UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Grega Tušar

Elektronsko bojevanje in sodobna uporaba elektronskih protiukrepov, podpornih ukrepov elektronskega bojevanja ter elektronskih zaščitnih ukrepov

Diplomsko delo

Ljubljana, 2010

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Grega Tušar

Mentor: doc. dr. Uroš Svete

Elektronsko bojevanje in sodobna uporaba elektronskih protiukrepov, podpornih ukrepov elektronskega bojevanja ter elektronskih zaščitnih ukrepov

Diplomsko delo

Ljubljana, 2010

ZAHVALA

Zahvalil bi se rad vsem, ki ste mi skozi vsa štiri leta stali ob strani, ko je bilo najbolj mučno in hudo. Nenehno vzpodbujanje staršev Marka in Barbare in sestre Vesne ter lastne želje po uspehu, se je odrazilo v tem diplomskem delu. Hvala, ker ste verjeli v moj uspeh!

Prijateljem se zahvaljujem za potrpežljivost, razumevanje skozi vsa ta leta in v času pisanja diplomske naloge. Tebi Sara pa še posebna zahvala, ker si me prenašala in vzpodbujala, ko je bilo najbolj naporno. Hvala vam!

Mentorju doc. dr. Urošu Svetetu se zahvaljujem za strokovno pomoč, usmeritve in predloge pri pisanju mojega diplomskega dela. Vaša požtrvovalnost in neizmerna želja po našem uspehu je hvale vredna!

Posebno bi se rad zahvalil stotniku Damjanu Golobu, ki je s svojo nesebično željo po pomoči pomagal ustvariti diplomsko delo. Kljub lastnim obveznostim, ste vedno žrtvovali svoj čas zame. Brez Vas bi ta diplomska naloga ostala nekje v zraku. Najlepša hvala!

Najlepša hvala vsem!

Elektronsko bojevanje in sodobna uporaba elektronskih protiukrepov, podpornih ukrepov elektronskega bojevanja ter elektronskih zaščitnih ukrepov

Elektronsko bojevanje je novejša vojaška aktivnost, ki jo izvajajo enote elektronskega bojevanja, s katero želijo doseči nadzor in premoč nad uporabo EMS. Opravlja več nalog in uporablja več različnih metod, s ciljem zavarovanja lastnih sil in sistemov lastnih komunikacij in zvez. Predstavlja nevidno zaščito pred sovražnim delovanjem EM aktivnosti nasprotnika. »Elektronsko bojevanje je integralni del vseh oblik vojaških delovanj in predstavlja neposredno povezavo z obveščevalnimi aktivnostmi« (Furlan 2006, 68). Obstaja znatna razlika med elektronskim bojevanjem in izvidovanjem, vendar eno brez drugega ne more obstajati. Enote elektronskega bojevanja pri svojem delu izvajajo različne ukrepe, od elektronskih podpornih ukrepov, elektronskih protiukrepov, elektronskih zaščitnih ukrepov. V Republiki Sloveniji se enote za elektronsko bojevanje še niso razvile svojih zmožnosti do te mere kot v tujini. Njihov učinek se kaže predvsem v operacijah kriznega odzivanja, kjer s svojim delom izvajanja nadzora in izkazovanjem superiornosti nad elektromagnetnim spektrom, delujejo predvsem v zaščiti lastnih in združenih sil.

KLJUČNE BESEDE: elektronsko bojevanje (EB), elektronsko izvidovanje (EI), podporni ukrepi elektronskega bojevanja (PUEB), elektronski protiukrepi (EPU), elektronski zaščitni ukrepi (EZU).

Electronic warfare and modern usage of electronic counter measures, electronic support measures and electronic protective measures

Electronic warfare is a relatively new military activity, performed by units of electronic warfare. The purpose of this activity is control and authority over the use of electromagnetic spectrum. They perform several tasks and use various methods to protect their forces and systems of communication and connection. It represents an invisible protection from the hostile electromagnetic activities of the adversary. “Electronic warfare is an integral element of all forms of military activities and represents a direct connection to intelligence activity” (Furlan 2006, 68). There is a significant difference between electronic warfare and signal intelligence, but they are interdependent. Units of electronic warfare apply several measures, including electronic support measures, electronic counter measures, and electronic protective measures. Slovenian units of electronic warfare have not developed their capabilities to the level seen abroad. Their effect is most apparent in crisis response operations, where their primary activity is the protection of own forces and joint forces by performing surveillance and presenting superiority over electromagnetic spectrum.

KEY WORS: electronic warfare (EW), signal intelligence (SIGINT), electronic support measures (ESM), electronic counter measures (ECM), electronic protective measures (EPM).

Kazalo

Kazalo tabel

Kazalo slik

SEZNAM KRATIC

C2	command and control
C3	command, control and communications
C4	command, control, communications and computerization
C4I	command, control, communications, computerization and intelligence
C4I	command, control, communications, computerization, intelligence and counter measures
COMINT	communication intelligence – zbiranje informacij s pomočjo komunikacij
EB	elektronsko bojevanje
EEB	enota za elektronsko bojevanje
EI	elektronsko izvidovanje
ELINT	electronic intelligence – zbiranje informacij s pomočjo elektronike
EM	elektromagnetno
EMP	elektromagnetni pulz
EMS	elektromagnetni pulz
EMV	elektromagnetno valovanje
EPU	elektronski protiukrepi
EZU	elektronski zaščitni ukrepi
GSM	global system for mobile communications – globalni mobilni sistem
HUMINT	human intelligence – zbiranje informacij s pomočjo človeških virov
IMINT	imagery intelligence – zbiranje informacij s pomočjo slikovnega gradiva
KIS	komunikacijsko – informacijski sistem
MASINT	measurments intelligence – zbiranje informacij s pomočjo tehničnih ukrepov
OKO	operacije kriznega odzivanaja
OSINT	open source intelligence – zbiranje informacij s pomočjo javno dostopnih virov
PUEB	podporni ukrepi elektronskega bojevanja
RADINT	radar intelligence- zbiranje informacij s pomočjo radarskih sistemov
RR	radiorelejna (naprava, sistem, zveza)
RV IES	radijsko vodeno improvizirano eksplozivno sredstvo
SIGINT	signal intelligence – elektronsko izvidovanje
SSL	single site location
TAS	tehnična analiza signalov
TECHINT	technical intelligence – zbiranje informacij s pomočjo tehničnih sredstev

1 UVOD

Hiter in nenehen razvoj elektronike v civilni sferi se posledično izraža tudi na vojaškem področju. Oborožitveni sistemi ter sistemi poveljevanja in kontrole praktično ne delujejo brez prisotnosti elektronskih sredstev, ne glede na formacijo oziroma nasprotnika, pa naj bo to oborožena sila, paravojaška skupina, teroristična ali kriminalna skupina. Govorimo o digitalnem bojišču. Digitalizacija bojišča, informacijska prenasičenost, novi sistemi poveljevanja in kontrole, nove grožnje in varnostni izzivi s katerimi se srečujejo sodobne vojske, vse bolj vplivajo na načrtovanje in pripravo bojevanja, s katero se želi vzpostaviti prednost na bojišču. Načrtovanje kot ena najbolj pomembnih strateških dejavnostih vojsk ne more biti uspešno, če ne temelji na verodostojnih in pravočasnih obveščevalnih informacijah in podatkih. Odlično načrtovanje in priprave sta skupaj s sodobno tehnologijo nekajkrat povečala hitrost, premičnost enot, natančnost izvajanja bojnih nalog ter vsekakor lažje sprejemanje odločitev in povelj poveljnikov na nižjih ravneh.

