ŠOLA ZA ČASTNIKE
XIX. GENERACIJA
SPECIALIZACIJA ZVEZE

Zaključna naloga

VLOGA ENOT ZA ELEKTRONSKO BOJEVANJE V OBVEŠČEVALNI DEJAVNOSTI

Kandidat, slušatelj: desetnik, Alojz Berginc

Mentor: stotnik, Damjan Golob

Ljubljana, september, 2008

POVZETEK

Pravočasno pridobivanje ažurnih in verodostojnih obveščevalnih podatkov je ključnega pomena za pravilno odzivanje na nevarnosti nove dobe. Izraba elektromagnetnega spektra (EMS) omogoča oddajo in prestrezanje kjerkoli in kamorkoli. Prestrezanje in analiza informacij je zahtevno in odgovorno delo - le pravočasno prestrezanje in analiza nas lahko opozorijo na morebitne nevarnosti ter odločilno pripomorejo k izvajanju obveščevalne dejavnosti.

Na začetku zaključne naloge so predstavljeni osnovni obveščevalni pojmi kot so informacija, podatek, obveščevalni podatek in obveščevalni krog. V nadaljevanju sta predstavljeni področji elektronsko izvidovanje (EI) in elektronsko bojevanje (EB) s podrobneje opisanimi ukrepi in aktivnostmi ter prikazano sinergijo/razmejitvijo obeh. V zaključnem delu je podana vloga pasivnih ukrepov/aktivnosti EI in EB v obveščevalni dejavnosti v mirnodobnem času ter krizni situaciji.

KLJUČNE BESEDE:

Elektronsko izvidovanje (EI), Elektronsko bojevanje (EB), Elektromagnetni spekter (EMS), Podporni ukrepi elektronskega bojevanja (PUEB), Obveščevalen podatek, Obveščevalna dejavnost.

SUMMARY

In time acquisition of continuous and valuable intelligence is a key factor of correct response to new age threats. Use of electromagnetic spectrum (EMS) gives possibilities of transmissions and interceptions with no limits. Interception and analysis is a demanding and responsible task – only timely interception and analysis can assure threat recognition and contribute to effective intelligence.

At the beginning, basic intelligence elements, as information, data, intelligence data and intelligence cycle are explained. Afterwards, functions as Signals Intelligence (SIGINT) and Electronic Warfare (EW) with their subelements and their synergy/deviation are presented. At the end, Communication Intelligence (COMINT) and Electronic Support Measures (ESM) role in intelligence is explained, in peaceful time as well as in crises situations.

KEY WORDS:

Signals Intelligence (SIGINT), Electronic Warfare (EW), Electromagnetic spectrum (EMS), Communication Intelligence (COMINT), Electronic Support Measures (ESM), Intelligence data, Intelligence.

KAZALO

1 UVOD

"In the case of electronic warfare, as in any other kinds of warfare, no weapon and no method is sufficient on its own." Martin van Creveld; Technology and War, 1989

Že od samega začetka uporabe elektromagnetnega spektra (EMS) za vojaške namene, so se pokazale velike prednosti. Skupaj z naraščanjem uporabe brezžičnih komunikacij in razvojem novih tehnologij, so se pokazale tudi potrebe po razvoju specifičnih tehnik bojevanja - elektronskega bojevanja (EB) in elektronskega izvidovanja (EI), kot enega ključnih virov obveščevalnih podatkov.

Zaradi narave širjenja elektromagnetnih valov (EMV), je na tem področju mogoče delovati tudi iz relativno varne razdalje, v času miru in vojne, ne da bi bili pri tem odkriti.

Zaključna naloga se bo iz vseh podzvrsti EB in EI posvetila predvsem tako imenovanim pasivnim ukrepom (aktivnostim) - prestrezanju podatkov in informacij, ter poskušala predstaviti njihov pomen oziroma vlogo k celotni obveščevalni sliki.

Nasprotujoče si sile imajo vedno interes in morajo konstantno spremljati premike, aktivnosti in stopnjo usposobljenosti nasprotnika. EB in EI sta ena redkih oblik bojevanja, ki se lahko izvaja tudi v miru, z večjih razdalj, ne da bi s tem ogrožali sebe ali izzvali nasprotnika.

Razvoj novih tehnologij, še posebej na področju računalništva in informatike, je dal velik zagon razvoju komunikacij, tako na vojaškem, kot na civilnem področju. Z razpadom blokovskega sistema je prišlo do velikih sprememb in razmaha terorizma, kjer so meje med nasprotniki zabrisane, in je težje odkriti vir grožnje. V takih okoliščinah glavno vlogo pri zagotavljanju nacionalne varnosti nosijo obveščevalne službe. Ključnega pomena je pridobivanje pravočasnih, verodostojnih ter ažurnih informacij. Le konstanten nadzor potencialnih sovražnikov nam omogoča pravočasno reagiranje in preprečitev nepotrebnih civilnih ter vojaških žrtev. To dosežemo tudi s kontrolo frekvenčnega spektra za potrebe odkrivanja novih groženj preden te prerastejo v nevarnost.
Za nadzor in odkrivanje nasprotnikovih aktivnosti na tem področju so odgovorne enote za elektronsko bojevanje (EEB), katerih učinkovitost je odvisna tako od usposobljenosti kadra kakor tudi zmogljivosti tehničnih sredstev.

1.1 HIPOTEZA

Vloga EEB je, skozi izvajanje COMINT in PUEB) ima v obveščevalni dejavnosti enega ključnih pomenov.

1.2 NAMEN IN CILJI RAZISKAVE

Namen naloge je izpostavitev vloge PUEB / COMINT, ena ključnih v okviru obveščevalne dejavnosti kot širokega pojma pridobivanja obveščevalnih podatkov.

Cilji raziskave so sledeči:

- predstaviti osnovne elemente obveščevalne dejavnosti kot uvod v opredelitev PUEB / COMINT,
- podrobneje opredeliti področje PUEB / COMINT.
- opredeliti vlogo PUEB / COMINT v obveščevalni dejavnosti.

1.3 METODE DELA

Pri izdelavi zaključne naloge sem uporabil:

- deskriptivno metodo,
- metodo analize virov,
- pogovore s pripadniki EEB in lastne izkušnje na tem področju.

1.4 STRUKTURA ZAKLJUČNE NALOGE

Zaključna naloga bo po strukturi temeljila na postopnem približevanju k bistvenemu delu.

V uvodnem delu bo podan splošen pregled nad varnostno situacijo ter pomembnostjo posedovanja pravih, ključnih, verodostojnih ter ažurnih informacij oziroma obveščevalnih podatkov.

V poglavju Obveščevalna dejavnost bodo obravnavani elementi kot so: pojem, definicija, informacija, obveščevalni podatek, vrste, oblike, discipline – v okviru tega elementa bodo prikazane discipline, kot so HUMINT (Human Intelligence), OSINT (Open Source Intelligence), TECHINT (Technical Intelligence), MASINT (*Measurement and Signature Intelligence*) ter SIGINT (Signals Intelligence).

V poglavju EI in EB bo poseben poudarek na pasivnih ukrepih oziroma aktivnostih, ki se izvajajo s ciljem zagotavljanja obveščevalnih podatkov, in sicer: EB (podporni ukrepi elektronskega bojevanja - PUEB) ter EI (Communication Intelligence - COMINT). Prav tako bo, kot neformalen uvod v naslednje – ključno poglavje, podana razmejitev oziroma sinergija med EI in EB.

V poglavju Vloga PUEB in COMINT v obveščevalni dejavnosti, bo podan poudarek na elementih izvajanja, s ciljem uspešnega pridobivanja informacij ter posledično obveščevalnih podatkov o določeni grožnji oziroma nasprotniku.

V zaključnem delu bo podana verifikacija hipoteze, kratek povzetek osrednjega dela ter spoznanj in ugotovitev analitičnega dela zaključne naloge.

1.5 OMEJITVE

Pri izdelavi zaključne naloge sem se srečal z vrsto omejitev.

O področju PUEB in COMINT v okviru literature Slovenske vojske (SV) , z določenimi izjemami, ni veliko napisanega, zaradi česar sem moral uporabiti tujo (znanstveno in strokovno vojaško literaturo) ter, z odobritvijo mentorja, interno literaturo EEB.

Drugo, ključno omejitev pri izdelavi zaključne naloge, pa predstavlja specifičnost in s tem posledično občutljivost (varnostna in protiobveščevalna) področja EI in EB, zaradi česar zaključna naloga ne zajema vseh (vsebinsko še bistveno bolj zanimivih) elementov.

2 OBVEŠČEVALNA DEJAVNOST

Obveščevalna dejavnost je proces, ki zajema zbiranje in analitično obdelavo surovih podatkov in posledično rezultira v celovit obveščevalni izdelek, ki ga uporabnik potrebuje pri oblikovanju in sprejemanju odločitev na nacionalnem (državnem), političnem, gospodarskem in varnostnem področju (Intelligence-Policy & Process, 1985:1-2).

2.1 OBVEŠČEVALNI PODATEK

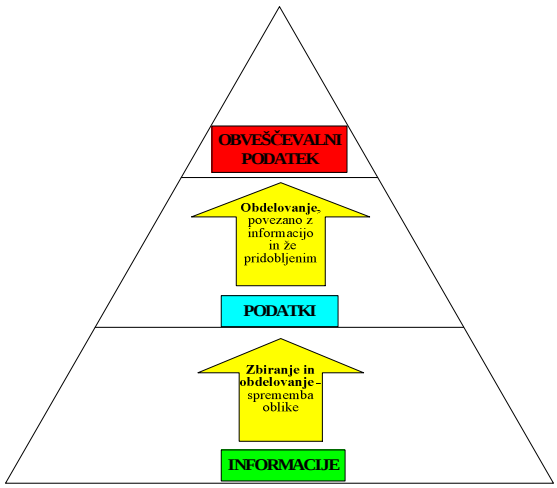
Obveščevalni podatek je predpogoj za uspešno delovanje in načrtovanje dela enot. Poveljujoči mora že na začetku oz. pred začetkom aktivnosti vedeti, katere informacije bo potreboval o nasprotniku in lastnih silah. Ob izvajanju aktivnosti doma in v tujini ter soočanju z grožnjami terorizma ta dejavnost predstavlja pomemben dejavnik. V situaciji, kjer je nasprotnik »pomešan« s civilnim prebivalstvom in so meje območij delovanja zabrisane, je pravočasnost in kontinuiteta pridobivanja obveščevalnih podatkov ključnega pomena.

