima nobenih pooblastil za uporabo posebnih metod in sredstev za pridobivanje podatkov. (Kolenc 2006) kljub vsemu trdi, da gre za zvrst vojaške obveščevalne dejavnosti. Zadnjo trditev sem s proučevanjem problematike sprejel kot veljavno in jo uporabil v tej nalogi.

Naravo vojaške obveščevalne dejavnosti lahko pojasnimo s pomočjo definicije obveščevalnega sistema, kot jo navaja ameriško obrambno ministrstvo:

"Obveščevalni sistem je vsak formalni ali neformalni sistem, ki se ukvarja s pridobivanjem, obdelavo in interpretacijo podatkov in ki odločevalcem zagotavlja razumno presojo za delovanje. Termin ni omejen le na obveščevalne organizacije ali službe, ampak opisuje tudi katerikoli drug sistem v vseh njegovih delih, ki izpolnjuje zgoraj navedene naloge" (Dictionary of Military and Associated Terms, 2009).

[23] V ameriški terminologiji se za razvejan obveščevalni sistem države uporablja izraz obveščevalna skupnost (Intelligence Community).
[24] Dejavnost je sinonim za aktivnost (Inštitut za slovenski jezik). Dejavnost je nasprotje od mirovanja in predstavlja neko dinamiko, gibanje, spremembo stanja ipd.

Iz navedene definicije lahko izvedemo tri pomembne sklepe (tudi v Kolenc 2006):

a) Obveščevalno dejavnost lahko izvaja vsak, tudi neformalni sistem (torej tudi sistem v okviru oboroženih sil), ki uporabniku s svojimi izdelki zagotavlja neko razumno presojo. V primeru oboroženih sil (s tem tudi SV) se taki izdelki nanašajo na nasprotnika, ostale grožnje in prostor operacij, uporabnik pa je poveljnik.

b) Da bi neko dejavnost lahko opredelili kot obveščevalno, mora ta obsegati pridobivanje, obdelavo in posredovanje podatkov. Navedene tri dejavnosti predstavljajo temelj metodologije, ki jo imenujemo obveščevalni ciklus. Obveščevalni ciklus je torej temeljna metoda obveščevalne dejavnosti. V SV obstajajo štabni organi in Obveščevalno-izvidniški bataljon, katerih temeljni namen je izvajanje te metodologije.

c) Merilo za to, da je neka dejavnost obveščevalna ali ne, torej ni ne velikost, vrsta ali umeščenost sistema, ki to dejavnost izvaja, niti ne viri ali načini zbiranja podatkov (npr. uporaba posebnih metod in sredstev za zbiranje). Niti ni merilo to, ali je dejavnost zakonsko urejena, ali le s podzakonskimi akti, ali pa sploh ni urejena z nobenim aktom[25].

Pri opredelitvi vojaške obveščevalne dejavnosti si lahko pomagamo tudi z definicijo sistema:

> *Sistem je celota, sestavljena iz istovrstnih ali raznovrstnih elementov, ki so med seboj povezani in odvisni. Sistem oblikuje človek zaradi zadovoljevanja določene potrebe. Nasprotje sistema je kaos, anarhija. Sistem kot entiteta ne obstaja, temveč obstaja v konkretni dejavnosti, zato je sam sistem metodološka značilnost te dejavnosti. Pomembno je, da sistema ne razumemo kot skupek (seštevek po številu) elementov, ampak gre pri tem za svojevrstno kooperacijo, interakcijo, odnose, pravice in dolžnosti* (Grizold 1999, 50–51).

Tudi Đorđević (Đorđević v Purg 2002, 19) v tem smislu pravi, da "sintagma obveščevalni sistem pomeni funkcije, organizacije, njihov stroj, medsebojne odnose in načela, ki predstavljajo zaokroženo celoto".

[25] Svojo obveščevalno dejavnost imajo tudi večje gospodarske organizacije in celo večje kriminalne združbe, pri čemer pa ta dejavnost seveda ni urejena z nobenim aktom (Kolenc, 2006).

Na splošno o vojaški obveščevalni dejavnosti znotraj oboroženih sil lahko govorimo kot o vrsti sistema, ki je nastal kot izraz in metodološka značilnost dejavnosti, s katero se ta sistem ukvarja. Ta dejavnost je pridobivanje, obdelava in posredovanje podatkov o nasprotniku, ostalih grožnjah in prostoru operacij. Ta sistem deluje na podlagi jasnih pravil o dolžnostih in pristojnostih njegovih posameznih elementov, ima svoja načela in ustroj in predstavlja zaokroženo celoto. Ameriška vojska na obveščevalni sistem v okviru oboroženih sil gleda kot na enega od sedmih *bojiščnih sistemov* (angl.: *Battlefield Operating System/ BOS*[26]).

Vojaška obveščevalna dejavnost (VODBE SV) torej predstavlja celoto funkcij, dejavnosti, procesov in ukrepov štabnih organov, enot in posameznikov, s katerimi ti neprekinjeno in celovito spremljajo, analizirajo in predvidevajo vojaško, vojaško-politično in varnostno situacijo ter delovanje nasprotnika, potencialnega nasprotnika in drugih vojaških in varnostnih groženj, s ciljem omogočiti poveljnikom in ostalim v procesu odločanja sprejem pravočasnih odločitev na vseh ravneh PINK (poveljevanje in kontrola) SV (Furlan 2006).

6.6 ISTAR - OBVEŠČEVALNA DEJAVNOST, NADZOR, DOLOČANJE CILJEV IN IZVIDNIŠTVO

6.6.1 Uvod

V svetu, predvsem v velikih vojskah z veliko sodobne tehnologije, kot je recimo ameriška, vedno več pozornosti posvečajo razvoju obveščevalne dejavnosti. V zadnjih dvajsetih letih se je razvila ideja, ki jo Američani imenujejo »revolution in military affairs (RMA)«. Ta predvideva, da bodo informacije in informacijska doba vojski dali toliko novega znanja, da bo to spremenilo naravo vojne.

(Ferris 2009) pojasnuje, da je cilj teh sprememb še nepredstavljiva elastičnost poveljevanja, ki omogoča veliko večjo svobodo oblikovanja sil (in s tem bistveno večjo učinkovitost) v času izvajanja operacij v primerjavi s sedanjim načinom predhodnega, relativno togega načrtovanja delovanja na osnovi predvidevanj namesto dejanskih aktivnosti nasprotnika.

Oblikoval se je nov koncept obveščevalne dejavnosti in poveljevanja. Namera je povečati učinkovitost z uporabo nove informacijske tehnologije in zmogljivosti ter povezanosti sistemov, ki so bili do sedaj oblikovani kot ločena »skladišča« podatkov. Ta koncept vključuje oblikovanje mrežno povezanega bojevanja, v katerem vojska ni povezana

[26] Za bojiščne sisteme glej tudi Žabkar 2003.

piramidno, temveč po shemi ravne plošče, z mrežno komunikacijsko povezavo enot v neposrednem stiku s poveljstvi različnih ravni na različnih lokacijah v sistem, ki lahko vodi operacijo glede na neposredni vpogled v dogajanja na bojišču in okolici. Drugače povedano, je to koncept, ki bo omogočal vojskam, da se organizirajo in delujejo glede na dejanska dogajanja na bojišču ali v okolici in ne samo glede na predvidevanja. Ta koncept se imenuje »Command, Control, Communication, Computers, Intelligence, Surveillance, Target Aquisition and Reconnaissance" ali skrajšano C4ISTAR.

General Fogleman, bivši poveljnik ameriških letalskih sil je v svojem govoru aprila 1995 o informacijskih operacijah kot peti dimenziji bojevanja omenil, da so se vojaki skozi zgodovino bojevanja ne glede kje in za koga so se bojevali, naučili ene veljavne lekcije: »Če lahko analiziraš, deluješ in ocenjuješ hitreje kot tvoj nasprotnik, si zmagal.«

Ferris, (2009) omenja tudi, da oblikovalci RMA razumejo vojno tako kot spretnost in strategijo, kot tudi strelsko učinkovitost. Pravijo, da biti viden pomeni biti ustreljen, biti ustreljen pomeni biti ubit in biti hiter pomeni zmagati.

Večji del ameriških analitikov se strinja (po Ferris 2009), da bo v 21. stoletju zelo pomembna sposobnost vojske za uresničitev svojih ciljev v čimkrajšem časovnem obdobju in tako razumevanje uokvirja razmišljanja o bodoči obveščevalni dejavnosti. Strinjajo pa se, da so obveščevalne službe še vedno organizirane in delujejo po drugačnih principih. Uveljevitev idej oblikovalcev RMA bi za te službe zahtevala revolucijo v kulturi obveščevalne dejavnosti. Taka sprememba bi zahtevala premik z iskanja predvidljivega na širše, intuitivno razumevanje potencialnih nasprotnikov – s fokusa na zbiranje in tehnologijo je potrebno preiti na poudarjanje pomembnosti poznavanja tujih jezikov, kulture in zgodovine.

General Myers[27] je v nekem intervjuju povedal, da so vedno imeli situacijo, v kateri so bili pripadniki obveščevalnih elementov v enem stebru in operativci ločeno v drugem in da so bili res zadovoljni, če so se uspeli pogovarjati med seboj. Spremembe pa zahtevajo, da so neprastano združeni v enovitem procesu odločanja. Ta mora biti nenehno sodelovanje in sinergija do te mere, da operativa pomaga obveščevalni sferi in obratno.

Admiral Cebrowski[28] je o tem povedal, da ima stara obveščevalna organiziranost ogromno podatkov in virov, ki so zbrani in shranjeni v ozko specializiranih in ločenih bazah. Tako je

[27] General Myers, nekdanji predsedujoči načelnikom združenega štaba ameriških sil, januar 2003.
[28] Admiral Cebrowski, direktor projekta preoblikovanja ameriških sil, 2003.

bila organizirana tudi obveščevalna analitika, vsaka specialnost je imela svojo, ki je bila ločena od drugih. Vendar ni potrebno, da ostane tako še naprej. Obveščevalno dejavnost bi lahko organizirali za zahteve po zaščiti sil, zgodnjega opozarjanja in neposredne obveščevalne dejavnosti na bojišču, kjer so izmenjevalci podatkov sposobni poiskati in združevati vse vire informacij, jih integrirati v geografske podlage in proizvajati take obveščevalne produkte, v katerih je možno hitro poiskati pravilne odgovore na zahteve odločevalcev.

Cebrowski nadaljuje, da je obveščevalna dejavnost po letu 1970 postajala vedno bolj neuravnotežena. Količina in kakovost informacij se je neprestano povečevala, analitika pa je ostajala izolirano specializirana za posamezne obveščevalne specialnosti, ne da bi bili na koncu produkti združeni v celovito in realno oceno. Službe so zbirale informacije, ne da bi v ospredje postavljale zahteve »naročnikov«. (Cebrowski 2003) v tistem času vidi rešitev v združevanju vsega zbranega materiala v »Information Dominance Centre ali IDC«, kjer bi se izvajalo nadaljnje urejanje, arhiviranje in analiziranje tako združenih informacij. Ta admiralova ideja predvideva, da lahko analitiki neprestano zbirajo, analizirajo in združujejo informacije ter posodabljajo obveščevalne produkte, upoštevajoč najbolj sveže podatke o sovražniku. Ta neprestano obnavljajoči se sistem izmenjuje in pridobiva obveščevalne produkte v mreži sodobne informacijske tehnologije, v katero so zajeti odločevalci na različnih ravneh do državnga vrha, s ciljem zagotoviti tri osnovne operativno-analitične funkcije: opozarjanje, protiobveščevalno dejavnost in zaščito sil ter neposredno obveščevalno dejavnost na bojišču.

Razumemo lahko, da je sodobna obveščevalna paradigma tesno povezana s hitrim razvojem umetne inteligence in zmožnosti zaznave, prepoznave in ocenjevanja sprememb v okolju. Ta razvoj na prvi pogled vedno bolj izloča človeški faktor in ga nadomešča z vrhunsko tehnologijo, ki v določenih fazah lahko celo avtomatizira analitični in sporočilni proces.

V zvezi s tem se (Ferris 2009) pojavlja še en fenomen. Sodobna tehnologija je namreč omogočila tudi razvoj sodobnih, preciznih, »pametnih« orožij, ki z veliko zanesljivostjo sledijo in uničijo točno določen cilj. Uporaba teh orožij zahteva natančne in sveže podatke o cilju in realne ocene posledic uporabe takih orožij na cilj in okolico. Ta orožja zahtevajo torej natančno in ažurno obveščevalno dejavnost, ki se je sposobna odzivati na sprotne spremembe situacije na bojišču.

Prihajamo torej v čas, ko zahteva po hitrem tempu bojnih operacij postaja realnost, kar tudi

pomeni, da se težišče obveščevalne dejavnosti vedno bolj premika v smer vojaških aktivnosti. To se lahko prepozna tudi v vedno bolj glasni zahtevi poveljnikov taktičnih enot po obvladovanju sodobnih obveščevalnih procesov in produktov za lastne potrebe brez izgubljanja časa in informacij v labirintu komunikacijskih kanalov med različnimi nivoji poveljevanja.

K temu je nedvomno potrebno dodati, da lahko en sam dogodek na bojišču pomembno spremeni tamkajšnje razmere do take mere, da je potrebno posodobiti strateške odločitve. Na drugi strani lahko neustrezne strateške odločitve pomenijo močno omejitev za izvajanje operacij na nižjih ravneh. Temu se v največji možni meri lahko izognemo le z ustrezno vgrajenim človeškim faktorjem in tako komunikacijsko povezavo, ki omogoča istočasno izmenjavo podatkov na vseh ravneh odločanja. Govorimo o sistemu C4ISTAR.

V poglavju 6.1 sem pojasnil, da je ena od značilnosti obveščevalne dejavnosti tajnost delovanja. Ta značilnost v sitemu C4ISTAR še naprej ostaja ena od temeljnih značilnosti, kar postaja ob zahtevi po hitri izmenjavi informacij med naslovniki v široki komunikacijski mreži zahtevna ovira. Široko razpredena komunikacijska mreža namreč pomeni, da je možnost nepooblaščenega odtekanja tajnih podatkov večja. Sistemi zaščite podatkov in sledenja manipulacije s tajnimi dokumenti morajo v razvoju tesno slediti spremenjenim zahtevam. Danes je možno velik del nadzora in zaščitnih ukrepov izvajati avtomatizirano, zato se dobro organizirane obveščevalne službe pri zaščiti lastne dejavnosti in tajnosti podatkov organizirajo v interesu pravočasnega zadovoljevanja bojevnikovih obveščevalnih potreb, kjerkoli se te pojavijo na najnižji možni stopnji tajnosti.

Državni organi za varovanje tajnih podatkov, ki so običajno zunaj obveščevalnih služb, skušajo v obveščevalno razvitih državah slediti naslednjim ciljem (Ferris 2009):

- Sodelovati z oblikovalci politike varovanja tajnih podatkov, tako da je možno obveščevalno dejavnost čimbolj približati potrebam »naročnikov«.
- Razširiti pravice in zmogljivost črpanja obveščevalnih podatkov in produktov, tako da naročniki lahko zahtevajo najbolj sveže podatke in produkte.
- Sodelovati z obveščevalnimi zmogljivostmi pri takem oblikovanju interaktivnih baz podatkov, ki bodo pooblaščenim omogočale čimbolj širok dostop.

Vizija sodobnih, razvitih obveščevalnih služb je zagotoviti dinamično bazo podatkov, ki je kadarkoli in kjerkoli enostavno dostopna pooblaščenim uporabnikom. General Noonan W.

Robert[29] (jr.) omenja »knowledge-centric army«, v kateri bodo analize izvajali z medsebojnim sodelovanjem v distribucijskem okolju ter z množično uporabo zmogljivosti internetno povezanih ekip strokovnjakov. Analitiki na vseh ravneh in na različnih lokacijah bodo združeni v mrežno povezane ekipe strokovnjakov. Vsak analitik bo imel takojšen dostop do vsega vedenja o določeni zadevi. Sodeloval bo pri oblikovanju interaktivne, združene in povezljive zbirke podatkov, ki bodo omogočale ažurno razumevanje obravnavane zadeve. Interesno območje analitikov se bo gradilo in razpadalo okoli posameznih vprašanj. Poveljnik v boju bo v celoti podprt z vsemi sodobnimi analitičnimi zmogljivostmi, ki so bile v prejšnjih obdobjih razdrobljene po ravneh poveljevanja.

In vendar – vsaka medalja ima dve plati. Ob opisanem silovitem razvoju informacijske tehnologije in posedovanju čisto svežih informacij o zadevah, ki nas zanimajo, bi bilo na prvi pogled odločanje bolj enostavno kot včasih. Vendar ni vedno tako! Poplava informacij namreč lahko s seboj nosi nevarnost, da se odločevalci ne bodo nikoli do konca odločili, ker bodo neprestano čakali na nove informacije. (Ferris 2009) piše o »nesigurnosti tipa B« kot o problemu odločanja v kontekstu preveč ali nenehno spreminjajočih se informacijah.

(Čretnik 2010) ob tem opozarja, da je lahko veliko centrov za združevanje ali analizo obveščevalnih podatkov v državah z dobro razvejano obveščevalno strukturo resna ovira. Vsak center se običajno ukvarja z analizo specifičnih podatkov, odločevalci pa ne dobijo celovite slike situacije, ker je centre zahtevno združevati v enovit sistem. Omenja, da v takih primerih ni jasno, kdo kaj dela, in namesto združitve toka informacij prihaja do zmede v obveščevalnem sistemu.

V ta namen predlaga, da se analitika združi v samo enem centru na državni ravni, ki bi imel dovolj zmogljivosti, s katerimi bi podprl odločevalce na strateški, kot na operativni in taktični ravni, ob tem pa bi bil lahko vključen še v mednarodno izmenjavo informacij.

Mnenja sem, da bi tudi tak sistem s seboj nosil izziv, kako določiti prioriteto zahtev po obveščevalnih informacijah z različnih ravni odločanja. Mnenja sem, da je sistem C4ISTAR že sam po sebi odgovor na to dilemo, v kolikor je sistem izmenjave dovolj zmogljiv, da zagotavlja tekočo komunikacijo.

Ključno vprašanje je, katere informacije so nepogrešljive, bistvene. Kako lahko nekdo ve, da

[29] Bivši namestnik načelnika štaba ameriške kopenske vojske za obveščevalno dejavnost, 2002.

ima prave in dovolj informacij za ukrepanje? C4ISTAR je kot sistem poln pasti zaradi preveč informacij, mikromanedžiranja in brezplodnega iskanja sigurnosti. Odgovor na te dileme je lahko le v spremenjenem načinu vodenja in poveljevanja. Poveljniki se morajo naučiti prepoznati trenutek, ko imajo dovolj dobro sliko situacije za ukrepanje, četudi je ta slika nepopolna in tok novih informacij ne presahne. C4ISTAR bo postal kombinacija kompleksnih sistemov ljudi in informacijske tehnologije. To pomeni, da se bodo pokazale pomanjkljivosti tako ljudi, tehnike in kompleksnih sistemov, vključujoč občasno razdrobljenost, nedosežene namere, nezaželene posledice, nepričakovane napake in nenačrtovanih uspehov.

C4ISTAR lahko razdelimo na C4, ki se ukvarja predvsem s komunikacijskimi povezavami v podporo poveljevanju in organizaciji linije vodenja in poveljevanja, ter na ISTAR, ki predstavlja »sistem sistemov«. Vključuje izdelke senzorjev v stopnjah zbiranja, usmerjanja in obdelave v obveščevalnem krogu ter procesa določanja ciljev. Zagotavlja informacije in obveščevalne podatke za realizacijo CCIR in PIR ter podpira manevrirne in napadalne udarne sisteme (Jakobsson 2008).

6.6.2 Značilnosti komponent sistema ISTAR:

a) **obveščevalna dejavnost – o**bveščevalna dejavnost v sistemu ISTAR predstavlja pretvarjanje podatkov, informacij in obveščevalnih podatkov iz številnih virov in služb v ustrezne ocene o sovražnikovih zmožnostih in namenih;

b) **nadzor –** »sistematično opazovanje zračnega prostora, področij, krajev, oseb ali stvari na površini ali pod njo, ob uporabi vizualnih**,** slušnih, elektronskih, fotografskih ali drugih sredstev« (AAP-6). Nadzor lahko poteka nad območji in dejavnostmi, in sicer pasivno v širokem območju delovanja ali pa aktivno, tako da nadzoruje točno določeno območje ali dejavnosti. Nadzorovanje je povezano z viri izvidništva in določanja ciljev, in sicer z namenom raziskati specifične dejavnosti ali zbrati podrobnejše podatke/informacije o določenem posebnem objektu nadzora. Zagotavlja tudi varnost lastnih sil z zgodnjim opozarjanjem na sovražnikove dejavnosti v medprostorih, izpostavljenih bokih in v zaledju. Nadzorovanje zagotavlja, da mora sovražnik delovati, se gibati ali delovati na razdalji, preden je lahko odkrit;

c) **določanje ciljev – z**agotavlja podrobne informacije o sovražnikovih enotah in lokacijah ter je dovolj natančen, da omogoča delovanje ognjenih sistemov na tiste

elemente, ki so bili določeni kot tarče. Proces določanja ciljev zagotavlja podatke o določenih ciljih tako za neposredne kot tudi posredne ognjene sisteme;

d) **izvidništvo** – to je usmerjena in začasna metoda zbiranja informacij o sovražniku. Lastna sredstva so angažirana, da zberejo informacije o sovražniku ne glede na njegove dejavnosti. Izvidništvo vključuje dejavnosti, ki jih opravljajo izvidniške enote, vendar niso omejene samo na to vrsto enot.

6.6.3 Načela ISTAR

Načela ISTAR temeljijo na načelih obveščevalne dejavnosti in te so (Foisseau 2009):

a) **centralizirano usklajevanje** – ISTAR mora biti centralno usklajen brez uvajanja načel decentraliziranega vpliva pri poveljevanju. To zagotavlja največjo učinkovitost in ustrezno uporabo virov;

b) **pravočasnost** – poveljniku morajo biti pravočasno dostavljene informacije in obveščevalni podatki, ki mu omogočajo delo v krogu sovražnikovega sprejemanja odločitev;

c) **točnost –** podatki pridobljeni z ISTAR morajo biti natančni in ustrezni glede na operacije, ki jih podpirajo;

d) **posredovanje informacij –** v sistemu ISTAR mora biti mogoče brez nevarnosti posredovati ustrezne informacije med pooblaščenimi poveljniki in štabi, tako da se sistem ne preobremeni z nepotrebnimi podatki;

e) **ekonomičnost delovanja –** sistem ISTAR zagotavlja izboljšano poznavanje situacije, ki omogoča poveljniku, da v svojem manevriranju in sredstvih za ognjeno podporo doseže ustrezne ekonomične učinke.

6.6.4 Želene zmogljivosti sistema ISTAR

Sistem ISTAR mora, kolikor je to le mogoče, zagotavljati zmogljivosti (Carr 2008):

a) **odzivnost** – sistem mora omogočati hitro odzivnost na poveljnikove zahteve po informacijah in obveščevalnih podatkih ter njihovo hitro izkoriščanje za določanje ciljev;

b) **stalno delovanje** – nadzor, določanje ciljev in izvidništvo morajo zagotavljati 24-urno delovanje v vseh vremenskih razmerah;

c) **trdnost** – naprave ISTAR morajo zagotavljati mešanico trdnosti delujočih

sistemov, in sicer v smislu tehnologije, dosega ter delovanja, katerih cilj je zaznati sovražnikove dejavnosti, spremembo metodologije in pogojev delovanja ter premagati sovražnikove načrte zavajanja;

d) **prožnost** – naprave ISTAR morajo omogočati modularno delovanje, tako da s sestavljanjem sistemov dosežemo primernost glede na sile in potrebe naloge.

6.6.5 Koncept delovanja ISTAR

Temelji koncepta delovanja ISTAR predstavljajo tri glavna funkcionalna področja v okviru sistema, in sicer so to ASC[30], senzorji in specializirane enote za delo na posameznih ISTAR dejavnostih.

Oddelek za vse vire. Ključ koncepta delovanja ISTAR je ASC. Vloga ASC je:

a) izvajanje CCIRM,
b) načrtovanje delovanja,
c) združitev in primerjava informacij,
d) analiza informacij,
e) posredovanje informacij,
f) vodenje senzorjev.

Oddelek za določanje ciljev. Za zagotavljanje največje sinergije s sistemom ISTAR mora biti oddelek za določanje ciljev vendar zelo tesno povezan z ASC in drugimi deli sistema ISTAR.

Sistem ISTAR zagotavlja uresničitev vedno večjih potreb, ki jih pred obveščevalni proces postavlja manevrsko bojevanje. Večnacionalne operacije od sistema ISTAR zahtevajo tudi njegovo maksimalno interoperabilnost v primeru, če posamezne komponente niso sposobne delovati in ni mogoče doseči ustrezne sinergije sistema.

Učinkovito delovanje sistema ISTAR zahteva, da vse njegove komponente delujejo na posameznih skupnih standardih ter da celotna operacija ISTAR temelji na skupni doktrini. Kadar morajo biti operacije ISTAR opravljene na večnacionalni podlagi, je prej navedena zahteva bistvena za uspeh.

[30] All Sources Cell.

7 TUJI KONCEPTI ISTAR

7.1 KONCPET NATO[31]

NATO nima lastnih ISTAR zmogljivosti, ker jih po vsakokratnem sporazumu o oblikovanju enot za posamezne operacije prispevajo države članice. Da bi bilo delovanje takih zmogljivosti učinkovito, je NATO sprejel vrsto mednarodno usklajenih pravil, ki opredeljujejo politiko in doktrino delovanja na obveščevalnem področju. Ta opredeljujejo ISTAR na naslednji način (Foisseau 2007):

7.1.1 Osnovne opredelitve

ISTAR je opredeljen kot operativno obveščevalna dejavnost, ki združuje in usklajuje načrtovanje in delovanje senzorjev, kolektorjev in drugih zmogljivosti z analitičnimi, načrtovalnimi in komunikacijskimi sistemi v podporo vodenju trenutnih in bodočih operacij.[32]

ISTAR povezuje obveščevalno dejavnost, nadzor prostora, določanje ciljev in izvidništvo s ciljem pravočasnega posredovanja tako kritičnih informacij o situaciji na bojišču kot tudi informacij o ciljih manevrskih in napadalnih sil v operaciji.

Glavni namen obstoja ISTAR zmogljivosti na vseh ravneh je izdelovati informacije in obveščevalne ocene, ki odgovarjajo na poveljnikove zahteve po ključnih informacijah (CCIR), ki so sestavni del procesa operativnega načrtovanja (OPP) in prispevajo k poveljnikovem razumevanju situacije na bojišču (SA) s prispevki za:

- proces operativnega načrtovanja,
- celovito sliko bojišča,
- obdelavo in opredelitev ciljev,
- INFO OPS,
- Zaščito sil.

ISTAR je zmogljivost, ki jo vodi poveljnik in je primerna za vse vrste operacij. Sestavni del ISTAR so tudi informacijsko-komunikacijski sistemi in infrastruktura, ki povezujejo sestavne dela ISTAR in omogočajo pravočasen prenos informacij in obveščevalnih produktov ustreznim poveljnikom in drugim naslovnikom.

[31] Celotno poglavje je povzeto po različnih NATO dokumentih in avtorjevih zabeležkah.
[32] Definicija ISTAR je bila sprejeta v NATO Joint ISTAR Custodial Group. Besedilo je prost prevod avtorja te naloge.

ISTAR dejavnost temelji na treh osnovah:

a. Informacija – obstaja lahko kot neobdelan podatek ali pa kot združena in analitično obdelana informacija.
b. Procesi - ISTAR neprestano združuje obveščevalni cikel z deli operativnega procesa načrtovanja (OPP) in s ciklom določanja ciljev.
c. Obveščevalna, nadzorna, izvidniška arhitektura ter arhitektura opredelitve ciljev – le-ta načrtno usmerja in združuje kolektorske zmogljivosti, analitične elemente, naročnike oziroma uporabnike obveščevalnih produktov in komunikacijsko-informacijsko infrastrukturo na vseh ravneh poveljevanja.