Iskanje informacijske prednosti in zagotavljanje obveščevalnih podatkov je privedlo do nastanka enot za elektronsko bojevanje, ki so ključne za prevlado na modernem bojišču. Asimetrično bojevanje, ki se danes dogaja predvsem na operacijah kriznega odzivanja, sili k novim oblikam bojevanja, ki pa niso le neortodoksne. »Elektronsko bojevanje, kot ena izmed oblik bojevanja, igra pomembno vlogo pred, med in po operaciji v celotnem področju konfliktov, od mirnodobnega časa, operacij v podporo miru pa vse do največjih oblik konfliktov, in ima eno od ključnih vlog pri zagotavljanju zaščite sil« (Golob 2005, 14). Značilne so predvsem nove grožnje improviziranih eksplozivnih naprav, ki predstavljajo novo obliko grožnje in nevidnega nasprotnika. Enote s svojo taktiko, sistemi in uporabo elektronskih ukrepov zagotavljajo dostop do informacij, zaščito lastnih in združenih lastnih sil in onemogočajo nasprotniku, da bi bil ta v teh aktivnostih boljši in bi predstavljal grožnjo lastnim silam. S tem bi pridobil premoč in obvladovanje modernega bojišča. Pomembna je učinkovitost elektronskega bojevanja, in ta učinkovitost je odvisna od več faktorjev, predvsem od sodobne tehnične opremljenosti, uspešnosti nadzora, preprečitev ali otežitvi uporabe elektromagnetnega spektra.

Vstop nacionalnih držav v sisteme kolektivne varnosti in obrambe so privedle nekaj novosti na področju delovanj vojaških enot. Nujno je sodelovanje, le-to pa je mogoče v primeru povezanosti na področju organiziranosti, postopkov in pa kompatibilnosti tehničnih sredstev na področju prenosa podatkov in ter usklajene uporabe elektromagnetnega spektra. Tako se je

tudi Enota za elektronsko bojevanje SV morala prilagoditi novim razmeram sodelovanja znotraj NATO-a in širšega zavezništva. Enote se srečujejo z novimi grožnjami in varnostnimi izzivi, s katerimi se srečujejo v operacijah kriznega odzivanja, ki jih izvaja zavezništvo NATO in ostali.

2 METODOLOŠKI OKVIR

2.1 Cilj in pomen

Cilj diplomskega dela je predstaviti elektronsko bojevanje kot podpora bojevanja, ki je vse bolj pomembna pri komunikacijski prednosti pred nasprotnikom. Pomen ima pri določanju novih oblik bojevanja, ki pa niso konvencionalna. Predstavil bom vrste zvez oziroma sisteme prenosa podatkov, ki uporabljajo elektromagnetni spekter. Opisal bom vrste elektronskega bojevanja, delovanje in uporabo metod elektronskih ukrepov ter sistemov in podsistemov, ki jih uporabljajo enote za elektronsko bojevanje SV.

2.2 Raziskovalno vprašanje

V diplomskem delu sem si zastavil naslednje vprašanje: *s kakšnimi metodami elektronskega bojevanja se srečujemo in ali so te metode dovolj učinkovite za sodobne razmere na bojišču?* Odgovore na zastavljeno vprašanje bom iskal s pomočjo spodaj naštetih metod.

2.3 Uporabljena metodologija

- **Primerjalna analiza teoretičnih virov.** Namen te metode je sistematična predstavitev osnovnih pojmov elektronskega bojevanja, elektronskih ukrepov in metod izvajanja elektronskega bojevanja. S pomočjo te metode bom primerjal značilnosti elektronskih ukrepov in metod med slovenskimi in zavezniškimi (ZDA) enotami za elektronsko bojevanje. V to metodo je vključena deskriptivna metoda in metoda analize sekundarnih virov.
- **Osebni pogovor s pripadnikom Enote za elektronsko bojevanje Slovenske vojske (EEB).**

3 PRENOS PODATKOV

Poznamo več načinov prenosa podatkov, in sicer preko vrst zvez (prenos podatkov-komuniciranje med uporabnikom A in B) in prenos preko elektronskih naprav, ki izrabljajo elektromagnetni spekter (prenos podatkov med elektronskimi napravami in s pomočjo le teh, izris informacijske slike). Prenosa podatkov ne smemo gledati samo kot način komuniciranja med uporabnikom A in B, ker je to le eden od načinov prenosa podatkov. Do prenosa podatkov prihaja pri vseh elektronskih napravah, ki za svoje delovanje potrebujejo elektromagnetno (v nadaljevanju EM) energijo. Tako s sprejemanjem in oddajanjem EM energije, signala ali pulza prihaja do uporabe EM spektra. Naprave, ki uporabljajo EMS so zelo ranljive s strani izvajanja elektronskega bojevanja. Celoten EMS je cilj delovanja elektronskega bojevanja, kjer želimo nasprotniku preprečiti njegovo uporabo ali pa vsaj preprečiti prenos podatkov preko EMS, s čimer pridobimo informacijsko prednost pred nasprotnikom.

Vrste zvez, ki jih uporabljamo za prenos podatkov so žične in brezžične zveze, kjer so kurirske zveze izvzete. Brezžične zveze dalje delimo na radijske, radio relejne in satelitske zveze, ki za svoje delovanje nujno potrebujejo delovanje EMS. Prenos podatkov poteka med uporabniki zvez, torej gre za klasično govorno obliko komuniciranja, vendar kljub temu obstaja tudi negovorna oblika komuniciranja, paketnega pošiljanja digitalnih podatkov (vendar morajo biti gesla vnaprej določena), ki jo omogočajo bolj napredne radijske postaje z različnimi modulacijami.

Prenos podatkov poteka tudi med napravami in s pomočjo le-teh. To so elektronske naprave, ki izrabljajo EMS za svoje delovanje. Vse elektronske naprave namreč sprejemajo in oddajajo elektromagnetno energijo (EME). Razdelimo jih v dve skupini, prvo, ki opravlja osnovno delovanje (sprejem in oddaja EME) in del procesa obdelave podatkov ter drugo, kjer sistemi poleg osnovnega delovanja in procesa obdelave tudi usmerjajo delovanje drugih elektronskih sistemov. V prvo skupino spadajo razni elektronski senzorji, radarji, GPS sistemi, v drugo pa sistemi kontrole in poveljevanja in sistemi za nadzor ognja, ki sta med seboj tesno povezana. Sistem kontrole in poveljevanja omogoča negovorno obliko komuniciranja (paket digitalnih podatkov, ki ne potrebuje predhodne določitve gesel, ker je sistem tako naravnan, da sam sprejema digitalne podatke preko filtrov med uporabniki elektronskih sredstev). Tako sistemi

za kontrolo in poveljevanje ter sistemi za nadzor ognja uskljajujejo prenos ter delovanje podatkov med elektronskimi napravami.

4 ELEKTRONSKO BOJEVANJE IN ELEKTRONSKI UKREPI

4.1 Razlika med podpornimi ukrepi elektronskega bojevanja (PUEB) in elektronskim izvidovanjem (EI)

Elektronsko izvidovanje, ki je slovenski izraz za angleški pojem SIGINT (Signal Intelligence), je razdeljeno na dve podpodročji in sicer spremljanje komunikacijskih in nekomunikacijskih signalov, torej vseh naprav, ki delujejo v EMS.

> Razlika med PUEB in EI izhaja predvsem iz namena, s katerim so signali sprejeti, načina, kako so obdelani, ter uporabe pridobljene informacije. Iz signalov, ki so v analizi in obdelavi dalj časa, dobimo poročilo oz. informacijo, ki ji v angleščini pravimo intelligence. S pridobivanjem takšnih informacij se ukvarjajo enote za elektronsko izvidovanje, ki tako predvsem zagotavljajo obveščevalne podatke za vse ravni, od strateške do taktične. Simboli, ki jih sprejmemo in so takoj uporabni, ne potrebujejo daljše analize ter nam dajo podatke, ki mu v angleščini rečemo combat information. Pridobivajo jih enote, ki izvajajo podporne ukrepe elektronskega bojevanja. Ti podatki so lahko uporabljeni tako ali pa so z določeno analizo obdelani in omogočijo pripravo poročila ali informacije. Razlika med področjema je tudi v času, ki ga enote potrebuje za pridobitev podatkov. Enote za PUEB pridobivajo podatke, ki so uporabni takoj ali z majhno zakasnitvijo, enote za EI pa na podlagi zbiranja podatkov in analiz ustvarijo sliko ali informacijo v daljšem časovnem obdobju. Takšni podatki so uporabni na višjih ravneh delovanja, na primer pri načrtovanju, podatki, ki jih pridobivajo enote za PUEB pa so uporabni že med bojevanjem in jih taktične enote uporabljajo na bojišču (Golob in drugi 2006, 13).