Da bi lažje razumeli aktivnosti, ki ob zgoraj navedenem potekajo, bodo predstavljeni osnovni pojmi kot so *podatek, informacija, obveščevalni podatek* ter *obveščevalni cikel* kot osnovni proces pridobivanja in obdelave obveščevalnih podatkov.

Obveščevalna dejavnost ne obsega zbiranja podatkov in informacij kot golih dejstev - pridobljen podatek je le eden delov procesa obveščevalne dejavnosti, podatki, ki so obdelani v obveščevalnem krogu ali ciklu, pa postanejo *obveščevalna informacija*.

Podatki, pridobljeni s pomočjo senzorjev, postanejo informacija. Če tako pridobljene informacije povežemo z že predhodno znanimi informacijami, dobimo nov niz dejstev, ki jih imenujemo *obveščevalni podatki*.

Slika 1: Razlika med podatki, informacijami in obveščevalnimi podatki

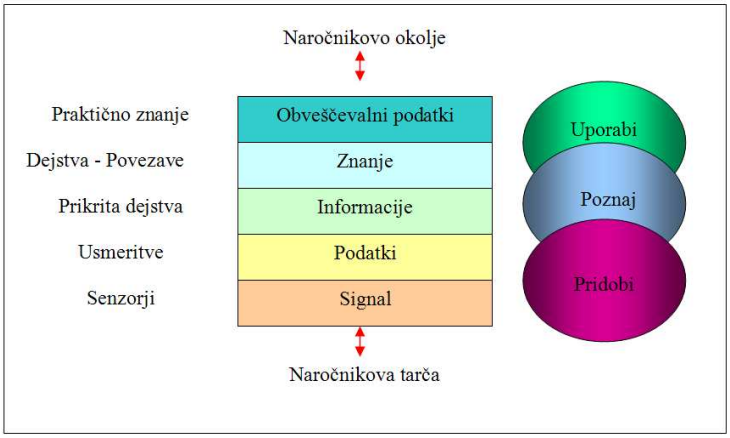


Vir: AJP-2 – SVS STANAG 2190; (Skupna obveščevalna, protiobveščevalna in varnostna doktrina; januar 2005; 2. poglavje/slika 1)

Informacije »predelane« v obveščevalne podatke zberejo viri, ki so oseba ali tehnično sredstvo, od katere je mogoče pridobiti informacije ter službe, ki so opredeljene kot organizacije ali posamezniki, ki se ukvarjajo z zbiranjem oz. obdelavo podatkov.

Obveščevalni podatki so predpogoj za uspešno delovanje enote na bojišču. So nujno potrebni za dobro načrtovanje. Poveljujoči mora že na začetku oz. pred začetkom aktivnosti vedeti katere informacije bo potreboval o nasprotniku in lastnih silah, le-te pa so združene v poveljnikovi zahtevi po ključnih informacijah, na podlagi katerih obveščevalno osebje izdela prednostne obveščevalne zahteve.

Slika 2: Postopek pridobivanja obveščevalnih podatkov od vira do naročnika

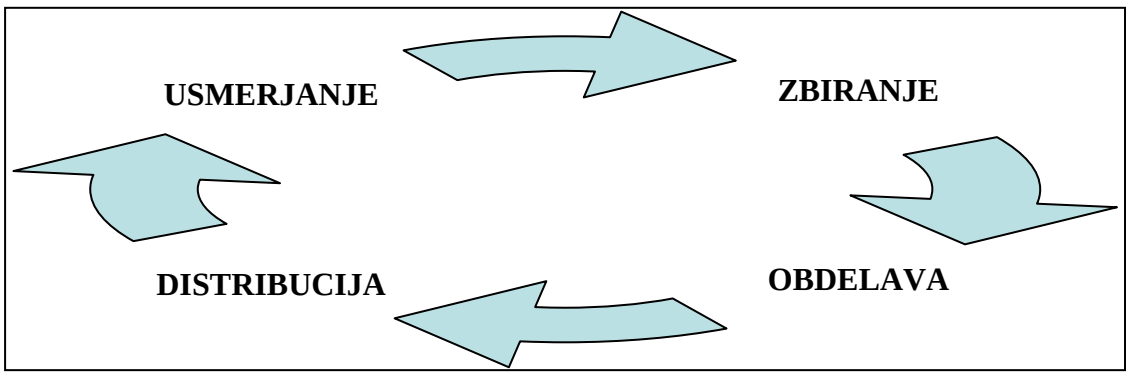


Vir: http://www.sigint.co.uk/learnmore.html

2.2 OBVEŠČEVALNI KROG

Obdelovanje dostopnih informacij zahteva strukturirano in sistematično izvajanje določenih postopkov. *Obveščevalni krog* oz. *cikel* je okvir, v katerem potekajo štirje ločeni postopki.

Slika 3: Koraki v obveščevalnem krogu

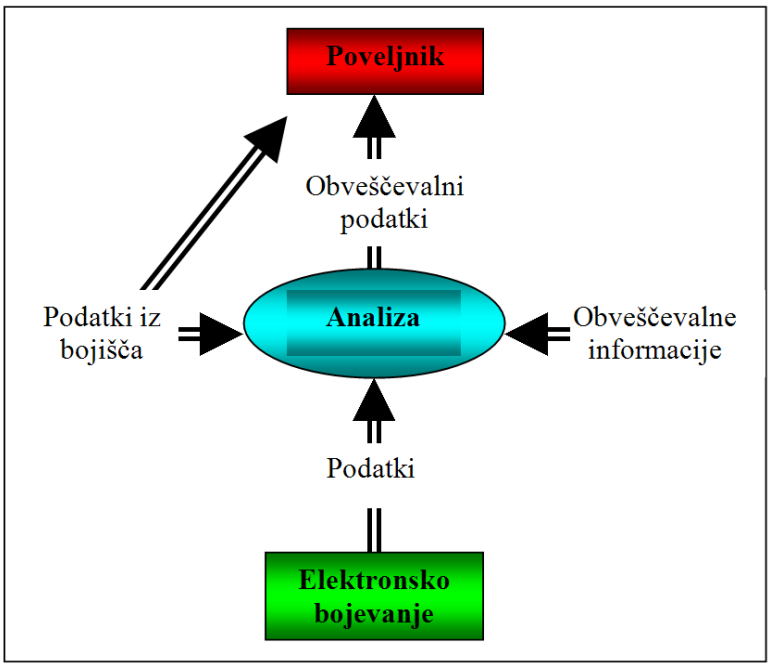


Vir: AJP-2 – SVS STANAG 2190; (Skupna obveščevalna, protiobveščevalna in varnostna doktrina; januar 2005; 3. poglavje/slika 2)

Zbiranje obveščevalnih podatkov je postopek, v katerem se informacije in obveščevalni podatki zbirajo zaradi zagotavljanja odgovorov na poveljnikove informacijske zahteve, ki so opredeljene v obveščevalnem ciklu na stopnji usmerjanja.

Poveljnik pridobiva informacije direktno z bojišča in skozi analizo pridobljenih obveščevalnih podatkov - ti so skupek podatkov iz bojišča ter obveščevalnih podatkov pridobljenih pred začetkom aktivnosti in morebitnih drugih virov na podlagi predhodno izdanih zahtev po ključnih podatkih.

Slika 4: Pridobivanje podatkov in obveščevalnih podatkov iz različnih virov



Vir: US ARMY SIGNAL CENTER AND FORT GORDON OFFENSIVE LECTRONIC WARFARE (SC 25C-RC); September 1994; 2. poglavje/slika 2-5

2.3 OBVEŠČEVALNE DISCIPLINE

Obstaja vrsta disciplin (področij), ki se ukvarjajo z zbiranjem obveščevalnih podatkov in informacij, pri čemer se za zbiranje uporabljajo tako tehnična sredstva kot (v nekaterih primerih) tudi človek, in sicer:

- *HUMINT (Human Intelligence)* – zbiranje informacij s pomočjo človeških virov, s prikritimi in neprikritimi postopki, pridobivanje tajnih ali javnih podatkov,

- *SIGINT (Signals Intelligence)* – zbiranje informacij z uporabo tehničnih sredstev za EI, cilj komunikacijska in ne-komunikacijska sredstva (signali),

- *RADINT (Radar Intelligence)* – specializirana tehnična disciplina, ki z uporabo tehničnih sredstev analizira delovanje radarskih sredstev,
- *IMINT (Imagery Intelligence)* – zbiranje informacij v obliki slikovnega gradiva,

- *MASINT (Measurement and Signature Intelligence)* – zbiranje informacij o znanstveno tehničnih karakteristikah sredstev,

- *OSINT (Open Source Intelligence)* – zbiranje informacij iz javno dostopnih virov.

Da zaobjamemo vse načine zbiranja podatkov, ki jih uporabljajo moderne obveščevalno službe in ne le posamezne specializirane službe, lahko te imenujemo *discipline zbiranja podatkov v obveščevalni dejavnosti* in ne samo obveščevalne discipline - discipline zato, ker vsaka izmed njih zahteva določena taktična pravila, posebna znanja in tehnična sredstva.

Delimo jih na tri skupine zbiranja obveščevalnih podatkov:

- *operativne*: zahtevajo praktično, fizično delo na terenu, govorimo o operativnem delovanju.
- *tehnične:* uporabljajo tehnična sredstva za pridobivanje in zbiranje podatkov (sredstva za strateški nadzor telekomunikacij oziroma za prisluškovanje, uporabo različnih posebnih načinov fotografiranja iz zraka ali vesolja, itd.)
- zbiranja *javno dostopnih* podatkov: iz elektronskih in pisnih medijev, z uporabo strokovne literature itd.