7.1.2 Način delovanja

ISTAR deluje na načelih klasične obveščevalne dejavnosti, vendar v svoji vlogi sega še dlje. V kolikor je ISTAR pravilno organiziran in vpet v procese odločanja, bistveno podpira proces operativnega odločanja, prispeva k razumevanju situacije in zagotavlja pravočasne podatke o ciljih. Načela ISTAR delovanja so:

a. **Vloga poveljnika** je v procesih ISTAR nenadomestljiva. V kolikor poveljnik ne posveča dovolj pozornosti in naporov postavljanju zahtev ISTAR, verjetno ne bo dobil potrebnih odgovorov in informacij, ki bi jih potreboval pri odločanju in uspešnem vodenju operacije.
b. **Centralizirano načrtovanje in usklajevanje**. ISTAR mora biti načrtovan in usklajevan centralizirano. Tak način zagotavlja sledenje poveljnikovim prioritetam in racionalnemu koriščenju razpoložljivih zmogljivosti. Ta princip pa ne sme omejevati načela razpršenega delovanja.
c. **Odzivnost in pravočasnost**. ISTAR zmogljivosti morajo biti hitro odzivne na sprotne zahteve poveljnika in istočasno zagotavljati pravočasne informacije za potrebe odločanja tudi v pogojih dinamičnega razvoja situacije.
d. **Natančnost in pravilnost**. Informacije morajo biti v procesu analize skrbno pretehtane in preverjene na več načinov. Izdelki ISTAR morajo zagotavljati potreben nivo zaupanja. Pogosto hitrost dogajanj v operaciji ne deluje v prid natančnosti in vsakokratnemu preverjanju informacij, zato je izurjenost in izkušenost analitikov ISTAR tista, ki zagotavlja, da se zaradi zagotavljanja natančnosti ne izgubi tempo operacije.

e. **Vzdržljiv in prilagodljiv nabor senzorjev**. Ti so pomembni zaradi hitrosti in natančnosti zaznave, posebno še, če so med seboj povezani v sistem, ki omogoča sprotno preverjanje ali potrjevanje informacij z več različnih senzorjev. Ti sistemi morajo biti modularno zgrajeni tako, da so lahko prilagodljivo uporabljeni glede na potrebe in vrsto operacije.

f. **Zavarovanje virov**. Način ter sredstva in sile za zbiranje podatkov morajo biti ustrezno zaščiteni tako v fizičnem kot tudi operativnem smislu. Pri tem delu vedno obstaja večje ali manjše politično, vojaško ali drugačno tveganje, zato je potrebno vedno oceniti stopnjo tveganja izgube ali uničenja vira v primerjavi s pomembnostjo informacije, ki jo tak vir lahko zagotovi. Prav tako lahko odkritje vira nasprotniku da namig o verjetnosti, namenu in načinu delovanja naših sil.

g. **Medsebojna povezanost**. Prilagodljivo, povezano in dostopno omrežje sredstev in sil za zbiranje podatkov, obveščevalnih procesov, oborožitvenih sistemov in situacijskih baz podatkov je nujno za zagotovitev čimbolj popolnega poznavanja situacije. To omrežje mora omogočati tudi dostop do informacij in obveščevalnih produktov sosedov in višjih poveljstev do strateške nacionalne ali mednarodne ravni.

h. **Podpora operacijskemu planiranju**. Začetno načrtovanje NATO operacij temelji na tekočih, trenutnih obveščevalnih produktih posameznih članic zveze, ki morajo že v mirnodobnem času biti procesirane na skupno dogovorjen način in oblika na nacionalni ravni. Po sestavi potrebnih sil za operacijo in njihovi napotitvi na operacijo morajo posamezne ISTAR zmogljivosti biti sposobne nadaljevati delo z enako natančnostjo in hitrostjo tudi v mednarodnem okviru.

i. **Celovita in skupna slika situacije**. To je sprotno posodobljena slika bojišča, na kateri so grafično prikazani podatki o lastnih in nasprotnikovih silah, ISTAR zmogljivostih in drugih značilnostih območja operacije. Podatki za oblikovanje slike prihajajo iz različnih obveščevalnih baz in analiz, ki so dosegljive skozi celotno verigo poveljevanja. Poleg tega tak grafični prikaz situacije pomaga pri upravljanju z ISTAR zmogljivostmi. Vizualizacija situacije je časovno povezana z dinamiko razvoja situacije na terenu in se lahko uporablja tudi za predvidevanje ali načrtovanje bodočih faz operacij.

j. **Podpora opredelitvi ciljev (Targeting)**. Opredelitev ciljev je poveljnikova odgovornost, in opredeljena je kot proces izbire ciljev in načina delovanja nanje glede na lastne operativne zahteve in zmogljivosti. ISTAR podpira targeting z zagotovitvijo

osnovnih podatkov o cilju, zmogljivostih, zaščiti in predvidenih rezultatih napada nanje. ISTAR je običajno vključen v sledeče faze targetinga:

a. **Določanje lokacije in vrste cilja.** S tem se skuša opredeliti nevarne cilje in njihove lokacije ter zagotoviti elemente za ustrezen napad nanje. Lahko pa je to tudi zbiranje informacij za najbolj ustrezen način delovanja na cilj z nebojnimi sredstvi, kot je na primer INFO OPS.
b. **Spremljanje ciljev.** ISTAR zmogljivosti so lahko uporabljene v različnih fazah delovanja na cilj, predvsem z nasveti in ocenami možnih učinkov na cilj, z uporabo različnih orožij ali načinov delovanja, upoštevaje zaželeno končno stanje.
c. **Ocena škode na bojišču.** To je pravočasna, pravilna in natančna ocena škode, povzročene z delovanjem ubojne ali neubojne vojaške sile na vnaprej opredeljene cilje. Sestoji se iz ocene stopnje fizičnega ali funkcionalnega uničenja ciljev v območju delovanja ali drugih efektov uporabe ubojnih ali neubojnih sredstev ali načinov delovanja.

k. **Podpora INFO OPS.** Uspešnost INFO OPS je neposredno povezana s podrobnim poznavanjem in razumevanjem ciljne populacije ter poti in načinov sprejemanja odločitev posameznikov in sistema. Celovite in pravilne analize psiholoških, političnih, kulturnih, vedenjskih in drugih človeških faktorjev, ki vplivajo na proces odločanja skupaj z natančnimi in podrobnimi analizami infrastrukture in vojaških zmogljivosti, so temelj za uspeh. ISTAR podpira te operacije z zagotavljanjem načrtnega zbiranja informacij in njihovega analiziranja za potrebe INFO OPS.
l. **Podpora zaščiti sil.** ISTAR prispeva k zaščiti sil, tako da zagotovi zahtevane informacije. Postopki odkrivanja, prepoznavanja in preprečevanja nevarnosti so rezultat neprestanega procesa ocenjevanja nevarnosti v sodelovanju z protiobveščevalno in varnostno dejavnostjo lastnih sil.
m. **Mednarodne operacije.** Obveščevalna podpora mednarodnim operacijam zahteva, da se ISTAR zmogljivosti in procesi izvajajo na mednarodno usklajen in dogovorjen način, vključno z mednarodno povezljivimi sistemi za izmenjavo informacij. Pri tem je razumljiva zahteva, da se vsi ti procesi odvijajo med članicami neprestano, še preden pride do napotitve mednarodnih sil na operacijo.

7.1.3 Načrtovanje

Načrtovanje v ISTAR sistemu koordinira, integrira in sinhronizira delovanje razpoložljivih ISTAR zmogljivosti. Je v neprestani povezavi s procesi operativnega načrtovanja in z opredeljevanjem ciljev. Obveščevalne zahteve (IRs), ki izhajajo iz poveljnikovih zahtev po ključnih informacijah (CCIR) in drugih zahtevah, usmerjajo delovanje ISTAR zmogljivosti.

V procesu načrtovanja v ISTAR je potrebno izdelati naslednje dokumente:

a. **Načrt zbiranja.** Ta je opredeljen kot načrt za zbiranje informacij z vsemi razpoložljivimi sredstvi in silami za zadovoljitev obveščevalnih zahtev in prevedbo teh zahtev v ukaze ali prošnje ustreznim zunanjim agencijam. Izdelava načrta zbiranja je v odgovornosti obveščevalcev v tesnem sodelovanju z drugimi organi poveljstva. To ni specifičen obveščevalni produkt, temveč skupen izdelek poveljstva.

b. **ISTAR priloge k ukazu za delovanje.** Te sta lahko ISTAR shema in ISTAR sinhronizacijska matrika.

    a. **ISTAR shema** v grafični obliki predstavlja načrt zbiranja in tako bolj nazorno ter fazno prikaže vključene ISTAR zmogljivosti in njihovo delovanje.

    b. **ISTAR sinhronizacijska matrika** je grafična ponazoritev, ki povezuje načrt zbiranja z izvedbo operacije in s poveljnikovimi obveščevalnimi potrebami. Razvije se na osnovi ocenjenih lokacij virov informacij in obveščevalnim organom ter poveljniku omogoča sprotno sledenje delovanja ISTAR zmogljivosti. Omogoča izvedbo načrta zbiranja z opredelitvijo razpoložljivih ISTAR zmogljivosti, njihovih usmerjanj na lokacijo virov informacij in časovnico izvedbe nalog.

V procesu načrtovanja morajo obveščevalni organi neprestano spremljati izvedbo načrta in predlagati morebitne spremembe glede na razvoj situacije.

7.1.4 Poveljevanje in nadzor (C2)

Poveljevanje in nadzor v ISTAR procesih je zagotovljeno z vključevanjem načrtovanja uporabe ISTAR zmogljivosti v poveljstva vseh ravni. Zagotovljeno je z vključevanjem vrste štabnih funkcij v proces načrtovanja ISTAR dejavnosti. Pri tem je posameznim članicam zveze dopuščena svoboda pri oblikovanju organizacijskih shem vključevanja teh funkcij v

proces načrtovanja. NATO standardizacija gre torej bolj v smer določanja procesov kot oblik organiziranosti. Pet štabnih funkcij je vključenih v ISTAR načrtovanje. Te so:

a. **Poveljnik,** ki usmerja ISTAR s svojimi zahtevami po ključnih obveščevalnih zahtevah (CCIR).
b. **J/G/S-3,** katerih naloga je:
    a. razlaga in predlaganje poveljnikovih ključnih obveščevalnih zahtev.,
    b. je glavni prejemnik obveščevalnih ocen in drugih ISTAR izdelkov,
    c. je koordinator vključevanja organskih[33] delov za zbiranje obveščevalnih podatkov.
c. **J/G/S-2**, katerih naloga je:
    a. pretvorba posameznih elementov CCIR v prioritetne obveščevalne zahteve (PIR);
    b. proces upravljanja z obveščevalnimi zahtevami, kjer se prioritetne obveščevalne zahteve razvijajo v zahteve po informacijah (RFI);
    c. združevanje podatkov iz vseh razpoložljivih virov (All Sources Process), ki je sestavljeno iz treh podprocesov:
        i. zbiranje, razvrščanje in analiziranje informacij iz vseh virov,
        ii. posodabljanje ocene nasprotnika glede na vse vire,
        iii. izdelava usmerjenih (glede na zahteve) obveščevalnih ocen.
d. **ISTAR koordinacijska funkcija**. Ta je lahko organizirana kot skupna obveščevalno operativna funkcija ali kot posebna (ISTAR) funkcija znotraj poveljstva. Zagotavlja:
    a. da so naloge ISTAR zmogljivosti (kolektorjev) usklajene z zahtevami po informacijah (RFI);
    b. da so naloge kolektorjev usklajene med obveščevalnimi in operativnimi organi poveljstva;
    c. da so zahteve po obveščevalnih informacijah od drugih enot vključene v načrt zbiranja;
    d. in da so po potrebi zahteve po obveščevalnih informacijah posredovane v druge enote in agencije.
e. **Funkcija zbiranja podatkov** zagotavlja procesiranje informacij s ciljem njihovega razvrščanja, shranjevanja in analiziranja ne glede na to, ali prihajajo od lastnih ali drugih zbirateljskih zmogljivosti.

[33] To so sestavni deli enot, ki jim tako poveljstvo poveljuje (npr. izvidniški vodi, CIMIC skupine, ipd.).

7.1.5 NATO ISTAR arhitektura

Najbolj pomembne značilnosti NATO ISTAR arhitekture so:

a. omogoča poveljniku, da usmerja obveščevalno dejavnost;
b. zagotavlja, da pripadniki ISTAR lahko upravljajo zbiranje na vseh ravneh;
c. podpira upravljanje z zahtevami, usmerjeno zbiranje informacij, njihovo procesiranje in pošiljanje na vseh ravneh poveljevanja;
d. podpira delovanje modularno sestavljenih zmogljivosti glede na preverjene obveščevalne zahteve;
e. omogoča izmenjavo informacij med obveščevalnimi celicami, zbirkami podatkov in kolektorji s pomočjo zmogljivega in varnega komunikacijsko-informacijskega omrežja;
f. podpira prenos odgovarjajočih nacionalnih obveščevalnih analiz in ocen v mednarodnem okolju.

Uspešnost in uporabnost ISTAR arhitekture temelji na odnosih med funkcionalnimi elementi. Ti so:

a. poveljniki in poveljstva, ki izvajajo ali uporabljajo ISTAR proces;
b. enote, v katere so ISTAR zmogljivosti vključene;
c. ISTAR zmogljivosti in enote.
d. Komunikacijsko-informacijski sistem, ki omogoča ISTAR proces.

Ker NATO nima svojih stalnih ISTAR zmogljivosti, je potrebno potrebne zmogljivosti zgraditi iz nacionalnih elementov, ki morajo skupaj delovati po enotnih načelih. Prav tako morajo članice pristati na dogovor o izmenjavi obveščevalnih informacij, kar je pogosto zelo občutljiva tema in zahteva posebne dogovore in večnacionalne ali bilateralne sporazume.

Posebno so opredeljene vloge Nacionalnih obveščevalnih celic (NIC) v operacijah, ki v osnovi zagotavljajo ločevanje nacionalnih in mednarodnih interesov posamezne države članice v določeni operaciji, po drugi strani pa zagotavljajo nemoten, pa vendar nadzorovan pretok nacionalno zbranih obveščevalnih informacij v mednarodno okolje.

7.2 KONCEPT EVROPSKE UNIJE (EU)

EU nima lastnih vojaških zmogljivosti, po sporazumu med članicami pa le te dajejo na razpolago del svojih vojaških zmogljivosti za delovanje po odločitvi EU. Te zmogljivosti so v osnovi modularne in sestavljene iz dogovorjenih nacionalnih zmogljivosti več članic. Ker take združene enote težje delujejo uspešno, je EU sprejela več dokumentov, ki usmerjajo oblikovanje in opredeljujejo kriterije, ki jih morajo moduli spoštovati in doseči, preden se vključijo v tako mednarodno enoto.

Enako velja tudi za ISTAR. Tudi za te zmogljivosti se načelno predvideva, da bodo modularno sestavljene, pri čemer izhajamo iz sledečih podmen:

- Nabor sil za EU operacije, vključno z operativno in strateško podporo, mora biti v visoki stopnji pripravljenosti.
- Poveljstvo in enote morajo imeti dovolj zmogljivo in povezljivo komunikacijsko opremo, pa tudi elemente vodenja in poveljevanja, ki so visoko operativni, premični in samozadostni.
- Sestavni deli EU združenih enot morajo biti sposobni delovati v polnem bojnem spektru in v vseh pogojih bojnega delovanja (RKB, EB, asimetrične grožnje, ipd.).
- Združene enote morajo imeti tudi sposobnost usklajevanja ognjene podpore.

EU razume ISTAR kot sistem sistemov, ki združuje informacije, pridobljene od različnih kolektorjev, proces zbiranja, usmerjanja in analize v obveščevalnem ciklu in določanje ciljev. ISTAR predstavlja sinergijo združenih sistemov za nadzor, izvidništvo in določanje ciljev z obveščevalnim procesom.

Načelno sestavo ISTAR zmogljivosti v EU razumejo kot sestavljenko posameznih kolektorjev (SSSS[34]), ki so prek analitične celice (SSIC[35]), ki združuje te kolektorje, združeni v Združeni celici za obveščevalno dejavnost (MSIC[36]). (Kerttunen, Koivula, & Jeppsson 2005).

7.2.1 Namen in cilji ISTAR v EU Battle Group

Glavni namen zagotavljanja ISTAR zmogljivosti v EU enotah je odgovoriti na poveljnikove kritične zahteve po informacijah (CCIR[37]). Glavne cilje pa lahko oblikujemo v naslednjih točkah (EU Defence Planning Staff 2002) :

- Zagotavljati podporo načrtovanju in odločanju s:

[34] Single Source Sensor System.
[35] Single source Intelliegence Cell.
[36] Multi Sources Intelligence Cell.
[37] Commander Critical Information Requirements.

- precizno oblikovanimi informacijami in obveščevalnimi ocenami, vključno z obveščevalno oceno bojišča (IPB[38]);
- usklajenim, usmerjenim in racionalnim delovanjem razpoložljivih ISTAR zmogljivosti.

- Zagotavljati informacije in obveščevalne ocene za združeno sliko situacije (COP[39]) z:
  - izdelavo in posodabljanjem situacijske slike v okviru območja obveščevalne odgovornosti (AIR)[40] in območja obveščevalnega interesa (AII)[41];
  - analizo vsake posamezne informacije in združevanje analiz v celovito;
  - obveščevalno analizo (ASI)[42].
- Prispevati k celovitem poznavanju situacije (SA)[43].
- Podpirati proces določanja ciljev z opredelitvijo ciljev, njihovo analizo, selekcijo in prioritizacijo in podpirati predvidevanje škode na bojišču.
- Podpirati INFO OPS z obveščevalnimi ocenami in informacijami ter z aktivnim elektronskim bojevanjem.
- Podpirati zaščito sil z:
  - ocenami groženj,
  - pravočasno opozarjanje na nevarnost in
  - protiobveščevalno dejavnostjo.

7.2.2 Organizacijska struktura ISTAR EU Batlle Group

7.2.2.1 Zahteve:

- Zagotavljati mora podporo EU operacije kriznega odzivanja od 2005 do najmanj 2010.
- Osnovana mora biti na dosedanjih zmogljivostih, procesih in standardih, pri čemer je potrebno dovoliti njihov nadaljnji razvoj.
- Mora biti sposobna združevanja, izmenjave informacij in obveščevalnih produktov med različnimi ISTAR zmogljivostmi in enotami.
- Mora biti povezljiva in prilagodljiva na nove tehnologije kakor tudi z novo opremo.

[38] Intelligence Preparation of the Battlespace.
[39] Common Operational Picture.
[40] Area of Intelligence Responsibility.
[41] Area of Inrtelligence Interest.
[42] All Source Intelligence.
[43] Situational Awareness.

- ISTAR aktivnosti morajo biti usklajene z drugimi procesi (npr. INFO OPS, PSYOPS, ipd.) (Sjoerd de Vries 2008).

7.2.3 Organizacijski modeli

Ker EU nima lastnih zmogljivosti, sta organizacija in opremljenost ISTAR enot odvisni od vrste operacije, grožnje in držav, ki prispevajo sile. Glede na to sta bila v EU sprejeta dva modela vključevanja in delovanja ISTAR zmogljivosti (Kerttunen, Koivula, & Jeppsson, 2005).

Pri obeh modelih upoštevamo naslednje podmene:

- Poveljstvo operacije usklajuje in upravlja tok vseh informacij v območju delovanja in obveščevalna dejavnost je vodena centralno iz obveščevalnega štabnega organa takega poveljstva kot del CCIRM[44].
- ISTAR zmogljivosti so podrejene poveljniku mednarodne enote z nacionalnim sklepom o prenosu pristojnosti za poveljevanje na mednarodno poveljstvo (TOA)[45].
- ISTAR senzorski sistemi morajo biti mednarodno povezljivi.
- Država, ki zagotavlja ISTAR komunikacijske in informacijske sisteme, mora zagotoviti toliko in takšno opremo, da zagotovi njihovo mednarodno povezljivost.
- V operaciji je omogočena izmenjava obveščevalnih podatkov in ocen tudi z bazami podatkov v mednarodnih organizacijah in nacionalnih agencijah.
- Izmenjava obveščevalnih izdelkov z nacionalnimi zmogljivostmi poteka prek nacionalnih obveščevalnih celic (NIC)[46] in/ali obrambnih obveščevalnih organizacij (DIO)[47].
- Vse ISTAR zmogljivosti je možno napotiti na naloge in so modularno sestavljene.

7.3 KONCEPT ISTAR V KANADI

Kanada je v svoji zgodovini preurejala, povečevala ali zmanjševala svoje obveščevalne zmogljivosti ob vsakem večjem vojaškem spopadu v okolici ali v času obeh svetovnih vojn in po njih. Ne glede na obseg zmogljivosti, je bila večina dejavnosti namenjena varovanju lastnega ozemlja in boju proti kriminalu. Posebno v prvi polovici 20. stoletja so bile kanadske obveščevalne zmogljivosti v službi bivših gospodarjev – Britancev, Francozov in velikega soseda – ZDA.

[44] Collection, Co-ordination and Information Requirements Management.
[45] Transfer of Authority.
[46] National Intelligence Cell.
[47] Defence Itelligence Organisation.

Sredi druge polovice 20. stoletja so bile javno razkrite nezakonitosti delovanja kanadske obveščevalne agencije, kar je v nadaljevanju pomenilo hudo moralno breme, ki je kanadsko obveščevalno dejavnost oviralo v razvoju (Gill 1991).

Šele razmah organiziranega kriminala, terorizma in nevarnosti nenadzorovanega širjenja orožij za masovno uničevanje konec prejšnjega stoletja je prisililo kanadsko družbo k bolj fleksibilnemu odnosu do obveščevalnih služb. Postopoma so v dejavnosti začeli uvajati informacijsko tehnologijo, čeprav je še vedno veljalo pravilo, da kar je vsaj delno uporabno, lahko ostane v naboru opreme še napej. Tudi prepričanje, da mora Kanada slediti globalnemu ogrožanju tudi na druge kontengente, si je le počasi utiralo pot med odločevalce. V tem smislu je močno spodbudo predstavljalo članstvo Kanade v NATU in bližina ter vpliv ZDA (Wark, 2003). V veliki meri se je Kanada pri pridobivanju in analizi obveščevalnih podatkov naslanjala prav na te zmogljivosti, dokler se niso na prelomu tisočletja odločili za oblikovanje lastnega sistema celovitega zajemanja, urejanja in analiziranja obveščevalnih informacij.

V kanadski vojski so do odločitve o vzpostavitvi ISTAR sistema prišli na osnovi analize vojn v Iraku in Afganistanu in drugih tujih izkušenj pri obveščevalnem delovanju. Temeljni cilj, ki so si ga zastavili s projektom ISTAR, je do leta 2011 združiti vse razpoložljive in nove obveščevalne zmogljivosti v združeno sliko nasprotnika na potencialnih bojiščih. Taka slika omogoča bolj celovit pogled na zmožnosti nasprotnika, ki danes niso skrite samo v orožju, temveč tudi v drugih prednostih ali slabostih nasprotnika. Poleg tega se na tak način smotrneje uporabljajo vedno dražji sistemi kakor tudi drugi viri, ki so vedno bolj omejeni (Connel 2003).

7.3.1 Izhodiščno stanje

Leta 2001 so izdelali projekt uvajanja ISTAR sistema v kopensko vojsko in pri tem v analizi stanja ugotovili, da imajo resne pomanjkljivosti v:

- Komunikacijski opremi, pri čemer je za ISTAR najbolj pomembna premajhna zmogljivost digitalnih povezav za prenos podatkov in nesposobnost prenosa obveščevalnih podatkov iz zračnih plovil.
- Omejenem dostopu do nacionalnih ali mednarodnih ISR[48] baz podatkov.

[48] ISR (Intelligence, Surveilance, Recconnaissance) je kratica, ki jo veliko držav uporablja namesto ISTAR, posebno če »targeting« ni sestavni del njihove obveščevalnega dejavnosti.

- Na taktični ravni niso imeli dovolj zmogljivosti za načrtno zbiranje, združevanje in analizo obveščevalnih informacij.
- Procesov načrtnega zbiranja in obdelave obveščevalnih informacij in podatkov na taktični ravni niso imeli.
- Obstoječa senzorska oprema ni bila med seboj primerljiva in združljiva.
- Imeli so omejene zmogljivosti za elektronsko bojevanje na taktični in operativni ravni.
- Niso imeli zmogljivosti za opazovanje in izvidništvo na večje razdalje.
- Niso imeli zmogljivosti za prepoznavanje delovanja in lociranje položajev nasprotnikove oborožitve.

Ker je bilo časovno obdobje za operativno uporabo ISTAR sistema relativno kratko, so se odločili, da bodo večino opreme in sistemov kupili na trgu, namesto da bi sami razvijali te zmogljivosti.

Iz razpoložljivih podatkov ni mogoče ugotoviti, kakšno organiziranost imajo sedanje kanadske ISTAR zmogljivosti, načeloma pa so v obstoječe enote uvedli novo opremo in sistem C2ISTAR[49]. Ta se od C4ISTAR razlikuje predvsem v zmanjšanem obsegu informacijske tehnologije, ki je vključena v sistem komunikacij in poveljevanja.

7.3.2 Ključne funkcije

Podatke o tem sem v veliki meri pridobil iz opisanih kanadskih izkušenj iz Afganistana, ki velja za nekakšen testni poligon pri odločanju o oblikovanju, opremljanju in uvajanju sistema ISTAR.

ISTAR zmogljivosti različno uspešno zagotavljajo izvajanje naslednjih ključnih funkcij (Lefevbre 2006):

- CCIRM[50] je funkcija, ki je po oceni nekaterih piscev taka novost v kanadski vojski, da predstavlja velik izziv dosedanjim tradicionalno organiziranim štabom in štabnemu delu. Največja težava se pojavlja v izredno povečanem številu informacij in vztrajnim poskusom, da bi čimbolj podrobno obvladovali tehnične zmogljivosti ISTAR komponent, namesto da bi poveljstva pozornost posvečala oblikovanju in upravljanju z obveščevalnimi zahtevami. Zaradi tega se izgublja sporočilna vrednost pridobljenih informacij, ker niso ciljno procesirane. To težavo so prepoznali in jo skušajo odpraviti,

[49] Command, Control, Intelligence, Surveillance, Target Aquisition and Reconnaissance.
[50] Upravljanje s poveljnikovimi zahtevami po informacijah.

ugotavljajo pa, da je potrebno spremeniti globoko zakoreninjeno, tradicionalno kulturo dela poveljstev (Lefevbre 2006).

- Upravljanje z zmogljivostmi senzorjev in kolektorjev ali drugače povedano – načrtovalno funkcijo imajo sicer oblikovano, vendar se je pri delu pokazala enaka težava kot v prejšnji točki. Tudi v tej točki ugotavljajo, da je potrebno še veliko dela z usposabljanjem poveljstev za vodenje takih zmogljivosti.
- Sprotna analiza podatkov predstavlja funkcijo v nižjih poveljstvih, kjer je potrebno hitro reagirati na spremembe na bojišču. Glede na to, da se informacijska tehnologija v kanadski ISTAR uvaja postopoma, imajo poveljstva precej težav pri učinkovitem in pravočasnem združevanju informacij v celovito sliko situacije. Postopoma te težave z dograjevanjem sistema informacijske podpore poveljevanju odpravljajo.
- Združevanje obveščevalnih podatkov je analitično načrtovalna funkcija, ki zagotavlja, da sproti preverjajo relevantnost prispelih informacij glede na obveščevalne zahteve, posodabljajo obveščevalne produkte in dopolnjujejo zahteve po informacijah glede na razvoj situacije ali manjkajoče podatke.
- Podpora določanju ciljev, ki je pomembna predvsem za usklajevanje delovanja artilerijskih ter letalskih enot z enotami na tleh ter za podporo izvajanju INFO OPS.
- Zaščita sil je funkcija ISTAR, ki zagotavlja neposredno zaščito enot v rajonih namestitev kakor tudi na predvidenih smereh delovanja.

7.3.3 Oprema

Najbolj pomembna nova ISTAR oprema v kanadski vojski je (Lefevbre 2006):

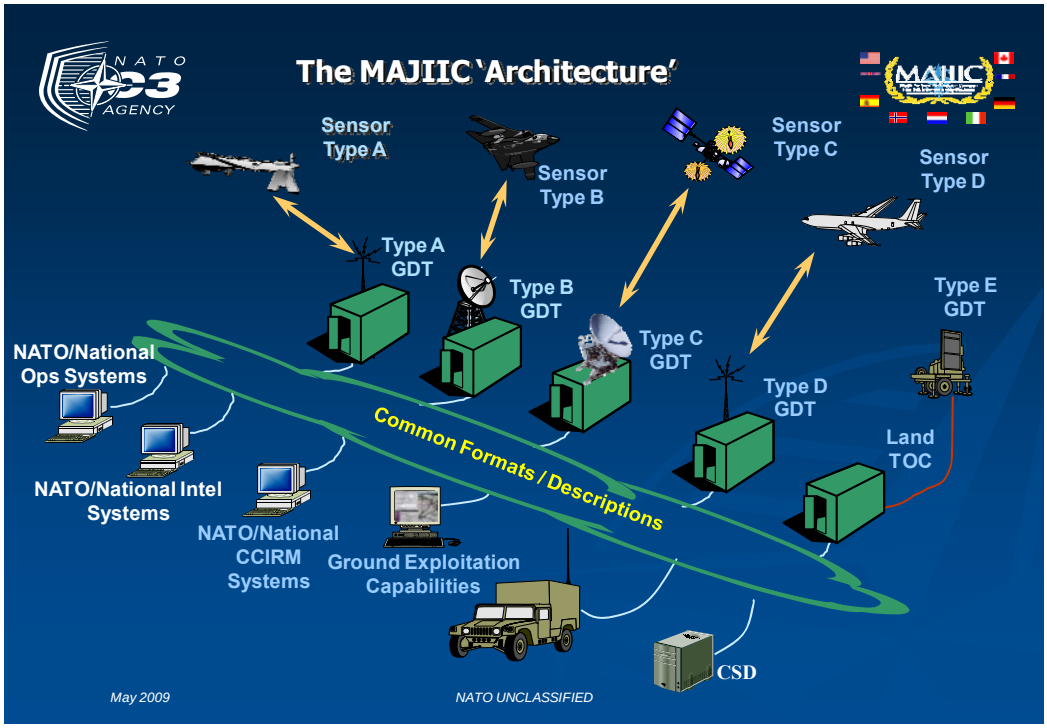
- sodobna komunikacijska oprema (HCDR[51]), ki lahko zadovolji potrebe po visoki hitrosti in zmogljivosti kanalov;
- visoko zmogljive informacijske sisteme za avtomatsko izmenjavo podatkov na taktični ravni (TCDL[52]);
- sodobna oprema za zaščito sil in odkrivanje delovanja ter položajev nasprotnikovega orožja;
- taktična brezpilotna letala;
- posodobljena oprema za elektronsko bojevanje;
- posodobljena obstoječa oprema za izvidništvo, opazovanje in nadzor prostora.

[51] High Capacity Data Radio.
[52] Tactical Common Datalink.

Modernizacija še ni zaključena, večina opreme in procesov pa je že v uporabi in preverjanju.

7.3.4 Kako deluje kanadski ISTAR

Slika 7-1: Načelna organizacija in zmogljivosti MAJIIC.



Vir: Ross 2009, 4

Kot sem že omenil v prejšnjih poglavjih, se je Kanada pri razvoju svojih obveščevalnih zmogljivostih naslanjala na sosedo, Britance in NATO, ob tem je vseskozi skušala obdržati samostojnost pri odločanju o nalogah, omejitvah in načinu izvajanja te dejavnosti. Kanada je aktivna članica skupine, ki se ukvarja s povezljivostjo nacionalnih in koalicijskih multisenzorskih in komunikacijskih sistemov v povezljiv kompleks. Ta kompleks v NATO imenujejo MAJIIC[53], namen skupine pa je razviti standarde za skupno delovanje ISTAR zmogljivosti v mednarodnem okolju. Vizijo tega projekta ponazarja slika 7-1. Končni cilj kanadskega ISTAR je sposobnost upravljanja in izkoriščanja z vsemi razpoložljivimi nacionalnimi in mednarodnimi zmogljivostmi za pridobivanje informacij in razvijanje lastnih načrtovalnih, analitičnih in komunikacijskih zmogljivosti (NATO Consultation, Command and Control Agency 2007).

[53] Multi Senzor, Aerospace/Ground, Joint ISR, Interoperability Coalition (MAJIIC).

V dosedaanjem razvoju so vzpostavili sistem medsebojne sodobne komunikacije, tehnično opremili senzorske in druge kolektorske zmogljivosti in preoblikovali procese dela poveljstev. Po dostopnih podatkih so uspeli oblikovati sledeče ISTAR discipline:

a) SIGINT je njihova najstarejša tehnično zahtevna disciplina obveščevalnega dela, ki so jo razvili že v času druge svetovne vojne. Uspeli so jo tehnično posodobiti in predstavlja hrbtenico kanadskega ISTAR (Wark 2003). Pri tem:

- odkriva neposredno nevarnost za enote v stiku,
- odkriva in potrjuje lokacije, namen ali aktivnosti potencialnih ciljev,
- odkriva cilje za nadaljnje zbiranje obveščevalnih informacij.

SIGINT podatke posredujejo v celice za združevanje obveščevalnih podatkov, potem ko jih predhodno shranijo in uredijo v SIGINT podregistrih. Podatki, zbrani v tej disciplini, gredo do najvišjih strateških ravni odločanja, ki jih po potrebi dopolnjujejo še z drugače pridobljenimi informacijami.

b) IMINT izdelki so lahko na voljo v normalnem svetlobnem ali infra rdečem oziroma rentgenskem spektru, ki v nadaljevanju zahtevajo posebno opremo in znanje za prepoznavanje podrobnosti na posnetkih. Skupaj z IMINT uporabljajo tudi opremo za:

c) GEOINT, to je disciplina, ki se ukvarja z digitalizirano analizo geografskih značilnosti območja in umeščanjem odkritih sprememb v okolju na karto v digitalni ali analogni obliki. Pri tem tesno sodelujejo z Američani, ki jim zagotavljajo digitalne podlage za delo.

d) WEAPONINT, ki se ukvarja z analiziranjem prepoznavnosti in lastnosti sovražnikovega orožja in opreme. V to kategorijo je vključena tudi analiza kemične in tehnološke sestave improviziranih minskih sredstev in sredstev za proženje.

e) Odkrivanje orožja in zaščita sil[54]. V to poglavje lahko vključimo vse tiste sisteme za odkrivanje nasprotnika, ki jih ni v prejšnjih zmogljivostih. Običajno so to tehnična sredstva za odkrivanje prisotnosti nasprotnika v neposredni bližini baz ali lokacij enot

[54] Weapon Location and Force Protection.

in/ali sredstva za odkrivanje lokacij težjih nasprotnikovih orožij v fazi njihovega delovanja (npr. artilerijski in pehotni radarji ali akustični senzorji).