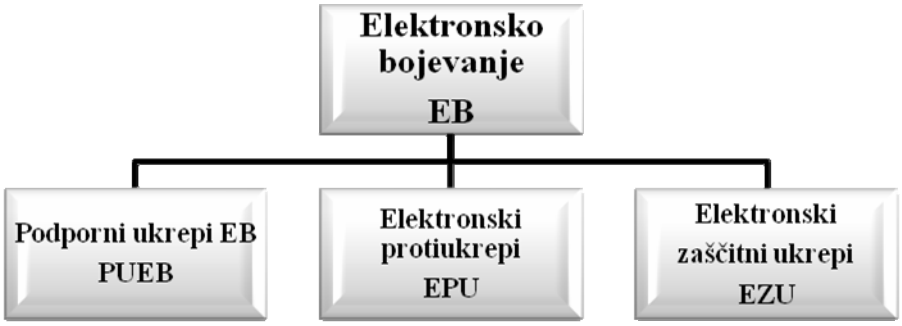
Gre torej za dve, zelo podobni aktivnosti, ki jih izvajajo enote elektronskega bojevanja, vendar pa med njima kljub temu obstajajo razlike. Ključna razlika je v končnem uporabniku informacije ali podatka. Kljub temu, da ima vsaka aktivnost svojega končnega uporabnika, je vsekakor zelo pomembno dejstvo, da sta aktivnosti soodvisni. Prihaja do izmenjave podatkov in informacij, ki so lahko ključne za posameznega končnega uporabnika, čeprav te v prvotno niso bile zbrane za njegovo uporabo. Potek prenosa podatkov poteka skozi obveščevalne filtre med obema aktivnostma, kjer imajo glavno vlogo nadrejeni štabi, kjer prihaja do povezave med štabnimi službami S-2/S-3 in višje.

Tabela 4.1: Razlika med EI in EB

Elektronsko izvidovanje (EI)	**Elektronsko bojevanje (PUEB)**
strateški fokus	operativno taktični fokus
nacionalni interes	zaščita sil
dolgotrajen (neprekinjen – 24/7) proces pridobivanja obveščevalnih podatkov o nasprotniku, velik poudarek na širši analitični obdelavi, visoka stopnja tajnosti podatkov (tajno, strogo tajno), nacionalne omejitve	časovno omejena aktivnost s takojšnjim učinkom, nižja stopnja tajnosti podatkov (zaupno)
zavedanje situacije	pravočasna identifikacija grožnje
operativno izvajanje v vojni in miru	operativno izvajanje v prehodu na in med operacijo, v miru v vlogi usposabljanja enot za delovanje v pogojih EI in EB
funkcijsko vezano na štabne organe G2/J2 in obveščevalne službe	funkcijsko vezano na štabne organe G3/J3
po naravi izvajanja pasivna aktivnost (izključno spremljanje EMOk)	po naravi izvajanja aktivna in pasivna aktivnost (ločnico predstavljajo ukrepi E-napada, ki pa se tesno navezujejo tako na E-nadzor kakor tudi na EI, saj oba predstavljata osnovo za izvajanje E-napada)
primarno izvajanje z zračnih in stacionarnih platform (objekti),	predvsem z zemeljskih platform
(predvsem) nezaščitene zveze	zaščitene zveze in dekodiranje

Vir: Golob (2010, 9).

Slika 4.1: Vrste elektronskih ukrepov



Vir: Berginc (2008, 12).

4.2 Podporni ukrepi elektronskega bojevanja - PUEB

Podporni ukrepi elektronskega bojevanja so po naravi izrazito pasivni. S tehničnimi sredstvi le sprejemamo elektromagnetno energijo, ki jo oddajajo opazovani sistemi, zato je enote, ki izvajajo takšne ukrepe, zato težko odkriti. Med podporne ukrepe elektronskega bojevanja se uvrščajo naslednji ukrepi:

- iskanje,
- prestrezanje,
- identificiranje,
- določanje lokacij izvorov elektromagnetnega sevanja-goniometriranje,
- določanje lokacije z metodo SSL.

S pomočjo pridobljenih podatkov simuliramo razmere na bojišču in tako takoj prepoznamo ali odkrijemo nevarnosti. Tako pridobljeni podatki so podlaga za izvedbo nadaljnjih odločitev vključno z načrtovanjem in izvajanjem elektronskih protiukrepov (EPU) in elektronskih zaščitnih ukrepov (EZU). S podpornimi ukrepi EB pridobljeni podatki močno vplivajo na taktiko bojevanja lastnih enot, zato jih morajo ciljni uporabniki dobiti v najkrajšem času - po potrebi tudi v izvorni ali delno obdelani obliki. Zavedati se je treba, da imajo takšni podatki večinoma omejen rok uporabnosti in so, če so posredovani prepozno, brez uporabne vrednosti (Golob in drugi 2006, 13).

Podporne ukrepe lahko štejemo med ofenzivne in defenzivne aktivnosti. Aktivnosti, ki jih izvajajo se namreč delijo na opozarjanje na nevarnosti, podporno iskanje obveščevalnih podatkov in informacij ter iskanje nasprotnikovega delovanja v EMS (povzeto po Department of the army 2009, 4). Ob tem je potrebno poudariti, da se metode med seboj ne razlikujejo veliko, vendar je kljub temu sistem v ZDA naravnan bolj v smeri definirane uporababe EMS

in tako tudi podpornih ukrepov elektronskega bojevanja. Med podporne ukrepe elektronskega bojevanja namreč štejejo osnovne tri aktivnosti, kar nakazuje novo razliko. PUEB se delijo na tri aktivnosti: elektronsko izvidovanje, elektronska obveščevalna aktivnost in elektronska varnost. Tako se že med podpornimi ukrepi elektronskega bojevanja izvajajo aktivnosti elektronske zaščite ukrepov, ki pri nas spadajo v elektronske zaščitne ukrepe.

4.2.1 Iskanje

Iskanje je postopek, pri katerem s pomočjo tehničnih sredstev iščemo aktivne signale na določenem frekvenčnem področju. Glede na prostor izvajanja ločimo iskanje:

- s kopnega; najkompleksnejše zaradi reliefa zemljišča, naravnih ovir ter umetnih, izvajamo ga iz stacionarnih in mobilnih centrov,
- z morja; uporabimo lahko vse vrste platform,
- iz zračnega prostora; najučinkovitejše, relativna bližina ciljev, na poti signala ni ovir, pokrijemo lahko večje območje, uporabimo lahko letala, helikopterje, brezpilotna letala, balone ipd.,
- iz vesolja; s pomočjo satelitov (Golob in drugi 2006, 14).

4.2.2 Prestrezanje

Prestrezanje komunikacij je ena glavnih nalog podpornih ukrepov elektronskega bojevanja, s čimer dobimo največ informacij. Prestrezanje je organizirano poslušanje nasprotnikovih komunikacijskih sistemov, namen pa je prestrezanje informacij in pridobivanje podatkov, ki se prenašajo po komunikacijskem kanalu. Ta ukrep navadno sledi iskanju in identificiranju. Skupaj s prestrezanjem ponavadi poteka tudi določanje lokacije izvora elektromagnetnega sevanja (glej prilogo B). Zavedati se moramo, da prestrezamo signale, ki so bili poslani točno določenemu sprejemniku za katere pošiljatelj ne želi, da jih sprejema še kdo drug, vendar pa je narava širjenja elektromagnetnih valov takšna, da je prestrezanje brezžičnih komunikacij zelo težko preprečiti. Kljub temu je prestrezanje težka naloga, še posebno pri novejših digitalnih komunikacijah (Golob in drugi 2006, 14).