Iz zgoraj navedenega je razvidno, da je delitev na discipline zbiranja podatkov veliko bolj širša in podrobna, kot pa je delitev na obveščevalne discipline ali na posebne operativne metode in sredstva dela.

2.4 OBVEŠČEVALNA DEJAVNOST NA PODROČJU VOJAŠKE OBRAMBE

Obveščevalna služba posreduje obveščevalne podatke določevalcem iz obrambnega področja in predstavlja pomemben del obveščevalno varnostnega sistema za zagotavljanje nacionalne varnosti. Ker so obveščevalne službe, ki opravljajo te naloge, del nacionalno-varnostnega sistema in zbirajo podatke z najbolj občutljivimi operativnimi disciplinami, ki posegajo v temeljne človekove pravice, so v večini obrambnih sistemov podrejene ministru za obrambo, svetu za nacionalno varnost, vladi ali pa so organizirane kot del nacionalnih civilnih obveščevalnih služb.

Vojaška obveščevalna dejavnost je dejavnost, katere izključni uporabnik so *oborožene sile* oziroma *vojska*.

Slika 5: Delitev na obrambno strateško in obveščevalno dejavnost

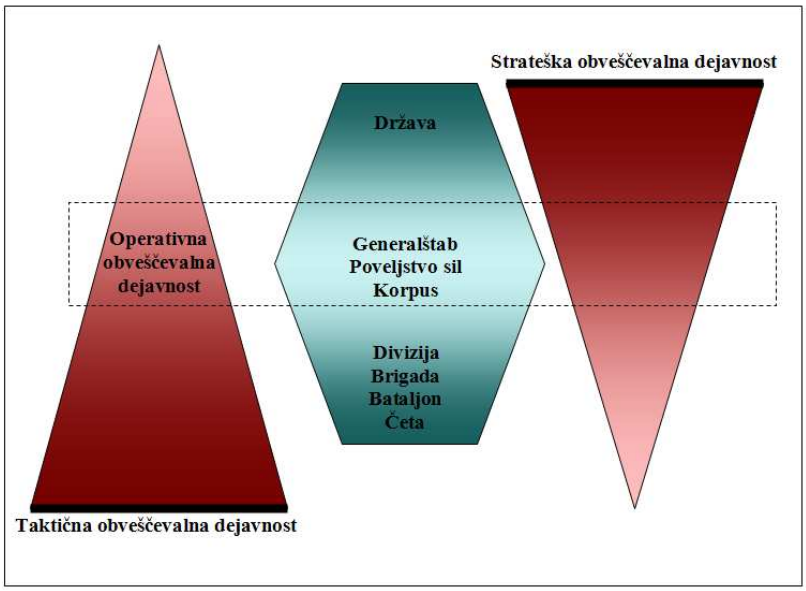
OBVEŠČEVALNA DEJAVNOST NA PODROČJU VOJAŠKE OBRAMBE	
OBRAMBNOSTRATEŠKA	***VOJAŠKA***
- odločanje o obrambni politiki na nacionalni ravni, - analiza in posredna uporaba pri odločanju (specifične obveščevalne discipline).	- odločanje pri izvajanju bojnih operacij v štabih, - neposredna uporaba podatkov za sprejem odločitev, - zbiranje s specializiranimi vojaškimi enotami ter tehničnimi disciplinami zbiranja podatkov. Prejme jih od drugih obveščevalnih služb (obrambno strateške in drugih).

Vir: Šaponja; Taktika dela obveščevalno varnostnih služb Visoka policijsko – varnostna šola; Ljubljana 1999; 3. poglavje/12. slika

Naloge posameznih vrst obveščevalne dejavnosti na obrambnem področju določajo tudi njihovo organiziranost znotraj obrambnega sistema. Obveščevalna dejavnost je lahko organizirana centralizirano (združuje obrambno strateško in taktično) ali pa v obliki obveščevalne skupnosti, sestavljene iz specialističnih vojaških obveščevalnih služb in obrambno strateške, ki so lahko del civilnega dela obrambnega sistema.

2.5 RAVNI OBVEŠČEVALNE DEJAVNOSTI

Slika 6: Ravni obveščevalnih dejavnosti



Vir: FM 34-1 Intelligence and electronic warfare operations; September 1994; 2. poglavje/slika 2-1

Ravni obveščevalnih dejavnosti so enake kot pri bojevanju in sicer *strateška*, *operativna* in *taktična*. Tako kot pri bojevanju različne stopnje obveščevalnih dejavnosti služijo za logično podajanje aktivnosti in informacij po liniji poveljevanja in odgovornosti. Stopnje obveščevalnih aktivnosti niso strogo omenjene vendar se prilagajajo posamezni operaciji.

Kot izhaja iz zgornje slike, je stopnja obveščevalne dejavnosti odvisna od političnih in vojaških ciljev in od potreb poveljnika. Poveljnik na bojišču dobi različno podporo iz vseh treh stopenj obveščevalne dejavnosti:

- *strateška*: pridobi podatke o politični klimi nasprotnika,
- *operativna*: poskrbi za ključne cilje aktivnosti,
- *taktična*: kje je nasprotnik najbolj ranljiv oz. kje ga je najbolje napasti.

Razvoj tehnologije je še dodatno zabrisal meje med posameznimi ravnmi delovanja.

Uporabnost oz. učinkovitost pridobljenih obveščevalnih podatkov se meri po naslednjih kriterijih:

- *ažurnost*: pridobljeni in posredovani pravočasno (pridobivanje in analiza mora potekati nepretrgoma pred, med in po aktivnosti ne glede na razdaljo in čas),
- *relevantnost*: v kontekstu poveljnikovih zahtev in nalog enote (podane morajo biti v obliki v kateri odgovarjajo posameznim potrebam),
- *točnost:* jasna in realna slika situacije (pridobljene morajo biti iz različnih virov z namenom podati čim bolj točno sliko),
- *predvidevanje* kaj nasprotnik dela, lahko naredi in kaj je zmožen narediti (Course Of Action - COU).

3 ELEKTRONSKO BOJEVANJE IN ELEKTRONSKO IZVIDOVANJE

Govoriti o (predvsem vojaški) obveščevalni dejavnosti, in pri tem zaobiti nosilce izvajanja aktivnosti EI in EB, je praktično nemogoče. Umestitev, vloga in organiziranost EEB se od države do države razlikuje.

Zaradi narave dela teh enot in občutljivosti področja je njih organizacijska struktura, tehnična opremljenost ter usposobljenost kadra tajna.

Enote delujejo v različnih rodovih, na različnih nivojih, tako iz stacionarnih, kakor tudi mobilnih platform (zemlja, zrak, morje).

V okviru sistema nacionalne varnosti Republike Slovenije (RS) deluje EEB (v sestavi 5. obveščevalno izvidniškega bataljona – 5. OIB), njeno ključno nalogo pa opredeljuje Zakon o obrambi, in sicer: »*Spremljanje mednarodnih sistemov zvez pomembnih za obrambne interese RS za potrebe OVS MORS in druge potrebe izvajajo enote za elektronsko bojevanje«*.

EEB, kot podporni element delovanja SV in del nacionalno varnostnega sistema, v skladu z normativnimi dokumenti izvaja dve vrsti aktivnosti:

- EI,
- EB

Prav tako Vojaška doktrina Slovenske vojske navaja, da Slovenska vojska (SV) izvaja tri skupine ukrepov EB:

- podporne ukrepe elektronskega bojevanja,
- elektronske protiukrepe,
- elektronske zaščitne ukrepe.

3.1 ELEKTRONSKO BOJEVANJE

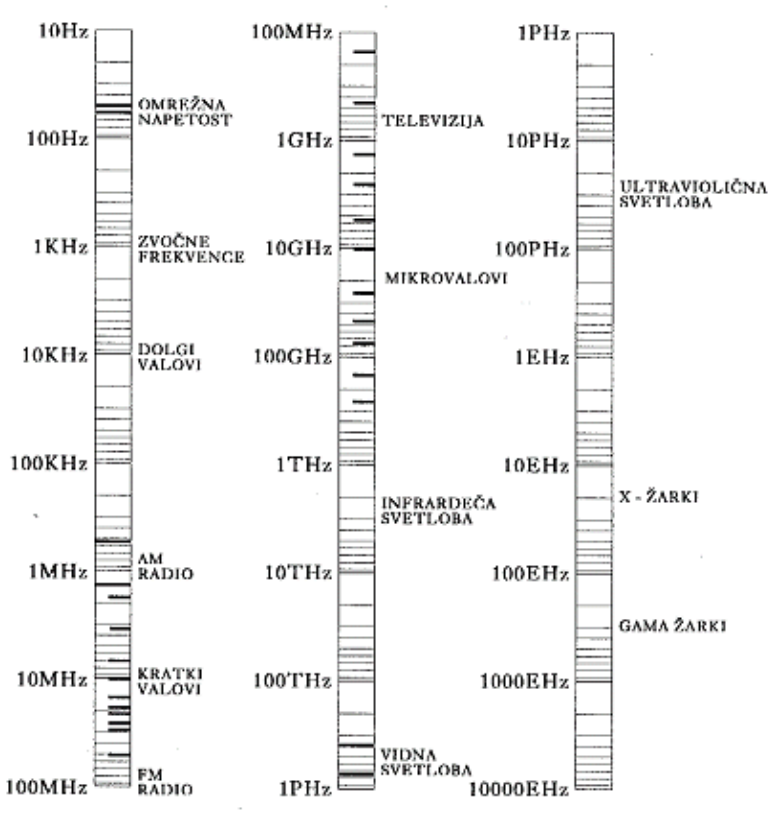
»Elektronsko bojevanje je vojaška aktivnost, s katero raziskujemo elektromagnetni spekter (EMS) in obsega iskanje, prestrezanje, identifikacijo oddajanja EMS, uporabo elektromagnetne energije(EME) (vključno z direktno energijo), s ciljem zmanjšati in preprečiti uporabo elektromagnetnega spektra s strani sovražnika in aktivnosti, ki zagotavljajo učinkovito uporabo EMS s strani lastnih sil.« (NATO Glossary of Terms And Definitions – AAP 06; 2006).