7.4 KONCEPT ISTAR V VELIKI BRITANIJI

Doktrina britanske vojske govori o tem, da operacije sledijo oziroma temeljijo na obveščevalnih ugotovitvah in ocenah v nadaljevanju pa uvršča STAR zmogljivosti pod domeno obveščevalnih organov, ki jim zagotavljajo informacije za obveščevalno analitični proces (UK Ministry of Defence 2007).

Britanski ISTAR lahko uspešno deluje le v okolju, kjer je zagotovljena neprestana izmenjava informacij in navodil s poveljnikom. Jasne zahteve in usmeritve so osnova za uspešno uporabo obveščevalnih zmogljivosti.

7.4.1 Ključne funkcije

ISTAR zmogljivosti zagotavljajo izvajanje naslednjih ključnih funkcij.

- IRM[55] (Upravljanje z zahtevami po informacijah) je ena od temeljnih dejavnosti ISTAR, s katero zagotavljajo pregled nad zbiranjem informacij, tako da lahko določijo prioritete pri delovanju, in zagotavljajo načrtno usmerjanje delovanja ISTAR zmogljivosti, usmerjenega analiziranja in pravočasnega obveščanja naročnikov o zahtevanih informacijah, ocenah ali drugih izdelkov.
- CC[56] (Načrtovanje zbiranja informacij) vključuje izbiro najbolj primernih oblik zbiranja informacij za zadovoljevanje IR[57] (obveščevalne zahteve) in optimizacijo koriščenja razpoložljivih ISTAR zmogljivosti. Skupine CC morajo dobro poznati in razumeti poveljnikove usmeritve, organizacijo bojnega razporeda in načrtovano dinamiko bojnih aktivnosti. Delati morajo usklajeno s skupinami IRM, ASAC[58] in morebitnimi zmogljivostmi ISTAR, ki v istem območju delujejo za potrebe višjih poveljstev.
- DE[59] (Osnovna (sprotna) analiza podatkov) zagotavlja hitro vključevanje neobdelanih informacij v obveščevalna poročila ali sheme, ki jih zlahka razume analitik na višji

[55] Information Requirements Management.
[56] Collection Coordination.
[57] Intelligence Requirements.
[58] All Source Assessment Cell.
[59] DATA Exploitation.

stopnji združevanja. Na tak način se po stopnjah zmanjšuje število informacij, poročila pa posodablja sproti, tako da se pomembnost in vsebina podatkov ne izgubi.

- ASA[60] (Analiza vseh podatkov – celovito analiziranje) zagotavlja pregled in vključevanje informacij tako iz vseh možnih odprtih virov kot tudi iz stopnjevanih predhodnih ali sproti zbranih informacij v celovito oceno, ki zagotavlja naročniku čimbolj celovit odgovor na prednostne obveščevalne zahteve. Pri tem običajno združujejo razpoložljive civilne in vojaške zmogljivosti v združene skupine.
- Obveščanje naročnikov zagotavlja, da naročniki dobijo prave, pravilno oblikovane in stopnjevane ocene ali poročila ob pravem času in v skladu z njihovimi zahtevami na varen in pregleden način.
- ST[61] (podpora določanju ciljev) zagotavlja v cilju svetovanja G-3/G-5 celicam v poveljstvu pri:
    - prepoznavanju ciljev visokih vrednosti,
    - analizi možnih stranskih posledicah uničenja potencialnega cilja,
    - izbiri pravega načina delovanja po cilju glede na vpliv takega delovanja na lokalno prebivalstvo, naravno okolje, kulturno dediščino ali pripadnike nasprotnikovih oboroženih sil.

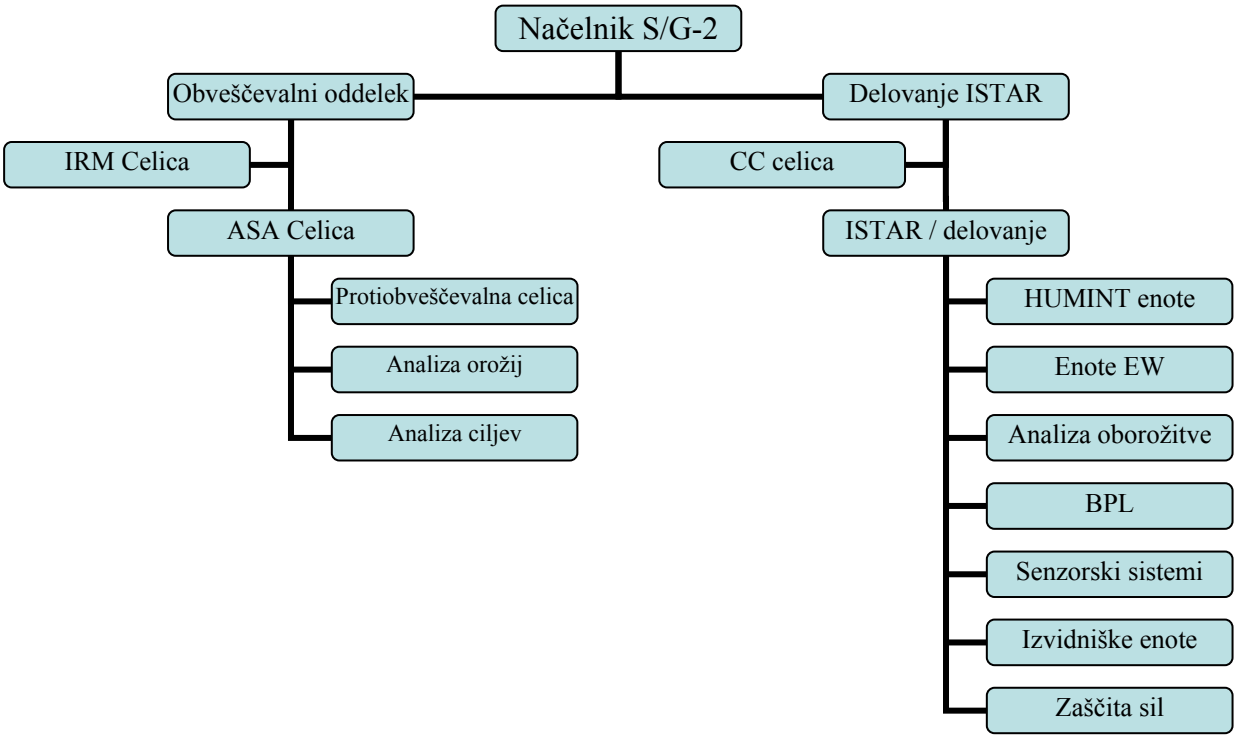
7.4.2 Organizacija ISTAR zmogljivosti

V Veliki Britaniji so ISTAR zmogljivosti organizirane na vseh ravneh, tako da so na nacionalni ravni podrejene vladi in civilnim agencijam in je vojska le eden od kolektorjev, na operativni in taktični ravni pa imajo organizirane specializirane ISTAR strukture, ki so lahko sestavni del enot in poveljstev ali pa modularno sestavljene in pridodane za določeno operacijo ali nalogo.

Podrobnejše strukture ni mogoče dobiti iz odprtih virov, načelno pa lahko ISTAR zmogljivost brigade prikažemo na naslednji sliki:

[60] All Source Analysis.
[61] Support to Targeting.

Slika 7-2: Načelna struktura ISTAR zmogljivosti britanske vojske na taktični ravni.



Slika 7-2 kaže, da ima ISTAR enota tako sestavo in organizacijo, ki ji omogoča samozadostnost v smislu načrtovanja in izvajanja operacij, logistično pa je vezana na nadrejeno enoto. Sestavljena je tako, da lahko deluje v vseh ISTAR dejavnostih in da lahko zagotavlja tudi širšo zaščito sil z ustreznimi tehničnimi sistemi. Neposredno ji naloge določa štabni obveščevalni organ (S/G-2) poveljstva, ki vodi operacijo, sistemi zvez in avtomatiziranih komunikacij pa zagotavljajo neprestano in sprotno izmenjavo informacij.

7.4.3 Kako deluje britanski ISTAR

Najbolj pomembna skrb načrtovalcev ISTAR dejavnosti je, kako čimprej in čimbolj natančno odgovoriti na obveščevalne zahteve poveljnika in njegovega štaba. Preden izdelajo načrt delovanja ISTAR zmogljivosti, je potrebno preveriti, ali zahtevane ocene lahko izdelamo na osnovi že prej pridobljenih informacij (British Arm Filed Manual 2009).

V kolikor je potrebno pridobivati nove informacije (kar je v procesu bojnega delovanja običajno), je to potrebno storiti z načrtovanjem, v katerem je potrebno najprej pridobiti jasne poveljnikove usmeritve in druge vhodne podatke o načrtovani operaciji, potem pa odgovoriti na 7 temeljnih vprašanj. Ta so:

1. Kaj namerava nasprotnik in zakaj?
2. Kakšna je naša naloga?

3. Katere rezultate moram doseči?
4. Kje je potrebno delovanje ISTAR?
5. Katere ISTAR enote in sredstva je potrebno vključiti?
6. Kako uskladiti delovanje različnih ISTAR zmogljivosti?
7. Katere kontrolne mehanizme je potrebno uporabiti za pravilno realizacijo nalog?

Rezultat teh razmišljanj so: načrt zbiranja obveščevalnih podatkov, matrika delovanja ISTAR elementov, upravljanje z obveščevalnimi zahtevami, načrt obveščanja naročnikov in izmenjave informacij, načrt izdelave ocen, poročil in drugih izdelkov, matrika usklajevanja delovanja ISTAR elementov z drugimi zmogljivostmi na bojišču.

7.4.4 Izdelki ISTAR zmogljivosti

7.4.4.1 IMINT

IMINT izdelki so lahko na voljo v različnih oblikah ali elektromagnetnih spektrih. Pomembno je, da naročnik ve, kaj bi rad imel na teh izdelkih prikazano in kako. Prav tako je pomembno, da ima opremo, na kateri je možno predstaviti izdelke IMINT.

V ISTAR zmogljivostih britanskih sil oprema zagotavlja predstavitev IMINT podatkov z:

- elektro optično opremo, ki zagotavlja prikaz slike v normalni dnevni svetlobi v obliki fotografij ali video posnetkov, ki jih analitik dobi v realnem času običajno v digitalni obliki;
- slikovnim materialom v infra rdečem spektru, kar je posebej uporabno v pogojih slabše vidljivosti. Britanci imajo te zmogljivosti na skoraj vseh tipih opazovalne opreme, posebej učinkovita pa je, kadar je oprema v zračnih plovilih povezana z IR senzorji na zemeljskih platformah;
- radarska slika tal prikaže podrobnosti še v tem spektru elektromagnetnega valovanja, posebna uporabnost teh sistemov pa je v tem, da lahko prikažejo situacijo pod naravno ali umetno masko.

7.4.4.2 SIGINT

SIGINT je neprecenljivo orodje za zagotavljanje informacij o nasprotnikovih lokacijah in namerah. Pogosto te informacije usmerjajo delovanja drugih ISTAR zmogljivosti. Kljub temu da je SIGINT načeloma razdeljen na več vej dejavnosti, pa v kopenski vojski VB na

operativni in taktični ravni uporabljajo predvsem COMINT[62], ki se ukvarja predvsem z nasprotnikovimi sistemi zvez. Pri tem lahko:

- odkriva neposredno nevarnost za enote v stiku,
- odkriva in potrjuje lokacije, namen ali aktivnosti potencialnih ciljev,
- odkriva cilje za nadaljnje zbiranje obveščevalnih informacij.

Podatki o SIGINT gredo na več naslovov, najbolj pogosto pa:

- v analitično celico pridodane enote za elektronsko bojevanje na taktičnem nivoju,
- EWCC[63], ki usklajuje delovanje različnih SIGINT zmogljivosti na brigadnem ali višjem nivoju, zbira rezultate njihovega dela, jih analizira in posreduje v nadaljnjo obdelavo analitiki ISTAR. Običajno je to IFC[64] ali ASAC;
- GCO[65], ki je v višjih enotah predstavnik SIGINT zmogljivosti nivojev nad kopensko vojsko. Običajno razpolaga s podatki SIGINT analiz, pridobljenih na državnem ali celo mednarodnem nivoju, ki jih po potrebi dopolnjuje s taktičnimi podatki ali obratno.

7.4.4.3 MASINT[66]

Večina teh zmogljivosti in opreme je opredeljena s stopnjo zaupnosti tajno ali višje in deluje na podmeni, da vse, kar obstaja in se premika po zemlji, za seboj pušča različne sledi, ki jih je mogoče na različne načine odkriti in prepoznati.

- GMTI[67] je v britanski vojski nabolj pogosta MASINT oprema, ki zahteva visoko usposobljene operaterje in analitike, nekatere sledi pa so lahko prepoznane kar takoj na osnovi baz podatkov o značilnih sledeh.
- Zaradi stopnje tajnosti zahteva prenos podatkov MASINT posebno, varno komunikacijsko omrežje, zaradi tega sta število in raven naslovnikov omejena.

7.4.4.4 GEOINT[68]

Ta zmogljivost omogoča naročniku vizualizacijo situacije in dogajanj na ali tik pod površjem zemlje na geografskih podlagah. Viri podatkov so različni, od brezpilotnih letal do drugih letal, vojaških ali komercialnih satelitov pa do geografskih baz podatkov vojaških ali civilnih

[62] Communication Intellegence.
[63] Electronic Warfare Coord. Cell.
[64] Intell Fusion Cell.
[65] Government Communication Officer.
[66] Measurement and Signals Intelligence.
[67] Ground Moving Target Indicator.
[68] Geospatial Intelligence.

geo agencij in inštitutov. Običajno so izdelki GEOINT rezultat dlje časa trajajočega opazovanja zemeljskega površja s ciljem odkrivati naravne ali umetne spremembe, ki lahko vplivajo na izvedbo operacij določenega območja.
Zmogljivosti za manj zahtevno GEOINT so v VB že na nivoju brigade, običajno pa višje, ker je pridobivanje podatkov vezano na letalske sile ali zmogljivosti v vesolju. Običajno se združujejo podatki, pridobljeni z IMINT, v združeno GEOINT sliko ali analizo.

7.4.4.5 HUMINT[69]

Ta zmogljivost pokriva vse informacije, ki jih pridobijo v pogovorih z ljudmi. Običajno se ta dejavnost izvaja neposredno na terenu z namenom, da se ali z nevezanimi pogovori z lokalnim prebivalstvom, ali načrtnimi kontakti virov s posebej izurjenimi operaterji, ali z zasliševanjem pridobijo informacije o namerah, lokacijah in strukturi nasprotnika.
Za uporabno zbiranje informacij na tak način je potrebno sprotno preverjanje pridobljenih informacij še na drugačne načine in njihova sprotna analiza, ki običajno usmerja nadaljnjo koriščenje HUMINT zmogljivosti.
Prednost te dejavnosti je, da so informacije na voljo takoj in na hiter ter enostaven način lahko posredovane naročnikom (Poucet 2006).

7.4.4.6 Odkrivanje orožja in zaščita sil[70]

V to poglavje lahko vključimo vse tiste sisteme za odkrivanje nasprotnika, ki jih ni v prejšnjih zmogljivostih. Običajno so to tehnična sredstva za odkrivanje prisotnosti nasprotnika v neposredni bližini baz ali lokacij britanskih enot in/ali sredstva za odkrivanje lokacij težjih nasprotnikovih orožij v fazi njihovega delovanja (npr. artilerijski radarji ali akustični senzorji).

7.4.5 Oprema

Oprema ISTAR zmogljivosti britanske vojske je raznovrstna, zagotavlja izvajanje vseh prej naštetih dejavnosti ter varen in deloma avtomatiziran prenos podatkov do naročnikov.
Glavno opremo lahko strnemo v sledeči seznam:

- letala za zračne ISR[71] aktivnosti,
- brezpilotna letala,
- oprema za odkrivanje orožij,

[69] Human Intelligence
[70] Weapon Location and Force Protection
[71] Intelligence, Surveillance, Reconnaissance

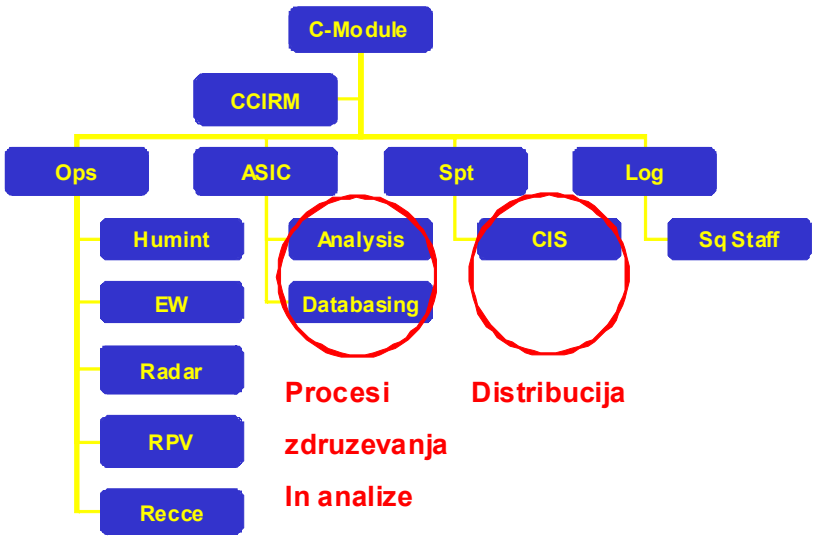
- goniometri in oprema za spremljanje zvez,
- oprema za zaščito sil in nadzor prostora,
- sile za izvidništvo globoko v nasprotnikovem zaledju (LRSP[72]),
- oprema za opazovanje na terenu (v vseh elektromagnetnih in svetlobnih spektrih),
- zmogljiva, avtonomna, terenska komunikacijska in informacijska oprema.

7.5 KONCEPT ISTAR NA NIZOZEMSKEM

7.5.1 Modularna organiziranost

Nizozemske oborožene sile so se odločile združiti zmogljivosti pridobivanja obveščevalnih informacij na različne načine pod enotno organizacijsko streho, ki jo imenujejo ISTAR. Ta sistem ali organizacijo razumejo kot s strani poveljnika vodeno, načrtno usmerjeno, vse-obsegajočo, neprekinjeno in analitično dejavnost posebej opremljenih in izurjenih sil in sredstev, s katerimi zagotavljajo čim bolj popolne, pravilne in pravočasne informacije za varno in uspešno realizacijo nalog. To dosežejo tako, da zagotovijo zbiranje, hranjenje, analiziranje in izmenjavo informacij na vseh nivojih v državi. Za potrebe vojske imajo organiziran ISTAR bataljon, ki je sestavljen tako, da zagotavlja modularno popolnjevanje enot ali poveljstev različnih nivojev do bataljona (Timmermans 2006).

Slika 7-3: Načelna organizacijska shema nizozemskega modula ISTAR.



Vir: Netherland Royal Army 2007, 1.

[72] Long Range Surveillance Patrol.

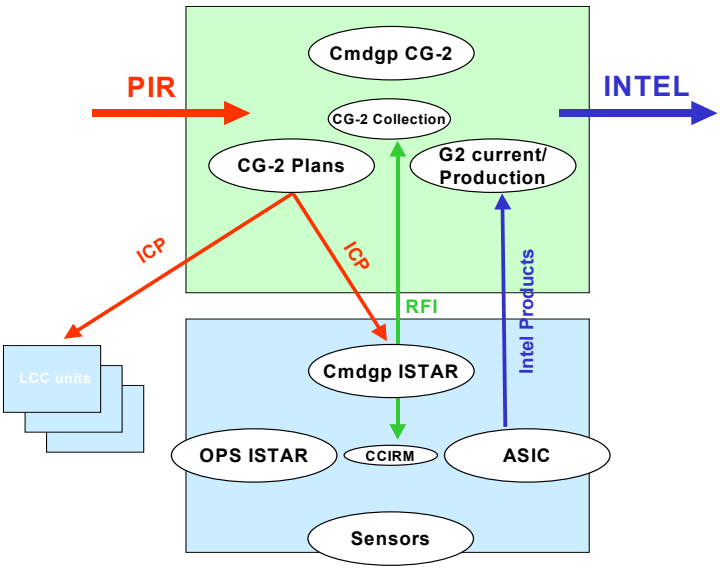
LEGENDA: C-module – poveljniški modul
CCIRM – modul za upravljanje s tokom informacij
Ops – operativni moduli za HUMINT, Elektronsko bojevanje, senzorski sistemi in radarji in izvidništvo.
ASIC – modul za združevanje, shranjevanje, razvrščanje in analizo informacij iz vseh virov.
Spt – skupina za komunikacijsko informacijsko podporo.
Log – skupina za logistično podporo.

Na sliki 7-3 je razvidno, da načelno ISTAR modul sestavljajo ekipe za zbiranje podatkov s človeškimi viri, senzorji in radarji različnih zmogljivosti, prisluhom elektronskim povezavam nasprotnika in klasičnim izvidništvom. Poleg tega so v drugih skupinah modula skriti še strokovnjaki za analizo odprtih virov, povezavo z zračno radarsko sliko, zbiranje in analizo geo podatkov in slikovnega materiala v različnih svetlobnih spektrih, povezavo v baze podatkov višjih poveljstev ter obrambnih in/ali civilnih agencij.

Sestav takega modula omogoča tudi povezavo na velike razdalje prek satelitov z oddaljenimi bazami podatkov, varno posredovanje podatkov, analiz in ocen naročnikom v poveljstvu ali enoti, ki ji pripadajo.

Načelno je lahko tak modul pridodan tudi v mednarodno enoto, deluje pa običajno pod okriljem obveščevalnega organa poveljstva, ki so mu pridodani.

Slika 7-4: Načelna shema sodelovanja pridodanega nizozemskega ISTAR modula z obveščevalnim organom poveljstva.



Vir: Netherland Royal Army 2007, 4.

.

Na sliki 7-4 je razvidna načelna shema sodelovanja nizozemskega modula ISTAR z obveščevalnim organom poveljstva, ki mu je pridodan.

Sodelovanje poteka tako, da obveščevalni organ poveljstva (CG-2) na osnovi prioritetnih obveščevalnih zahtev (PIR – Priority Information Requirement) izdela načrt zbiranja obveščevalnih podatkov (ICP – Intelligence Collection Plan), ki ga pošlje tako v podrejene enote kot v ISTAR modul. V ICP so opredeljeni cilji in dodeljene naloge enotam ter ISTAR modulu z namenom dekonflikcije obveščevalnih aktivnosti in usmerjenemu delovanju na obveščevalnem področju.

Težišče obveščevalnega dela je na ISTAR modulu, ki podrobneje razdela naloge za svoje skupine in enote in opredeli morebitna dodatna vprašanja (RFI – Request for Information) za sodelujoči obveščevalni organ. Tok RFI v eno in v drugo smer je neprestan in nujen v času delovanj enot za izmenjavo informacij in sprotno usmerjanje dela ISTAR elementov.

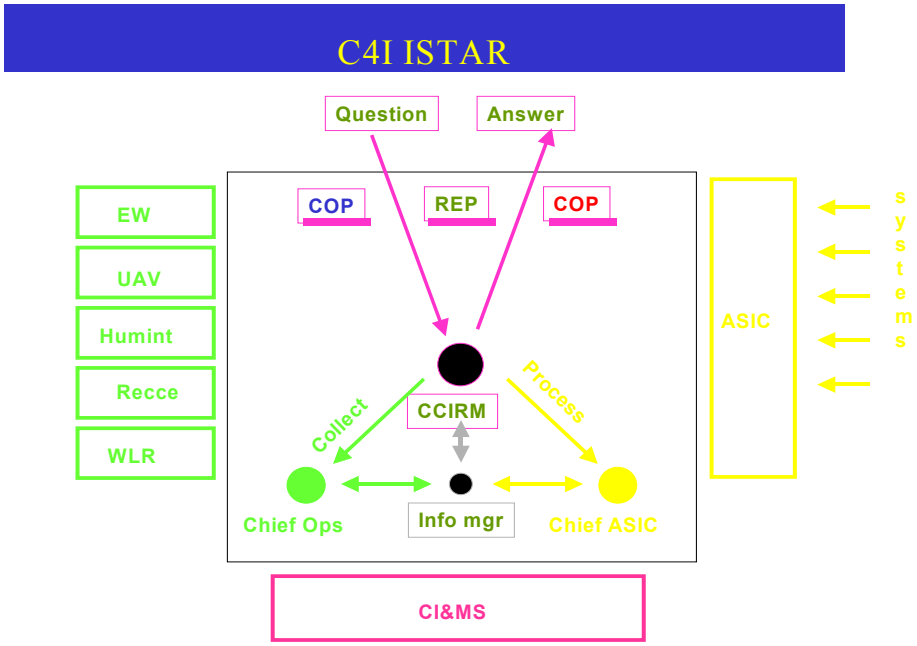
V ISTAR modul se neprestano stekajo obveščevalni podatki skupin modula in enot nadrejenega poveljstva, kjer se razvrščajo, uredijo po prioriteti in zanesljivosti, primerjajo s prej ali drugače dobljenimi podatki in izdelujejo zaključki v obliki posodobljenih pisnih obveščevalnih ocen, grafičnih izdelkov v obliki kart, klasičnih ali digitalnih slik območja delovanja ali zgolj odgovorov na prejete obveščevalne zahteve.

7.5.2 Notranji tok informacij

Notranja organiziranost tako CG-2 kot tudi ISTAR modula mora zagotoviti urejen, pregleden in razumljiv tok informacij in dokumentov, ki mora zagotoviti nadzorovan dostop do informacij, ocen in drugega gradiva brez zamud vsem, ki so jim le-te potrebne.

Slika 7-5 prikazuje avtomatiziran tok informacij med uporabniki ISTAR zmogljivosti in notranjim ustrojem ISTAR enote. Ker mora komunikacija potekati na varen in sledljiv način, je zahtevnost tako glede strojne in programske opreme kot tudi organiziranosti pretoka informacij zelo visoka. Zahteva se namreč, da ISTAR enote (prikazane v zeleni barvi) s svojim delom zbrane podatke pri sebi shranijo v svoje baze podatkov, jih glede na obveščevalne zahteve opremijo ali povežejo z relevantnimi podatki, ki so jih na svojem nivoju morda zbrali že prej, in posredujejo že tako deloma obdelane informacije v ASIC .

Slika 7-5: Shema C4I ISTAR sistema v nizozemski vojski.



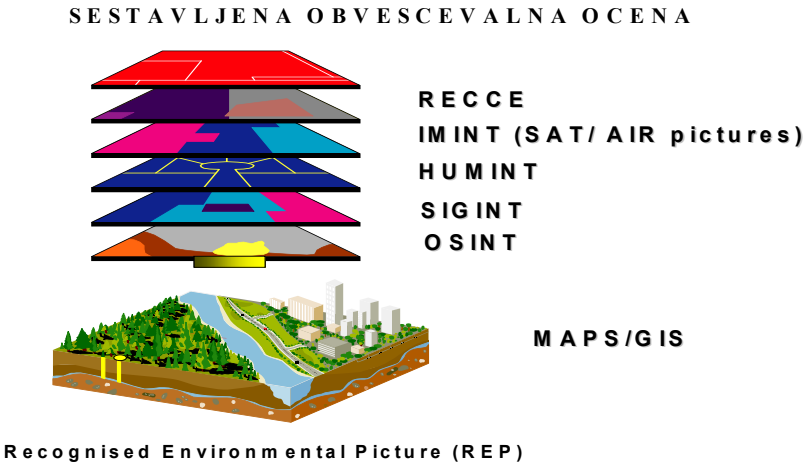
Vir: Netherland Royal Army 2007, 6.

Tam jih združijo z drugače pridobljenimi informacijami (glede na PIR ali RFI) in izdelajo posodobljene ali na novo dognane ocene in zaključke. Ti gredo prek sistema urejanja toka informacij nazaj naročnikom v njihovo nadaljnjo uporabo. Proces mora potekati hitro, varno in istočasno na več naslovov. Obenem se posodabljajo tudi ustrezne baze podatkov.

7.5.3 Združevanja informacij v obveščevalni izdelek in posredovanje naslovnikom

ISTAR enote nizozemske vojske so opremljene s sodobno informacijsko in komunikacijsko tehnologijo, ki omogoča izmenjavo informacij na velike razdalje na varen način, tako tudi neposredno upravljanje s kolektorji na daljavo. Ta oprema predstavlja kritično točko uspešnosti dela ISTAR enot in sistema. Slika 7-6 prikazuje enega od izdelkov analitične skupine ISTAR, potem ko je združila in smiselno uredila pridobljene podatke glede na PIR in RFI, tako da lahko naročniki uporabijo oziroma dobijo celovito informacijo ali pa le njene dele.

Slika 7-6: Načelni primer sestavljenega obveščevalnega izdelka ISTAR enote.

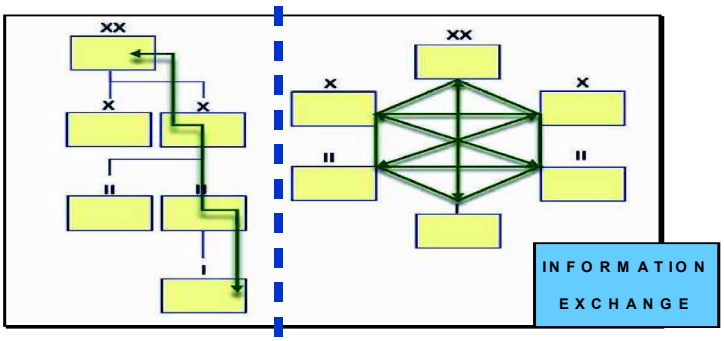


Vir: Netherland Royal Army 2007, 7.

Smisel tako sestavljene informacije je tudi v tem, da v primeru sprememb lahko dopolnimo ali posodobimo le tisti segment, kjer je sprememba nastala. Na ta način prihranimo čas in zmogljivosti in zagotovimo boljšo preglednost razvoja situacije. Tudi za take izdelke je potrebna sodobna in zmogljiva informacijska tehnologija ter dobro izurjena ekipa operaterjev in analitikov.

Slika 7-7 prikazuje razliko med sedanjim načinom izmenjave informacij in tistim v preteklosti. Najbolj pomembna razlika je v tem, da je pot informacij še ne dolgo tega potekala strogo po organizacijski piramidi, danes pa je izmenjava organizirana mrežno in ploščno, tako da lahko vsak izmenjuje informacije z vsakomer in vendar na sledljiv in urejen način. Leva stran slike 7-7 prikazuje potek informacij v preteklosti, desna stran pa ponazarja današnje mreže uporabnikov in posredovalcev informacij. ISTAR sistem deluje na principu mrežne in ploščne organiziranosti izmenjave informacij.

Slika 7-7: Prikaz razlik v poteku informacij v nizozemski vojski danes in v preteklosti.



Vir: Netherland Royal Army 2007, 10.

.

8 ISTAR SLOVENSKE VOJSKE

ISTAR zmogljivosti SV so v razvoju in predvidevajo, da bi v nekaj letih sistem razvili do stopnje, ko bi lahko polnopravno sodeloval v mednarodnem okolju. Trenutno ni jasno začrtanih zmogljivosti ali organigrama, razmišljajo pa predvsem o senzorskih sistemih za pravočasno odkrivanje nevarnosti in avtomatiziranem prenosu signalov.