4.2.3 Identificiranje

Identificiranje sistema poteka s pomočjo sprejemanja oz. prestrezanja elektromagnetne energije, ki jo sistem oddaja. Določene podatke, kot sta pasovna širina in modulacija, pridobimo že iz glavnih značilnosti sprejetega signala. Pri govornih komunikacijah s poslušanjem pridobimo tudi podatke o pripadnosti, pozivnih signalih, organizaciji zvez itn. pri kompleksnejših signalih poteka njihova obdelava s pomočjo tehnične analize signala (TAS).

To je postopek, s pomočjo katerega določamo tehnične lastnosti določenega signala. Tako dobimo podatke o širini signala, vrsti modulacije, posebnosti signala (določena odstopanja), hitrosti prenosa pri digitalnih modulacijah itd. Prestrezanje pogosto poteka z neprimernih lokacij, v kar nas prisilijo razmere, zato se lahko zgodi, da ujamemo šibke signale, ki se komaj ločijo od šuma. Določitev takšnih signalov je za analizo poseben izziv (Golob in drugi 2006, 15).

4.2.4 Določanje lokacij virov elektromagnetnega sevanja-goniometriranje

Goniometriranje je določanje azimuta oziroma lokacije vira elektromagnetnega 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.

Iz navedenega je razvidno, da je radijsko goniometriranje zelo pomembna aktivnost podpornih ukrepov elektronskega bojevanja in izvidovanja, s katero potrdimo in izpopolnimo podatke, pridobljene z prestrezanjem in drugimi oblikami zbiranja obveščevalnih podatkov. Določeni sistemi imajo poseben način komuniciranja, tako da jih že na podlagi te značilnosti identificiramo, ko pa dodamo še podatke o lokaciji dobimo sliko razporeditve teh sistemov na terenu. Treba se je zavedati, da v mnogih primerih ne potrebujemo natančne lokacije teh sistemov. Pri pripravi slike je za poveljstvo dovolj, če je podatek na kilometer natančen. Pri napadih s posrednim ognjem z minometi, topovi, in podobnim potrebujemo podatek, ki nimajo odstopanja večjega od 100 metrov. Pri napadih s pametnim orožjem ni nujna takšna natančnost, saj je dovolj natančnost 5 kilometrov, da se vodeni projektil približa izvoru, naprej pa sam najde cilj in ga uniči. Natančnost podatka je zelo odvisna od uporabljene taktike goniometriranja, torej od števila goniometrov in njihove lokacijske razporeditve (Golob in drugi 2006, 15).

4.2.4.1 Določanje lokacij s triangulacijo

Določanje lokacije s to metodo je najosnovnejši način določanja lokacije izvora elektromagnetnega sevanja. Na podlagi metode triangulacije določimo lokacijo, tako da z dvema ali več goniometri določimo smer, iz katere prihaja elektromagnetno valovanje. Goniometri poznajo svojo lokacijo, smer iz katere prihaja EM valovanje, zato lahko določimo območje, kje se vse smeri križajo. Na tem območju je najverjetneje oddajnik (glej prilogo C). Če uporabimo tri goniometre ali več, dobimo bolj natančno meritev. Pri meritvah so zmeraj

odstopanja, zato se izmerjene smeri ne križajo v eni točki. Ponavadi določimo območje, na katerem je najverjetneje oddajnik, nato pa z matematičnim algoritmom določimo sredino območja. To je točka, kjer je največja verjetnost izvora EM valovanja. Natančnost določanja lokacije je odvisna od mnogo dejavnikov, med drugim tudi od frekvence signala oddajnika. Na nižjih frekvencah je težje določiti točno lokacijo, ker na razširjenost valov na tem območju vpliva precej dejavnikov okolja, in sicer stanje ionosfere, ozračje, ovire na poti, poraščenost terena. Višje kot so frekvence, natančneje lahko določimo lokacijo. Pri meritvah višjih frekvenc mora biti zagotovljena optična vidljivost do oddajnika (Golob in drugi 2006, 15).

4.2.4.2 Določanje lokacije z metodo SSL

»Pri nižjih frekvencah, torej na HF področju, se uporablja metoda SSL (single site location), ki temelji na izmerjenem kotu, pod katerim se elektromagnetni valovi odbijejo od ionosfere (glej prilogo Č). Sistem, ki uporablja to metodo, potrebuje za določitev lokacije le en goniometer, ponavadi stacionarne vrste, lahko pa je tudi premični« (Golob in drugi 2006, 17).

4.2.5 Globina zbiranja podatkov

Globina zbiranja podatkov oziroma oddaljenost, na kateri lahko odkrijemo nasprotnikova elektronska sredstva in druge cilje, spremljamo delo in zbiramo podatke je odvisna od tehničnih značilnosti sredstev, ki jih izvidujemo, zmožnosti tehničnih sredstev elektronskega izvidovanja oziroma elektronskega bojevanja in pogojev razširjanja EM valov na razdalji od oddajnika EM sevanja do tehničnega sredstva EI oziroma EB. Globina zbiranja podatkov torej lahko znaša nekaj sto metrov (na višjih frekvenčnih področjih najpogosteje optična vidljivost) do nekaj tisoč kilometrov (na nižjih frekvencah) (Golob in drugi 2006, 17).

4.2.6 Uporabna vrednost podatkov

Podatek in informacija postaneta uporabna šele takrat, ko ju pravilno in ob pravem času interpretiramo, analiziramo in posredujemo končnemu uporabniku. Na tem mestu je zelo pomembno sodelovanje in načrtovanje dela med elektronskim izvidovanjem in elektronskem bojevanju. Kljub temu, da je elektronsko izvidovanje primarna obveščevalna aktivnost, ki posreduje combat information-bojne informacije in podatke enotam elektronskega bojevanja, mora potek informacij teči tudi v obratno smer. Kajti tudi preko elektronskega bojevanja se pridobijo informacije in podatki, ki so potrebni na višjih ravneh in vplivajo na načrtovanje in pripravo operacij. Oba načina obveščevalnih aktivnosti sta ključna za uspešno implementacijo podatkov in informacij v ciklusu bojnega načrtovanja, priprav in odločanja.

Vsak poveljnik na bojišču mora imeti jasno sliko dogajanja na bojišču v pravem času. Enote elektronskega bojevanja izrisujejo sliko EMS, katere preko nadrejenih poveljstev pridobijo poveljniki na bojiščih, kateri morajo poznati vsako spremembo na bojišču.

Pomembni so kakovostni podatki, ki jih pridobijo enote za elektronsko izvidovanje in elektronsko bojevanje. Ta svoja poveljstva oskrbujejo s podatki in informacijami o navzočnosti radijskih sredstev lastnih in nasprotnikovih sil, njihovi razmestitvi, vrsti radijskega omrežja, o uporabi radijskih sredstev in prenehanju uporabe, pojavu novih sredstev, združevanju sredstev v skupine-mrežo (povzeto po Golob in drugi 2006, 17). Le pravilna interpretacija in uporaba pravilnih sistemskih filtrov, ki urejajo posredovanje obveščevalnih podatkov in informacij na vse ravni, lahko v tem primeru posreduje ključne informacije in podatke do končnega uporabnika. Zelo pomembna je torej pravilna interpretacija, ki pa se razlikuje glede na končnega uporabnika. Na taktični ravni se bodo obveščevalne informacije in podatki spremenili v bojne informacije, ki so ključne za poveljnika na bojišču, na operativni ravni bodo obveščevalni podatki in informacije ključni za pripravo in načrtovanje operacij, na strateški pa se bodo spremenili v strateške podatke, ki bodo usmerjali celotno strategijo bojevanja. Strateške usmeritve pa narekujejo nov način operativnega delovanja in taktike na najnižji ravni enot za elektronsko bojevanje in drugih lastnih ali združenih enot in sil.

4.3 Elektronski protiukrepi – EPU

> Elektronski protiukrepi si vsi ukrepi za zmanjšanje učinkovitosti delovanja ali popolno onesposobitev nasprotnikovih komunikacij, sodobnih orožij in elektronskih izvidniških naprav. Elektronski protiukrepi se delijo na:
>
> - elektronsko motenje- načrtno sevanje elektromagnetne energije za onemogočanje ali oteževanje uporabe nasprotnikovih elektronskih naprav oziroma sistemov,
> - elektronsko zavajanje- načrtno sevanje, odboj in absorpcija EM energije za zavajanje nasprotnika, da napačno sklepa o stanju in namenih naših ali njegovih sil,
> - elektronska nevtralizacija- začasno ali nenehno uničevanje nasprotnikovih elektronskih sistemov z uporabo EM energije (Golob in drugi 2006, 18).