Osnovni namen EB je preprečiti nasprotniku prednost v EMS in omogočiti lastnim enotam nemoten dostop do EMS. Izvaja se lahko iz *zraka, morja, kopna*, z načrtnim in nenačrtnim prestrezanjem. EB se uporablja kot podpora vojaškim operacijam na vseh nivojih.

Da bi razumeli delovanje tehničnih sredstev za EI/EB, je potrebno poznavanje osnovnih pojmov, ki urejajo področje frekvenc in frekvenčnega spektra.

Za označevanje posameznih delov frekvenčnega spektra se uporabljajo naslednje delitve in poimenovanja frekvenc, pri čemer je potrebno upoštevati, da imajo posamezne skupine frekvenc imajo različne lastnosti pri širjenju EMV.

Slika 7: Razdelitev elektromagnetnega spektra



Vir: Priročnik za radioamaterje; Zveza radioamaterjev Slovenije; Ljubljana 1995; 6. poglavje/slika 6.4.1.

Enota za frekvenco je en *hertz* (1 Hz), za njene mnogokratnike pa se uporabljajo še naslednje sestavljene enote:

- Hz = 1kHz (en kilohertz),
- Hz = 1MHz (en megahertz),
- Hz = 1GHz (en gigahertz).

Frekvenčna področja so razdeljena na:

- zelo nizke frekvence -VLF (very low frequencies) obsegajo frekvence od 3kHz do 30kHz,
- nizke frekvence - LF (low frequencies) obsegajo frekvence od 30kHz do 300kHz,
- srednje frekvence - MF (medium frequencies) obsegajo frekvence od 300kHz do 3MHz,
- visoke frekvence - HF (high frequencies) obsegajo frekvence od 3MHz do 30MHz,
- zelo visoke frekvence - VHF (very high frequencies) obsegajo frekvence od 30MHz so 300MHz,

- ultra visoke frekvence - UHF (ultra high frequencies) obsegajo frekvence od 300MHz do 3GHz,
- super visoke frekvence - SHF (super high frequencies) obsegajo frekvence od 3GHz do 30GHz,
- ekstremno visoke frekvence - EHF (extremely high frequencies) obsegajo frekvence od 30GHz do 300GHz.

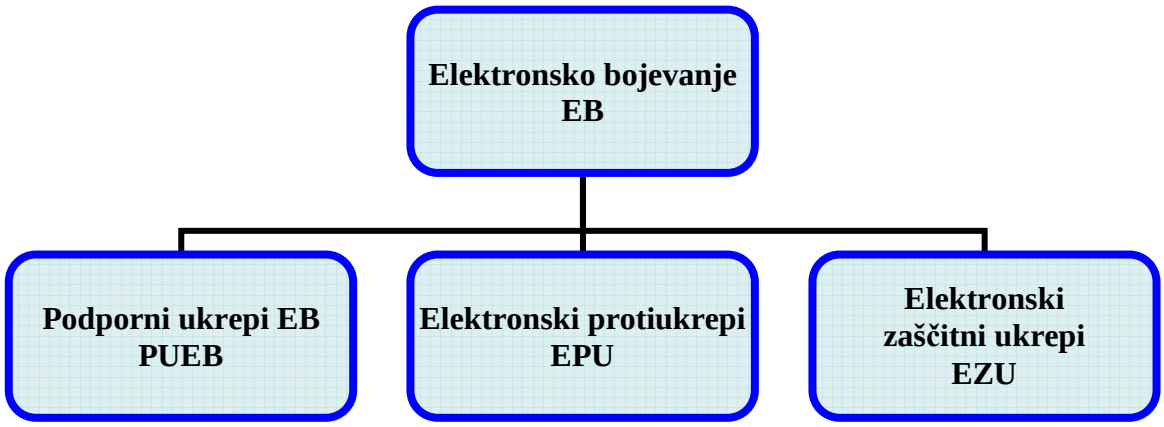
Radijski spekter si delijo mnogi uporabniki in je javno dobro nad katerim bedi država ter nekatere mednarodne institucije kot je International Telecommunication Union (ITU). Pravice do uporabe posameznega spektra so določene z zakonom, katerega nadzor izvajajo temu namenjene inštitucije. Pregled načrta razporeditve frekvenčnih pasov z uporabniki podajam v prilogi iz uredba o načrtu razporeditve radiofrekvenčnih pasov.

3.1.1 Delitev EB

Elektronsko bojevanje zajema tri vrste ukrepov:

- *Podporni ukrepi elektronskega bojevanja* (PUEB) - (angl. Electronic Support Measures - ESM),
- *Elektronski protiukrepi* (EPU) - (angl. Electronic Counter Measures - ECM),
- *Elektronski zaščitni ukrepi* (EZU) - (angl. Electronic Protective Measures - EPM).

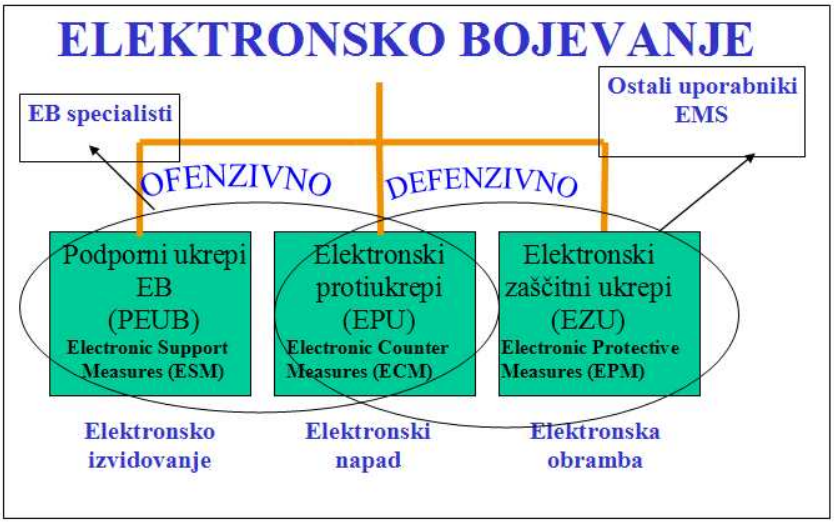
Slika 8: Vrsta ukrepov EB



Vir: Golob Damjan PDRIU; Skripta Elektronsko bojevanje 2006; 1. poglavje/slika 1

Zaradi narave dela in potrebnih strokovnih znanj in izkušenj, PUEB in EPU izvajajo predvsem specialisti EB , medtem ko EZU poleg specialistov EB izvajajo oz. morajo izvajati vsi uporabniki komunikacijsko informacijskih sistemov (KIS).

Slika 9: Ofenzivni in defenzivni ukrepi EB



Vir: Interno gradivo EEB

V nadaljevanju sledi kratek vsebinski prikaz EPU in EZU, medtem ko bo nekoliko večji poudarek podan na PUEB.

3.1.1.1 Elektronski protiukrepi

Po naravi izvajanja so izrazito *aktivni*, saj s sredstvi izključno oddajamo EMS. Ukrepi se izvajajo s ciljem napada na sovražnikove zmožnosti, vključno s sistemi poveljevanja in kontrole ter sistemi ISTAR (angl. Intelligence, Survillence, Targeting, Aqusition, Recconnaissance). Cilj, ki ga želimo doseči, je začasno ali permanentno, motenje, zavajanje ali nevtralizacija sovražnikovih elektronskih sredstev in sistemov.

Ločimo tri vrste aktivnosti:

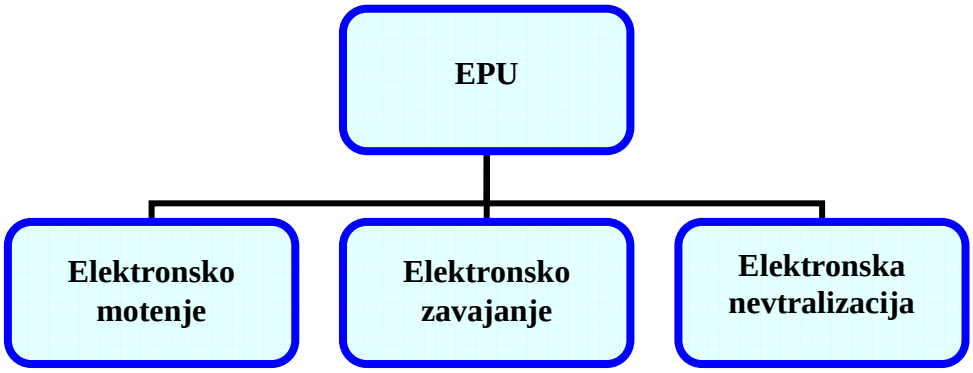
- *Elektronsko motenje* - namerno oddajanje (sevanje) ali odbijanje EMS s ciljem zmanjšanja učinkovitosti delovanja sovražnikovih elektronskih sredstev in sistemov.

- *Elektronsko zavajanje* - namerno oddajanje (sevanje), absorbiranje, odbijanje EMS s ciljem zmesti, preusmeriti, zavesti sovražnika ali njegova elektronska sredstva in sisteme.

  Ločimo tri vrste elektronskega zavajanja: *manipulativno, stimulativno* in *imitativno*.

- *Elektronska nevtralizacija* - namerna uporaba EME s ciljem začasne ali permanentne okvare ali uničenja sovražnikovih elektronskih sredstev in sistemov.