Ker je naše izhodišče, da je ISTAR sistem sistemov, bi rad v tej nalogi predstavil tudi druge, ravno tako ali pa še bolj pomembne elemente sistema ISTAR, ki jih je potrebno vključiti v koncept izgradnje slovenskega ISTAR. Rad bi predstavil tako različico možnega modela slovenskega ISTAR, ki bi upošteval že zgrajene obveščevalne zmogljivosti ter tiste, ki so danes še v povojih in so finančno dosegljive.

8.1 OBVEŠČEVALNA DEJAVNOST V SLOVENSKI VOJSKI

Iz navedene definicije so razvidni nosilci vojaške obveščevalne dejavnosti. V ožjem smislu so to:

1- štabni obveščevalni organi (S/G/J-2), ki načrtujejo obveščevalni ciklus, obdelujejo in posredujejo obveščevalne podatke;
2- obveščevalno-izvidniški bataljon (OIB) SV, ki je namenjen za izvajanje taktične obveščevalne dejavnosti SV oziroma za izvajanje vseh faz obveščevalnega ciklusa;
3- izvidniške enote SV (v bataljonih in brigadah), ki večinoma izvajajo le fazo zbiranja in posredovanja neobdelanih oziroma delno interpretiranih informacij.

V širšem smislu so nosilci vojaške obveščevalne dejavnosti vsa poveljstva, enote in pripadniki SV, saj so dolžni neprekinjeno spremljati situacijo in poročati o njej. Med temi so enote, ki imajo tudi ustrezna tehnična sredstva za zbiranje informacij (enota za nadzor in obrambo zračnega prostora in akvatorija, artilerijske enote s svojimi opazovalnicami ipd.).

Delovanje obveščevalne dejavnosti znotraj SV je urejeno s podzakonskimi akti ter akti poveljevanja in kontrole (PINK), razen Enote za elektronsko bojevanje (EEB) v delu, ki se nanaša na elektronsko izvidništvo[73]. Glede na nesporno dejstvo, da vojaška obveščevalna dejavnost v Slovenski vojski obstaja, in glede na dvome o legalnosti delovanja, še posebej v

[73] Urejeno v Zakonu v obrambi.

mednarodnih vojaških operacijah, se zastavlja vprašanje, ali ne bi bilo morda smotrno to dejavnost primerno urediti tudi v ustreznih zakonih.

Obveščevalni dejavnosti na obrambnem področju in znotraj Slovenske vojske bi morali biti neločljivi, zato bi Obveščevalno varnostna služba Ministrstva za obrambo (OVS-MORS) in vojaški obveščevalni organi SV morali med seboj tesno sodelovati. Načelno sicer sodelovanje že sedaj opredeljuje ReDPROSV[74], točka 3.6.2.

Z opredelitvijo osnovnih pojmov (npr. varnost, varnostna politika, oborožene sile, obveščevalna dejavnost, vojaška obveščevalna dejavnost …) in definicij (npr. vojaška obveščevalna dejavnost), kakor so jih opredelili različni avtorji in kakor jih razumem in uporabljam v tem delu, smo dobili kategorijalni aparat, nujno potreben za nadaljnje delo, tako da se lahko lotimo proučevanja vojaške obveščevalne dejavnosti.

8.1 VOJAŠKA OBVEŠČEVALNA DEJAVNOST (VODBE)

VODBE je namenjena podpori poveljevanju in kontroli v SV. Organizirana mora biti tako, da v največji možni meri omogoča zavedanje situacije ter podpira odločanje na vseh ravneh poveljevanja in v celotnem spektru operacij, za katere se pripravlja SV.

Za dosego tega cilja VODBE potrebuje koncept razvoja, ki ima dva temeljna namena:

1. Predstavlja razvojne, organizacijske in druge usmeritve ter izhodišča za pripravo in izvedbo oblikovanja obveščevalnega področja v SV ter delovanje v strukturah in operacijah zavezništev.

2. Predstavlja stališča in vizijo stroke o bodoči organiziranosti in delovanju tega področja, ki bo kot okvirni načrt služil stroki sami, in tudi preostali sestavi SV.

VODBE ne odpira novega poglavja v razvoju, pač pa je nadgradnja predloga *Koncepta obveščevalno izvidniške zagotovitve iz 2003*, ki je nastal pred vstopom Slovenije v NATO in EU.

Današnje naloge in poslanstvo SV so:

1. Preprečevanje agresije in ustrezno reagiranje na agresijo:

[74] Resolucija o dolgoročnem programu razvoja in opremljenosti Slovenske vojske.

a. izvajanje operacij nacionalne vojaške obrambe (nadzor, kontrola in zaščita kopnega, morja in zračnega prostora ter obramba državnega ozemlja);
b. sodelovanje v operacijah v okviru mednarodnih organizacij (kolektivna obramba po 5. členu Severnoatlantske pogodbe in tudi operacije zunaj tega člena).

2. Vojaško prispevanje k mednarodnemu miru, varnosti in stabilnosti, ki obsega:

   a. obrambno diplomacijo (dvostransko in večstransko sodelovanje);
   b. graditev varnosti in zaupanja, uravnavanje oboroževanja in preprečevanje širjenja orožja za množično uničevanje (nadzor oborožitve in razorožitve, inšpekcijski nadzor tujih vojaških enot ter verifikacijske dejavnosti);
   c. operacije kriznega odzivanja:
      - NATO operacije o čl. 5. pogodbe in zunaj tega člena (non article 5. operations),
      - EU operacije,
      - preventivna diplomacija, preprečevanje konfliktov in ohranjanje, vsiljevanje ali vzdrževanje miru, humanitarna pomoč, pomoč pri izvajanju humanitarne pomoči ter boj proti mednarodnemu terorizmu in drugim grožnjam miru.

3. Podpora sistema zaščite, reševanja in pomoči ter drugim državnim organom in organizacijam obsega:

   a. sodelovanje pri nalogah zaščite, reševanja in pomoči ob naravnih in drugih nesrečah v skladu z načrti, opremljenostjo in organizacijo vojske;
   b. sodelovanje s policijo v skladu z načrti pri varovanju državne meje, sodelovanje pri obvladovanju velikih in ilegalnih migracij, sodelovanje pri preprečevanju in boju proti terorizmu ter pri izvajanju drugih nalog z njenega področja dela;
   c. iskanje in reševanje iz zraka, na morju in na kopnem;
   d. podporo znanstvenoraziskovalni in tehnološki razvojni dejavnosti na obrambnem področju (sodelovanje pri načrtovanju, organizaciji in upravljanju nacionalnih obrambnih raziskav ter tehnologij in podpora projektom namenske industrije);

e. evakuacijo državljanov Republike Slovenije iz tujine v kriznih in vojnih razmerah.

Poslanstva in naloge neposredno določajo obseg in zmogljivosti Slovenske vojske, ki se že intenzivno prilagaja in reorganizira v tej smeri. Ti procesi, naloge in poslanstvo terjajo tudi ustrezno (re)organizacijo obveščevalne dejavnosti SV. Ta mora biti sposobna Slovenski vojski zagotoviti obveščevalno podporo odločanja v celotnem spektru navedenih poslanstev in nalog SV.

8.2 POSLANSTVO VOJAŠKE OBVEŠČEVALNE DEJAVNOSTI SLOVENSKE VOJSKE

Na podlagi prednosti članstva v zavezništvu se je Republika Slovenija odpovedala razvijanju določenih obrambnih zmogljivosti. Zato vojaška obramba Republike Slovenije temelji na uporabi združenih sil zavezništva, v katerih bodo integrirane sile Slovenske vojske (Furlan 2006). Republika Slovenija in Slovenska vojska sta se kljub temu odločili za celovito vojaško obveščevalno dejavnost.

VODBE SV neprekinjeno podpira delovanje SV v miru, krizi in vojni na strateški, operativni in taktični ravni poveljevanja in v celotnem spektru operacij, za katere se pripravlja SV.

V Slovenski vojski se vojaška obveščevalna dejavnost izvaja izključno za podporo vojaških načrtovanj in delovanj in za podporo drugih državnih organov na podlagi usmeritev ministra za obrambo.

VODBE mora biti usklajena z dejavnostjo Obveščevalno-varnostne službe Ministrstva za obrambo (OVS MORS).

8.3 NAČELA OBVEŠČEVALNE DEJAVNOSTI SLOVENSKE VOJSKE

Načela so zbrana in urejena splošna strokovna vodila za delovanje, potrjena v praksi SV in tujih oboroženih sil. Pomembnost posameznega načela je pogosto odvisna od ravni poveljevanja in drugih dejavnikov. Pripadniki SV so pri svojem delu načela dolžni poznati in upoštevati. Načela namreč zagotavlja optimalne možnosti za uspeh. Priznati je potrebno, da se uveljavljanje načel zmanjšuje sorazmerno z nižanjem ravni poveljevanja, kar pomembno vpliva na slabo izkoriščenost ter organizacijske in strokovne pomanjkljivosti VODBE SV na vseh ravneh poveljevanja.

a) **Načelo zakonitosti.** Celotna vojaška obveščevalna dejavnost SV se izvaja v skladu z obstoječo zakonodajo in podzakonskimi akti in sprejetimi standardi in doktrinami. Dolžnost vseh pripadnikov VODBE SV je, da stalno skrbijo za uresničevanje tega načela.

b) **Centraliziranost načrtovanja in decentraliziranost izvedbe.** To načelo je sicer splošno sprejeto v sodobnih obveščevalnih službah, vendar mu VODBE SV ne sledi. Dejstvo je, da strokovna linija J/G/S-2 ni centralizirano vodena, temveč je to prepuščeno posameznim poveljnikom. Organske[75] enote in sredstva (senzorji) so uporabljeni skladno z zamislijo in načrtom nadrejenega, uporaba enot in sredstev pa temelji na iniciativi in kreativnih zamislih podrejenih na vseh ravneh poveljevanja. Za pravilno delovanje obveščevalnih organov je odgovoren poveljnik enote.

c) **Pravočasnost.** Obveščevalni podatek nima nikakršne vrednosti, če ni pravočasno poslan ali dostopen uporabniku. VODBE trpi za kroničnim pomanjkanjem hitrega sporočilnega sistema, ki bi varno in pregledno izmenjeval informacije in obveščevalne izdelke.

d) **Sistematično obdelovanje.** V procesu izvajanja obveščevalne dejavnosti se vsi obveščevalni podatki obdelujejo sistematično, z metodičnim delom, ki temelji na obveščevalnem krogu. VODBE je pri svojem delu manj uspešna tudi zato, ker se sistematično procesirajo le nekateri tipi podatkov, večina pa ne.

e) **Objektivnost.** Preprečujemo vsako skušnjavo, da bi prirejali informacije skladno z našim mnenjem in zamislimi.

f) **Dostopnost.** Uporabna informacija ali obveščevalni podatek mora biti dostopen obveščevalnemu osebju in uporabnikom, vendar je izmenjava teh izdelkov počasna in nepregledna, zato jih poveljniki uporabljajo zelo omejeno.

g) **Zaščita virov in informacij.** Vsi viri informacij, tudi vse informacije in informacijska infrastruktura so ustrezno zaščiteni v skladu z načelom zakonitosti.

h) **Stalno ocenjevanje.** Obveščevalne podatke je treba stalno pregledovati in po potrebi tudi dopolnjevati, upoštevaje nove informacije in primerjave z že znanimi podatki.

i) **Odzivnost.** Obveščevalno osebje se odziva na obveščevalne zahteve, ki jih postavlja poveljnik, vendar so zahteve poveljnikov zelo redke, zaradi česar je VODBE zelo omejeno in slabo izkoriščena.

[75] To so tisti deli enot, ki so v redni, vsakodnevni sestavi – npr. izvidniški vod v motoriziranem bataljonu.

8.4 METODE DELA

Temeljna metoda dela VODBE je obveščevalni krog. Sestoji se iz štirih korakov: usmerjanje, pridobivanje podatkov, obdelava in posredovanje. Iz obveščevalnega kroga izhajajo ali se nanj nanašajo druge, predvsem analitične metode (OPB, indukcija, dedukcija) in metode načrtovanja in usklajevanja različnih disciplin pridobivanja podatkov.

Pri tem je potrebno poudariti, da to v Sloveniji ni enotno rešeno in da različne službe uporabljajo različno število korakov v ciklu. (Črnčec 2009) pojasnuje vlogo obveščevalnega cilka s šestimi in petimi koraki. Obveščevalni krog je po njegovem razvijanje neobdelanih podatkov v obdelane obveščevalne izdelke za potrebe odločevalcev. Sestavljen je iz šestih korakov in sicer:

- zahteve (potrebe po infromacijah),
- načrtovanja in usmerjanja (upravljanje z zahtevami),
- zbiranja surovih informacij,
- obdelave in izkoriščanja (urejanje, združevanje, shranjevanje zbranih informacij),
- proučevanja in izdelave (pretvarjanje surovih podatkov v obveščevalne izdelke),
- posredovanja (distribucija izdelkov uporabnikom).

Isti avtor omenja še drugo možnost organizacije korakov obveščevalnega cikla, pri katerem se lahko združita prvi in drugi korak v enega, v katerem so zahteve, usmeritve in načrtovanje združene. Zahteve so namreč le osnova za načrtovanje in usmerjanje obveščevalne dejavnosti.

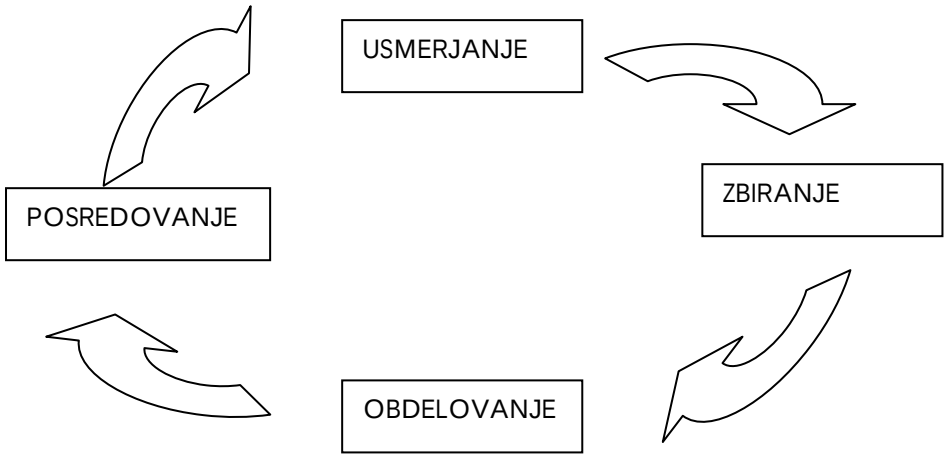
Vzpostavljen obveščevalni cikel je osnovni, prvi pogoj za uspešno in učinkovito delovanje vseh obveščevalnih služb. Potrebno je poudriti še to, da krog ne deluje kot samo stalen, enosmeren tok, temveč zahteva neprestano sodelovanje med različnimi deli in občasno zaradi posebnih potreb tudi s preskokom katerega naprej ali nazaj.

Tudi (Žabkar 2004) pojasnuje etape obveščevalne oskrbljenosti boja tako, da na prvo mesto postavi ugotovitev potreb uporabnikov, temu sledi načrtovanje zbiranja podatkov, potem zbiranje podatkov, v četrti etapi sledi proučevanje in preverjanje točnosti in zanesljivosti zbranih podatkov, v zadnji etapi je oblikovanje obveščevalnih informacij in seznanitev porabnikov z njihovo vsebino.

8.4.1 Obveščevalni cikel v Slovenski vojski

V SV načeloma sledijo štirikoračnemu obveščevalnemu ciklu, kot jih opredeljuje AJP 2.0. Ta standard je s sprejemom v zbirko slovenskih vojaških standardov postal obvezen za SV, istočasno pa zagotavlja načelno povezljivost z obveščevalnimi sistemi članic NATA. Izvajanje korakov cikla je različno v različnih enotah, 5.OIB pri svojem delu uporablja proces, ki je bolj podoben Žabkarjevi različici, ob tem da za pisne izdelke uporablja formate, ki so predpisani v AJP 2.0 in 2.1

Slika 8-1: Obveščevalni cikel.



Vir: AJP 2.0 – Združena obveščevalna, protiobveščevalna in varnostna doktrina

8.4.1.1 Usmerjanje

1. **Pomanjkljivo usmerjanje organov S/G/J-2** s strani poveljnika je v VODBE SV glavna pomanjkljivost, čeprav je to njegovo osnovno orodje, s katerim daje jasna in precizna navodila o tem, kakšne informacije in obveščevalne podatke potrebuje (KIZ in POZ – angl. CCIR[76]), po kakšnem vrstnem redu prioritete in do kdaj jih potrebuje.

2. **Usmerjanje enot in virov** za zbiranje informacij s strani S/G/J-2, ki predstavlja temelj *načrta zbiranja.* Načrt se sestoji iz *informacijskih zahtev*[77] (IZ), *indikatorjev* ter *nalog organskim in pridodanim enotam in virom*. Tudi v tem segmentu ne zajemamo vseh razpoložljivih zmogljivosti, najbolj so zapostavljene ozko specializirane obveščevalne discipline.

[76] KIZ: Kritične informacijske zahteve; POZ: Prioritetne obveščevalne zahteve (praviloma 7−10 zahtev). CCIR: Commander's Critical Information Requirement.
[77] Information Requirement.

Usmerjanje se načeloma uresničuje skozi proces *koordinacije zbiranja in upravljanja z obveščevalnimi zahtevami* (CCIRM)[78], ki je sestavljen iz dveh komponent: *koordinacije pridobivanja podatkov* in *upravljanja z obveščevalnimi zahtevami*, vendar v SV upravljanje z obveščevalnimi zahtevami ni najbolj razvito.

S ciljem pridobiti odgovor na informacijske zahtevke, ki jih S/G/J-2 ne more zbrati z organskimi ali dodanimi enotami in viri, S/G/J-2 na ustrezni organ naslovi *Zahtevek za informacijo* (ZZI).

8.4.1.2 Zbiranje podatkov

Predstavlja zbiranje podatkov iz različnih virov (osebe ali stvari) ter njihovo pravočasno dostavo ustreznemu organu za obdelavo in izdelavo obveščevalnega izdelka. Podatke lahko pridobivajo enote od virov ali pa organi S/G/J-2 od enot in virov.

Pridobivanje izvajajo z eno ali več obveščevalnimi disciplinami in metodami zbiranja. SV pridobiva podatke na vseh ravneh poveljevanja z lastnimi zmogljivostmi, ob sodelovanju z OVS ter z mednarodno izmenjavo obveščevalnih podatkov. Poleg resničnosti in pravočasnosti morajo biti podatki tudi kakovostni (relevantni).

Pri razvrščanju obveščevalnih podatkov obstajajo tri ravni, na podlagi katerih je predviden namen njihove uporabe.

Strateška obveščevalna dejavnost. Strateška obveščevalna dejavnost je obveščevalna dejavnost, ki je potrebna za oblikovanje politike in vojaških načrtov na državnih in/ali mednarodnih ravneh in predstavlja najvišjo raven obveščevalnih podatkov.

Operativna obveščevalna dejavnost. Operativna obveščevalna dejavnost je obveščevalna dejavnost, ki je potrebna za načrtovanje in izvajanje vojaških operacij na operativni ravni.

Taktična obveščevalna dejavnost. Taktična obveščevalna dejavnost je obveščevalna dejavnost, ki je potrebna za načrtovanje in izvedbo operacij na taktični ravni.

8.4.1.3 Obdelava

Obdelava je korak, v katerem informacija postane obveščevalni podatek (angl.: *Intelligence*). Obdelava poteka na vseh ravneh obveščevalne dejavnosti. Na najnižji ravni zbiranja se surove

[78] Angl.: CCIRM: Collection, Coordination and Infomation Request Management.

informacije med obdelavo spremenijo v razumljiv izdelek. Na vsaki naslednji (višji) ravni poveljevanja se te informacije postavijo v kontekst novih dejstev, ki na nižji ravni niso bila dostopna, kar prvotni informaciji vsakič dodaja novo vrednost.

Obdelava obsega: *sortiranje*, *vrednotenje, analizo in integracijo* ter *interpretacijo*.

Rezultat interpretacije je obveščevalni izdelek (obveščevalno poročilo, ocena, informacija, povzetek, analiza ipd.). Ti izdelki v SV ne morejo slediti obveščevalnim zahtevam, ker jih poveljniki običajno ne opredelijo, to pa pomeni, da niso izdelani ciljno, temveč običajno vsebujejo splošne ocene situacije, ne glede na raven enote, za katero se izdelujejo. Ta pomanjkljivost je še najmanj izražena na strateškem nivoju.

8.4.1.4 Posredovanje

Posredovanje (angl.: *Dissemination*) uporabnikom pomeni pravočasno zagotovitev informacije ali obveščevalnega izdelka. Pri tem je najpomembneje, da ima izdelek uporabno vsebino (odgovori na POZ poveljnika) in je dovolj zgodaj poslan, da ga uporabnik lahko pravočasno prejme. Pomembni so tudi pravilna oblika in format ter ustrezen obseg izdelka, pri komunikaciji z NATOM pa tudi uporaba razumljivega[79] angleškega jezika. Pravočasnost je najbolj kritična na taktični ravni, kjer je na razpolago najmanj časa in osebja, potreba po pravočasnih in točnih informacijah pa izredno velika.

Obveščevalni podatki morajo biti ustrezno stopnjevani (označeni z ustrezno stopnjo tajnosti) in šifrirani (prevelika stopnjevanost otežuje dostop do informacij, premajhna pa ogroža varnost operacije in obveščevalnih virov). Kot splošno pravilo velja, da če nasprotnik nima časa za reakcijo, informacije ni potrebno stopnjevati in šifrirati. V vsakem primeru pa je potrebno zaščititi vir informacij. Kompromitirani vir praviloma postane neuporaben, človeški vir pa lahko tudi življenjsko ogrozimo.

Uporabnik na koncu oceni ustreznost izdelka in po potrebi izda nov zahtevek za informacijo, oziroma poveljnik izda novo *prioritetno obveščevalno zahtevo* (POZ), s čimer se prične nov obveščevalni krog. V nasprotnem se obveščevalni krog s tem zaključi.

[79] Izraz "razumljiv" tukaj pomeni, da je bolj pomembna razumljivost izdelka kot pa odlična uporaba angleščine. Uporabnik bo bolj cenil uporabnost informacije kot pa lepoto jezika ter pestrost izrazov, s katerimi je napisana. To pa seveda ne pomeni, da je lahko analitik po vprašanju angleškega jezika "na pol pismen".

8.5 DISCIPLINE PRIDOBIVANJA PODATKOV

SV že sedaj razpolaga z omejenimi zmogljivostmi nekaterih obveščevalnih disciplin, manjkajoče pa mora zaradi zagotovitve celovite obveščevalno-varnostne podpore postopoma razviti oziroma nadgraditi. Trenutne zmogljivosti so prisotne v sledečih disciplinah:

a. Pridobivanje podatkov z izvidniškim delovanjem in nadzorom prostora (angl.: *Reconnaissance & Surveillance*).
b. Pridobivanje podatkov iz dostopnih javnih virov (angl.: *Open Source Intelligence/ OSINT*).
c. Pridobivanje podatkov s pomočjo človeških virov (angl.: *Human Intelligence/ HUMINT*).
d. Pridobivanje podatkov s prestrezanjem signalov (angl.: *Signals Intelligence/ SIGINT*).
e. Pridobivanje podatkov iz geografskih virov (angl.: *Geograffical Intelligence/ GEOINT*).

Za določene discipline je potrebno dograditi tehnično in kadrovsko bazo, za nekatere (npr. HUMINT in SIGINT) pa tudi urediti normativno podlage (zakonodajo in predpise).

8.6 NOSILCI OBVEŠČEVALNE DEJAVNOSTI SLOVENSKE VOJSKE

VODBE SV izpolnjuje svoje poslanstvo na strateški (OVS, GŠSV, OOA, OPVD), operativni (PSSV) in taktični ravni poveljevanja (podrejena poveljstva in enote). Ravni obveščevalne dejavnosti se medsebojno močno prepletajo in dopolnjujejo. Posamezni organi, ki izvajajo obveščevalno dejavnost SV, jo lahko izvajajo za več ali celo za vse ravni. Med njimi mora veljati načelo sodelovanja in dopolnjevanja. Pretok obveščevalnih izdelkov med vsemi nivoji mora biti jasen in preprost, in omogočati mora neposredne, direktne povezave med uporabnikom in izvajalcem, ob hkratni možnosti nadzora. S tem najbolje dosegamo glavni cilj VODBE.

Organizacijsko je sistem vojaške obveščevalne dejavnosti SV umeščen na treh ravneh:

- Strateška raven: OVS, J-2[80] GŠSV, Oddelek za obveščevalne analize (OOA) ter

[80] J-2 je štabni organ za varnostno-obveščevalno dejavnost v Generalštabu Slovenske vojske (GŠSV). Pri tem je številka 2 oznaka organa za varnostno-obveščevalno dejavnost. V štabni organiziranosti ima vsak štabni organ/sektor svojo številko; 1 za kadrovske zadeve, 2 za varnostno-obveščevalno dejavnost, 3 za operativne

Oddelek za posebne vojaške dejavnosti (OPVD) v Centru za doktrino in razvoj (CDR).

- Operativna raven: G-2 Poveljstva sil SV (PSSV), G-2 Poveljstva za doktrino, izobraževanje in usposabljanje (PDRIU), Obveščevalno-izvidniški bataljon (OIB), Nacionalne obveščevalne celice (NOC).
- Taktična raven: S-2 poveljstva brigad SV, S-2 poveljstva bataljonov SV, taktične izvidniške enote.

V širšem smislu so elementi oziroma nosilci obveščevalne dejavnosti SV tudi:

1. pehotne in artilerijske opazovalnice,
2. enota za zaznavanje in opazovanje RKB dogodkov,
3. letalske enote,
4. enote za nadzor zračnega prostora in zračne obrambe,
5. enota za nadzor morske površine in globine,
6. vsak pripadnik ali enota SV, kadar sporoča podatke obveščevalnega pomena[81],
7. državni organi, družbene organizacije in državljani, ki v okviru svojega delovanja in pristojnosti prihajajo do obveščevalno zanimivih podatkov.

8.7 STRATEŠKA RAVEN ORGANIZIRANOSTI OBVEŠČEVALNE DEJAVNOSTI SLOVENSKE VOJSKE

Nosilci VODBE SV so v širšem smislu vsa poveljstva, enote in posamezniki, saj so dolžni spremljati situacijo, poročati o aktivnostih nasprotnika, sodelovati v medsebojnem obveščanju in izvajati ukrepe za zaščito sil. V ožjem smislu VODBE SV načrtujejo in izvajajo namensko organizirani in usposobljeni štabni organi (S/G/J-2), obveščevalno-izvidniške enote ter posamezniki, s svojim znanjem, veščinami, opremo in oborožitvijo.

Na strateški ravni se zbirajo, analizirajo in posredujejo obveščevalne informacije, ki jih za odločanje potrebujejo Generalštab SV in Ministrstvo za obrambo, v širšem smislu pa tudi ostali organi nacionalno-varnostnega sistema Slovenije (Svet za nacionalno varnost (SNAV) in Državni operativni štab obrambe (DOŠO), kadar se formira). Na strateški ravni odločanja VODBE SV omogoča analiziranje, spremljanje in predvidevanje splošne vojaško-politične

zadeve, 4 za logistiko. J označuje posamezne štabne sektorje na GŠSV, G na operativnem nivoju in S na taktičnem nivoju.

[81] Od enot v stiku z nasprotnikom med bojevanjem pa vse do pripadnika, ki se vrača s službene poti in poroča o svojih ugotovitvah. Vsak pripadnik SV lahko vedno opazi kaj, kar ima obveščevalni, protiobveščevalni ali varnostni pomen, in je to dolžan sporočiti najbližjemu obveščevalno-varnostnemu organu.

situacije, situacije na obstoječih in bodočih kriznih žariščih ter vseh pojavov, ki predstavljajo dejansko ali potencialno grožnjo za SV ali interese R Slovenije kjerkoli po svetu. Na ta način VODBE na strateški ravni omogoča oblikovanje obrambne politike in vojaških načrtov ter uresničevanje nacionalnih interesov države. Na strateški ravni VODBE SV preko OVS na podlagi posebnih pogodb omogoča tudi povezovanje z obveščevalno-varnostnim sistemom zavezništva, EU in drugimi subjekti.

Integracija med J-2 in OVS s ciljem racionalizirati uporabo virov in procesov ter doseganja višje stopnje učinkovitosti na področju obrambne obveščevalne dejavnosti v *Strateškem pregledu obrambe (SPO) 2002-2003 z vizijo razvoja 2015* že obsega funkcijsko vključitev Oddelka za obveščevalne analize GŠSV (OOA) v strukturo obveščevalne analitike OVS. Cilj funkcionalne integracije OOA v OVS je doseganje višje stopnje racionalizacije, usklajenosti in dopolnjevanja z obveščevalno analitiko OVS. Na ta način povezana obrambna analitika bo z večdisciplinarnim pristopom izdelovala obveščevalne analize, ocene, poročila in druge izdelke s področja obrambe in varnosti in s tem omogočala razumevanje situacije, njeno spremljanje in predvidevanje na strateški ravni. Danes je ta integracija v zaostanku za zamislimi in ne dosega zastavljenih ciljev.

8.7.1 Obveščevalno varnostna služba (OVS) MORS

OVS opravlja obveščevalne (protiobveščevalne in varnostne) naloge na obrambnem področju. Na podlagi Strateškega pregleda obrambe (SPO) 2002–2003 in zamisli o integraciji OVS–J-2, bo OVS v zvezi z obveščevalno dejavnostjo SV postopoma prevzel naslednje naloge:

1. Zagotoviti obveščevalne podatke in izdelke na strateško- obrambnem področju za potrebe SV (obveščevalne ocene, povzetki, bilteni, analize, pregledi, opozorila ipd.),
2. *koordiniranje zbiranja in upravljanja z obveščevalnimi zahtevami* (KZUOZ) na obrambno-strateški ravni[82],
3. predvidevati, odkrivati, prepoznavati, analizirati, posredovati in spremljati indikatorje groženj na obrambnem področju na strateški ravni[83],
4. opravljati vloge edine vstopno- izstopne točke za izmenjavo obrambnih in vojaških obveščevalnih podatkov SV s tujino,
5. Organizirati in voditi nacionalne obveščevalne celice (NOC) v tujini,
6. Pripravljati ocene vojaške ogroženosti R Slovenije, v sodelovanju z OOA,

[82] Angl.: CCIRM: Collection Coordination and Infomation Request Management.
[83] Angl.: Indications and Warning.

7. izdelovati ocene varnostnega tveganja za enote in pripadnike SV, ki sodelujejo v mednarodnih operacijah, v sodelovanju z OOA,
8. navezovati stike s strokovnimi nosilci kompleksnih načinov pridobivanja obveščevalnih podatkov, ki jih SV ne izvaja (npr. za analizo zajete opreme in orožja (*TECHINT*), ter izvajati znanstvene meritve različnih sevanj (*MASINT*)) in rezultate analiz posredovati uporabnikom,
9. pripravljati in funkcionalno usmerjati delo vojaških diplomatskih predstavnikov,
10. sodelovati z J-2 pri načrtovanju in usmerjanju obveščevalne dejavnosti SV na strateški ravni,
11. sodelovati z OOA pri izdelavi in ažuriranju *Obveščevalne priprave bojišča* na strateški ravni, pri čemer zagotovi analizo dejavnikov iz svojega strokovnega področja (demografski, gospodarski, politični, varnostni ipd.),
12. sodelovati z J-2 v načrtovanju obveščevalne podpore procesov ciljenja, ocenjevanja bojnega delovanja, informacijskih in psiholoških operacij na strateški ravni,
13. sodelovati pri obveščevalno-varnostni pripravi moštva SV,
14. sodelovati pri obveščevalnem debrifingu moštva po končani operaciji,
15. sodelovati pri specialističnem usposabljanju enot in pripadnikov OD SV.