Čeprav so to vsi elektronski protiukrepi, ki jih poznajo enote elektronskega bojevanja SV, se poleg njih v drugih dokumentih pojavljajo tudi druge vrste elektronskih protiukrepov. Eden tak je uporaba protiradarskih raket (Department of the army 2009, 5), ki jih uporabljajo enote

za elektronsko bojevanje v ZDA, kjer gre za uporabo raket, ki delujejo elektronsko in imajo negativen vpliv na radarje - mrtva radarska slika. To obliko delovanja štejemo kot elektronski napad na zračno obrambo in njihove bojne aktivnosti. Ob enem pa ZDA vključujejo elektronsko aktivno zavajanje kot del elektronskih protiukrepov, kjer s pomočjo aktivnih zavajalcev napadajo naprave v EMS.

4.3.1 Elektronsko motenje

> Elektronsko motenje izvajamo, da nasprotniku onemogočimo uporabo EM spektra. EM motnja je lahko šum, neželeni signal ali sprememba lastnosti prenosnega medija. Elektronsko motenje je vrsta elektronskih protiukrepov, ki z zmanjšanjem obsega ali popolno prekinitvijo nasprotnikovih komunikacijskih poti povzroči oslabljeno sposobnost prenosa podatkov in zmanjša oziroma ohromi nasprotnikovo zmožnost uporabe elektronskih sistemov ter tako bojno sposobnost. Največji učinek je mogoče doseči, kadar je nasprotnik odvisen od uporabe elektronske opreme, torej upravljanja ognja, sistemov protizračne obrambe ter komunikacije vodenja in poveljevanja. Pri tem je potrebno vedeti, da nasprotniku ne moremo preprečiti oddajanja, zato nikoli ne motimo oddajne strani, temveč moramo čim bolj otežiti ali celo onemogočiti sprejem (glej prilogo D). Nasprotnik sicer lahko oddaja, vendar podatki ne dosežejo naslovnika ali se jih del izgubi. Tako smo dosegli naš temeljni namen, torej delno ali popolno izključitev nasprotnika iz boja. Motenje mora potekati v čim manjšem obsegu in šele takrat, ko so izkoriščene vse druge možnosti oziroma ko je to smiselno in nujno. Najboljše rezultate elektronskega motenja dosežemo s koncentracijo sredstev in selektivnim motenjem nasprotnikovih komunikacijsko-informacijskih sistemov (KIS). Elektronsko motenje je učinkovito in smiselno le v omejenem obdobju, in sicer od trenutka, ko nasprotnik uporabi elektronske zaščitne ukrepe, ki bodo izničili učinke elektronskega motenja. Centralizirano vodenje in poveljevanje zagotavljata minimiziranje nezaželenih motenj lastnih KIS, radarskih sistemov, in tistih nasprotnikovih KIS, ki so vir obveščevalnih podatkov. Izogibati se je potrebno nekritični uporabi elektronskega motenja. Pri tem je potrebno v taktiko vključiti vse podatke, pridobljene s podpornimi elementi elektronskega bojevanja. Da bi to dosegli, morajo biti elementi elektronskega bojevanja razviti pravočasno, vse aktivnosti elektronskega bojevanja pa morajo biti vključene v načrte delovanja in se prilagajati nastalim taktičnim razmeram (Golob in drugi 2006, 19).

Naloge in cilji skupine za elektronsko motenje (glej prilogo E) so:

- zagotavljanje varnosti konvojev z motenjem EMS in s tem preprečitev daljinskega aktiviranja improviziranih eksplozivnih teles,
- motenje nasprotnikovih zvez,

- motenje radarjev in namerilnih oborožitvenih sistemov,
- zagotavljanje nemotenega delovanja lastnega EMS,
- preprečevanje delovanja nasprotnikovega delovanja v EMS,
- zavajanje nasprotnikovega EMS, s čimer si zagotovimo prednost v načrtovanju, pripravi vojaških operacij,
- zavajanje s ciljem preprečevanja razporeditve in onemogočanje zmožnosti bojne organiziranosti nasprotnika (povzeto po Golob in drugi 2006, 19).

4.3.1.1 Izvajanje elektronskega motenja, uporaba elektronskega motenja, vrste elektronskega motenja

V uporabi poznamo dva načina izvajanja elektronskega motenja:

1. aktivno elektronsko motenje - motenje sistemov, ki sprejemajo in oddajajo EM sevanje, radijska, radijsko-relejna sredstva, televizija,
2. pasivno elektronsko motenje - motenje sistemov, ki izrabljajo EMS po načelu sprejemanja odboja EM signalov, ki se ti odbijejo od cilja, radarski sistemi, infrardeče kamere (povzeto po Golob in drugi 2006, 20).

Glede na namen ločimo elektronsko motenje na:

1. taktično motenje (manjše globine),
2. operativno motenje (večje globine) (povzeto po Golob in drugi 2006, 20).

Glede na širino motilnega signala ločimo naslednje vrste elektronskega motenja,:

1. širokopasovno elektronsko motenje- motenje vseh frekvenc v določenem široko pasovnem območju (glej prilogo G),
2. ozkopasovno elektronsko motenje- motenje točno določene frekvence (glej prilogo F),
3. brišoče motenje (glej prilogo H) - motenje širšega frekvenčnega pasu s hitrim »prebrisavanjem« oziroma ozkopasovno motenje s pomikanjem čez širši frekvenčni pas (povzeto po Golob in drugi 2006, 20).

4.3.2 Elektronsko zavajanje

Druga vrsta elektronskih protiukrepov je elektronsko zavajanje, ki v nasprotju z elektronskim motenjem predstavlja uporabo EM energije za zavestno napeljevanje nasprotnika v napačne sklepe o namerah in stanju lastnih sil ali k navajanju na zmotne sklepe o stanju naših sil in njihovih namerah. EM spekter delimo z nasprotnikom, zato je zelo primeren za zavajanje. Prav zaradi tega je zavajanje močno sredstvo, kljub temu pa je ob neustrezno načrtovani

uporabi lahko vzrok velikih lastnih izgub. Elektronsko zavajanje na širokem območju zahteva sodobno tehnologijo, usposobljenost visoko strokovnega kadra (poznavanje tujih komunikacij in postopkov, jezika do podrobnosti narečij in slengov, ritma izgovorjave besed, uporabe vzdevkov in nadimkov, jakosti in barve glasu, hitrosti izgovorjave besed) kakor tudi dolgotrajnost postopkov pri pripravi virov. Če niso ustvarjeni vsi pogoji za izkoriščanje sodobne elektronske tehnologije, s katero se lahko izvaja obsežno zavajanje, podatki pa se ne prenašajo zelo hitro, lahko postane elektronsko zavajanje brez uporabne vrednosti oziroma nasprotnika opozori na naše poskuse elektronskega zavajanja, da postane pozoren. Tako analizira naše sposobnosti in zmogljivosti ter jih uporabi proti našim enotam. Zavajanje je uspešnejše, če je načrtovano za točno določen objekt, omejen v času in prostoru. Oborožene sile v operacijah raje uporabljajo omejeno območje zavajanja v izbranem obdobju in času boja. Elektronsko bojevanje mora biti obvezno vključeno kot del načrta zavajanja. Oblike elektronskega zavajanja so naslednje, tako je mogoče zavajati nasprotnika z neposrednim vpadom v njegov KIS in prenašati lažna sporočila ter posredovati ali preklicevati ukaze, ki bodo našim silam zagotovili taktično prednost. Takšne aktivnosti morajo biti skrbno načrtovane in usklajene s taktiko uporabe naših sil, dobro premišljeni pa tudi vsi scenariji, drugače se ne doseže želenih rezultatov. Elektronsko zavajanje govornih zvez je najpreprostejši način zavajanja s predvajanjem posnetka iste zveze. Poseben način uporabe sredstev za elektronsko zavajanje se lahko uporablja pri psiholoških operacijah. V tem primeru se naprave za motenje in zavajanje uporabljajo le kot zelo močni oddajniki, vsebina sporočila pa je v domeni enote za psihološko bojevanje. Elektronsko zavajanje negovornih zvez je bolj zapleteno, kjer se uporabljajo ključi za vdor v kodirane sisteme (Golob in drugi 2006, 23).