Slika 10: Podzvrsti EPU



Vir: Golob Damjan PDRIU; Skripta Elektronsko bojevanje 2006; 3. poglavje

Področje EPU in njih vloga je podrobneje obdelana v zaključni nalogi *Elektronsko bojevanje s poudarkom na elektronskih protiukrepih (elektronsko motenje, elektronsko zavajanje); Matej Žaže, Damjan Golob (mentor), Mitja Pintarič (komentor), 2008.*

3.1.1.2 Elektronski zaščitni ukrepi

Po naravi izvajanja so aktivni in pasivni. Zajemajo aktivnosti, ki zagotavljajo učinkovito uporabo EMS s strani lastnih sil navkljub sovražnikovi uporabi EMS.

Ločimo dve vrsti ukrepov:

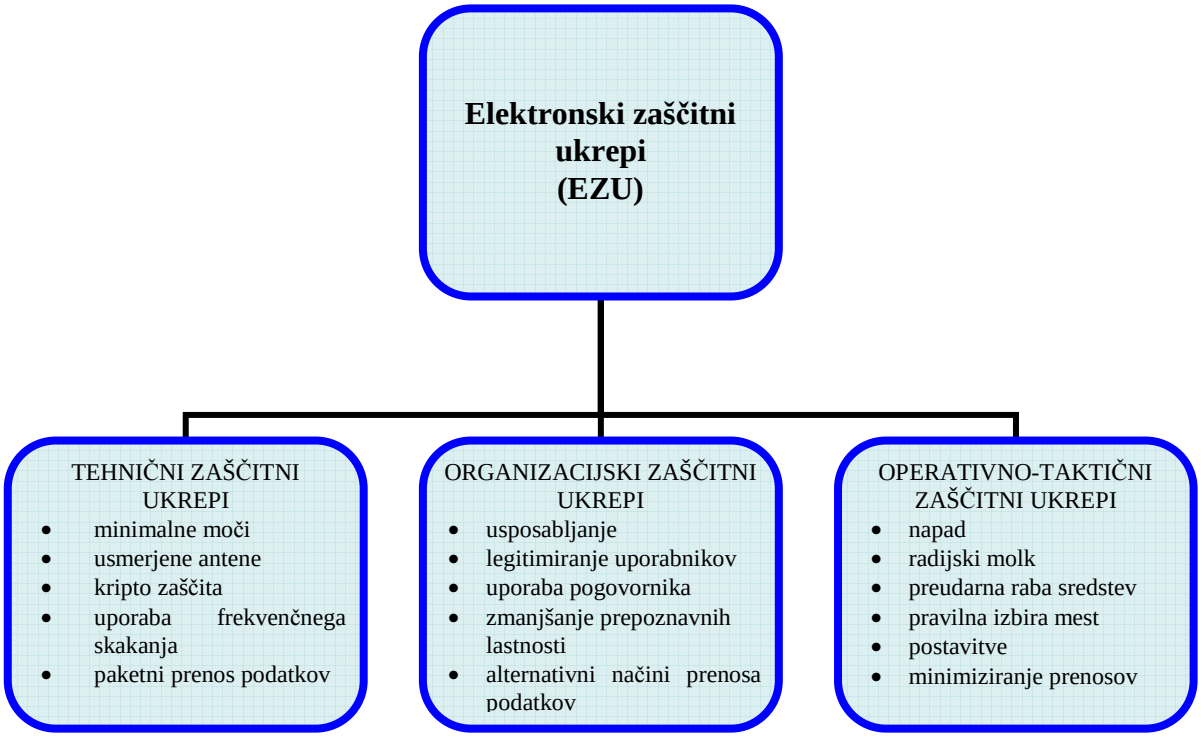
- *aktivni* - ukrepi, ki so lahko zaznani, kot npr. spreminjanje parametrov oddajnika za zagotovitev učinkovite uporabe EMS s strani lastnih sil.
- *pasivni* - ukrepi, ki niso zaznani (merljivi), kot na primer operativni postopki, tehnični parametri za zagotovitev učinkovite uporabe EMS s strani lastnih sil.

Nadalje delimo EZU na:

- tehnične,
- organizacijske,
- operativno – taktične.

EZU so pomemben del usposobljenosti pripadnikov enot na področju upravljanja z radarskimi sistemi in KIS.

Slika 11: Delitev elektronskih zaščitnih ukrepov glede na način izvajanja



Vir: Golob Damjan PDRIU; Skripta Elektronsko bojevanje 2006; 4. poglavje/slika 8

Področje EZU in njih vloga je podrobneje obdelana v zaključni nalogi *Vloga in ukrepi za zaščito komunikacij z vidika elektronskega bojevanja; Aleksander Jović, Aleksander Hren (mentor), 2008.*

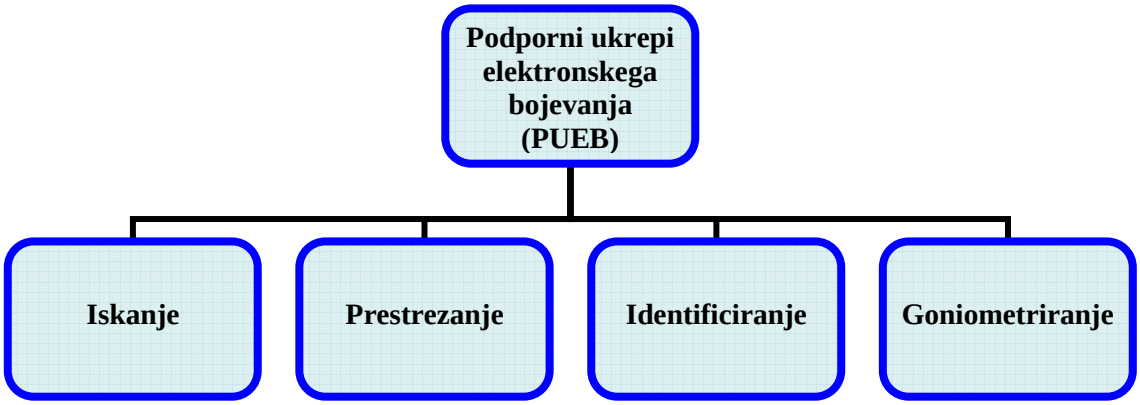
3.1.1.3 Podporni ukrepi elektronskega bojevanja - (PUEB)

Po naravi izvajanja so izrazito pasivni - s tehničnimi sredstvi le sprejemamo EME, ki jo oddajajo komunikacijski sistemi, zato je enote, ki izvajajo tovrstne ukrepe, zelo težko odkriti.

Med PUEB uvrščamo:

- iskanje,
- prestrezanje,
- identificiranje,
- določanje lokacij izvorov EM sevanja – goniometriranje.

Slika 12: Podporni ukrepi elektronskega bojevanja - (PUEB)



Vir: Golob Damjan PDRIU; Skripta Elektronsko bojevanje 2006; 2. poglavje

3.1.1.3.1 Iskanje

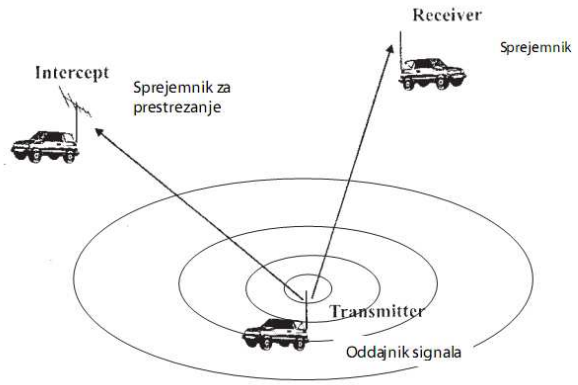
Iskanje je postopek, v okviru katerega preiskujemo frekvenčni spekter – iščemo frekvence (aktivne signale) ključnega pomena za kasnejše pridobivanje obveščevalnih podatkov ali pa samo s ciljem kontinuiranega pregleda nad zasedenostjo frekvenčnega spektra. Aktivni signal lahko predstavlja govorni signal ali prenos podatkov.

3.1.1.3.2 Prestrezanje

Prestrezanje predstavlja drugi (naslednji) korak in se zelo navezuje na postopek iskanja – predstavlja del njegovega rezultata. Samo prestrezanje aktivnega signala samo po sebi še ne predstavlja vsebinske opredelitve, temveč osnovo za opredelitev osnovnih podatkov, npr. v primeru govorne komunikacije: delovna frekvenca, pasovna širina signala, modulacija, …

Postopek prestrezanja se posledično odraža v podatkovnih bazah, kjer so zapisani vsi pomembni tehnični parametri posameznega signala, in služijo kot preglednica zasedenosti frekvenčnega spektra.

Slika 13: Osnovne elektronskega prestrezanja



Vir: Golob Damjan PDRIU; Skripta Elektronsko bojevanje 2006; 2. poglavje/slika 2

3.1.1.3.3 Identificiranje

Tehnični podatki o posameznem signalu vsekakor predstavljajo le tehnično ne pa tudi vsebinsko komponento postopka prestrezanja. Vsak prestrežen signal je potrebno tudi identificirati oziroma opredeliti podatke, kot npr. uporabnik (rod, čin, ime, priimek, naziv enote), pozivni znaki, način komuniciranja, ….

3.1.1.3.4 Goniometriranje

Prestrežen in identificiran signal ni popolnoma opredeljen, dokler ni določena tudi kar se da natančna lokacija oddajnika (komunikacijskega sredstva). Postopek določanja lokacije imenujemo tudi goniometriranje.

Goniometriranje je ključnega pomena, saj lahko zelo hitro in natančno določimo mikrolokacijo grožnje, kar je ključnega pomena predvsem v operacijah kriznega odzivanja (OKO).