Na vojaško strateški ravni so nosilci VODBE: J-2 GŠSV, Oddelek za obveščevalne analize (OOA), ki je integriran v strukturo OVS, ter Oddelek za posebne vojaške dejavnosti v PDRIU/CDR. Tako na vojaško-strateški kot tudi na operativni ravni je SV uporabnik obveščevalnih izdelkov, ki jih na obrambnem področju zagotavlja OVS.

8.7.2 J-2 Generalštaba Slovenske vojske (GŠSV)

Je glavni nosilec vojaško-strateške VODBE v SV, opravlja razvojno, usmerjevalno in nadzorno funkcijo VODBE v SV na vseh ravneh poveljevanja in kontrole (PINK). Poleg te svoje osnovne funkcije, s sodelovanjem z OVS, zagotavlja tudi obveščevalno podporo GŠSV in PSSV. Obveščevalno podporo J-2 izvaja preko Oddelka za obveščevalne analize (OOA).

J-2 usmerja delo **Oddelka za obveščevalne analize (OOA)**, ki je funkcionalno umeščen v strukturo analitičnega sektorja OVS. Takšna organiziranost omogoča multidisciplinarni pristop pri izdelavi obveščevalnih izdelkov na področju obrambe in varnosti. OVS in OOA zagotavljata usklajeno obveščevalno podporo na vojaško-strateški ravni PINK. Prek OVS sta

J-2 in OOA na podlagi posebnih pogodb povezana tudi z obveščevalno-varnostnim sistemom zavezništva in z drugimi subjekti.

Naloge OOA so:

1. pridobivanje, obdelava in posredovanje obveščevalnih podatkov za potrebe SV;
2. preučevanje vseh vidikov organizacije, usposobljenosti, oborožitve, opremljenosti in morale tujih oboroženih sil (TOS), njihovih vojaških strategij in doktrin ter taktik, tehnik in postopkov (TTP) delovanja;
3. izdelava in ažuriranje *obveščevalne priprave bojišča (OPB)* na strateški ravni, v sodelovanju z OVS;
4. odkrivanje, prepoznavanje, analiziranje, posredovanje in spremljanje vojaških indikatorjev, in izvajanje zgodnjega opozarjanja na strateški ravni;
5. zagotavljanje obveščevalne podpore procesom ciljenja, ocenjevanja bojnega delovanja, informacijskih in psiholoških operacij na strateški ravni;
6. zagotavljanje strokovne podpore OVS na področju vojaške analitike;
7. *koordinacija zbiranja in upravljanja z obveščevalnimi zahtevami* (KZUOZ)[84] na vojaško- strateški ravni;
8. sodelovanje z VERC na področju načrtovanja in priprave vojaških verifikacij; inšpekcij in misij *Open Skies*, in obdelava ter posredovanje zbranih informacij;
9. načrtovanje in izvajanje funkcionalnega usposabljanja častnikov SV na področju obveščevalne analitike;
10. polnjenje in upravljanje z obveščevalnimi bazami podatkov VODBE SV;
11. sodelovanje z J-2 v načrtovanju obveščevalne podpore procesov ciljenja, ocenjevanja bojnega delovanja, informacijskih in psiholoških operacij na strateški ravni;
12. sodelovanje z OVS pri izdelavi ocene vojaške ogroženosti Republike Slovenije;
13. sodelovanje z OVS pri izdelavi ocene varnostnega tveganja za enote in pripadnike SV, ki sodelujejo v mednarodnih operacijah in
14. sodelovanje pri pripravah in usposabljanjih enot in pripadnikov SV;

[84] Slovenska kratica za angleški original CCIRM.

8.7.3 Center za doktrino in razvoj (CDR), oziroma Oddelek za posebne vojaške dejavnosti (OPVD)

Je nosilec raziskovalnega in znanstvenega dela, strokovnega razvoja, izdelave razvojnih in doktrinarnih dokumentov, in izdelave programov usposabljanja VODBE SV. OPVD je tudi nosilec nekaterih oblik usposabljanja na področju VODBE.

Naloge OPVD so:

1. izdelava konceptualnih, razvojnih in doktrinarnih dokumentov VODBE SV,
2. izdelava taktičnih študij in zahtevnikov za potrebe VODBE SV,
3. priprava strokovne literature za potrebe VODBE SV,
4. sodelovanje pri analizah "učenja na izkušnjah" na področju VODBE SV in predlaganje ustreznih ukrepov s področja dejavnosti,
5. je nosilec vojaško-strokovnega izobraževanja in usposabljanja (VSIU) z obveščevalnega področja,
6. izvajanje standardizacijskih postopkov na funkcijskem področju in
7. sodelovanje z domačimi in tujimi izobraževalnimi in znanstvenoraziskovalnimi ustanovami.

8.7.4 Verifikacijski center (VERC)

VERC je namenjen za izvajanje nalog na področju mednarodnih vojaških inšpekcij in verifikacij (sporazuma *CFE* in *Dunajski dokument*) ter dejavnosti v okviru sporazuma *Open Skies*. Pri tem na mednarodno dogovorjeni način prihaja do koristnih informacij o tujih OS, njihovi organizaciji, opremi, oborožitvi in objektih. V okviru misije Open Skies (sporazum o prostem preletu ozemlja držav podpisnic) VERC pridobiva tudi zračne posnetke ozemlja in objektov, ki prispevajo pomemben delež znanja o tujih OS.

VERC svojo dejavnost tesno povezuje z OOA.

8.8 OPERATIVNA RAVEN ORGANIZIRANOSTI OBVEŠČEVALNE DEJAVNOSTI SLOVENSKE VOJSKE

Na operativni ravni so nosilci VODBE: G-2 PSSV, G-2 PDRIU, Poveljniški center (POVC), Nacionalne obveščevalne celice (NOC), Obveščevalno-izvidniški bataljon (OIB), skupine za tehnično analizo, G-2 Poveljstva za podporo (PP), bataljon za nadzor zračnega prostora

(BNZP), bataljon zračne obrambe (BZO), artilerijski bataljon, bataljon RKBO, mornariški divizion, ter letalske enote SV.

8.8.1 G-2 Poveljstva sil Slovenske vojske (PSSV)

Je glavni nosilec VODBE na operativni ravni PINK. G-2 izvaja načrtovanje, organiziranje, usmerjanje in kontrolo VODBE PSSV. Zaradi pomembne vloge, nalog in pristojnosti PSSV, so tudi vloga, naloge in pristojnosti G-2 veliko večje od poveljstev primerljive ravni v tujih OS. PSSV načrtuje in izvaja vse vojaške operacije SV doma in v okviru operacij zavezništva, zato mora tudi G-2 zagotoviti učinkovito obveščevalno podporo za vse navedene operacije. V tem smislu mora G-2 zagotoviti potrebne organizacijsko-formacijske, strokovne, tehnične in druge kapacitete, s katerimi mora opraviti svoje poslanstvo v celotnem spektru operacij SV. Konkretna vsebina, intenziteta, obseg in zahtevnost obveščevalne podpore se spreminjajo glede na vrsto naloge, kompleksnost groženj, razpoložljivi čas in fazo delovanja. G-2 PSSV mora biti sposoben opravljati svoje poslanstvo tako v času, ko ni velikih aktivnosti, kot tudi v času intenzivnih delovanj in krize, ko nastopi nagla potreba po dodatnih virih. Te kompleksne in spreminjajoče se zahteve pred G-2 postavljajo velike izzive, ki terjajo prožno in dinamično organiziranost G-2, posledično pa tudi celotne VODBE SV.

Ena od pomembnih oblik organiziranosti G-2 je zato dopolnjevanje stalnih delovnih mest (angl.: *Permanent Establishment*/ *PE*) z občasnimi (kriznimi) (angl.: *Crisis Establishment*/ *CE*). Delo G-2 v času povečanih potreb temelji na vključevanju pripadnikov občasne sestave (angl.: *Augmentees*), ki se iz (trenutno) manj aktivnih poveljstev in enot SV za določen čas napotijo v G-2 ali S-2 POVC. Okrepitev G-2 z občasno sestavo omogoča večjo stopnjo odzivnosti VODBE, gospodarnejšo izrabo vojaških obveščevalnih kapacitet, boljše medsebojno poznavanje pripadnikov VODBE SV in večjo stopnjo usposobljenosti pripadnikov za različne naloge v okviru VODBE. Na enak način in z enakimi načeli je možno okrepiti vse organe VODBE, od poveljstva bataljona in višje.

8.8.2 Poveljniški center (POVC)

Je element osnovnega poveljniškega mesta (OPM), ki poveljniku PSSV zagotavlja funkcijo neprekinjenega PINK z enotami SV in zbiranja ter posredovanja informacij o aktivnostih tujih oboroženih sil na ozemlju RS in v tujini. POVC spremlja situacijo na območjih obveščevalnega interesa poveljnika PSSV oziroma tam, kjer se nahajajo enote in pripadniki SV.

8.8.3 Nacionalne obveščevalne celice (NOC)

Namenjene so (med ostalim) obveščevalni podpori SV, ko SV sodeluje na mednarodni vojaški operaciji. NOC je organizirana kot izpostava OVS v SV. NOC vzpostavi, organizira in vodi OVS, podrejena je poveljniku slovenskega kontingenta (SIKON), po strokovni liniji pa generalnemu direktorju OVS. Medsebojna razmerja OVS in SIKON so urejena z ustreznimi akti. NOC je vedno pod nacionalno pristojnostjo PINK (se ne podredi poveljniku mednarodne operacije, razen če ta prihaja iz SV). Strokovno pripravo moštva NOC izvaja OVS. Poleg delavcev OVS so v sestavi NOC tudi pripadniki SV.

8.8.4 Obveščevalno- izvidniški bataljon (OIB)

Namenjen je za usmerjanje, pridobivanje, obdelavo in posredovanje vojaških obveščevalnih podatkov, podatkov za usmerjanje ognjenih sistemov in ocenjevanje učinkov ognjenega delovanja, ter elektronsko bojevanje. Postopoma razvija zmogljivosti za izvajanje naslednjih nalog:

a. operativno- taktično izvidništvo in nadzor nasprotnika, vremena in zemljišča,
b. elektronsko bojevanje in elektronsko izvidništvo,
c. izvajanje ocene bojnega delovanja (OBD),
d. usposabljanje za izvedbo namenskih nalog skladno z operativnim ciklom,
e. preizkušanje nove obveščevalno- izvidniške opreme in oborožitve in
f. polnjenje in vzdrževanje specialističnih baz obveščevalnih podatkov.

Organizacijska struktura OIB

- Poveljstvo
- Poveljniško-logistična četa (POVLOGČ)
    - Vod za načrtovanje in analizo (VNA)
    - Vod za taktično zbiranje podatkov (VTZP)
    - Vod za komunikacijsko-informacijsko podporo (VKIP)
    - Logistični vod
- Enota za elektronsko bojevanje (EEB)

Organizacijsko-formacijska struktura OIB se bo razvijala postopoma in naraščala do leta 2018.

8.8.5 Skupine za tehnično analizo

V primeru najdbe novega tehničnega sredstva na bojišču je po položaju najstarejši pripadnik SV na kraju samem to sredstvo dolžan zavarovati in o najdbi poročati po liniji PINK (SVS STANAG[85] 2084). Obveščevalni organ enote, v katere coni odgovornosti se sredstvo nahaja oceni, ali lahko iz razpoložljivih pripadnikov SV glede na razmere in kompleksnost tehničnega sredstva sestavi skupino za tehnično analizo (angl.: *Technical Intelligence*). Če to ni možno, posreduje predlog za tehnično analizo nadrejenemu poveljstvu.

8.8.6 S-2 Poveljstva za podporo (PP)

Usmerja in usklajuje delo VODBE podrejenih poveljstev in enot, še posebej zdravstvene službe in EVOJ.

8.8.7 Zdravstvena služba Slovenske vojske

Pridobiva in obdeluje podatke in informacije s področja zdravstva, s katerimi načrtuje ukrepe zdravstvene oskrbe za enote in pripadnike SV in zavezništva. Podatke pridobiva od zveze NATO in EU, različnih mednarodnih organizacij ter pristojnih ministrstev in služb Republike Slovenije. V sestavi zdravstvene službe deluje organ S-2, ki skrbi za posredovanje zdravstveno pomembnih obveščevalnih informacij uporabnikom. Zdravstvena služba, poleg svoje redne dejavnosti, zagotavlja tudi podatke o zdravstveno-epidemiološki situaciji v območju delovanja sil SV ter predlaga zdravstvene ukrepe za zaščito sil.

8.8.8 Bataljon za nadzor zračnega prostora (BNZP) in bataljon zračne obrambe (BZO)

Formirata omrežje, sestavljeno iz radarjev dolgega dosega z namenom zgodnjega odkrivanja, prepoznavanja, sledenja in posredovanja podatkov o ciljih v zračnem prostoru ter premičnih radarjev kratkega dosega z namenom pokrivati "radarske sence" (angl.: *Gap Fillers*). Podatki iz radarskega omrežja so podlaga za računalniško obdelano sliko situacije v zračnem prostoru (angl.: *Recognised Air Picture/* RAP), ki predstavlja pomemben in neločljivi del celotne situacije v prostoru. Radarska slika je povezana tudi v skupno sliko situacije v zraku zveze NATO. Del sistema je tudi Operativni center nadzora zračnega prostora Republike Slovenije (angl.: *Air Souvereignity Operations Center*/ ASOC), namenjen spremljanju situacije v

[85] Angleška kratica za standardizacijski sporazum med članicami NATA, v katerem so navedene tehnične podrobnosti ali postopki, ki jih v svoje delo ali opremo uvedejo vse članice podpisnice takega sporazuma. Standardi so označeni z enoznačno štirištevilčno oznako in kratkim naslovom. Ko ga država sprejme, postane del nacionalnih predpisov in v Sloveniji dobi oznako SVS (Slovenski vojaški standard).

zračnem prostoru in ukrepanju pri različnih izrednih dogodkih. Skladno z načrti bo postopoma izvedena integracija podatkov slike o situaciji v zračnem prostoru v taktični informacijski sistem (TIS) PINK.

8.8.9 Artilerijski bataljon (AB)

Razpolaga z zmogljivostmi za odkrivanje ciljev na bojišču ter avtomatiziranim taktičnim sistemom za upravljanje ognjene podpore. Artilerijski bataljon formira artilerijske opazovalnice, opremljene z različnimi senzorji in sistemi za odkrivanje ciljev in usmerjanje ognja. Poleg svoje osnovne funkcije usmerjanja artilerijskega ognja ti sistemi s posredovanjem podatkov o ciljih v TIS PINK pomembno dopolnjujejo sliko o nasprotniku. Iskanje ciljev, določanje njihove lokacije in prenos slike za korekcijo ognja bo za potrebe artilerijskega bataljona lahko izvajala tudi enota brezpilotnih letal (BPL) iz sestave OIB. SV bo izvedla oceno izvedljivosti opremljanja AB s cenejšimi brezpilotnimi letali krajšega dosega (Srednjeročni obrambni program (SOPr) 2005-2010 in SOPr 2007-2012), namenjenimi za iskanje ciljev in usmerjanje artilerijskega ognja.

8.8.10 Bataljon za jedrsko, radiološko, kemično in biološko obrambo (BRKBO)

Zagotavlja zmogljivosti za RKB izvidništvo, oziroma za odkrivanje in ugotavljanje navzočnosti nevarnih kemičnih, bioloških in radioloških snovi. Za ta namen BRKBO formira RKB izvidniške skupine, ki se skladno s situacijo modularno vključijo v sestavo izvidniških enot SV in zavezništva. Poleg podatkov o RKB situaciji, BRKBO v TIS PINK posreduje tudi vremenske podatke na svojem območju odgovornosti. Pripadniki BRKBO v poveljstvih in štabih zagotavljajo tudi potrebne specialiste za področje RKBO (časnike za povezavo), ki na svojem specialističnem področju podpirajo proces OPB in izdelavo ostalih obveščevalnih izdelkov.

8.8.11 Mornariški divizion (MOD)

Postopoma povečuje zmogljivosti na področju opazovanja in nadzora na morju, pod površino in na obali, zmogljivosti za podvodno delovanje, minsko in protiminsko zaščito, poveljevanje in kontrolo ter iskanje in reševanje na morju. V sestavi MOD deluje Pomorski operativni center (POC), ki izvaja nadzor akvatorija in obale v območju odgovornosti. POC sodeluje pri kreiranju in vzdrževanju pomorske operativne slike in zagotavlja izmenjavo informacij z NATO v okviru mornariškega poveljniškega informacijskega sistema (MCCIS). Postopoma

bo izvedena integracija podatkov iz pomorske operativne slike v TIS PINK (Srednjeročni obrambni program (SOPr) 2005–2010 in SOPr 2007–2012).

8.8.12 Letalske enote Slovenske vojske

Niso namensko opremljene za izvidništvo iz zraka. Vseeno pa jih je možno uporabiti za vizualno izvidništvo, v omejenem obsegu pa tudi za tehnično snemanje iz zraka (z vkrcanjem osebe – snemalca s kamero), iz lebdenja ali v letu. Opremljanje letal in helikopterjev SV z namensko izvidniško opremo (izvidniški zabojniki, aerofoto kamere ipd.) vsaj do leta 2010 ni predvideno. Prednosti uporabe letal in helikopterjev SV pri izvidovanju iz zraka so velika odzivnost, zmožnost izvidništva velike površine v relativno kratkem času in zmožnost izvidništva na relativno veliki globini ozemlja. Slabosti uporabe letal in helikopterjev SV pri izvidovanju iz zraka so velika občutljivost na delovanje zračne obrambe in relativno omejene zmožnosti posadke za beleženje objektov izvidništva. Glede na navedene prednosti in slabosti je letalstvo SV najbolj primerno za vizualno iskanje in odkrivanje ciljev, ki so iz zraka dobro vidni. To še posebej velja za premične in skupinske (kolone vozil, premiki in položaji večjih enot, vojaške baze, objekti ipd.). Dobre rezultate letalstvo SV lahko doseže tudi z nalogo oceniti učinke bojnega delovanja. Pred izdajo naloge izvidništva je potrebna temeljita ocena tveganja in koristi uporabe zrakoplovov SV. Letala in helikopterji lahko uporabimo tudi za vrinjanje in izmik globinskih izvidnikov ter hitro vzpostavitev zveze z enoto, kadar ni druge možnosti za njeno vzpostavitev.

8.9 TAKTIČNA RAVEN ORGANIZIRANOSTI OBVEŠČEVALNE DEJAVNOSTI SLOVENSKE VOJSKE

Na taktični ravni so nosilci VODBE: S-2 poveljstev brigad, S-2 poveljstev bataljonov in taktične izvidniške enote. Poveljstva in enote na taktični ravni razpolagajo z najmanj formacijskimi zmogljivostmi za pridobivanje in obdelavo podatkov, za odločanje imajo na razpolago najmanj časa, obenem pa imajo zelo velike potrebe po informacijah, še posebej po informacijah za usmerjanje ognja. VODBE na taktični ravni zato zahteva posebno pozornost, med operacijo pa tudi vso razpoložljivo podporo nadrejenega, predvsem v zmogljivostih za izvidništvo in nadzor ter posredovanje podatkov o ciljih za potrebe usmerjanje ognja.

8.9.1 S-2 poveljstva brigade

Brigada SV bo sposobna za obrambo nacionalnega ozemlja v enem letu organizirati združeno taktično enoto brigadne ravni, ki bo sposobna izvajati vse kopenske oblike delovanja v sestavi višje enote zavezništva in ob ognjeni podpori zaveznikov, oziroma dve združeni taktični enoti brigadne ravni v daljšem časovnem obdobju. S-2 poveljstva brigade SV v miru skrbi za ustrezno usposobljenost svojega oddelka in poveljstva v celoti, za formiranje in pripravo brigade in njeno delovanje skladno z nalogo. S-2 poveljstva brigade dobi večino obveščevalnih izdelkov iz G-2 PSSV in izdela večino obveščevalnih izdelkov za potrebe S-2 poveljstev bataljonov. Poleg stalne sestave, v okviru S-2 poveljstva brigade, lahko kot okrepitev delujejo tudi občasni pripadniki in dodeljeni organi, npr. obveščevalni častniki za povezavo, celica za načrtovanje in analizo (iz ISTAR elementa), obveščevalni častniki v brigadni celici za ciljenje ipd.

8.9.2 S-2 poveljstva bataljona

Organizira in usmerja VODBE na bataljonski ravni. Osnova njegovega dela je načrt izvidništva in nadzora, ki je osnova za izdajanje nalog izvidniškemu vodu in ostalim dodeljenim enotam za izvidništvo in nadzor ter ciljenje. V načrtu S-2 uskladi tudi zbiranje podatkov od manevrskih čet bataljona, načrt pa uskladi s S-3 poveljstva bataljona. Večino izdelkov za OPB[86] S-2 poveljstva bataljona dobi od S-2 poveljstva brigade. Te izdelke bataljonski S-2 preveri in potrdi oz. dopolni. S-2 bataljona zagotavlja podrejenim poveljnikom čet informacije v obsegu, potrebnem za vodenje trenutnega in načrtovanje prihodnjega bojevanja. Poleg stalne sestave, v okviru S-2 bataljona ali bataljonske bojne skupine, lahko kot okrepitev delujejo tudi občasni pripadniki in dodeljeni organi, npr. obveščevalni častniki za povezavo, celica za načrtovanje in analizo (iz ISTAR elementa) ipd. Bataljoni SV bodo v svojo sestavo postopoma prejemali tudi različne senzorje za zaščito sil in nadzor območja.

8.9.3 Izvidniški vod bataljona (IZVV)

Je osnovna izvidniška enota bataljona. Sestava in formacija sta določeni s formacijo bataljona (motorizirani, oklepni, oklepno-mehanizirani, gorski). Naloge IZVV so opazovanje,

[86] Obveščevalna priprava bojišča je proces, v katerem S-2 poveljstva bataljona analizira vpliv zemljišča, vremena, cestnih in drugih povezav, poseljenosti, vodnih ovir, razpoloženja prebivalstva in drugih značilnosti območja, na katerem namerava delovati. V OPB je vključena tudi ocena nasprotnika in njegovih zmogljivosti ter namenov.

izvidništvo, patruljiranje, zaščita bokov in medprostorov bataljona ter izvajanje zasednega delovanja. Izvidniški vod formira izvidniško patruljo, skupino ali opazovalnico.

8.9.4 Manevrska četa Slovenske vojske.

Za izvidništvo in nadzor poveljnik čete v svojem območju odgovornosti določi oddelek, ki je posebej usposobljen za izvajanje nalog izvidništva. Za usposabljanje in pripravo tega oddelka so odgovorni poveljniki čet.

8.10 SKLEP

V poglavju predvsem pa v točkah 8.4, 8.7, 8.8 in 8.9, so opisane trenutne obveščevalne zmogljivosti SV kot so zamišljene v različnih dokumentih. Najpomembnejša pomanjkljivost teh struktur in zmogljivosti v praksi je, da je zelo razdrobljena, ni enotno usmerjana, niti ni povezana v celovit sistem zajemanja podatkov, analiziranja in poročanja. Ob tem je tehnično podhranjena, zaznamo pa lahko tudi precejšnja odstopanja od zamisli v dokumentih in rešitev v praksi.

9 PRIMERJAVA ISTAR NIZOZEMSKE, KANADE IN VELIKE BRITANIJE S SEDANJIMI REŠITVAMI V SV

S primerjavo ISTAR sistemov, ki smo jih opisali v prejšnjih poglavjih, želimo prikazati prednosti in slabosti sedanjega sistema obveščevalne dejavnosti SV in predlagati izboljšave, ki bodo slovenski ISTAR približali mednarodnim zahtevam in ciljem sil SV.

9.1 VEČPARAMETRSKO ODLOČANJE S POMOČJO RAČUNALNIŠKEGA PROGRAMA DEXI 03

DEXI 03 je računalniško orodje za večparametrsko odločanje, ki je sposobno medsebojne primerjave več variant rešitev po enakih kriterijih. Program sloni na metodologiji DEX, ki se od ostalih metodologij večparametrskega odločanja razlikuje predvsem po kvalitativnem pristopu in neposrednem določanju funkcij koristnosti več spremenljivk, kar pomembno poveča transparentnost izgradnje in uporabe odločitvenih modelov. To pa so tudi atributi metodologije ekspertnih sistemov, katere cilja sta večja razumljivost in uporabnost eksplicitnega znanja, s katerim upravljamo. V našem primeru gre za upravljanje z odločitvenim znanjem, ki tako postane dostopno širšemu krogu ljudi, ne le za validacijo in verifikacijo, ampak tudi in predvsem za razumevanje odločitve. Slednje je v tesni povezavi z doseganjem boljših odločitev, saj je pri odločitvi, kjer res vemo, zakaj smo se odločili tako, kot smo se, verjetnost, da bi kaj pomembnega spregledali, manjša, s tem pa je manjša tudi verjetnost napačne odločitve. V orodje vnesemo kriterije, po katerih bomo primerjali različne predloge ali rešitve, jim določimo vrednosti in uteži ter medsebojna razmerja. Potem vsak predlog ali rešitev posebej ocenimo glede na vnesene kriterije in vrednosti, orodju pa pustimo, da jih medsebojno primerja in predlaga optimalno rešitev.

Medsebojno primerjavo variant naredimo tako, da pri vsaki varianti preverimo, do katere mere izpolnjuje zahteve kriterijev. Pri primerjavi različnih variant ali vzorcev pravzaprav iščemo, katera varianta najbolj odgovarja zahtevam, in prikažemo, kateri bistveni elementi so pri posameznem vzorcu neustrezni.

Odločitev o najbolj primerni rešitvi je na koncu še vedno prepuščena uporabniku, orodje ponudi le objektivno analizo variant po enakih kriterijih in tehnično najbolj primerno rešitev. Pri tem nazorno prikaže primere, ki glede na postavljene kriterije zadovoljijo zahteve uporabnika z zeleno barvo, tiste ki ne zadovoljijo kriterijev z rdečo barvo, ter tiste, ki jih je potrebno izboljšati, vendar niso v celoti negativni s črno barvo. Pri tem lahko oblikujemo

komentar k barvi v nekaj besedah, ki ga DEXI avtomatsko doda v grafikon ali tabelo z rezultati.

Slika 9-1: Drevo kriterijev in zaloge vrednosti kriterijev za primerjavo ISTAR sistemov

DEXi Ocena primernosti modelov ISTAR sistemov.dxi 8.6.2010 Stran 1

Drevo kriterijev

Kriterij	Opis
Ocena primernosti modelov ISTAR sistemov	Primerjava sistemov ISTAR glede na izbrane kriterije
├Kompletnost	Ali sistem zagotavlja obdelavo vseh obv. disciplin in virov
├Zanesljivost	sistem zagotavlja podatke iz lastnih virov
├**Preglednost**	sitem zagotavlja pregledno shranjevanje podatkov in njihovo distribucijo
│ ├Avtomatizirani prenos podatkov	ali obstaja avtomatiziran prenos podatkov v zbirni center
│ ├Graficne podlage	ali se podatki vežejo na geo podlage
│ └Baze podatkov	ali obstajajo ločene baze podatkov po dejavnostih in skupna
├**Načrtovanje in analiza**	ali ima sistem lastne zmogljivosti načrtovanja in analize
│ ├Povezanost v PINK	ali je načrtovanje vezano na CCIRM, RFI, PIR
│ ├Tok informacij	ali obstaja načrtovan tok informacij
│ ├IFC (OZOP)	ali obstaja oddelek za združevanje obveščevalnih podatkov
│ └Obveščevalni ciklus	ali je obveščevalni ciklus sklenjen
├**Senzorji**	alli sistem ISTAR vsebuje tudi SENZORJE
│ ├Avtomatizirano upravljanje	ali obstaja avtomatizirano upravljanje s senzorji
│ └BPL	ali obstajajo BPL
└Povezanost v sistem	kako visoko v nacionalni sistem obv. dejavnosti je povezan ISTAR sistem

Zaloge vrednosti

Kriterij	Zaloga vrednosti
Ocena primernosti modelov ISTAR sistemov	**ne**; deloma; ***da***
├Kompletnost	**ne**; samo nekatere; večina opreme; ***da***
├Zanesljivost	**ne**; ***da***
├**Preglednost**	**ni urejen**; manj pregleden; deloma urejen; ***urejen sistem***
│ ├Avtomatizirani prenos podatkov	**ne**; ***da***
│ ├Graficne podlage	**ne**; ročno na karto; ročno na digitalno podlago; ***da, avtomatizirano***
│ └Baze podatkov	**ne**; da, vendar samo nekatere; ***da***
├**Načrtovanje in analiza**	**ne**; pomanjkljivo; ***da***
│ ├Povezanost v PINK	**ne**; deloma; ***da***
│ ├Tok informacij	**ne**; deloma; ***da***
│ ├IFC (OZOP)	**ne**; ***da***
│ └Obveščevalni ciklus	**ne**; ***da***
├**Senzorji**	**ne**; uporabno, vendar ne popolno; ***da***
│ ├Avtomatizirano upravljanje	**ne**; ***da***
│ └BPL	**ne**; samo za neposredno zaščito; ***da,***
└Povezanost v sistem	**v okviru misij v tujini**; ***celovita***

Kriteriji so določeni s pomočjo zahtev, ki povedo, kaj je potrebno, da vzorec zadovolji kriterij v celoti, deloma in pa ne. Na sliki 9-1 je razvidno, kakšni kriteriji in katere zahteve so bile postavljene pri ocenjevanju posameznih ISTAR sistemov. Tako je na primer kriterij »Pregledenost« razdeljen še na tri podkriterije, ki zahtevajo odgovor na vprašanja, ali so prenosi podatkov avtomatizirani, ali so podatki prikazani na grafičnih geo podlagah in ali obstajajo baze podatkov in kako so organizirane. V rubriki »Zaloge vrednosti« lahko najdemo enostavne zahteve, ki opredeljujejo, katere so naše minimalne zahteve za pozitivno oceno.

Rezultati medsebojne primerjave zadovoljevanja zahtev podkriterijev dajejo oceno kriterija. V nadaljevanju postavimo razmerja med vsemi zahtevami podkriterijev in na ta način določimo utežno vrednost kriterija v celotni oceni primernosti vzorca (glej tč. 9.1.2.). Tam, kjer kriteriji

nimajo podkriterijev, v sistemu primerjamo zaloge vrednosti takega kriterija z vsemi podkriteriji. To je zahteven proces, ki od avtorja zahteva dobro poznavanje značilnosti vzorcev in dosledno spoštovanje v začetku postavljenih pravil. V našem primeru smo med seboj primerjali 576 medsebojnih kombinacij zahtev.

Uporabnost orodja je tudi v tem, da jasno pokaže na pomanjkljivosti rešitev. Posodabljanje rešitev z odpravljanjem pomanjkljivosti je v orodju preprosto in postopek lahko ponavljamo toliko časa, dokler ne najdemo pravega odgovora. To seveda ne pomeni, da spreminjamo kriterije ali zahteve, temveč relativno enostavno prepoznamo pomanjkljivosti posameznih vzorcev in jih odpravljamo ali popravljamo toliko časa, dokler vzorec ni pozitiven.