Še posebej to velja za način dela, klicne signale, s katerimi dokažemo verodostojnost podatkov in identifikacijo.

4.3.2.1 Vrste zavajanja

Vrste zavajanja delimo na:

1. manipulativno elektronsko zavajanje; sprememba v delovanju lastnih KIS za določene naloge,
2. emitirano elektronsko zavajanje; vključevanje EM sevanja v nasprotnikove kanale, ki oddajajo lastno emisijo,
3. simulacijsko elektronsko zavajanje; ustvarjanje EM emisije za ustvarjanje pozornosti ali aktualnih sposobnosti za zavajanje nasprotnika, vendar pa morajo biti ti ukrepi podprti z drugimi ukrepi zavajanja (simulacija premika lastnih sil) (povzeto po Golob in drugi 2006, 24).

4.3.3 Elektronska nevtralizacija

Tretja vrsta elektronskih protiukrepov je elektronska nevtralizacija, kjer s preudarno uporabo EM energije začasno ali trajno poškodujemo ali uničimo elektronske naprave, ki so odvisne od uporabe EMS. Gre za sisteme, ki z oddajanjem EM pulza poškodujejo ali uničijo zelo občutljive sisteme, radarske sisteme, sisteme poveljevanja in kontrole (C2), optoelektronske sisteme. Pri tem je potrebna optična vidljivost do cilja, kajti sistemi delujejo po principu oddajanja usmerjene energije, ki delujejo z žarkom delcev (povzeto po Furlan 2006, 71).

Elektronska nevtralizacija je eden od najbolj skrajnih elektronskih protiukrepov, ki jih uporabljajo enote za elektronsko bojevanje. Čeprav je v okviru veljavnih doktrinarnih dokumentov SV izrecno prepovedana (povzeto po Žaže 2008, 25), tudi ne posedujemo sredstev, s katerimi bi lahko izvajali to metodo elektronskih protiukrepov. V nasprotju z doktrinarnim dokumentom elektronskega bojevanja ZDA, se v njem nahaja posebna metoda elektronskih protiukrepov, ki opisuje proces elektronskega napada na cilj, z direktno usmerjeno EM energijo. S to metodo se lahko uničijo elektronska sredstva ali oborožitveni sistemi, ki so odvisni od EMS, sprejemnike ali oddajnike EM valovanja, IR senzorje, termične senzorje, lasersko vodene izstrelke, sisteme kontrole ognja itd.

4.4 Elektronski zaščitni ukrepi –EZU

Elektronski zaščitni ukrepi (EZU) so del elektronskega bojevanja, ki vključuje vse ukrepe, s katerimi zagotavljamo nemoteno uporabo EM spektra, kljub nasprotnikovim podpornim ukrepom elektronskega bojevanja in elektronskim protiukrepom. Elektronske zaščitne ukrepe delimo na:

1. aktivne elektronske zaščitne ukrepe; to so vsi ukrepi za nemoteno uporabo EMS, ki jih nasprotnik hitro zazna (spreminjanje parametrov oddajnika, komunikacijskih poti),
2. pasivne elektronske zaščitne ukrepe; to so prikriti ukrepi za nemoteno uporabo EMS, ki jih je težje zaznati in so veliko odvisne od tehnične prednosti na področju elektrotehnike in optike (tehnične značilnosti opreme, načini dela).

Elektronski zaščitni ukrepi so aktivnost EB, ki vključuje tako pasivne kot aktivne ukrepe in postopke, ki jih izvajamo za zaščito lastnih tehničnih sredstev in KIS, preprečitev nevtraliziranja ali uničenja lastnih enot, objektov, opreme. So skupek organizacijskih, operativno-taktičnih ukrepov in postopkov, ki so pogosto spregledani in premalo upoštevani. Elektronske zaščitne ukrepe izvajajo vsa poveljstva, enote in zavodi Slovenske vojske skladno

z načeli bojnega delovanja in značilnostmi bojnih sistemov, ki so v njihovi sestavi, ter z zaščito lastnih elektronskih sredstev pred nasprotnikovim EI in EB. Glavna zaščita proti EB je predvsem izogibanje, da bi nas nasprotnik izsledil, kar večinoma sicer ni mogoče, vendar pa se signali majhnih moči na bojišču, prenasičenim s signali »izgubijo« in jih je zato težje odkriti. Če nasprotnik ni sposoben identificirati KIS v doglednem času ali pa ni pridobil dovolj podatkov, na katerih bi to mrežo določil kot obveščevalno zanimivo, se mu tudi uporaba PUEB ne bo zdela smiselna. Pri načrtovanju mora biti poudarek na preventivnih EZU, pri tem pa je potrebno upoštevati, da ima nasprotnik prav tako sredstva in znanje, s katerimi nam bo poskušal preprečiti uporabo EM spektra. Prav tako je treba EZU uporabljati neprestano, tako v miru in vojni, saj je potrebno predvidevati, da nasprotnik nenehno prestreza naše KIS. Sposobnost preživetja elektronskega napada in učinkovite ter varne rabe KIS je najbolj odvisna od nas, naše usposobljenosti in uporabe EZU.

Defenzivni ukrepi se ponavadi izvajajo v dveh delih:

1. preprečitev nasprotnikovih PUEB,
2. preprečitev EPU (Golob in drugi 2006, 25).

Slika 4.2: Delitev elektronskih zaščitnih ukrepov glede na način izvajanja

Vir: Golob in drugi (2006, 26).

Zelo pomembno je, da v razmerah EB dosledno upoštevamo načela EZU. Pomembno je predvsem hitro vzpostavljanje in prekinjanje zveze ter kratko zadrževanje na njej. Pri tem nam pomagajo že vnaprej pripravljeni načrti, ki jih pripravimo s pomočjo znanih parametrov o lokaciji, delovnih frekvencah, kombinacijah anten in sprejemnikov. Med priprave sodi tudi

meritev razprostiranja EM valovanja v vseh vremenskih razmerah in z različno uporabo sredstev zvez. Vnaprej predvidimo konfiguracijo KIS, zahteve uporabnikov in organizacijo dostopnih točk. V tem delu štabni organ v sodelovanju z organom S-3 opravi tudi frekvenčno načrtovanje, in sicer spisek delovnih frekvenc, seznam klicnih simbolov, menjavo delovnih frekvenc in klicnih simbolov. Rezultat teh priprav je »paket« podatkov, ki obsegajo naslednje informacije:

- lokacije in njihove koordinate,
- azimute in polarizacije anten,
- delovne frekvence, modulacije, spremembe frekvenc (redne, izredne),
- operativne čase za posamezne dele,
- konfiguracijo komunikacijskega omrežja (Golob in drugi 2006, 26).