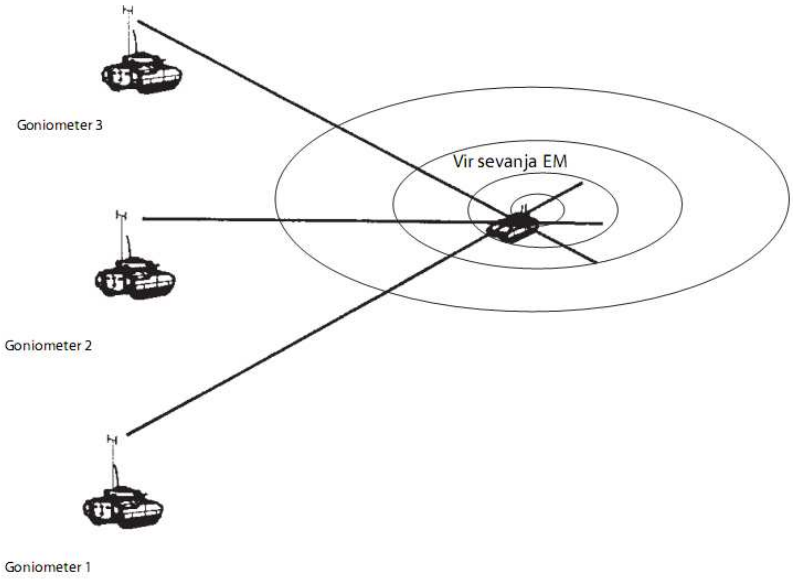
Princip dela goniometrov temelji na principu usmerjenega sprejema EM energije. Goniometriranje je določanje azimuta oziroma lokacije vira EM sevanja med delovanjem oziroma oddajanjem signala. Z določitvijo lokacije oddajnikov na zemljišču lahko sklepamo o:

- razporeditvi in razmestitvi poveljniških mest ter centrov zvez,
- združevanju v skupine in o razporeditvi nasprotnikovih sil,
- smereh uporabe, premikih nasprotnikovih sil ipd.

Natančnost določanja lokacije je odvisna od več dejavnikov in sicer:

- mesta postavitve goniometrov,
- števila goniometrov,
- pogojev razprostiranja EM valovanja,
- geološke sestave zemljišča,
- konfiguracije zemljišča,
- izurjenosti uporabnikov,
- ...

Slika 14: Goniometriranje



Vir: Golob Damjan PDRIU; Skripta Elektronsko bojevanje 2006; 2. poglavje/slika 3

Določanje lokacije z metodo *triangulacije* predstavlja najosnovnejši način določanja lokacije izvora EM sevanja. Na podlagi metode triangulacije določimo lokacijo tako, da s tremi ali več goniometri določimo smer, iz katere prihaja EMV. Goniometri poznajo svojo lokacijo in smer iz katere prihaja EMV, zato lahko določimo območje, kjer se smeri križajo. Na tem območju se najverjetneje nahaja oddajnik – sredina območja se določi z
z matematičnim algoritmom. To je točka, kjer je največja verjetnost izvora EM sevanja.

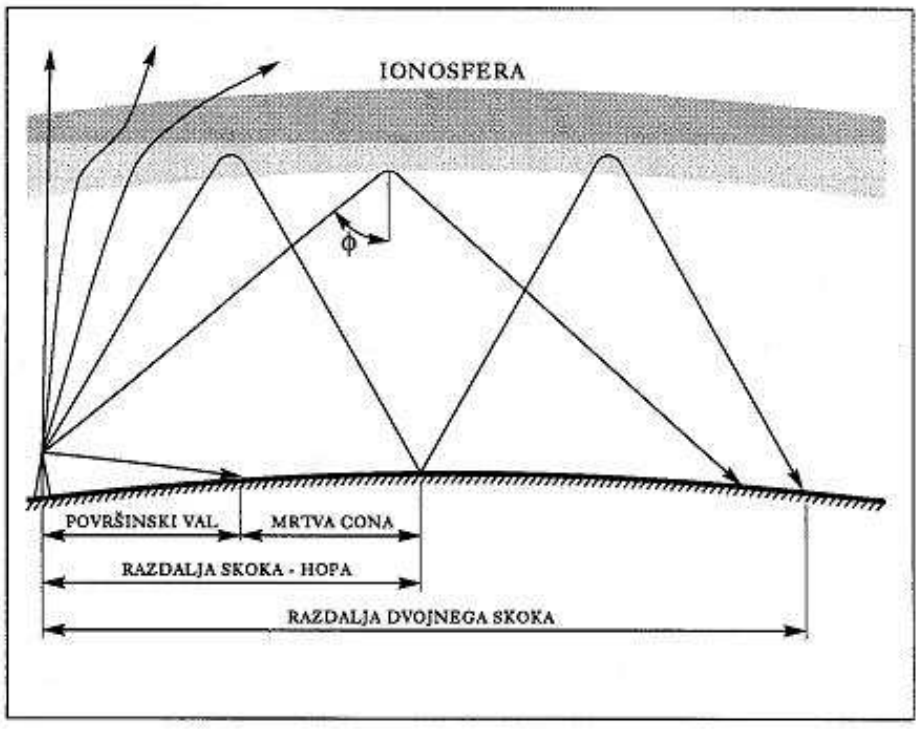
Natančnost določanja lokacije je odvisna od veliko dejavnikov, med drugim (poleg navedenih) tudi od frekvence signala oddajnika. Na nižjih frekvencah je točno lokacijo težje določiti, ker na razširjenost valov na tem območju vpliva precej dejavnikov okolja, in sicer stanje ionosfere, ozračje, ovire na poti, poraščenost terena itn. Višje kot so frekvence, natančneje lahko določimo izvor.

Pri meritvah višjih frekvenc mora biti zagotovljena optična vidljivost do oddajnika. Zanimiva je tudi možnost postavitve takšnega sistema na letalske platforme ali še bolje na brezpilotna letala (BPL). Razlika med obema možnostma je predvsem v natančnosti določanja lokacije.
Pri nižjih frekvencah, na HF-področju, se uporablja metoda SSL (single site location), ki temelji na merjenju kota, pod katerim se EM valovi odbijejo od ionosfere. Sistem, ki uporablja to metodo, potrebuje za določitev lokacije le en goniometer, ponavadi stacionarnega tipa. Signali se na tem frekvenčnem področju odbijajo od ionosfere, zato lahko razdaljo do izvora določimo na podlagi merjenja kota, pod katerim signal prihaja, in iz znane višine ionosfere.

Naj v zaključku poudarim, da je učinkovitost izvajanja PUEB odvisna od vrste elementov, predvsem pa od:

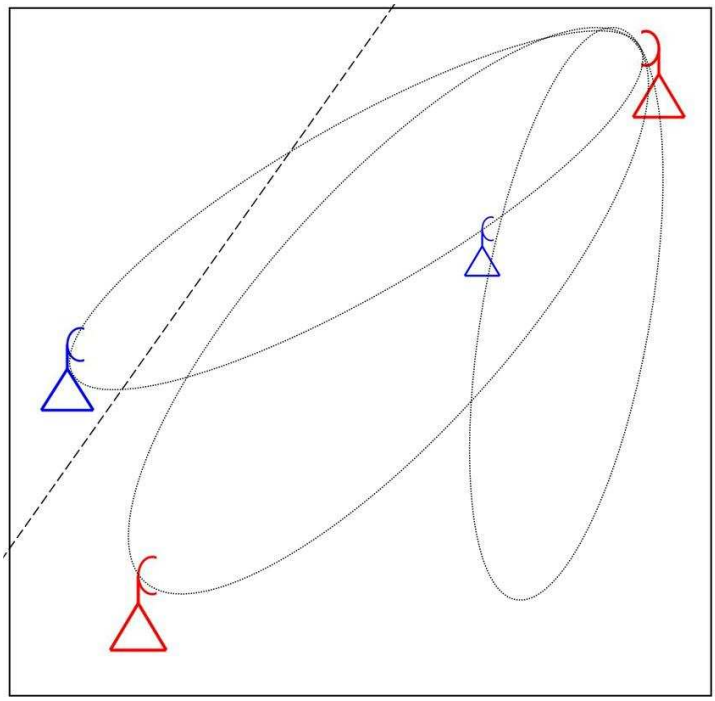
- razpoložljivih tehničnih sredstev EB in njih prilagodljivosti za izvajanje nalog v terenskih pogojih,
- razpoložljivost varnih KIS za pravočasno poročanje (posredovanje podatkov),
- ustrezna logistična podpora (samozadostnost),
- frekvenčnega področja delovanja ciljnih KIS ter njih lokacij (oddaljenosti):
  - na nižjih frekvenčnih področjih (HF) se uporabljajo visoke izhodne moči in neusmerjene antene, razdalja med KIS je velika, sevanje EMV je krožno - 360°.
  - na višjih frekvencah (V/U/SHF) se uporabljajo vedno manjše izhodne moči, usmerjene antene, razdalja med KIS je vedno manjša, sevanje pa je usmerjeno, zato je zelo pomembna optična vidljivost ter čim večja bližina do oddajnika.
- usposobljenosti kadra,
- razpoložljivosti platform za izvajanje EB,
- razpoložljivosti časa za izvedbo naloge,
- razpoložljivosti vhodnih podatkov (poznavanje situacije).
-

Slika 15: Širjenje EM valov na HF področju



Vir: Priročnik za radioamaterje; Zveza radioamaterjev Slovenije; Ljubljana 1995; 6. poglavje/slika 6.5.5

Slika 16: Širjenje EM valov pri usmerjenih (večkanalnih – RR zvezah)



Vir: Interno gradivo EEB

Podatki, pridobljeni z izvajanjem PUEB, predstavljajo osnovo za izvajanje tako EPU kakor tudi EZU.

3.2 ELEKTRONSKO IZVIDOVANJE

EI je ena izmed štirih ključnih disciplin obveščevalne dejavnosti (poleg HUMINT, OSINT, IMINT in MASINT).

EI se lahko izvaja iz različnih platform (zrak, zemlja, morje).

3.2.1 Delitev EI

EI se z vsebinskega (ciljnega) elementa deli na dve podpodročji, in sicer:

- Communications Intelligence – COMINT (spremljanje komunikacijskih signalov)
- Electronic Intelligence – ELINT (spremljanje ne-komunikacijskih signalov)

3.2.1.2 COMINT

Aktivnost COMINT je po naravi izvajanja zelo sorodna PUEB (o čemer več v enem naslednjih poglavij).