V nadaljevanju je seveda potrebno oceniti, ali so spremembe objektivno izvedljive in stroškovno upravičene, to pa lahko naredimo ročno ali pa ponovno uporabimo DEXI.

9.1.1 Uporabljeni primerjalni kriteriji

Primerjavo smo izvedli z uporabo naslednjih kriterijev:

- **Kompletnost sistema.** Pri tem smo ocenjevali, ali so upoštevane obveščevalne dejavnosti (SIGINT, HUMINT, IMINT, GEOINT, MASINT itd.).
- **Zanesljivost izdelkov.** Pri tem nas je zanimalo, ali sistem zagotavlja uporabo več informacij o istem cilju z več viri in preverjanjem.
- **Preglednost izdelkov.** Pri tem smo ocenjevali, ali sistem zagotavlja pregledno shranjevanje in sledljivo distribucijo podatkov. Zanimalo nas je, ali gre za avtomatiziran prenos podatkov z uporabo digitalne geografske podlage in ali so oblikovane lastne baze podatkov.
- **Stopnja urejenosti načrtovanja in analiziranja.** Pri tem nas je zanimalo, ali obveščevalni proces sledi poveljnikovim zahtevam po informacijah, ali je tok informacij načrtovan in pregleden, ali obstaja oddelek za združevanje obveščevalnih podatkov in ali je obveščevalni ciklus v procesu sklenjen.
- **Opremljenost s senzorji.** V tej točki smo ocenjevali, ali imajo enote ISTAR senzorske zmogljivosti, do kakšne stopnje je proces upravljanja z njimi avtomatiziran in so v zmogljivosti vključena tudi brezpilotna letala.
- **Povezanost**. Pri tem nas je zanimalo, kako je vojaška ISTAR zmogljivost povezana v višje domače ali mednarodne obveščevalne sisteme.

9.1.2 Pomembnost (»teža«) posameznega kriterija v primerjalnem modelu

Potem ko so razmerja med zahtevami kriterijev določena, DEXI 03 izračuna težo posameznega kriterija. Na ta način lahko preverimo, ali smo razmerja med zahtevami določili tako, da vrstni red kriterijev po pomembnosti odgovarja prej opisanim teoretičnim izhodiščem. Ob velikem številu medsebojnih razmerij zahtev se namreč lahko pojavi napaka zaradi preveč subjektivno določenih razmerij, ki iz različnih vzrokov ne sledijo strokovnim temeljem. Uteži za posamezni kriterij so prikazane kot procent od skupne ocene. Seštevek vseh uteži oziroma procentov mora biti 100.

V našem primeru ima največjo težo kriterij »Senzorji«, kar 30 % celotne ocene, ker z njihovo uporabo in vključenostjo v ISTAR lahko neposredno in v realnem času preverjamo ali pridobivamo zelo zanesljive podatke.

Drugi kriterij po pomembnosti je »Načrtovanje in analiza« s 25 % celotne ocene, ker upoštevamo pravilo, da je ISTAR lahko uspešen le ob načrtnem zbiranju in analiziranju podatkov in informacij.

Tretji kriterij je »Povezanost v sistem« s 15% celotne ocene. Ker ISTAR ne predstavlja klasično, linearno organiziran sistem, temveč mrežno strukturo, je pomembno, kako visoko sega ta mreža v obrambni ali nacionalni obveščevalni sitem. Ker ima danes lahko taktični podatek tudi strateški pomen in obratno, je pomembno, kako dobro je ta mreža razvejana na vse strani. To je pomembno predvsem zato, ker je v dobri mrežni povezavi enostavno izmenjevati in pridobivati informacije, ki jih enota sama sicer ne more zbrati, lahko pa pomembno vplivajo na uspešnost operacij in obratno.

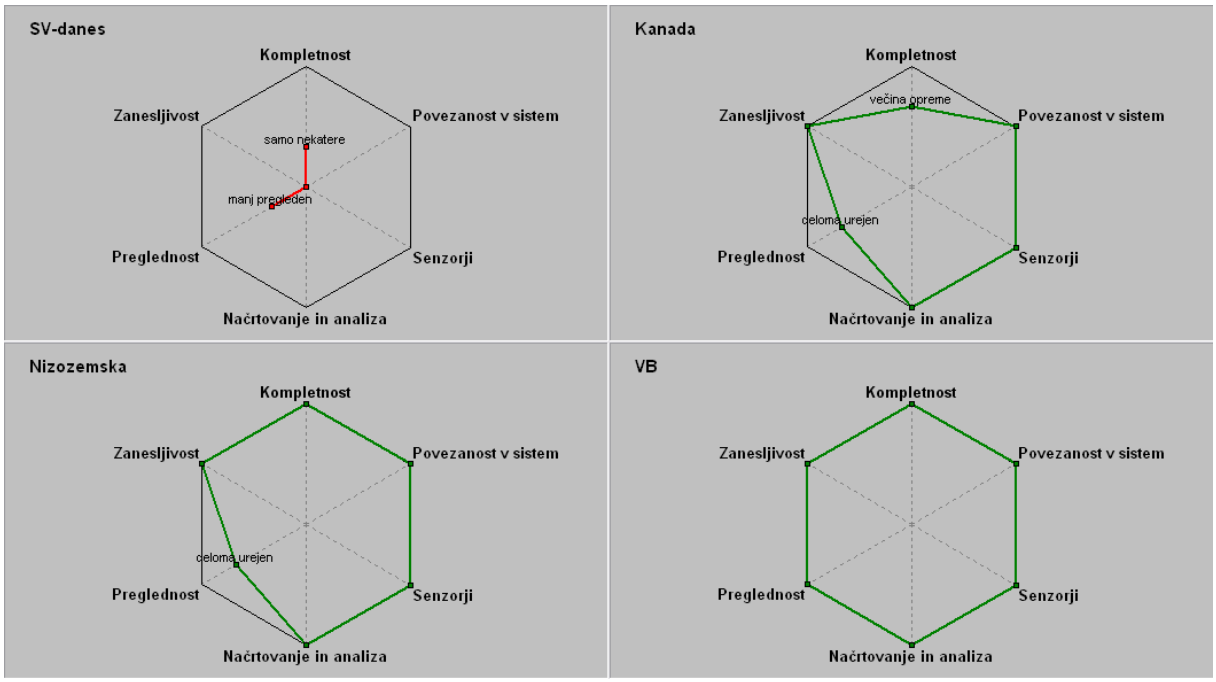
Četrti kriterij je »Preglednost« s 15 % celotne ocene. Urejenost podatkovnih baz in pregleden sistem distribucije podatkov in drugih obveščevalnih izdelkov pomembno prispeva k odzivnosti ISTAR na zastavljene naloge. Urejen in pregleden sistem zagotavlja tudi bolj gospodarno izrabo virov

Peti kriterij po teži je »Zanesljivost« s 10 % celotne ocene. Zanesljivost obveščevalnih podatkov in ocen nikoli ni popolna, je pa višja, če razpolagamo z lastnimi viri, ki jih lahko glede na izkušnje z njimi ocenimo in če razpolagamo s sistemi, ki omogočajo preverjanje pridobljene informacije na več načinov.

Šesti kriterij po teži je »Kompletnost« z 5 % celotne ocene. ISTAR povezuje različne obveščevalne dejavnosti in opremo v celovit in pregleden sistem. Več kot je opreme in dejavnosti vključenih v sistem, bolj je ta uspešen in zanesljiv, ni pa nujno uporabljati ali imeti vseh, ki so sicer v svetu dosegljivi. Posebno danes imajo članice NATA možnost medsebojnega izmenjevanja obveščevalnih podatkov na hiter in varen način, na ta način lahko deloma nadomestijo manjkajoče elemente.

9.2 REZULTATI PRIMERJAVE

Slika 9-2: Grafični prikaz ustreznosti ISTAR v SV danes, v Kanadi, na Nizozemskem in v Veliki Britaniji



Grafično so rezultati prikazani v šestkotniku, kjer obod predstavlja v celoti izpolnjene zahteve kriterija, sredina lika pa točko nič. Ocena izpolnjevanja zahtev posameznega kriterija je prikazana s krivuljo, ki poteka znotraj lika, tako da z oddaljenostjo od sredine lika prikazuje procent zadovoljitve zahtev kriterija. Zelena črta prikazuje pozitiven vzorec, rdeča pa negativnega. Rezultati so s kratkim komentarjem, ki pove, do katere mere je zahteva kriterija izpolnjena, tudi opisno opredeljeni.

Grafikon nam tako zelo nazorno prikaže kvaliteto posameznega vzorca in njegove glavne pomanjkljivosti ali prednosti. Bolj podrobno lahko pregledamo rezultate v preglednici, kjer nam DEXI rezultate ponovno prikaže v barvah (rdeče je negativno, zeleno pozitivno, črno

problematično) in opisno. Sami se lahko odločimo, kakšna oblika poročila nam bolj ustreza in taka navodila vgradimo v model.

Na sliki 9-2 je razvidno, da današnji obveščevalni sistem SV daleč zaostaja za ISTAR sistemi treh primerjanih držav. Kot smo že v prejšnjih poglavjih ugotovili, ima današnji sistem v SV majhen del vsake glavne ISTAR discipline, ki pa med seboj niso povezane v sistem, poleg tega pa vsem manjka velik del opreme. Problematično je tudi načrtovanje, ker se ne začenja s poveljnikovimi zahtevami po ključnih informacijah. To pomeni, da obveščevalno delo ni analitično, temveč zbirateljsko. Tudi baze podatkov so redke in neprimerno organizirane in med seboj nepovezane. Senzorjev v SV praktično še niso začeli uporabljati, pa tudi tiste, ki so, niso povezali v sistem. Sistem ne zagotavlja enostavne sledljivosti pretoka informacij, niti nima povezanih baz podatkov in večino informacij še vedno spremlja na tiskanih grafičnih podlagah. Pretežni del informacij se izmenjuje v tiskani obliki. Velika pomanjkljivost je neaktivna vloga poveljnikov pri usmerjanju delovanja obveščevalnih zmogljivosti. Razpoložljive zmogljivosti so v sistem povezane le za potrebe misij v tujini.

Zato nam DEXI v analizi prikaže negativno oceno in jasno pokaže, da sedanji sistem ne zadosti kriterijem sodobne, mednarodno veljavne in uveljavljene obveščevalne strukture.

Popolnoma drugačna je slika ustreznosti ISTAR sistemov Kanade, Nizozemske in Velike Britanije. Rezultati na sliki 9-2 so v praksi dokazani na sodobnih bojiščih in operacijah kriznega odzivanja. Taka organiziranost in zmogljivost je pogoj za preživetje v sodobnih pogojih asimetričnega bojevanja v običajno slabo poznanih okoliščinah, kamor se Slovenska vojska vedno bolj odločno usmerja. Rezultati vrednotenja v opisni obliki so razvidni na sliki 9-3

Ti bolje od grafikonov prikažejo ocene posameznih vsebin in lahko vidimo, da je Kanada od treh tujih dežel najslabše ocenjena. Glavne pomanjkljivosti so vezane na to, da nimajo razvitih vseh glavnih disciplin ISTAR (glej tč. 7.3.2) ter nedodelan sistem načrtovanja in sledenja toku informacij. Ocena je kljub temu pozitivna in sistem uspešno podpira delovanje kanadske vojske in strateških odločevalcev, kar je dokazano v Afganistanu.

Nizozemska je ena od evropskih članic NATA, ki ima vojaške sisteme zelo visoko razvite, je aktivno prisotna na vseh kriznih območjih in je skozi zgodovino zelo razvejala obveščevalno dejavnost. Ta je tudi danes sodobno opremljena in organizirana v celotni strukturi državnih inštitucij in tesno povezana v zavezniški sistem izmenjave informacij. Po meni poznanih

informacijah in iz literature lahko zasledimo določene nedorečenosti v preglednosti razpoložljivih obveščevalnih podatkov. Zaradi izjemno velikega števila različnih obveščevalnih podatkov je zelo pomembno, da je proces kar se da avtomatiziran, vendar tako, da je možno slediti in preverjati, ali se združujejo tako, da uporabnik dobi realne produkte. Glede na nizozemske izkušnje iz njihovega sodelovanja v NRF[87], je poplave informacij občasno težavno upravljati.

V oceni izpolnjevanja zahtev podkriterija »grafične podlage« nizozemski ISTAR ni ocenjen z najvišjo oceno. Komentar »Ročno na digitalno podlago« pomeni, da nizozemska vojska uporablja digitalizirane geografske podlage, na katere dodaja zbrane obveščevalne podatke, tako da je lahko videti, kje se kaj dogaja. Ročno ne pomeni dobesedno ročno, ampak pomeni, da dodatne podatke na digitalno podlago vnašajo po odločitvi analitikov v digitalni tehniki, ne pa avtomatizirano, kot se to dogaja v ISTAR Velike Britanije ali ZDA. To na eni strani predstavlja določen časovni zaostanek, je pa na drugi strani tak izdelek bolj zanesljiv. Skupna ocena je visoko pozitivna, kar potrjujejo tudi rezultati delovanja Nizozemske v operacijah kriznega odzivanja in drugih krizah.

Ocena doseganja zahtev ISTAR Velike Britanije je najvišja od primerjanih vzorcev. Praktično ne moremo prepoznati večjih pomanjkljivosti. Naj kot zanimivost omenim, da je šolanje britanskih častnikov kljub visoki stopnji informacijske tehnologije še vedno v pretežni meri izvedeno tako, da jih učijo vojaške umetnosti z uporabo klasičnih metod načrtovanja in analiziranja. Šele ko obvladajo klasiko, jih usmerijo k uporabi visoke informacijske tehnologije, predvsem ko gre za združeno bojevanje rodov in zvrsti.

9.3 PREDLOG ORGANIZIRANOSTI ISTAR V SLOVENSKI VOJSKI

Glavno vodilo pri razmišljanju o predlogu organiziranosti ISTAR v SV je bilo, da ostanemo o okvirih razpoložljivih ali dosegljivih virov in da vključimo čim več že do sedaj zgrajenih zmogljivosti.

[87] NATO Responce Force – enote članic NATA, ki so v zelo visoki stopnji pripravljenosti (pripravljene za delovanje v 5 dneh), načeloma se menjajo v šestmesečnih intervalih ali delujejo v NATO misijah.

Slika 9-3: Rezultati vrednotenja sedanje organiziranosti ISTAR v SV v primerjavi s Kanado, Nizozemsko in Veliko Britanijo.

DEXi — Ocena primernosti modelov ISTAR sistemov.dxi 8.6.2010 — Stran 1

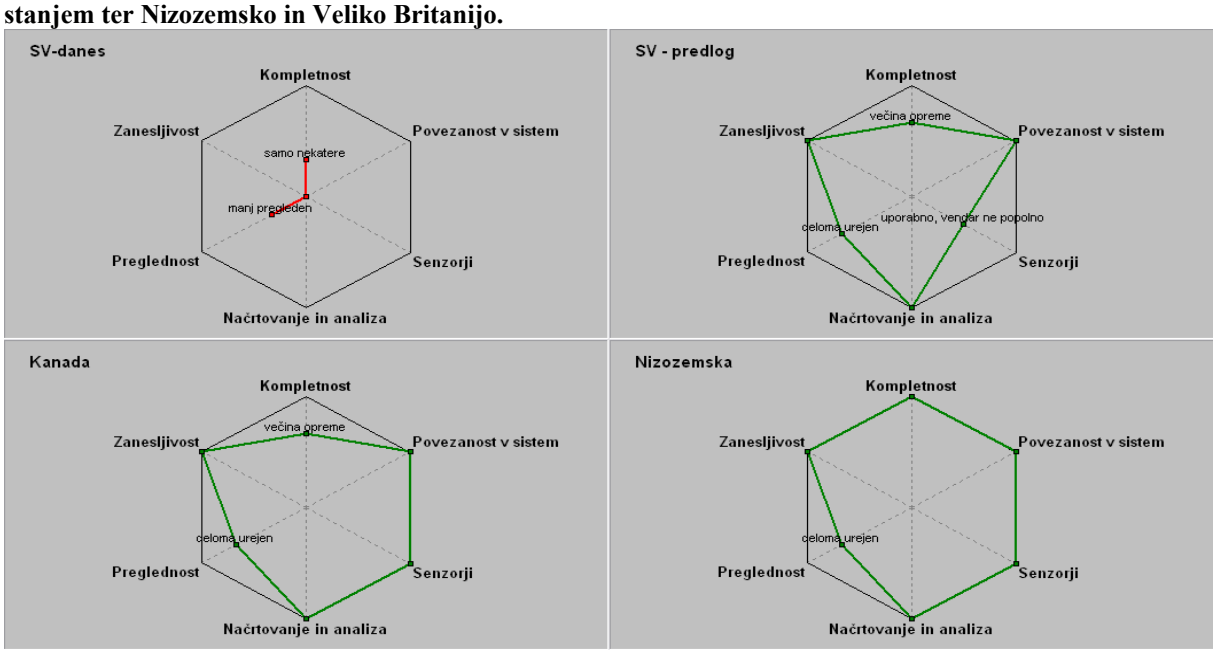
Rezultati vrednotenja

Kriterij	SV-danes	Kanada	Nizozemska	VB
Ocena primernosti modelov ISTAR sistemov	***ne***	***da***	***da***	***da***
Kompletnost	samo nekatere	večina opreme	***da***	***da***
Zanesljivost	***ne***	***da***	***da***	***da***
Preglednost	manj pregleden	deloma urejen	deloma urejen	***urejen sistem***
Avtomatizirani prenos podatkov	***ne***	***da***	***da***	***da***
Graficne podlage	ročno na karto	ročno na digitalno podlago	ročno na digitalno podlago	***da, avtomatizirano***
Baze podatkov	da, vendar samo nekatere	***da***	***da***	***da***
Načrtovanje in analiza	***ne***	***da***	***da***	***da***
Povezanost v PINK	deloma	***da***	***da***	***da***
Tok informacij	deloma	deloma	***da***	***da***
IFC (OZOP)	***ne***	***da***	***da***	***da***
Obveščevalni ciklus	***ne***	***da***	***da***	***da***
Senzorji	***ne***	***da***	***da***	***da***
Avtomatizirano upravljanje	***ne***	***da***	***da***	***da***
BPL	***ne***	***da,***	***da,***	***da,***
Povezanost v sistem	***v okviru misij v tujini***	***celovita***	***celovita***	***celovita***

Kljub temu da je formalno najbolj pomembna naloga SV nacionalna obramba, se pri pisanju te naloge zavedamo, da se SV z največjimi izzivi srečuje pri delu v tujini, zato bi slovenski ISTAR moral biti povezljiv s tujimi rešitvami. V ta namen smo na osnovi rezultatov analize s programom DEXI 03 poskušali dobiti predlog bolj primerne, nove organiziranosti ISTAR zmogljivosti SV.

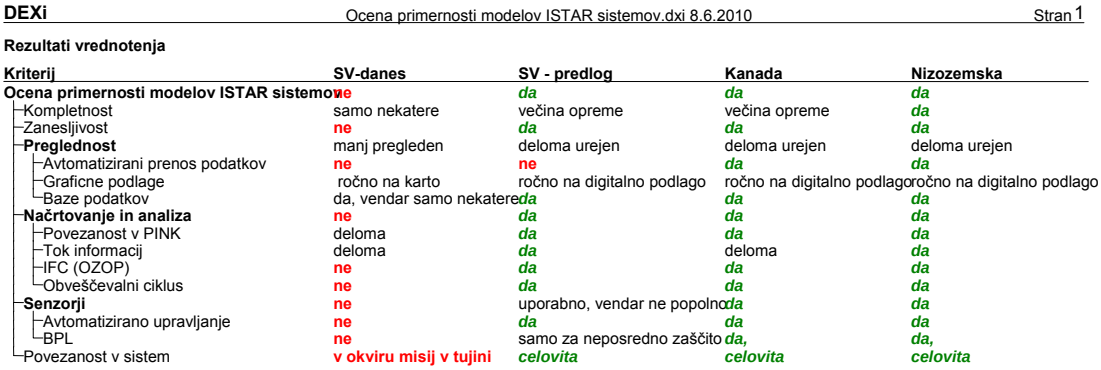
Na sliki 9-4 lahko vidimo, da predlog nove organiziranosti ISTAR v SV ne izpolnjuje v celoti vseh kriterijev. Poskušali smo poiskati model, ki bo še zagotavljal povezljivost s tujimi modeli, pa vendar ne bo zahteval prevelikih finančnih sredstev. Iz grafikona »SV – predlog« je razvidno, da v predlagani sestavi ne predvidevamo vseh sistemov, ki jih na primer vključuje britanski model in odstopamo od popolne kompletnosti, prav tako pa ne predvidevamo, da bi morali imeti celotno paleto senzorjev, ki se dobijo na tržišču.

Slika 9-4:Grafični prikaz ustreznosti predloga nove organiziranosti ISTAR v SV v primerjavi s sedanjim stanjem ter Nizozemsko in Veliko Britanijo.



Pomembno nam je bilo, da organizacijsko, tehnično in kadrovsko zagotovimo povezanost vseh razpoložljivih zmogljivosti v pregleden in sledljiv sistem, v katerem bo mogoče pridobivati podatke in informacije preverljive stopnje zanesljivosti in ki bo deloval načrtno ter tako zagotavljal pogoje za zanesljive analize.

Slika 9-5: Rezultati vrednotenja predloga nove organiziranosti ISTAR SV v primerjavi s Kanado in Nizozemsko.



DEXi — Ocena primernosti modelov ISTAR sistemov.dxi 8.6.2010 — Stran 1

Rezultati vrednotenja

Kriterij	SV-danes	SV - predlog	Kanada	Nizozemska
Ocena primernosti modelov ISTAR sistemov	ne	*da*	*da*	*da*
├Kompletnost	samo nekatere	večina opreme	večina opreme	*da*
├Zanesljivost	ne	*da*	*da*	*da*
├**Preglednost**	manj pregleden	deloma urejen	deloma urejen	deloma urejen
│├Avtomatizirani prenos podatkov	ne	ne	*da*	*da*
│├Graficne podlage	ročno na karto	ročno na digitalno podlago	ročno na digitalno podlago	ročno na digitalno podlago
│└Baze podatkov	da, vendar samo nekatere	*da*	*da*	*da*
├**Načrtovanje in analiza**	ne	*da*	*da*	*da*
│├Povezanost v PINK	deloma	*da*	*da*	*da*
│├Tok informacij	deloma	*da*	deloma	*da*
│├IFC (OZOP)	ne	*da*	*da*	*da*
│└Obveščevalni ciklus	ne	*da*	*da*	*da*
├**Senzorji**	ne	uporabno, vendar ne popolno	*da*	*da*
│├Avtomatizirano upravljanje	ne	*da*	*da*	*da*
│└BPL	ne	samo za neposredno zaščito	*da,*	*da,*
└Povezanost v sistem	v okviru misij v tujini	*celovita*	*celovita*	*celovita*

Slika 9-5 še bolj podrobno prikazuje, kje so predvidene pomembne spremembe v primerjavi s sedanjim sistemom. Če sledimo utežnim vrednostim kriterijev, potem je najbolj pomembno dopolniti opremo z dovolj razvejanim sistemom senzorjev, ki bodo zagotavljali dobro zaščito sil in podpirali delovanje enot ranga bataljona. V sistem je potrebno vpeljati brezpilotna letala, vendar samo do srednjega dosega. To pomeni, da ni potrebno nabaviti najdražjih sredstev, je pa potrebno vzpostaviti avtomatiziran sistem upravljanja, zajemanja informacij in združevanja v skupne ocene.

Drugi najbolj pomemben kriterij je »načrtovanje in analiza«. Če želimo odziven in zanesljiv sistem, potem se pri tem kriteriju ne moremo odrekati sodobni informacijskih tehnologiji na področju komunikacij, varnemu in sledljivemu sistemu izmenjevanja obveščevalnih produktov, principu centraliziranega vodenja in decentraliziranega izvajanja obveščevalne dejavnosti, načrtovanju obveščevalnih operacij na osnovi obveščevalnih zahtev in mrežno organizirani analitiki. Za zadovoljitev zahtev tega kriterija je potrebno nameniti precej denarja, ki pa je lahko porabljen brez rezultatov, če se ne spremeni kultura dela poveljstev (in obveščevalne komune nasploh). Na sliki 13 je razvidno, da pri tem kriteriju predvidevamo izpolnitev zahtev v celoti.

Tretji kriterij po pomembnosti v modelu je »povezanost v sistem«, pri čemer nam je pomembno, da imamo zmogljivosti povezovanja v vse smeri tako v mednarodnem kot tudi v

domačem okolju. Prihodnji ISTAR v SV mora biti povezljiv tako doma kot v tujini, ker lahko le tako nadomestimo lastne pomanjkljivosti in smo ob tem sposobni tudi sami prispevati svoj delež k celoviti sliki situacije. Povezljivost ne pomeni le komunikacijske povezanosti, temveč tudi to, da smo sposobni in pripravljeni pravilno oceniti svoje zmogljivosti in pomanjkljivosti in o tem obvestiti svoje partnerje.

Največja novost v obveščevalnem sistemu SV bodo verjetno predstavljali ukrepi za zadovoljitev zahtev četrtega kriterija – »preglednost«, ki bo zahteval uvedbo baz podatkov, močno GIS podporo in v temelju spremenil razumevanje tajnosti pri izmenjavi podatkov znotraj kroga odločevalcev in obveščevalcev. Ker pri tem ne gre toliko za novosti v tehnologiji kot za veliko spremembo v filozofiji, pričakujem, da bo to morda najtrši oreh pri uvajanju sodobnega ISTAR v obrambni sistem Slovenije. Tudi zato v iskanju sprejemljivih rešitev nismo predvideli nujnost zadovoljitve zahtev kriterija v celoti, temveč dopuščamo možnost, da avtomatizacija prenosa podatkov ne bo zagotovljena v celoti in da bomo digitalizacijski prikaz bojišča do neke mere še vedno upravljali ročno.

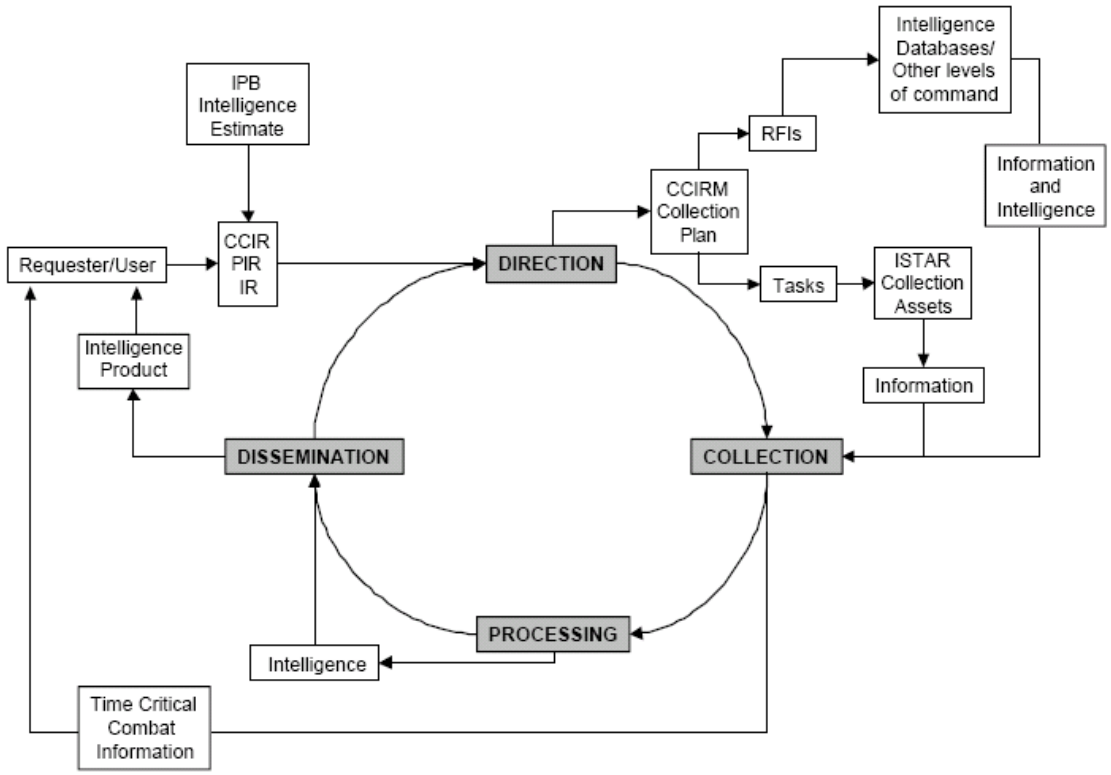
Peti kriterij je »zanesljivost«, ki od nas zahteva, da so izdelki preverljivi, pravočasni, natančni in posredovani tako, da vmes ni mogoča nepooblaščena manipulacija s podatki. Sistem je lahko le zanesljiv ali pa ni. Vmesne variante v tem primeru niso sprejemljive, zato predvidevamo, da bo bodoči slovenski ISTAR zanesljiv.

Zadnji kriterij je »kompletnost«. Kot sem že večkrat omenil, ne predvidevamo, da bi moral sistem vključevati vso opremo, kot je primer v Veliki Britaniji, mora pa je imeti večino. Ni namen te naloge v podrobnosti naštevati vso opremo, ki je potrebna, so pa izdelane študije v ta namen. V opisni obliki so sklopi opreme omenjeni v prejšnjih odstavkih, odrekamo se le najdražji opremi, ki je v osnovi namenjena za podpiranje veliko večjih sistemov, kot je ali bo slovenski. Zahteva je, da oprema zagotavlja dobro zaščito sil za delovanje enote v rangu bataljona, da zagotavlja varno in zanesljivo izmenjavo informacij znotraj in zunaj vojske v civilno ter mednarodno okolje, omogoča avtomatizacijo procesov vodenja senzorjev, zbiranja in urejanja podatkov ter deloma načrtovanja, analitike in distribucije produktov. Pri tem kriteriju je pomembno tudi, da imamo razvite vsaj glavne discipline ISTAR, kot so: SIGINT, ELINT, IMINT, HUMINT, WEAPONINT in OSINT.

Na sliki 9-6 je razvidno, kako si poenostavljeno predstavljamo bodočo organiziranost ISTAR v SV. Krog se bo začel z zahtevami, s ključnimi poveljnikovimi, v nadaljevanju pa prioritetnimi zahtevami po informacijah, ki bodo osnova za načrtovanje aktivnosti ISTAR

dejavnosti in drugih enot ali zbiralcev podatkov. Pridobljene informacije bodo urejeno shranjevali in v analitičnih celicah dopolnjevali z že znanimi podatki, krog pa se bo zaključil z izdelavo zahtevanih produktov in njihovo distribucijo naročnikom.

Slika 9-6: Poenostavljena shema ISTAR sistema



Vir: Teleplan AS[88] 2009, 5.

Proces s tem ne bo zaključen, temveč bo na osnovi nalog, izdelanih produktov in novih dejstev z bojišča, celica za načrtovanje dopolnjevala svoj načrt zbiranja podatkov in usklajevala aktivnosti zmogljivosti pri pridobivanju novih in dodatnih informacij.