4.4.1 Temeljni zaščitni ukrepi

Prvi zaščitni ukrep je vedno minimalna in preudarna raba sredstev, ki oddajajo EM sevanje. Tako nasprotniku otežimo uporabo PUEB, s katerimi bi pridobil koristne podatke o stanju in namenih naših enot in ki bi mu koristili pri načrtovanju ukrepov EB proti našim silam. S tehničnega vidika morajo biti ukrepi elektronske zaščite uvedeni šele, ko je vpeljana in pregledana vsa strojna in programska oprema in ko poznamo njene pomanjkljivosti. Potreba po takojšnjem varnem prenosu podatku določa uporabo samodejnih zaščitenih KIS. S takimi sistemi so omogočeni učinkovito izvajanje ukrepov EB, ažurno posredovanje podatkov in največja mogoča stopnja zaščite. Pred uporabo katerega koli sistema moramo vedno imeti pripravljen rezervne oz. alternativne načine komuniciranja, kajti na voljo moramo imeti toliko različnih komunikacijskih poti, da izguba ali prekinitev posamezne zveze ne oslabi zmožnosti celotnega KIS. Tako je potrebno določiti prednostno lestvico alternativnih načinov komunikacije (vrstni red: kurirska, žična, signalna, radiorelejna, radijska zveza). Kakovostnejše izvajanje EZU dosegamo z nenehnim usposabljanjem uporabnikov in nadziranjem uporabe EM spektra. Vsi uporabniki in načrtovalci KIS morajo imeti splošno znanje o elektronskih sistemih in komponentah, njihovem delovanju, ogroženosti in ranljivosti ter uporabi v razmerah EB. Skrbna uporaba KIS zmanjša možnost detekcije in izniči natančnost in učinkovitost nasprotnikovega delovanja. Vsak uporabnik mora znati oceniti, kdaj je komunikacija motena in kako ob tem ukrepati. Prvi pokazatelj nasprotnikovega motenja je večja interferenca pri sprejemu. Ali gre za elektronsko motenje, ugotovimo, tako da najprej izklopimo anteno iz sprejemnika. Če motnja izgine, je izvor motnje zunanji, če pa ostane, gre najverjetneje za napako sprejemnika oziroma KIS. Če ugotovimo, da se zunanja motnja pojavlja ob poskusih vzpostavitve komunikacije ali prenosu sporočil, gre za nasprotnikovo motenje, kar naprej javimo nadrejenemu poveljstvu oziroma upravni postaji.

Komunikacijo nadaljujemo z nujnimi spremembami v nastavitvah sprejemnika, s čimer se poskusimo izogniti vplivom motenja. Nikakor ne prenehamo dela, saj nasprotnik ne sme izvedeti, kakšna je učinkovitost njegovih EPU. Če se elektronsko motenje nadaljuje, lahko poskusimo spremeniti lokacijo antene, povečati moč oddajanja ali zamenjati frekvenco. V vsakem primeru naj vsaj dva udeleženca ostaneta na isti frekvenci in še naprej simulirata obstoječo komunikacijsko mrežo ter tako prepričata nasprotnika, da so njegovi poskusi elektronskega motenja neuspešni. Tako bo ta nadaljeval motenje na isti frekvenci in nesmotrno izrabljal svoja tehnična sredstva za EPU (Golob in drugi 2006, 27).

Najpogostejša metoda zaščite pred motenjem je frekvenčno skakanje (frequency hopping). To je metoda, pri kateri prenosi podatkov potekajo po kanalu, ki naključno skače prek širšega frekvenčnega področja, zato mora biti vsa razpoložljiva sevalna moč nasprotnikovega sistema za elektronsko motenje porazdeljena po vsem uporabljenem frekvenčnem področju. Posledica tega je opazno zmanjšanje motilne moči (širši pas/manjša moč motilnika). Učinkovitejši način elektronskega motenja takšne zveze je mogoč le z napravami za elektronsko motenje, ki lahko spremljajo spremembo frekvence (Golob in drugi 2006, 27).

Naslednja metoda je elektronsko maskiranje s pomočjo terena. Je zelo uporaben ukrep na razgibanem terenu ali v urbanem okolju. Je lahko izvedljiv in pripomore k zmanjšanju občutljivosti KIS na nasprotnikove PUEB in EPU. Oddajno anteno postavimo, tako da je med njo in nasprotnikom naravna ali umetna ovira, torej stavba, vzpetina, nasip. To pripomore k zmanjšanju širjenja EM valovanja k nasprotniku. Tako mu otežimo pridobivanje informacij, elektronsko motenje in zavajanje (Golob in drugi 2006, 28).

»Ena od metod je tudi metoda maskiranja s pomočjo aktivnih frekvenc, na primer frekvenc radijskih postaj. S pomočjo signala radijske postaje, ki je usmerjen proti nasprotniku in oddaja na isti frekvenci, kot je naša, maskiramo svojo komunikacijo, saj je zaradi prekrivanja EM valovanja obeh signalov v smeri nasprotniku sprejem signala otežen« (Golob in drugi 2006, 28).

»Potem imamo še paketni prenos podatkov, kjer kratka sporočila pretvorimo v digitalno obliko in jih v obliki paketov prenesemo po običajni komunikacijski poti. Tako je čas prenosa bistveno krajši, krajši pa je tudi čas, ki ga ima nasprotnik na voljo za izvajanje PUEB in EPU« (Golob in drugi 2006, 28).

Elektronskemu zavajanju se lahko učinkovito izognemo z legitimiranjem uporabnikov KIS. Če uporabnik z legitimiranjem ne dokaže svoje identitete oziroma potrebuje za postopek preveč časa, lahko predvidevamo da gre za poskus zavajanja. Za prepoznavanje zavajanja

> morajo biti vsi operaterji usposobljeni, pri uporabi zvez pa disciplinirani. Zelo pomembni so tudi izkušnje in medsebojno poznavanje uporabnikov. Vsak uporabnik mora ob sumu zavajanja obvestiti vse udeležence v komunikacijski mreži. Za preprosto izogibanje elektronskemu zavajanju veljajo enaki ukrepi kot pri elektronskemu motenju, vendar je bolj priporočljivo spoznanje o poskusih zavajanja izkoristiti dezinformiranje nasprotnika. Vedno se je potrebno zavedati, da je nasprotnikovo zavajanje mogoče premagati. Uspešnost naših poskusov je najbolj odvisna od naših priprav, usposobljenost porabnikov in njihovih izkušenj, kar pomeni, da je treba v vsako usposabljanje za uporabo zvez v razmerah EB nujno vključiti tudi usposabljanje o EZU (Golob in drugi 2006, 28).

V poglavju elektronskih zaščitnih ukrepov bi rad razložil nekatere možnosti pri poimenovanju tovrstnih elektronskih ukrepov. Zelo zanimivo je namreč poimenovanje elektronskih zaščitnih ukrepov leta 2001, kjer avtor članka, elektronske zaščitne ukrepe poimenuje kot »anti-ECM, Electronic Counter-Counter Meausers« (Streetly 2001). To poimenovanje lahko razumemo kot zaščito, pri čemer se izvaja preventivni napad na nasprotnikovo uporabo in naprave, ki so odvisne od EMS. Čeprav je ta izraz že nekoliko star in je sedaj v uporabi novejši termin »Electronic protection« (Department of the army 2009, 5) nam starejši izraz lahko pove, kakšna je naravnanost oziroma doktrinarna usmerjenost delovanja elektronskega bojevanja, po naravi torej ofenzivna. S to usmerjenostjo se v celoti strinjam, ker le z nenehnim nadzorom EMS lahko uspešno zavarujemo lastne interese po uporabi EMS, ker le tako lahko izvajamo obveščevalne aktivnosti, ki so nujno potrebne za načrtovanje in pripravo bojnega delovanja, ker le tako lahko izvajamo vse vrste elektronskih ukrepov in nazadnje le tako lahko pridobimo informacijsko prednost pred nasprotnikovim uporabo in delovanjem v EMS.

4.5 Pogoji za učinkovitost elektronskih ukrepov

Učinkovitost sistemov elektronskih ukrepov je odvisna od več faktorjev. Kar se tiče človeškega faktorja je odvisna od pravilne izbire in izvedbe elektronskih ukrepov ter pravilne uporabe sistemov za izvajanje elektronskih ukrepov. Zelo pomemben pa je tudi tehnični vidik, ki vpliva na učinkovitost elektronskih ukrepov.