Gre za pasivno aktivnost, usmerjeno v spremljanje komunikacijskih sredstev, kot so:

- radijske naprave,
- večkanalni (predvsem digitalne) komunikacijski sistemi,
- IP telefonski sistemi,
- SATKOM,
- GSM,
- SATGSM.

kjer se srečujemo tako s signali z, kakor tudi (sicer redko) brez zaščite.

V okviru širšega sistema zaščite lastnih KIS v miru in vojni imajo svojo vlogo tudi tovrstne aktivnosti predvsem s ciljem preprečitve uporabe KIS za prenos podatkov nacionalnega pomena.

3.2.1.3 ELINT

Aktivnost ELINT je prav tako pasivnega značaja, usmerjena v ne-komunikacijske sisteme, kot so:

- radarski sistemi
- radionavigacijska sredstva
- GPS

Za razliko od COMINT je ELINT usmerjen predvsem v tehnično analizo signalov. Naloga tovrstnih segmentov je nazorno, celovito in detajlno analiziranje vseh signalov, katerih vsebina ni neposredno dostopna. Gre za zelo kompleksne signale, katerih obdelava je dolgotrajna a neizbežna.

Podatkovne baze, s katerimi operirajo enote ELINT, so namenjene predvsem detajlni specifikaciji vsake prestrežene komunikacije (delovanja), pa naj si bo to npr. radarskih sistemov – opredelitev vseh tehničnih parametrov (frekvenca, pasovna širina, način delovanja, pulz, polarizacija, jakost signala, hitrost obračanja antene, …) skratka podatke, na osnovi katerih je mogoče tekoče spremljanja uporabe in eventualne lokacijske premestitve radarskega sistema.

3.3 SINERGIJA / RAZMEJITEV MED EI IN EB

Vsebinski presek aktivnosti EI in EB zajema vrsto vzporednic kakor tudi deviacij in nekaj le-teh bo prikazanih v nadaljevanju.

- ključna sinergija se izkazuje v tem, da tako EI kot EB uporabljata enake postopke iskanja, prestrezanja, goniometriranja ter analize;

- osnovna razmejitev (vsebinska) med EI in EB se izkazuje v aktivno/pasivnem izvajanju EB ter pasivnem izvajanju EI – glavno ločnico predstavljajo EPU, ki pa se tesno navezujejo tako na PUEB kakor tudi na COMINT, ki predstavljata osnovo za izvajanje EPU – vsekakor ne neposredno temveč skozi analizo in načrtovanje le-teh;

- v časovni komponenti izvajanja sta si zelo deviantni – predvsem v miru, saj se EI izvaja kontinuirano, po principu 24/7, medtem ko EB po potrebi (usposabljanja). Vsekakor je deviacija bistveno manjša v primeru, npr. OKO, saj je prisotnost aktivnosti EB bistveno večja predvsem zaradi zaščite lastnih sil. Torej, EI se izvaja v vojni in v miru, medtem ko EB izključno v prehodu na in med operacijo;

- s postopki EI pridobivamo obveščevalne podatke o nasprotniku, medtem ko (v miru) z EB, predvsem v okviru usposabljanj s področja uporabe KIS, zagotavljamo usposobljenost lastnih sil in se z nasprotnikom neposredno ne ukvarjamo;

- obe aktivnosti lahko izvajamo z različnih platform, kjer pa je izvajanje COMINT primarno orientirano na zračne, medtem ko izvajanje PUEB in EPU na zemeljske platforme;

- nivojsko je EI vezana na strateški, EB pa na operativno taktični nivo;

- področje delovanja EI je funkcijo vezano na organe G2/J2, medtem ko EB na organe G3/J3;

- frekvenčno področje delovanja (nadzora) je v določenem obsegu enako, na področju S/EHF pa je pokrito izključno le z EI;

- EI se na zemlji izvaja predvsem iz stacionarnih platform, EB pa izključno iz mobilnih platform.

V nadaljevanju bo podan poudarek na vlogi pasivnih ukrepov (aktivnostih) EI in EB, to je COMINT (ELINT zaradi ne-povezljivosti z PUEB ne bom obravnaval) in PUEB, v obveščevalni dejavnosti.

4 VLOGA COMINT IN PUEB V OBVEŠČEVALNI DEJAVNOSTI

Kot sem v predhodnih poglavjih navedel, se v okvir obveščevalne dejavnosti vsake države, tako v miru, kakor tudi v okviru kriznih situacij (npr. OKO), vključujejo posebne oblike bojevanja oziroma pridobivanja obveščevalnih podatkov kot dela celotne obveščevalne slike.

Vloga in predvsem vpliv izvajanja aktivnosti COMINT in PUEB je v prvi vrsti (in predvsem) razmejena na varnostno situacijo – mirnodobni čas oz. npr. OKO.

4.1 MIRNODOBNI ČAS

4.1.1 COMINT

V mirnodobnem času se na nacionalnem nivoju izvaja izključno COMINT, predvsem iz stacionarnih (zemeljskih) in zračnih platform. Razlog za izvajanje COMINT iz zračnih platform izhaja predvsem iz dejstva, da ni geografskih ovir, zelo dobra optična vidljivost ter zmožnost angažiranja širokega obsega tako kadra (specialistov) kakor tudi tehničnih sredstev.

Za učinkovito izvajanje COMINT je poleg ustrezne opremljenosti, ter usposobljenosti kadra, potrebna tekoča in ažurna obveščevalna predpriprava - razpoložljivost vseh potrebnih informacij, pridobljenih iz drugih virov. – torej tistih, katerih zaradi določenih omejitev ni mogoče pridobiti z izvajanjem COMINT.

Podatki, pridobljeni z COMINT platform (zrak, zemlja), se preko ustrezno zaščitenih KIS posredujejo v t.i. analitični center (AC), kjer se podatki centralizirajo, selekcionirajo, delno analizirajo, dopolnjujejo se podatkovne baze ter izdelujejo poročila oziroma posledično nadaljnje usmeritve – načrtovanje in koordinacija izvajanja aktivnosti.

Na nacionalnem nivoju so na področju izvajanja COMINT vzpostavljene neposredne relacije z obveščevalnimi organi na vseh nivojih, vse do organov znotraj obveščevalnih služb.

Izvajanje nalog v mirnodobnem času, po principu 24/7 je nujno potrebno, saj zagotavlja ažuren pregled zasedenosti EM (frekvenčnega) spektra – tako z tehničnega kakor tudi vsebinskega vidika, kar v primeru grožnje bistveno zmanjšuje reakcijski čas oz. selekcioniranje podatkov.

Skladno z NATO dokumenti (predvsem MC 101/13) se posamezni elementi delovanja stopnjujejo z najvišjimi stopnjami tajnost, ranga Cosmic Top Secret (CTS) in Cosmic Top Secret – Bohemia (CTS-B), kar posledično predstavlja tudi rigorozne omejitve pri dostopu do prostorov tehničnih sredstev EI, prostorov, kjer se podatki obdelujejo ter poročil (produktov) samih. V okviru RS bi se tovrstne aktivnosti izvajale v 1. varnostnem območju.

Ključna značilnost COMINT je, da kot edina obveščevalna disciplina omogoča pridobivanje podatkov neposredno od uporabnika (načrtovalca, koordinatorja, nadzornika ali »eksekutorja«) - ima tako neposreden stik z grožnjo.

4.1.2 PUEB

Kot je navedeno v točki a1, se v mirnodobnem času izvaja izključno COMINT, medtem ko je izvajanje PUEB osredotočeno predvsem na usposabljanje – lastno, kakor tudi enot in pripadnikov, ki uporabljajo KIS ali radarske sisteme - vse s ciljem zagotovitve ustreznega izvajanja EZU t. j. pravilne uporabe.

Načrtovanje, koordinacija in izvajanje poteka v sodelovanju z operativnimi organi S3/G3 (predvsem na taktičnem in operativnem nivoju) ter delno tudi z organi za informatiko/komunikacije S6/G6 in obveščevalnimi organi S2/G2.

4.2 KRIZNA SITUACIJA - OKO

Sinergija izvajanja COMINT in PUEB v okviru OKO, je tesna in bistveno večja kot na nacionalnem ozemlju, v mirnodobnem času.

Kljub temu, pa obstaja ločnica, ki ima jasno izhodišče v elementih:

- načrtovanja,
- kontrole,
- poveljevanja (vodenja),
- poročanja,

V okviru OKO se za podporo poveljujočemu formirajo (v kolikor poveljujoči to zahteva) tako imenovani operativni centri EI/EB (SIGINT EW Operations Center - SEWOC), v okviru ter preko katerih potekajo analize pridobljenih podatkov prejetih s strani COMINT/PUEB platform– centri predstavljajo vez med platformami ter obveščevalnimi organi J2/G2. SEWOC deluje v mednarodni sestavi, nima pa ukazovalnega značaja – ne poveljuje z enotami na terenu, temveč deluje predvsem po principu »bilo bi dobro«, »predlagamo, da ….«.
Tovrstni centri so formirani v okviru NATO operacij, npr. KFOR in ISAF.

4.2.1 COMINT

Elementi (skupine), ki izvajajo COMINT (imenujemo jih tudi Skupine EI), so neposredno (strokovno) vezani na nacionalne obveščevalne celice (NOC). Te se načeloma formirajo v okviru vsake OKO, kjer država sodeluje z večjim številom pripadnikov oziroma je odgovorna za določeno cono delovanja.

Aktivnosti izvajajo v vnaprej opredeljeni coni odgovornosti, tako iz stacionarnih centrov kakor tudi zemeljskih/zračnih platform. Skupine so načeloma v sestavi do 5 pripadnikov, opremljene z najbolj sofisticiranimi tehničnimi sredstvi ter lahkimi terenskimi vozili.