Tok informacij se na tak način vrti v krogu in pri tem skozi ustrezne filtre iz kroga spušča del podatkov v baze, jih od tam zopet pobira in skozi analitične procese na novo združuje, na območju obveščevalnega interesa manjkajoče informacije in podatke ponovno zbira ter se praktično nikoli popolnoma ne ustavi.

[88] Teleplan AS je norveško podjetje, ki se med drugim ukvarja z avtomatizacijo procesov v oborožitvenih sistemih in oboroženih silah.

9.4 VKLJUČENOST SV V OBVEŠČEVALNO DEJAVNOST NA STRATEŠKI RAVNI

Slika 9-6 prikazuje, da je ena od pomembnih točk dejavnosti ISTAR izmenjava informacij, podatkov in ocen z obveščevalnimi zmogljivostmi na višjih ravneh. V primeru SV je to OVS ali/in J-2 GŠSV, v določenih pogojih pa tudi visoka tuja poveljstva.

Glede na dejstvo, da danes obveščevalna dejavnost ne more biti osamljena le na raven poveljstva, za katerega izvaja naloge, temveč je povezana v mrežni sistem izmenjave informacij na vseh ravneh, je potrebno razmisliti tudi o načelnih rešitvah organiziranosti celotne verige obveščevalnih zmogljivostih v sistemu SV.

Pri tem bomo izhajali iz opredelitev na strateški ravni, da je potrebno integrirati obveščevalni del OVS in obveščevalno-analitični del J-2 GŠSV v enotno strukturo.

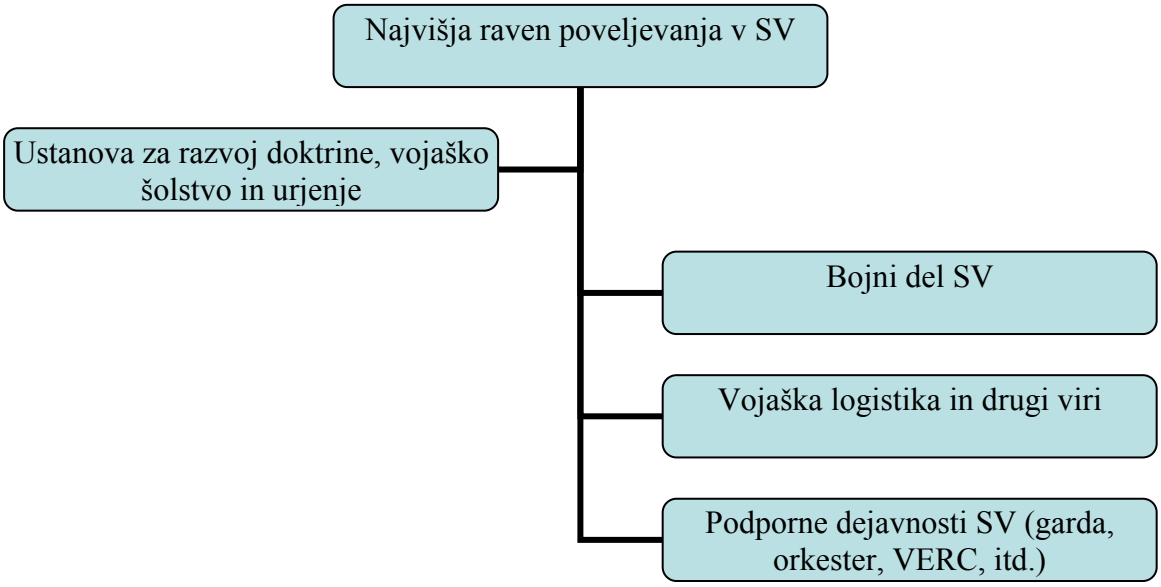
Zaradi lažje predstave bomo v naslednji sliki predstavili poenostavljeni model organiziranosti SV.

Iz tako poenostavljenega modela lahko razberemo, da je obveščevalna dejavnost potrebna na najvišji ravni poveljevanja in v bojnem delu, zaradi razvoja doktrine in šolanja kadrov pa tudi v ustanovi za razvoj doktrine in vojaškega šolstva. V nalogi me zanimata predvsem sistema na ravni poveljevanja vojski in v bojnem delu. Najvišje ravni poveljevanja namenoma nisem poimenoval z današnjimi najvišjimi nazivi poveljstev v shemi PINK, ker odločitev o prihodnji organiziranosti še ni sprejeta.

Ne glede na odločitev predlagam, da taka raven obdrži obveščevalni organ kot štabno funkcijo, izvedbo operativnih dejavnosti načrtovanja, obdelave podatkov in usmerjanja ISTAR zmogljivosti pa prepusti združenemu ONOP (Oddelku za načrtovanje zbiranja in obdelave podatkov) med OVS in SV. Pomembno je, da oblikovanje CCIR in PIR za SV ostane v domeni SV.

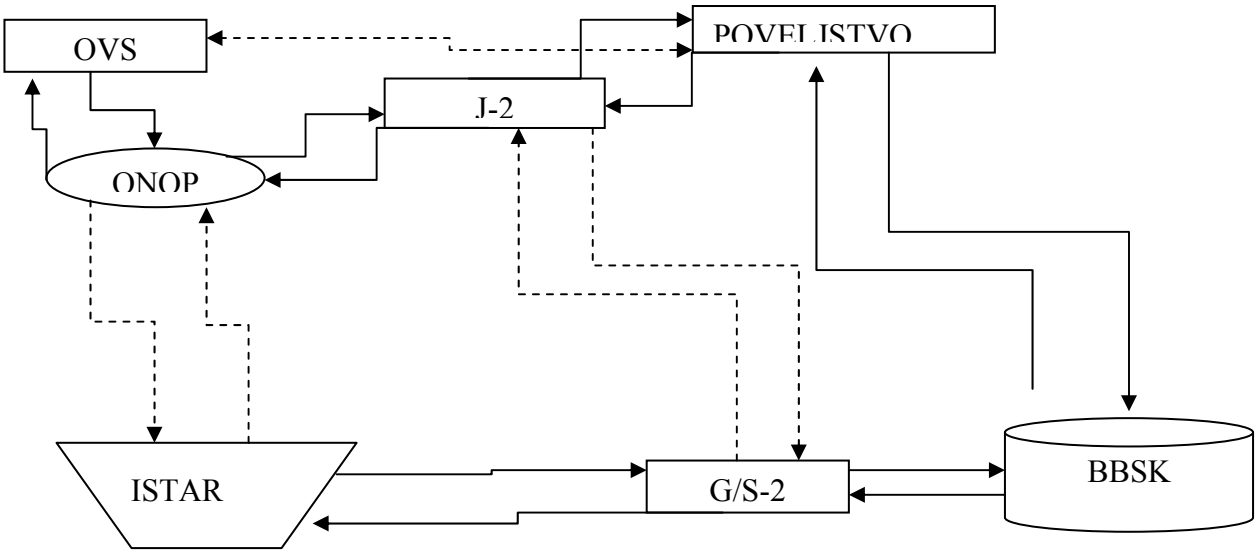
Pojem bojni del razumemo kot oblikovanje sil za bojno delovanje. Pri tem ne predvidevamo podrobnejše organiziranosti enot ali zmogljivosti. Predlagali bomo, da take enote obdržijo štabno funkcijo obveščevalnega organa in da oblikujemo modularno zgrajeno ISTAR enoto, ki bo sposobna na taktičnem nivoju podpirati enote do ranga bataljonske bojne skupine ali polka. V določenih pogojih dele takih modulov lahko uporabijo neposredno za višje ravni.

Slika 9-7: Poenostavljena shema organiziranosti SV



Štabna funkcija obveščevalnega organa bo namenjena predvsem sodelovanju pri načrtovanju in spremljanju mirnodobnih aktivnosti obveščevalnih zmogljivosti enote ali poveljstva in udeležbi v procesu odločanja poveljnika in štaba. Skrbela bo za upravljanje s CCIR, oblikovanjem PIR in IR, usmerjala delo pridodanega ISTAR modula, dokončno oblikovala ali odobravala odgovore na prej omenjene zahteve in o njih obveščala štab in poveljnika. Poenostavljena shema predlaganih povezav je predstavljana na sliki 9-8.

Slika 9-8: Poenostavljena shema predlaganih povezav OVS, SV, Poveljstva vojske, bojne skupine in ISTAR modula pri obveščevalni zagotovitvi delovanja SV.



Slika 9-8 prikazuje, kako so med seboj povezani glavni dejavniki obveščevalne dejavnosti SV. Na sliki lahko vidimo, da so povezave mrežne, pri čemer smo črtkano označili tiste povezave, ki so namenjene le izmenjavi informacij, s polno črto pa linijo PINK, ki je pri obveščevalnem delu namenjena prenosu obveščevalnih izdelkov.

Oddelek za načrtovanje zbiranja in celovito obdelavo podatkov deluje v okviru OVS, sestavljen pa je iz pripadnikov OVS in SV, ukvarja se z načrtovanjem zbiranja in celovito obdelavo zbranih informacij. Izdelke posreduje naročnikom, ki so posredovali svoje zahteve po ključnih ali prioritetnih informacijah, obvezno pa direktorju OVS in J-2 ali glavnemu poveljujočemu v SV.

Osnova za načrtovanje so CCIR ministra za obrambo in glavnega poveljujočega v SV, poleg tega tudi druge zahteve vojaških ali civilnih struktur, ki sledijo zahtevam ministra ali poveljstva SV. Načrti zbiranja informacij zajemajo vse ustrezne razpoložljive zmogljivosti OVS in SV glede na zahteve naročnikov.

Oddelek oblikuje in vzdržuje baze podatkov za posamezne dejavnosti ISTAR ter druge baze, ki so pomembne za obveščevalno delo.

Poleg tega predlaga izgradnjo takega informacijskega in komunikacijskega sistema, ki omogoča hitro, zanesljivo in sledljivo izmenjavo informacij v celotnem obveščevalnem sistemu MORS.

Na misijah v tujini neposredno sodeluje z ISTAR moduli vojaških enot SV na terenu in zagotavlja neposredno pomoč iz domovine pri obdelavi podatkov in izdelavi njihovih produktov (Vance 2008).

9.5 ISTAR V ENOTAH SLOVENSKE VOJSKE

Predlagamo, da so ISTAR moduli mirnodobno združeni v ISTAR bataljonu, katerega mirnodobna naloga je razvijati ISTAR zmogljivosti na taktični ravni, usposabljati, sodelovati pri nabavah opreme, vključevati in vzdrževati namensko opremo, pomoč pri usposabljanju poveljstev bojnih skupin za uporabo ISTAR modulov, sodelovati z ONOP pri oblikovanju in polnjenju baz obveščevalnih podatkov in priprava moštva za operacije v tujini.

Moduli so sestavljeni namensko, tako da je glede na nalogo in območje delovanja bojne skupine možno oblikovati ustrezno velike ASC ter module senzorjev in kolektorjev. Glede na

verjetno število bojnih skupin, bi ISTAR bataljon lahko zagotovil 2–4 module. Zaradi omejenosti virov, predvsem kadrov, bo možno kombinirano popolnjenvanje pripadnikov ONOP in ISTAR v modulih in NOC[89] na misijah v tujini.

Na sliki 9-9 predstavljam, kako sem si zamislil novo organizacijsko strukturo ISTAR v SV. Najprej lahko opazimo, da so posamezni sklopi dejavnosti označeni z različno barvo. To sem storil zato, da prikažem, kaj organizacijsko predstavlja določeno dejavnost, in zato da ponazorim predlog organizacije ISTAR bataljona SV kot osrednje vojaške zmogljivosti ISTAR.

Z elementi v črni barvi ponazarjam tiste zmogljivosti SV ali zunaj nje, ki so sicer sestavni del drugih enot SV ali organov MORS, ki morajo biti za celovit ISTAR nujno povezani v celovit sistem s pomočjo naprednega komunikacijskega omrežja in ustrezno opredeljenih procesov usklajevanja delovanja in izmenjave informacij.

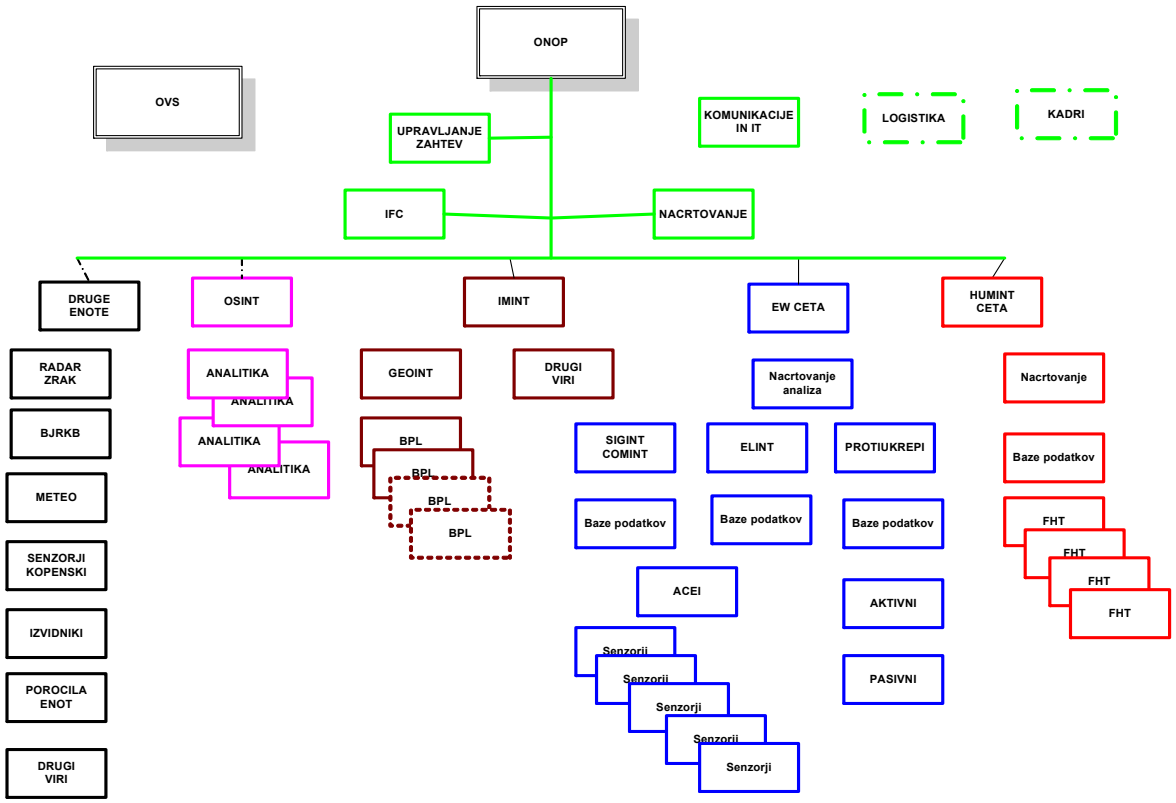
Predlagam, da obstoječe zmogljivosti 5. OIB (HUMINT in SIGINT) nekoliko preoblikujemo in povečamo v skladu s cilji sil ter dodamo IMINT in OSINT zmogljivosti.

Posebej izpostavljam OVS, ki vojaškemu sistemu zagotavlja široko paleto različnih obveščevalnih podatkov in ocen iz lastnih virov ali mednarodne izmenjave, istočasno pa se podatki in ocene iz vojaškega ISTAR neposredno pretakajo nazaj. S tem je zagotovljena mrežna organiziranost obveščevalne dejavnosti MORS in prost pretok informacij.

ONOP bi lahko predstavljal najvišji organ ISTAR, kamor bi posredovali zahteve po ključnih informacijah, na eni strani bo povezan z OVS, na drugi pa s štabno obveščevalnim stebrom v poveljstvih SV (S/G/J-2). ISTAR bo na eni strani zagotavljal sistem za načrtno zbiranje in posredovanje informacij, na drugi pa oblikoval specializirane module za izvedbo obveščevalnih aktivnosti, ki jih štabni organi ali organski deli običajnih enot ne morejo zagotoviti.

[89] Nacionalna obveščevalna celica–oblika delovanja obveščevalnih agencij v tujini za lastne nacionalne potrebe. Običajno niso sestavni del vojaških kontingentov.

Slika 9-9: Predlog organizacijske strukture ISTAR v SV



Pravokotniki v zeleni barvi so tisto, kar je v tem predlogu najbolj novo in pomembno. To je ustanovitev celic za upravljanje z zahtevami in koordinacijo, za načrtovanje aktivnosti ter za zbiranje in analizo vseh podatkov. Poleg tega je v sistem potrebno pritegniti močno celico za upravljanje s komunikacijskimi in informacijskimi sistemi, zagotoviti načrtno upravljanje s kadri in dovolj močno logistiko za podpiranje posebnih zahtev namenskih sredstev ISTAR.

Celica za upravljanje z zahtevami in koordinacijo bi lahko nadomestili tudi v ustrezno organiziran in usposobljenim S-2 bojne skupine, kar bi poenostavilo ves proces.

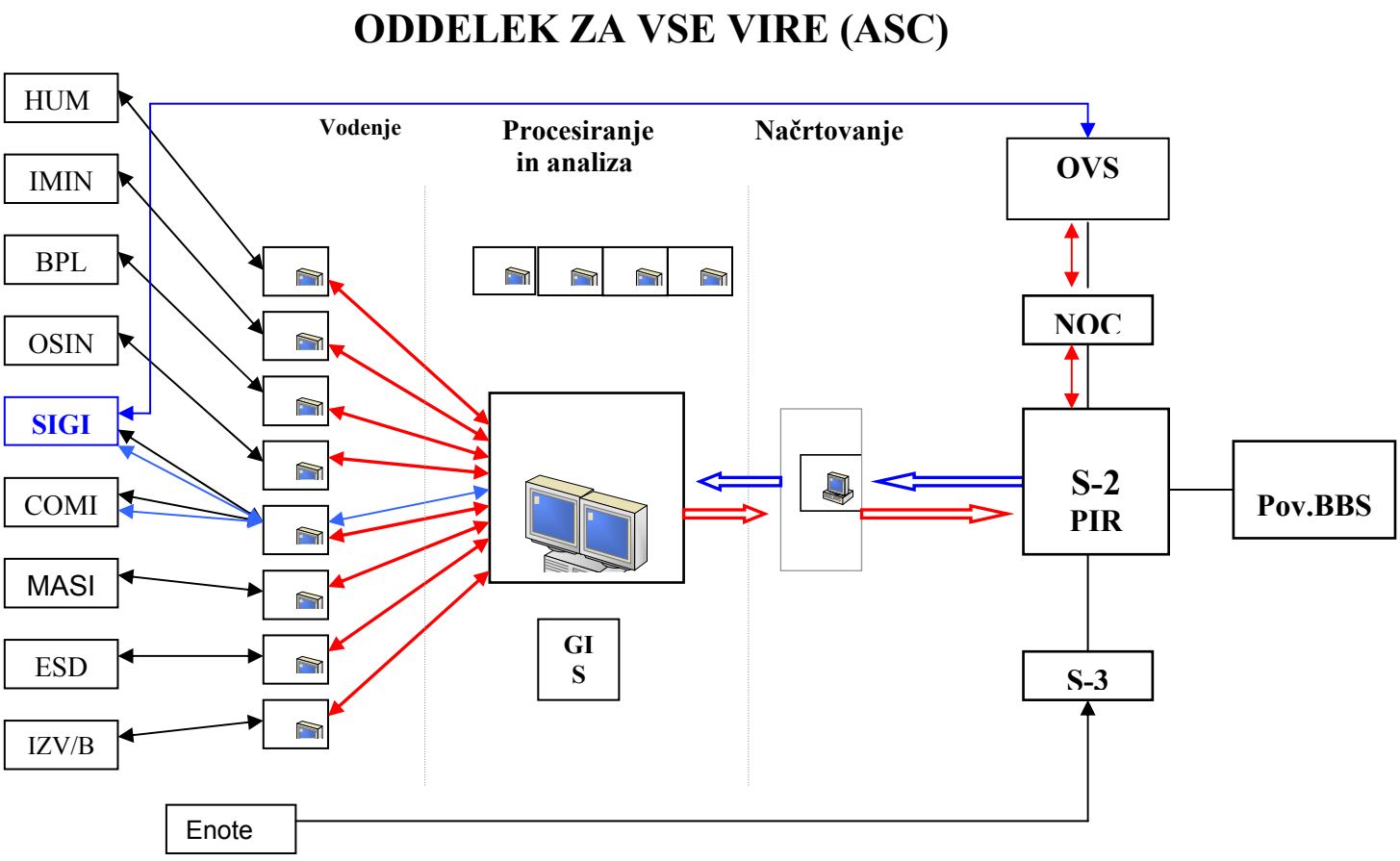
Najbolj pomemben člen v predlogu nove organiziranosti ISTAR bi bil vsekakor oddelek za vse vire (ASC), ki ga shematsko prikazujem na sliki 9-10. Sestavljen bi bil iz treh delov, in sicer:

- skupine za vodenje senzorjev,
- skupine ali celice za analizo vseh obveščevalnih podatkov in
- celice za načrtovanje zbiranja obveščevalnih podatkov.

ASC so srce in možgani ISTAR zmogljivosti, kjer zbirajo zahteve naročnikov (poveljnika, S-2 in S-3, oddelka za določanje ciljev in drugih), ki se preoblikujejo v načrt delovanja delov za zbiranje informacije in senzorjev, in se tako pridobljene informacije v obratni smeri sistematično uredijo, združijo z že obstoječimi, analizirajo in oblikujejo v odgovore na vprašanja ali zahteve naročnikov.

Vsa dejavnost ASC je močno povezana s sodobno informacijsko in komunikacijsko tehnologijo in je kolikor se le da avtomatizirana. (Dosse 2006)

Slika 9-10: Struktura oddelka za vse vire in njegova povezava v delovanje ISTAR modulov.



9.6 KAKO ISTAR VKLJUČITI V ZMOGLJIVOSTI SLOVENSKE VOJSKE

ISTAR sistem kot enota sama zase ne more obstajati, njeno delo je brez jasnih obveščevalnih zahtev in usmeritev lahko politično, strokovno in pravno sporno. Zato je potrebno določiti, na kakšen način se ISTAR moduli vključujejo v strukturo SV. Ker trenutno in po ocenah še nekaj časa ne bo resne vojaške grožnje proti Sloveniji, je na operativnem in taktičnem nivoju ISTAR najbolj uporaben v strukturah enot, namenjenih na OKO[90].

Slovenska vojska svoje zmogljivosti za OKO gradi modularno, tako da določi nosilno enoto moči bataljona, ki ga okrepi z rodovskimi moduli in multiplikatorji bojne moči. ISTAR modul štejemo med multiplikatorje moči, ker s posredovanjem prave in pravočasne informacije o nasprotniku ali cilju pomembno poveča preciznost in učinkovitost bojne moči bataljona in pridodanih enot. Kot tak bi moral biti obvezen sestavni del bojnih skupin, kar zahteva premislek o načinu vključevanja.

Na sliki 9-12 sem prikazal, katere naloge posamezni deli ISTAR enote izvajajo v različnih fazah izvedbe. Zmogljivostim ISTAR sem dodal še modul PSYOPS in globinske izvidnike enote za specialno delovanje. Dejavnost je precej razpredena in raznolika in obsega tako zbiranje informacij kot tudi ocenjevanje učinkov in zaščito delovanja enot bojne skupine.

To pomeni, da ISTAR deluje za potrebe obveščevalnih organov in v tesni povezavi z načrtovalci bojnih delovanj – operativci. V štabni shemi bi ISTAR morali povezati s S/G-2 in s S/G-3. V tej nalogi se ukvarjam z obveščevalnimi izzivi, zato bom povezavo ISTAR z operativci le omenil, podrobneje pa je ne bomo obravnaval.

Vključenost ISTAR procesov v vodenje in poveljevanje bojne skupine

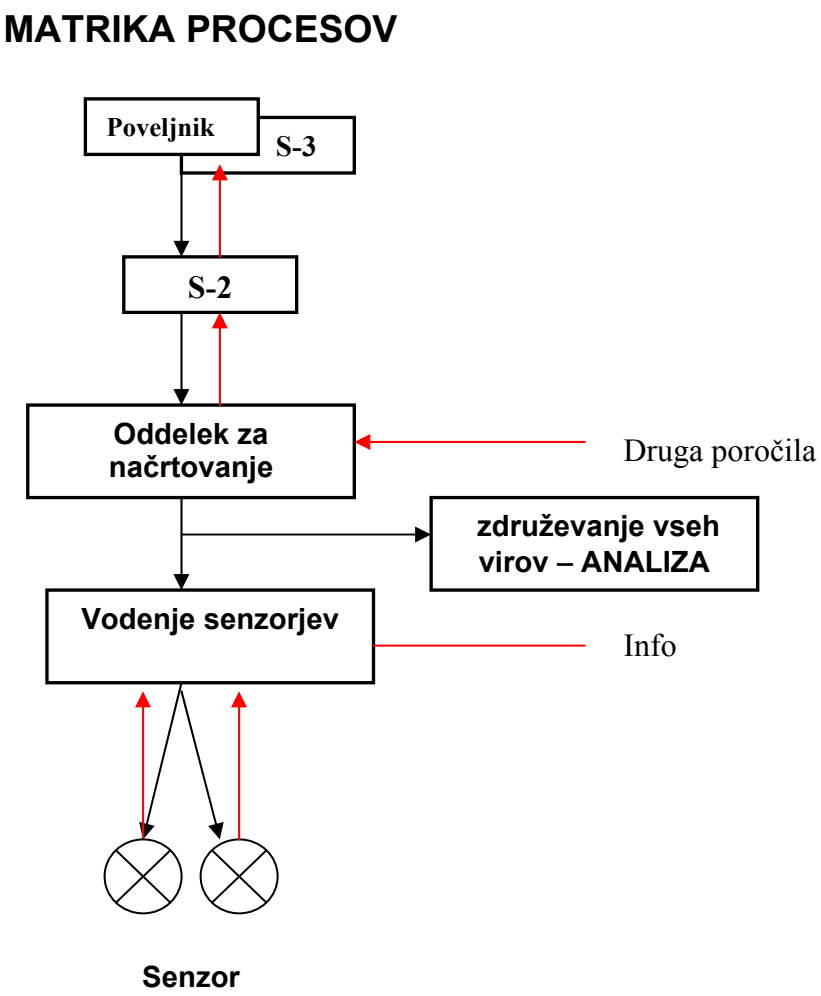
Slika 9-11 prikazuje, kako je poveljniški del ISTAR zmogljivosti s procesi povezan v linijo vodenja in poveljevanja bojne skupine. Delo s svojimi prioritetnimi in kritičnimi zahtevami po informacijah usmerja poveljnik bojne skupine (BBSK). Izdela jih v sodelovanju s štabnim organom za operativne zadeve – S-3, ki jih obveščevalni organ S-2 razdela v bolj podrobne zahteve in jih posreduje oddelku za načrtovanje ISTAR modula. Ta izdela načrt in matriko zbiranja podatkov, ki jih posreduje posameznim delom ISTAR modula v realizacijo.

V obratni smeri senzorji pošiljajo zahtevane informacije, ki gredo v oddelek za združevanje vseh virov, in analizo. Tam informacije združijo s tistimi, ki že obstajajo v njihovih bazah

[90] Operacije kriznega odzivanja.

podatkov in poročilo pošljejo v oddelek za načrtovanje. V tem oddelku lahko dopolnijo načrt zbiranja podatkov in pošljejo senzorjem nove zahteve po informacijah, ki bodo dopolnile odgovore na postavljene zahteve, ali pa poročila pošljejo v S-2, kjer izdelajo obveščevalni povzetek ali

Slika 9-11: Predlog povezav ISTAR poveljniškega dela s štabnimi organi poveljstva bojne skupine



Slika 9-12: Shematski prikaz delovanja ISTAR zmogljivosti v pripravi in izvedbi OKO

Delovanje ISTAR na OKO Obveščevalna dejavnost, nadzor, prepoznavanje ciljev in izvidništvo													
Načrt zbiranja obv. podatkov	**I.FAZA** Priprava na nalogo			**II.FAZA** Izvedba naloge						**III.FAZA** Po izvedbi naloge		
POSTOPKI	**H**	**H**	**H**	**H**	**H**	**H**	**H**	**H**	**H**	**H**	**H**	**H**
Analiza obm. Delovanj	**AOD**	**AOD**	**AOD**	**AOD**	**AOD**	**AOD**	**AOD**	**AOD**	**AOD**	**AOD**		
Bojevanje PSYOPS		**PSYB**	**PSYB**			**PSYB**	**PSYB**			**PSYB**	**PSYB**	
Izvidništvo		**IZV**	**IZV** **IZV**	**IZV** **IZV**	**IZV**	**IZV**	**IZV**	**IZV** **IZV**	**IZV**	**IZV**		
Elektronski zaščitni ukrepi		**EZU**										
Podporni ukrepi EB		**PUEB**			**PUEB**		**PUEB**			**PUEB**	**PUEB**	
Elektronski protiukrepi			**EPU**	**EPU**		**EPU**				**EPU**		
Nadzor in varovanje		**NV**	**NV**							**NV**	**NV**	
Ocena posledic - (BDA)						**O** **c** **P**				**O** **c** **P**		
Odkrivanje ciljev VV				**OCi** **VV**			**Ci** **VV**					
Pridobivanje obv. podatkov	**PO** **P**			**POP**			**POP**			**PO** **P**		
Analiza obv. podatkov		**AO** **P**			**AOP**			**AOP**			**AO** **P**	
Posredovanje obv. podatkov			**PO** **S**			**POS**			**POS**			**PO** **S**
Upravljanje z ognjem					**UO**			**UO**				
Senzorski sistemi	HUMINT	IMINT/BPL		SIGINT/COMINT		PSYOPS		OSINT		IZVIDNIKI	ESD	

oceno, ki je načeloma odgovor na poveljnikove zahteve po ključnih informacijah in jo pošljejo v S-3 in drugim naročnikom (poveljnik, mednarodno obveščevalno mrežo, OVS, itd.)

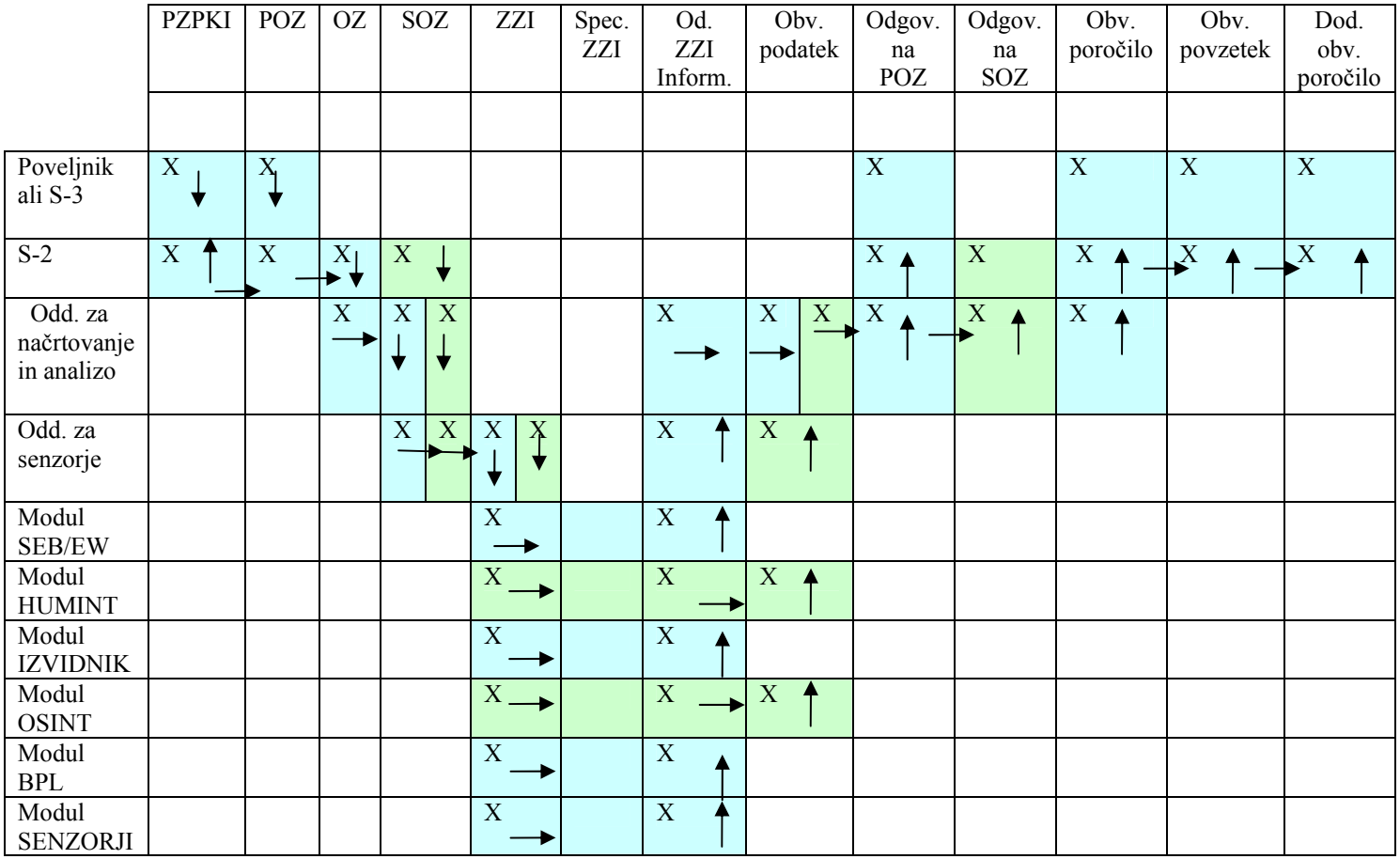
Sliki 9-11 in 9-12 lahko združeno prikažemo v sliko 9-13, kjer lahko v obliki matrike sledimo, kaj se v procesu zbiranja in analize obveščevalnih podatkov dogaja s poveljnikovimi zahtevami po ključnih informacijah. Možno je ugotoviti, da se taka zahteva razdeli v bolj podrobne zahteve in se s procesi usklajevanja, aktivnega zbiranja novih informacij, preverjanja že obstoječih in tehtanja verodostojnosti v obliki različnih poročil, ocen in povzetkov postopno združuje v čim bolj celovit odgovor na postavljena vprašanja. Cikel se lahko kadarkoli vrne v proces zbiranja in dopolnjevanja informacij, če S-2 ali analitična skupina oceni, da odgovor ni ustrezen oziroma je pomanjkljiv.

9.6.1 Sodelovanje ISTAR modula pri določanju ciljev

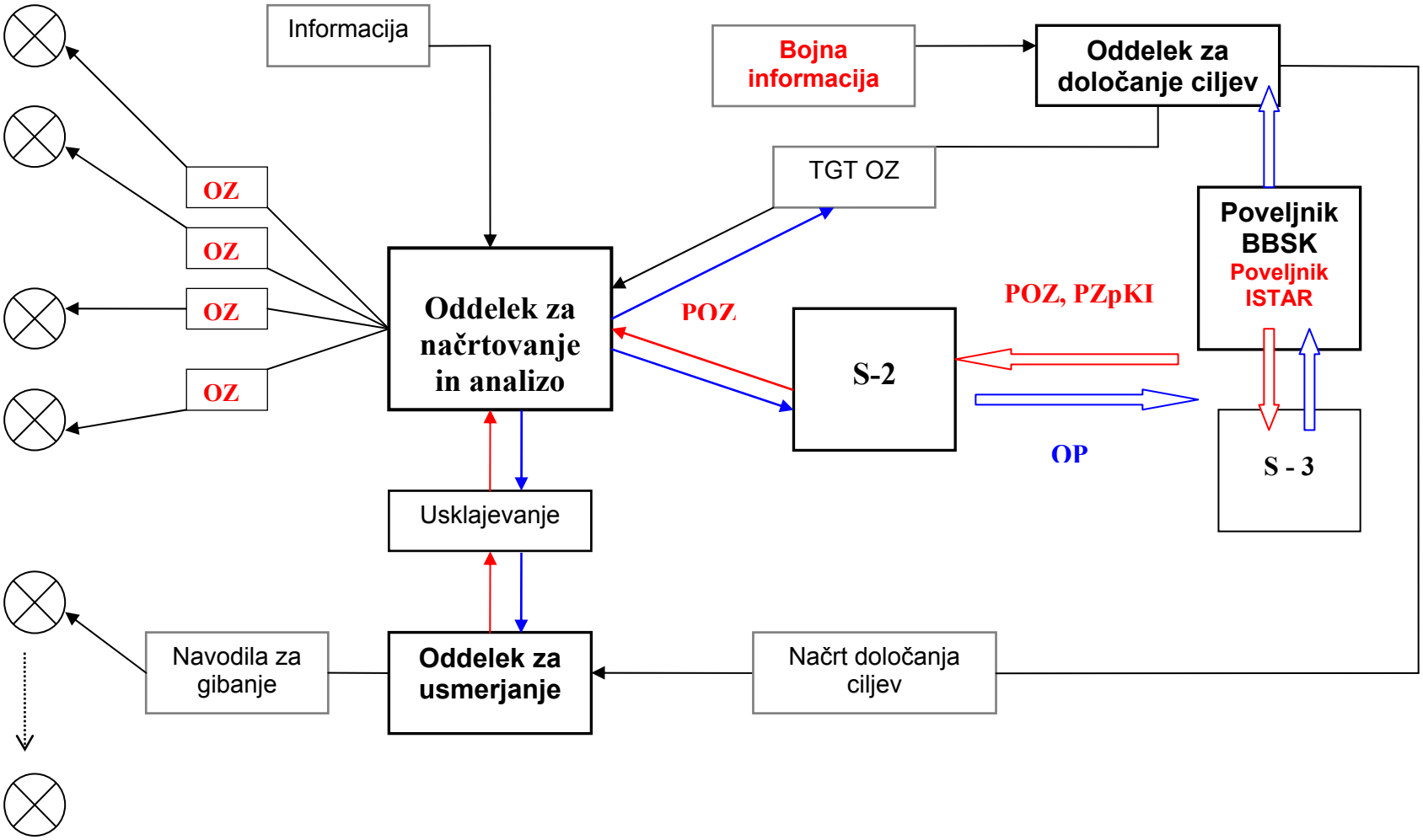
Posebno zahtevna naloga je sodelovanje pri določanju ciljev. Bolj podrobno sem ta proces opisal v poglavjih 6.6.2 in 6.6.5. V tem poglavju pa bi radi predlagal vpetost ISTAR modula v proces načrtovanja ciljev v bataljonski bojni skupini SV. Slika 9-14 prikazuje povezanost ISTAR modula v proces določanja ciljev. Procesom, ki sem jih opisoval do sedaj, se na tej sliki pridružuje še proces sodelovanja v določanju ciljev, tako da lahko oddelek za določanje ciljev (za katerega predlagamo, da ni sestavni del ISTAR, temveč štabne strukture BBSK) oblikuje svoje obveščevalne zahteve in jih pošilja neposredno v oddelek za načrtovanje in analizo. Ta zahteve vključi v svoj proces in odgovore posreduje neposredno oddelku za določanje ciljev.

V proces določanja ciljev je aktivno vključen tudi poveljnik in S-3, ki obveščevalne zahteve v zvezi s cilji običajno vključi v svoje zahteve zato, da lahko oblikuje ustrezne odločitve. Kasneje se v proces usmerjanja delovanja po ciljih ISTAR vključuje ponovno prek oddelka za načrtovanje in analizo, tako da neposredno z načrtovalci izvedbe usklajuje predhodne informacije o cilju z najnovejšimi. Ti procesi zahtevajo dobro medsebojno usklajenost in izurjenost vseh, ki v procesu sodelujejo.

Slika 9-13: Matrika toka obveščevalnih zahtev in informacij v BBSK z ISTAR modulom.



Slika 9-14: Vključevanje ISTAR modula v določanje ciljev BBSK.



10 ZAKLJUČKI

V nalogi sem opredelil razvojne, organizacijske in druge usmeritve ter izhodišča za pripravo in izvedbo oblikovanja vojaške obveščevalne dejavnosti SV ter njeno delovanje v strukturah in operacijah zavezništev. Opredelil sem pojem in poslanstvo, funkcije, načela, metode dela, discipline zbiranja, nosilce, podporo in nadzor ter usmerjanje vojaške obveščevalne dejavnosti.

Tako kot ugotavlja (Prezelj 2005, 97–98), prihaja do netradicionalne uporabe oboroženih sil v nevojnih vojaških operacijah, kjer so še posebej pomembne zanesljive in pravočasne informacije. Transnacionalni značaj groženj zahteva intenzivno mednarodno sodelovanje tudi na obveščevalnem področju.

Tudi v Slovensko vojsko je tako potrebno uvesti nove zmogljivosti in metode vojaške obveščevalne dejavnosti ter spremeniti organizacijsko kulturo, posvetiti večjo pozornost razvoju človeških virov ter okrepiti informacijsko podporo.

V določbah 32. člena Zakona o obrambi so definirane obveščevalne in protiobveščevalne ter varnostne naloge. Obveščevalne in protiobveščevalne naloge obsegajo zbiranje, dokumentiranje in analiziranje informacij ter podatkov, ki so pomembni za obrambne interese države oziroma varovanje takih podatkov, zlasti pa:

- ugotavljanje in ocenjevanje vojaških in politično-varnostnih razmer ter vojaških zmogljivosti zunaj države, ki so posebnega pomena za varnost države;
- zbiranje in ocenjevanje podatkov o razmerah na območjih, kjer med izvrševanjem obveznosti, prevzetih v mednarodnih organizacijah oziroma pri opravljanju vojaške službe, delujejo tudi pripadniki Slovenske vojske;
- odkrivanje in preprečevanje dejavnosti obveščevalnih služb vojaških organizacij ter drugih organov in organizacij, ki ogrožajo obrambne interese države, Slovensko vojsko ali ministrstvo.

V 3. točki 32. člena Zakona o obrambi je navedeno, da obveščevalne in protiobveščevalne ter varnostne naloge na obrambnem področju opravlja obveščevalno-varnostna služba ministrstva.

Iz zakonodaje je tudi razvidno, da je oblikovanje sektorjev na nivoju Generalštaba, Poveljstva sil SV in ostalih poveljstev in enot v Slovenski vojski stvar notranje organiziranosti vojske. Tako štabni sektor za obveščevalne in varnostne zadeve oziroma J/G/S-2, kot mu rečemo v Slovenski vojski, nima nobenih posebej zakonsko določenih nalog in pooblastil. Naloge štabnega sektorja za obveščevalne in varnostne zadeve (J/G/S-2) in enot, ki jih le ta funkcijsko usmerja, torej izhajajo iz splošnih nalog SV, konkretno podpora poveljevanja (Furlan 2006).

Vsi vojaški profesionalci pa dobro vemo, da poveljnik ne more sprejeti pravih odločitev brez relevantnih informacij (npr. v štabnem procesu dela je začetna osnova obveščevalna priprava bojišča). Tudi ostale naloge, ki jih mora opravljati štabni sektor za obveščevalne in varnostne zadeve (J/G/S-2) in enote, ki jih le ta funkcijsko usmerja, so nujne za učinkovito podporo poveljevanja. Vsaj nekaterih temeljnih funkcij VODBE SV (prepoznavanje indikatorjev in opozarjanje, izvajanje obveščevalne priprave bojišča, podpora skupne operativne slike in zavedanje situacije, podpora ciljenju, ocenjevanje bojnega delovanja, podpora zaščiti sil, priprava sil za delovanje, protiobveščevalne in varnostne naloge) ki jih definira AJP-2.0, pa je nemogoče izvajati brez ustrezne spremembe organiziranosti obveščevalno izvidniških zmogljivosti SV.

Z vstopom Slovenije v zvezo NATO in povečanjem udeležbe SV na mednarodnih vojaških operacijah se povečuje tudi stopnja ogroženosti SV. Enote SV v sestavi mednarodnih vojaških operacij so na območju operacij v enaki meri izpostavljene istim varnostnim tveganjem kot sile sodelujočih držav. Vrsta tveganj in stopnja ogroženosti sta odvisna od vrste operacije, varnostne situacije na področju operacij, nalog enot SV ter drugih dejavnikov.

Vojaška obveščevalna dejavnost SV (ob tesnem sodelovanju s protiobveščevalno in varnostno dejavnostjo SV, OVS, SOVA ter obveščevalnimi organi mednarodne operacije) mora biti sposobna pravočasno predvideti, odkriti, oceniti in spremljati navedene grožnje ter s tem poveljniku SVNKON in poveljnikom enot omogočiti učinkovito odločanje.

Sprejeti NATO standardi (AJP-2.0: Skupna zavezniška obveščevalna, protiobveščevalna in varnostna doktrina 2003, in AJP-2.1: Intelligence Procedures 2002), ki smo jih sprejeli brez

omejitev in od koder je Slovenska vojska črpala svoje pojmovanje funkcij, načel, metod dela in disciplin pridobivanja podatkov, zahtevajo od SV več, kot ji je dopuščeno po Zakonu o obrambi.

V nalogi smo prikazali oblike in načela organiziranosti in delovanja tujih obveščevalnih zmogljivosti in opredelili koncept ISTAR v EU in NATO. Prikazali smo tudi sedanjo organiziranost in načela delovanja obveščevalnih zmogljivosti SV in jo primerjali s tujimi.

S tem sem dokazal, da sedanja organiziranost in sposobnost obveščevalne strukture SV daleč zaostaja za mednarodnimi standardi, pa tudi za lastnimi razvojnimi cilji, ki se časovno vedno bolj oddaljujejo. Na ta način sem dokazal pravilnost hipoteze 1, po kateri ima Slovenska vojska vojaško obveščevalno-varnostno zagotovitev organizirano na način, ki ni primerljiv s koncepti ISTAR NATO in EU.

Zaradi navedenega SV za sedaj v mednarodnih vojaških operacijah ne more izvajati vseh svojih obveznosti, ki jih je sprejela Republika Slovenija. Tako se lahko zgodi, da SV in RS ne bosta predstavljali kredibilnega partnerja v mednarodnem okolju.

Opisal in analiziral sem zmogljivost ISTAR sistemov Kanade, Nizozemske, Velike Britanije. Primerjal sem jih med seboj in s sedanjimi ter predlaganimi rešitvami obveščevalne dejavnosti v SV. Rezultati so pokazali, da so vse tri države po organiziranosti, opremljenosti in uspešnosti ISTAR sistemov daleč pred Slovenijo, njihove izkušnje so lahko dobro vodilo za graditev našega sistema. Ugotovil sem, da ima Kanada nekaj slabše zmogljivosti od Nizozemske in da ISTAR Velike Britanije praktično izpolnjuje vse zahteve kriterijev primerjalnega modela. S tem sem potrdil pravilnost druge hipoteze, da imajo Nizozemska, Kanada in Velika Britanija obveščevalno dejavnost organizirano po načelih sistema ISTAR.

Kot vodilo pri izdelavi zahtev in kriterijev primerjalnega modela, sem upošteval razmišljanja raziskovalcev obveščevalnih sistemov iz ZDA, Kanade, Velike Britanije, Srbije, Nemčije, bivše SFRJ in koncepte ISTAR NATO in EU, ki sem jih v nalogi predstavil.

Vključitev Republike Slovenije v zvezo NATO in varnostne zahteve, ki jih zavezništvo postavlja svojim članicam, predstavljata potrebo po urejenosti obveščevalno-varnostnega področja v Slovenski vojski. Na omenjeno potrebo kažejo tudi dejstva, da so se v zadnjem času pojavili novi dejavniki, zaradi katerih so se močno spremenile varnostne razmere v svetu.

Zato je tudi za Slovensko vojsko še kako aktualen izrek, da ne smemo zadržati vojske, ki smo je vajeni, temveč moramo zgraditi vojsko, kot jo potrebujemo. V ta namen sem predlagal takšno prihodnjo organiziranost in opremljenost obveščevalne strukture SV, ki povezuje obstoječe zmogljivosti v pregleden, odziven in uporaben sistem, primerljiv z mednarodnimi standardi ISTAR. Dokazal sem tudi, da mora biti ISTAR sestavni del procesa odločanja, ker je to bolj zanesljiv, odziven in pregleden sistem od dosedanjega.

Na prvi pogled je nelogično, da grafikon ustreznosti novega modela ISTAR kaže kar nekaj odmikov od zahtev kriterijev, vendar je pomembna razlika v dobri povezanosti posameznih elementov novega sistema. Pomembna novost je stopnja zanesljivosti, ki jo v novem predlogu skušam zadovoljivo uresničiti. V predlogu želim zagotoviti tudi pregleden, urejen in deloma avtomatiziran sistem hranjenja in distribucije podatkov. Pri tem sem se osredotočil predvsem na oblikovanje dobrih baz podatkov in digitalizacijo geografskih podlag. Ena največjih pomanjkljivosti današnjega obveščevalnega sistema je premalo načrtno delovanje, čemur je v predlogu posvečena posebna skrb. Oblikovane bodo celice za upravljanje z zahtevami, celice za analizo in združevanje vseh podatkov, uveljavljen bo celovit obveščevalni cikel z dobro povezavo obveščevalnih organov v linijo PINK[91]. Če danes senzorjev v SV skoraj ne uporabljajo, bo to v novem predlogu bolj pomemben člen. Pri tem ne predvidevamo, da bodo kupili in uporabljali vse na tržišču dosegljive sisteme. Težišče uporabe senzorjev bo na zaščiti sil in pravočasnem opozarjanju na nevarnosti.

Zaključim lahko z ugotovitvijo, da predlagam nakup nove opreme in vztrajam na dobrem sistemu načrtovanja, medsebojnem pretoku informacij, celoviti analizi in preglednem sistemu distribucije.

S tem sem dokazal pravilnost tretje hipoteze, ki trdi, da sedanji način organiziranja obveščevalne dejavnosti predstavlja osnovo za dograditev v povezljiv, uporaben in sodoben ISTAR sistem. V ta namen bo potrebno spremeniti način dela poveljstev, posodobiti informacijsko opremo, nakupiti precej sodobne obveščevalne in izvidniške opreme in dodatno usposobiti obveščevalni kader.

Filozofija ISTAR izhaja iz domneve, da sta mrežna organiziranost in nemotena izmenjava informacij med različnimi strukturami odločilna za uspešnost delovanja. Zakon o obrambi opredeljuje OVS kot nosilko obveščevalne dejavnosti v obrambnem sistemu tudi za potrebe

[91] Poveljevanje in kontrola.

SV, vendar se OVS pri svojem delu ne spušča na operativni in taktični nivo, ne sodeluje v štabnem delu poveljstev SV, niti nima svojih obveščevalnih enot. V nalogi sem premišljeval tudi o tem in predlagal take organizacijske posege, ki bi zagotovili racionalno uporabo razpoložljivih obveščevalnih zmogljivosti OVS in SV, in jasno razdelili naloge in pristojnosti ene in druge organizacije. Prikazali smo tudi predloge rešitev medsebojnih povezav in procesov, ki so osnova za načrtovanje sodobnih medsebojnih komunikacijskih povezav.

11 LITERATURA

1. ***AAP – 6.*** 2010. *NATO Glossary of Terms and Definition.*
2. ***AAP - 15.*** 2008. *NATO Glossary of Abbreviations.*
3. ***AJP 2.0***. 2003. NATO *Allied Joint Intelligence, Counter Intelligence and Security Doctrine.*
4. **Andrew, Christopher.** 1991. The British View of Security and Intelligence. V *Security and Intelligence in a Changing World,* ur. Stuart Farson, David Stafford in K. Wesley Wark, 10–25. London : Frank Cass & Co. Ltd.
5. **Bajagić, Mladen.** 2008. *Špijunaža u XXI veku. Savremeni obaveštajno-bezbednosni sistemi.* Beograd : Book & Marso.
6. **Carr, Karen.** 2008. *C4ISTAR Capability: Human Aspects.* London: Defence Academy of the United Kindom.
7. **Clapper, R. James Jr.** 2003. *Happiness is never having to refold the map.* Defender. Vol. 1, No. 4. Dostopno prek. http://raytheon.com/defender (15. maj 2010).
8. **NATO Consultation, Command in Control Agency.** 2007. *Coalition Interoperable ISR&TA Tactics, Techniques and Procedures, Draft Version 2.*
9. **Cogan, Charles.** 2004 *Hunters not Gathers*. *Intelligence in the Twenty-first Century.* V *Understanding Intellgence in the Twenty-First Century. Journeys in Shadows,* ur. V. Len Scott in Peter Jackson. 147–161. London: Routledge.
10. **Connel, David.** 2003. *Canadian Forces Project Land Force ISTAR.* Department of National Defence. Dostopno prek: http://www.dtic.mil/cgi (15. maj 2010).
11. **Cosquer, Christian.** 2007. *Consequences of Data Fusion and Networking capabilities on Intelligence, Command and Control Organization.* Predstavitveno gradivo. Ministere de la Defense. Francija.
12. **Črnčec, Damir.** 2009. *Obveščevalna dejavnost v informacijski dobi.* Ljubljana: Defensor d.o.o.
13. **DeWolf, Paul.** 2007. *Intelligence Fusion and Data Management.* Predstavitveno gradivo. London: Northrop Grumman Corporation.
14. ***Dictionary of Military and Associated Terms – dopolnjena izdaja.*** 2009. Washington: Department of Defense,

15. **Dosse, Stephane.** 2006. The All Sources Analysis Cell, An Improved Way to Process Information. *Doctrine.* Paris : Centre de Doctrine d'Emploi des Forces, dostopno: http://www.cdef.terre.defense.gouv.fr/publications/doctrine/doctrine09 (15. maj 2010).
16. **Dupuy, N. Trevor.** 1993. *International Military and Defense Encyclopedia,*. Washington: Maxwell & Macmillan, Inc.
17. **EU Defence Planning Staff,** 2002. *Military ISTAR Concept for EU Crisis Management and EU-led Operations.*
18. **Ferris, John.** 2004. Netcentric Warfare, C4ISR and Information Operation. V *Understanding Intelligence in the Twenty First Century, Journeys in Shadows,* ur. Scott Len and Jackson Peter. 54–74. London : Routledge.
19. **Finacchio, Pietro.** 2008. *The Implementation and Exploitation of Italian Network Centric Capabilities.* Predstavitveno gradivo. Brussels: C4ISTAR Procurement Agency (TELEDIFE).
20. **Foisseau, Jack.** 2009. *Extract of NATO MAJIIC AWG meeting.* Toulouse: The French Aerospace Lab,
21. **Furlan, Branimir in sodelavci.** 2006.*Vojaška doktrina.* Ljubljana: Defensor d.o.o,
22. **Furlan, Branimir in sodelavci.** 2007. *Navodila za štabno delo.* Ljubljana: PDRIU SV.
23. **Gažević, Nikola.** 1970. *Vojna enciklopedija, druga izdaja, prva knjiga.* Beograd: Redakcija vojne enciklopedije.
24. **Gažević, Nikola.** 1973. *Vojna enciklopedija, druga izdaja, šesta knjiga.* Beograd: Redakcija vojne enciklopedije.
25. **Generalštab SV.** 2003. *Koncept obveščevalno izvidniške zagotovitve SV.* Ljubljana.
26. **Gill, Peter.** 1991. The Evolution of the Security Intelligence Debate in Canada Since 1976. V *Security and Intelligence in a Changing World,* ur. A. Stuart Farson, David Stafford in K. Wesley Wark. 75–94. London: Frank Cass & Co. Ltd.
27. **Goodrich, Dan.** 2003, *Flexibility.* 5–9. Defender, Vol. 1, No. 4. Dostopno prek: http://raytheon.com/defender (15. maj 2010).
28. **Grizold, Anton.** 1998. Institucionalizacija zagotavljanja mednarodne varnosti. V *Perspektive sodobne varnosti.* 3–29. Ljubljana: Fakulteta za družbene vede.
29. **Grizold, Anton.** 1999. *Evropska varnost.* Ljubljana: Fakulteta za družbene vede.

30. **Herman, Michael.** 2004. Ethics and Intelligence after September 2001. V *Understanding Intelligence in the Twenty First Century,* ur. V. Len Scott in Peter Jackson. 180–193. London: Routledge.

31. **Hinsley, F. H.** 1963. *Power and Persuit of Peace.* Cambridge: Cambridge University Press.

32. **Jakobsson, Johan.** 2008. *Swedish Knowledge Support System.* Predstavitveno gradivo. Upssala : Swedish Intelligence & Security Centre.

33. **Kerttunen, Mika, Koivula, Tommi in Jeppsson, Tommy.** 2005. *EU Battlegroups. Theory and Development in the Light of Finnish-Swedish Co-operation.* Helsinki: National Defence College.

34. **Kolenc, Marjan.** 2006. *Institucionalizacija obveščevalne politike EU.* Ljubljana: Fakulteta za družbene vede.

35. **Lefevbre, John.** 2006. *The ISTAR Capability of the Canadian Forces.* Doctrine. Paris: Centre de Doctrine d'Emploi des Forces. Junij. Dostopno prek: http://www.cdef.terre.defense.gouv.fr/publications/doctrine/doctrine09 (15. maj 2010).

36. **Majcenovič, Matjaž.** 2004. *Obveščevalna podpora odločanja poveljnika brigade.* Poljče: Poveljniško Štabna šola SV.

37. **Netherland Royal Army.** 2007. NATO Responce Force (NRF-10). Predstavitveno gradivo.

38. **Norell, Magnus.** 2007. Intelligence Coordination and Counterterrorism: A European Perspective. V *Countering Terrorism and Insurgency in the 21st Century,* ur. J.F. James Forest. 440–465. London : Praeger Security International.

39. **Omand, David.** 2009. Ethical guidelines in using secret Intelligence for public security. V *Secret Intelligence, A Reader,* ur. Christopher Andrew, J. Richard Aldrich in K. Wesley Wark. 395 - 407. Abingdon: Routledge.

40. **Phythian, Mark.** 2009. The British Experience With Intelligence Accountability. *Secret Intelligence. A Reader,* ur. Christopher Andrew, J. Richard Aldrich in K. Wesley Wark. 337 - 356. Abingdon: Routledge.

41. **Poucet, Emmanuel.** 2006. HUMINT Intelligence, Expectation and Problems. - Intelligence for Land Forces. V *Doctrine.* Paris: Centre de Doctrine d'Emploi des Forces. Junij. Dostopno prek: http://www.cdef.terre.defense.gouv.fr/publications/doctrine/doctrine09 (15. maj 2010).

42. **Purg, Adam.** 1995. *Obveščevalne službe.* Ljubljana: ČZP Enotnost.
43. **Purg, Adam.** 2002. *Primerjalni obveščevalni sistemi.* Ljubljana: Ministrstvo za notranje zadeve.
44. ***Resolucija o strategiji nacionalne varnosti Republike Slovenije.*** Uradni list RS 27/10. Dostopna prek: http://zakonodaja.gov.si/rpsi/r01/predpis_RESO61.html (15. maj 2010).
45. **Ross, Joe.** 2009. *The MAJIIC Project and Coalition JISR Reporting Methods.* Predstavitveno gradivo za NATO JISR Panel.
46. **Ministrstvo za obrambo RS.** 2000. *Odredba ministra za obrambo o izvajanju nalog organa, pristojnega za obveščevalno podporo poveljevanju in vodenju ter za izvajanje štabno varnostnih nalog SV.*
47. **Scott Len, Jackson Peter.** 2004. *Understanding Intelligence in the Twenty-first Century, Journeys and Shadows.* Introduction. London: Routledge.
48. **Scott, Len.** 2004. Secret Intelligence, Covert Actions and Clandestine diplomacy. V *Understanding Intelligence in The twenty First Century,* ur. V. Len Scott in D. Peter Jackson. 162–179. London: Routledge.
49. **Shpiro, Shlomo.** 2007. *Speak no Evil: Intelligence Ethics in Israel.* Ramat Gan, Izrael: Bar-Ilan University, ISA Annual Conference 2007. Dostopno prek: http://intelligence-ethics.org/articles/ethics_in_israel.pdf (15. maj 2010).
50. **Shulsky, N. Abram.** 2002. *Silent Warfare: Understanding the World of Intelligence.* Washington D.C: Brassey's.
51. **Sjoerd de Vries, Jan.** 2008. *EU Capability Development on ISTAR.* Predstavitveno gradivo. Brussels: European Defence Agency, Capability Directorate.
52. **Šaponja, Vladimir.** 1999. *Taktika dela obveščevalnih služb.* Ljubljana: Visoka varnostno policijska šola.
53. **Teleplan AS.** 2009. NORCCIRM Briefing na NATO JISR Panel. Predstvitveno gradivo.
54. **Timmermans, Jan.** 2006. The Dutch Approach of ISTAR concept during NRF-4. Doctrine. Paris: Centre de Doctrine d'Emploi des Forces. Junij. Dostopno prek: http://www.cdef.terre.defense.gouv.fr/publications/doctrine/doctrine09 (15. maj 2010).
55. **Turner, Stansfield.** 1986. *Secrecy and Democracy.* London: Sidgwick & Jackson.
56. **UK Ministry of Defense.** 2009. British Army Filed Manual, Volume 1, Part 10, Countering Insurgency. London.

57. **Ustava Republike Slovenije.** 2006. Ljubljana: Uradni list 33/91. Dostopno prek: http://www.dz-rs.si/?id=150 (15. maj 2010).

58. **Vance, Matt.** 2008. *CEDRIC – Centre for Experimentation, De-Risking and Integration of C4I Capability.* Predstavitveno gradivo. Norfolk.

59. **Vovk, Slavko.** 2006. *Posebne operativne metode versus človekove pravice.* Poljče: Poveljniško Štabna Šola.

60. ***Zakon o obrambi - prečiščeno besedilo.*** 2004. Uradni list 103/2004. Dostopno prek: http://zakonodaja.gov.si/rpsi/r07/predpis_ZAKO4187.html (15. Maj 2010).

61. **Žabkar, Anton.** 2003.*Marsova dediščina. Temelji vojaških ved, 1. knjiga.* Ljubljana: Fakulteta za družbene vede.

62. **Wark, K. Wesley.** 2003. Canada and the Intelligence Revolution. V *Secret Intelligence in the Twenty First Centrury,* ur. Heike Bungert, G. Jan Heitmann in Michael Wala. 176–194. London: Frank Cass & Co. Ltd.

63. **Warner, Michael.** 2009. Wanted. A definition of "intelligence". V *Secret Intelligence. A Reader,* ur. Aldrich J. Aldrich, Wark K. Wesley Andrew Christiopher. 3–11. Abingdon: Routledge.

64. **Whitaker, Reg.** 1991. The Canadian Security and Intelligence System: Fighting the Last War or the Next? V *Security and Intelligence in a Changing World,* ur. A Stuart Farson, David Stafford in K. Wesley Wark. 126–135. London: Frank Cass & Co. Ltd.

65. **Wolf, Ulrich.** 2008. *C4ISTAR Challenges 2008.* Predstavitveno gradivo. Brussels: NATO Communication Systems Agency.