Zaradi specifičnosti podatkov, tehničnih sredstev in specialistov, so te skupine nenehno pod fizičnim nadzorom, saj predstavljajo tarčo visoke vrednosti, ali drugače rečeno »ušesa« vsake operacije. Pridobljeni podatki se zaradi stopnje tajnosti ne prenašajo preko KIS, temveč se združujejo ter obdelujejo znotraj varovanih območij (stacionarnih centrov).

V okviru OKO se, ali zaradi problematike pomanjkanja lingvistov na eni, ali velikega obsega podatkov na drugi strani, pogosto uporabljajo postopki, v okviru katerih se surovi (neobdelani) podatki preko ustrezno zaščitenih KIS pošiljajo v državo ali pa celo izvaja neposredno daljinsko krmiljenje tehničnih sredstev lociranih v stacionarnih centrih.

4.2.2 PUEB

Elementi (skupine), ki izvajajo PUEB (imenujemo jih tudi Skupine EB), so neposredno podrejene poveljniku v okviru katere sestave se nahajajo – npr. poveljniku Bataljonske Bojne Skupine (BBSk), ki ima v okviru svoje sestave tudi ostale elemente za izvajanje nalog v določeni coni odgovornosti.

Skupine PUEB (katere dopolnjujejo tudi Skupine EPU, o katerih pa v tem delu ne bom govoril), so formirane v sestavi 3 – 5 pripadnikov, opremljene s podobnimi tehničnimi sredstvi kot Skupine COMINT ter lahkimi oklepnimi in/ali terenskimi vozili.

Vloga Skupin PUEB je osredotočena na taktični nivo, na zaščito lastnih sil – le to izvaja z nadzorom frekvenčnega spektra in posledično pravočasnim evidentiranjem grožnje. Skupine izvajajo naloge izključno iz zemeljskih platform, vedno neposredno oz. v sestavi enot, ki izvajajo naloge na terenu.

Pridobljeni podatki se posredujejo preko nadrejenih strokovnih organov BBSk (načeloma) v brigado ter nadrejena poveljstva oziroma centre. V kolikor se na v okviru OKO nahaja tudi NOC, je razumljivo tudi posredno (neformalno) sodelovanje.

Slika 17: Primeri platform EI / EB

U2 – Dragon Lady (EI)

EA6B – Prowler (EB)

E2C – Hawk Eye (EI)

8 x 8 (EB)

Fux, 6 x 6 (EB)

Henglund (EB)

Vir: Interno gradivo EEB

5 ZAKLJUČEK

"There is much more to electronic warfare than simply detecting enemy transmissions."
Martin Van Creveld

V Vojaški doktrini Slovenske vojske je navedeno, da je EB neposredno povezano z obveščevalno dejavnostjo in je eden od stebrov informacijskega delovanja.

Prestrezanje nasprotnikovih govornih in ne-govornih komunikacij, je zaradi načina dela ena izmed glavnih oblik pridobivanja obveščevalnih podatkov, tudi zaradi načina širjenja EMV, ki se širi po etru ne ozirajoč se na meje in želje posameznika, ki jih oddaja. Pomembno je, da se izvaja tako v miru, kot v vojni, 24 ur dnevno, 7 dni v tednu. Zaradi količine podatkov in komunikacij, ki se dnevno oddajo v eter, je potrebna podrobna analiza, da se ločijo potencialno uporabne od neuporabnih informacij.

Izvajanje (predvsem) EI predstavlja temelj obveščevalne dejavnosti, saj omogoča pridobivanje podatkov v skoraj vseh pogojih in je poleg tega eden redkih, ki se lahko izvaja v miru. Omogoča pravočasno javljanje potencialnih groženj, ki jih s pomočjo drugih oblik pridobivanja obveščevalnih podatkov lahko pravočasno preučimo. V sedanjem času nenadnih groženj s strani nekonvencionalnih sovražnikov, je pozornost in skrb na tem področju izrednega pomena.

Samo pravočasno pridobljeni in točni obveščevalni podatki nas lahko opozorijo na morebitne grožnje, da se jim lahko izognemo ali preprečimo, ne da bi s tem ogrožali civilno sfero ter kršili zakonodajo. Zaradi občutljivosti področja delovanja je pomembno, da so osebe, ki delujejo na tam področju visoko usposobljene in primerno izbrane, da ne pride do zlorab pooblastil, ki jih to področje potrebuje za nemoteno delo.

Bistvena razlika med EI in EB je predvsem v nivoju izvajanja nalog (uporabniku informacij) ter časovni komponenti vrednosti informacij. EEB izvaja naloge na strateškem in operativno-taktičnem nivoju.

Uspehi oz. neuspehi v vojni ali spopadu so pogosto odvisni od naših priprav v miru. V vojni uporabljamo že v miru zbrane strateške in taktične podatke in obveščevalne informacije. Delo obveščevalnih služb je v vojni bolj intenzivno na taktičnem področju, ker mora zbrati konkretne podatke na vojskovališču na vseh ravneh poveljevanja, med tem ko se na strateškem področju aktivnosti izvajajo neprestano in mnogo preje, ne glede na to ali obstaja direktna grožnja s strani potencialnega nasprotnika.

EI in EB v sodelovanju z ostalimi zvrstmi obveščevalne dejavnosti zagotavljata ključen element obrambe države in sil na aktivnostih v tujini.

LITERATURA

- 34-1 Intelligence and electronic warfare operations; September 1994.

- AJP-2 – SVS STANAG 2190; (Skupna obveščevalna, protiobveščevalna in varnostna doktrina; 2005

- Electronic Warfare; Joint Publication 3-13.1, 2007.

- Furlan Branimir; VOJAŠKA DOKTRINA, Poveljstvo za doktrino, razvoj, izobraževanje in usposabljanje, Ljubljana, 2006.

- GOLOB Damjan, MOŽINA Uroš, FRANGEŽ Zdenko: Skripta ELEKTRONSKO BOJEVANJE, Poveljstvo za doktrino, razvoj, izobraževanje in usposabljanje, Ljubljana, 2006.

- GOLOB, Damjan: Vloga elektronskega bojevanja v zaščiti sil (Force protection), Zaključna naloga štabnega tečaja za častnike, Šentvid, 2005.

- HORVAT Lidija; Zaključna naloga ELEKTRONSKO BOJEVANJE V SLOVENSKI VOJSKI, Center vojaških šol, 2000.

- KOSIĆ Miloš: Diplomsko delo VLOGA IN POMEN OBVEŠČEVALNIH SLUŽB V BOJU ZOPER MEDNARODNI TERORIZEM, Univerza v Ljubljani, Fakulteta za družbene vede, Ljubljana, 2006.

- Martin van Creveld; Technology and War, 1989.

- Priročnik za radioamaterje; Zveza radioamaterjev Slovenije; Ljubljana 1995.

- ŠAPONJA Vladimir; Taktika dela obveščevalnovarnostnih služb, Visoka policijsko – varnostna šola, Ljubljana 1999.

- US ARMY SIGNAL CENTER AND FORT GORDON OFFENSIVE LECTRONIC WARFARE (SC 25C-RC); September 1994.

VIRI

- http://www.sigint.co.uk.
- http://www.uradni-list.si/1/objava.jsp?urlid=2004107&stevilka=4500.
- http://en.wikipedia.org/wiki/Signals_intelligence#Targeting.
- NATO Glossary of Terms And Definitions – AAP 06, 2006
- Interno gradivo enote za elektronsko bojevanje.

SEZNAM SLIK

SEZNAM UPORABLJENIH KRATIC

AC	- analitični center
BBSk	- bataljonska bojna skupina
EB	- elektronsko bojevanje
EEB	- enota za elektronsko bojevanje
EM	- elektromagnetno
EMS	- elektromagnetni spekter
EMV	- elektromagnetno valovanje
EI	- elektronsko izvidovanje
EPU	- elektronski protiukrepi
EZU	- elektronski zaščitni ukrepi
KIS	- komunikacijsko informacijski sistem
MORS	- Ministrstvo za obrambo Republike Slovenije
NOC	- nacionalna obveščevalna celica
OIB	- obveščevalno izvidniški bataljon
OKO	- operacije kriznega odzivanja
OVS	- obveščevalno varnostna služba
PUEB	- podporni ukrepi elektronskega bojevanja
RR	- radiorelejna (naprava, sistem, zveza, ...)
RS	- Republika Slovenija
SV	- Slovenska vojska
ŠČ	- šola za častnike
TAS	- tehnična analiza signalov

SLOVAR TUJIH IZRAZOV

C2 - command and control - poveljevanje in kontrola

COMINT - communication intelligence - spremljanje komunikacijskih signalov

ECM - electronic counter measures - elektronski protiukrepi

EW - electronic warfare - elektronsko bojevanje

EMS - electromagnetic spectrum - elektromagnetni spekter

ELINT - electronic intelligence - spremljanje ne-komunikacijskih signalov

ESM - electronic support measures - podporni ukrepi elektronskega bojevanja

EPM - electronic protective measures - elektronski zaščitni ukrepi

EHF - extremely high frequencies - ekstremno visoke frekvence

GSM - global system for mobile communications - globalni sistem za mobilne komunikacije

HF - high frequency - visoke frekvence

HUMINT - human intelligence - zbiranje informacij s pomočjo človeških virov

IMINT - imagery intelligence - zbiranje informacij v obliki slikovnega gradiva

MASINT - measurement intelligence - zbiranje informacij o znanstveno tehničnih karakteristikah sredstev

OSINT - open source intelligence - informacij iz javno dostopnih virov

RADINT - radar intelligence - analizira delovanje radarskih sredstev

SHF - super high frequencies - super visoke frekvence

SIGINT - signals intelligence - elektronsko izvidovanje

TECHINT - technical intelligence

UHF - ultra high frequency - ultra visoke frekvence

VHF - very high frequency - zelo visoke frekvence

IZJAVA O AVTORSTVU

Kandidat za častnika desetnik Alojz Berginc izjavljam, da sem avtor zaključne naloge, ki sem jo izdelal pod mentorstvom stotnika Damjana Goloba in dovoljujem uporabo zaključne naloge v študijske namene.

V Ljubljani, dne _____ Podpis: _____