Zelo pomembna je pravilna uporaba in pravilna izvedba elektronskih ukrepov. Da bi bili uspešnejši je potrebno določiti cilj oziroma kaj želimo doseči. Ta podatek nam pove katero vrsto elektronskih ukrepov ali paket elektronskih ukrepov bomo uporabili. Učni proces in urjenje operaterjev elektronskega bojevanja nam zagotavlja utečene procese aktivnosti, ki vpliva na pravilnost izvedbe in pravilnost uporabe. Pravilna izbira in pravilnost izvedbe

elektronskih ukrepov v soodvisnosti od pravilne uporabe nam da največji učinek elektronskega ukrepa ali paket elektronskih ukrepov. Upoštevati je namreč potrebno, da nepravilna izraba elektronskih ukrepov lahko poslabša situacijo v kateri deluje in posledično preda iniciativo nasprotniku, da lahko še bolj izrablja EMS. Včasih je potreben premislek o tem od katerega elektronskega ukrepa bomo imeli večjo korist, kar se bo odrazilo v prihodnji učinkovitosti elektronskega bojevanja in pa o lastnem izkoriščanju EMS. Kajti lahko se zgodi, da z nepremišljeno uporabo elektronskih ukrepov onesposobimo lastno delovanje in izrabo EMS. Pomembno pa je tudi nenehno usposabljanje porabnikov EMS, kar omogoča izkušnje ter sprejemanje pravilnih odločitev, ki vodijo v pravilno uporabo in zaščito lastne izrabe EMS.

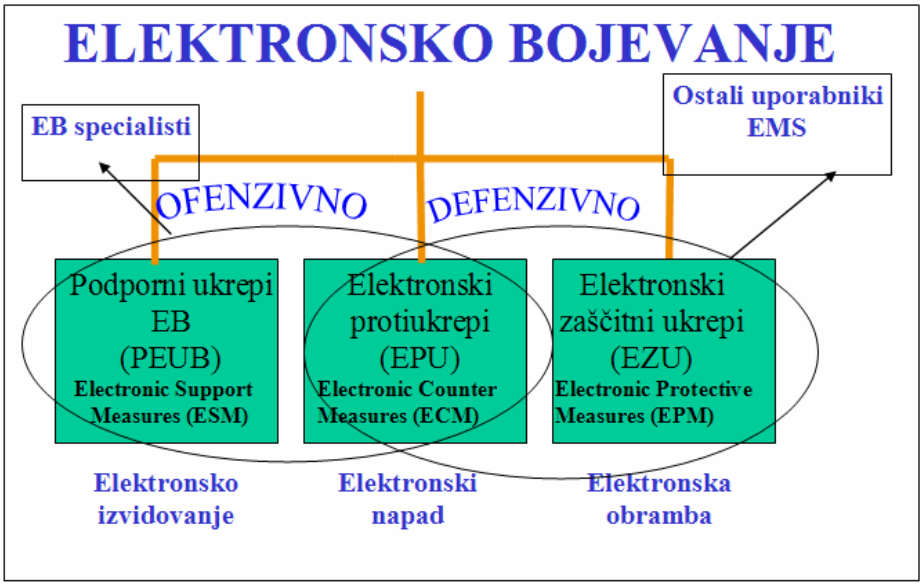
Tehnični vidik se kaže predvsem v tehnološki superiornosti in kompatibilnosti sistemov za elektronsko bojevanje. Tehnološki razvoj elektrotehnike in optoelektronike namreč narekuje trend razvoja sodobnih sistemov za elektronsko bojevanje. Učinkovitost elektronskih ukrepov povečamo tudi z bolj naprednimi, močnejšimi in predvsem natančnimi sistemi za izvajanje elektronskih ukrepov, kar omogoča tehnološki razvoj na področju računalništva (zmogljivejši procesorji, povečana hitrost branja podatkov, programska oprema, hladilni sistemi). Pomembna je predvsem digitalizacija sistemov, kar omogoča hitrejšo zaznavo dogajanja v EMS in EMOk. Tehnološka prednost nam omogoča prednost v izrabi in nadzoru EMS, postanemo tudi bolj imuni na nasprotnikove elektronske ukrepe. Kompatibilnost in modularnost sistemov pa nam omogoča še širšo uporabo elektronskih ukrepov, mišljeno na uporabljene platforme ter povezljivosti sistemov samih, kjer se na platformi upravlja z različnimi sistemi, ki združujejo vse tri vrste elektronskih ukrepov.

4.6 Klasifikacija elektronskih ukrepov

Elektronske ukrepe v osnovni delitvi delimo na tri vrste: torej podporne ukrepe elektronskega bojevanja, elektronske protiukrepe in elektronske zaščitne ukrepe. V tem poglavju bom razdelil te ukrepe glede na vrsto oziroma način aktivnosti. Razdelil jih bom na ofenzivne in defenzivne ukrepe oziroma aktivnosti. Že sam termin ofenzivnost nam pove, da gre za napadalno aktivnost, defenzivna aktivnost pa izraža obrambno aktivnost. V primeru elektronskega bojevanja prihaja do prepletanja elektronskih ukrepov. Vsak od ukrepov namreč dovoljuje in omogoča delovanje naslednjega. Tako so elektronski protiukrepi del ofenzivne oblike delovanja, kjer z aktivnimi metodami onemogočamo uporabo in delovanje v EMS. Podporni ukrepi elektronskega bojevanja spadajo med ofenzivne in defenzivne aktivnosti, kajti s to obliko aktivno ščitimo lastne sile, ko jih svarimo pred morebitno

nevarnostjo in pa ofenzivno kjer z aktivnimi metodami preiskujejo EMS in iščejo in določajo lokacijo nasprotnikovih ciljev in njihovo uporabo in delovanje v EMS. Zaščitni elektronski ukrepi spadajo med defenzivne aktivnosti, s pomočjo katerih zavarujemo lastno delovanje EM naprav, uporabo in neprekinjeno delovanje v EMS. V primerjavi z zavezniško doktrino (mišljeno ZDA), je uporaba vseh elektronskih ukrepov mišljena kot možna oblika preventivnega napada, zato so vsi elektronski ukrepi naravnani ofenzivno, kjer so sami zaščitni elektronski ukrepi aktivni in že s samo ofenzivno obrambo ne dovoljujejo elektronskega napada na lastne sile.

Slika 4.3: Klasifikacija elektronskih ukrepov glede na aktivnost



Vir: Berginc (2008, 13).

4.6.1 Primerjava elektronskih ukrepov z zavezniškimi silami

Elektronski ukrepi, ki jih izvajajo enote elektronskega bojevanja SV in zavezniške enote elektronskega bojevanja, so si med seboj podobni, vendar kljub temu obstaja nekaj razlik. Ena takšnih razlik je usmerjenost elektronskega bojevanja, kjer zavezniške sile delujejo na preventivnem napadu in so sami ukrepi in metode ofenzivno usmerjene, pri nas pa se razvoj dogodkov ni razvijal v to smer. Elektronski ukrep so defenzivne narave (zaščita pred RV IES), nadzor EMS je bolj mešanica pasivnega in aktivnega spremljanja EMS, vendar bi se v primeru nevarnosti aktivirale vse skupine elektronskega bojevanja. Ena od razlik se kaže tudi v uporabi naprav za elektronsko nevtralizacijo, ki jih naše sile ne posedujejo, vendar jih priznavajo kot aktivnost elektronskih protiukrepov. Potrebno je omeniti, da so načeloma vse metode skoraj identične zavezniškim, pri čemer nam manjkajo le bolj agresivne metode

elektronskih protiukrepov. Med tem ko zavezniške sile posedujejo takšne oborožitvene sisteme, s katerimi se uničuje ali delno poškoduje EM naprave ali pa naprave, ki izrabljajo in delujejo EMS, enote za elektronsko bojevanje SV takšnih oborožitvenih sistemov nimajo. Potrebno je razumeti, da sta obe doktrini pisani na drugačnih izkušnjah. Po pregledu literature sem dobil občutek, da je elektronsko bojevanje bolj razvito pri zavezniških vojskah, kot pa pri nas, kjer je prišlo do pozitivnega premika, ampak zaradi večjih potreb in nuje v zavezniških silah, se je razvilo elektronsko bojevanje v eno ključnih vojaških podpornih bojnih aktivnosti. Ukrepi, metode in način uporabe so bolj natančno zapisane v zavezniški doktrini ZDA FM 3-39 iz leta 2009, kjer so zapisani tudi vsi postopki v operacijah kriznega odzivanja in njihova razčlenitev.

Pri podpornih ukrepih elektronskega bojevanja in elektronskih zaščitnih ukrepov ne prihaja do razlik v metodah, zato ker kljub temu, da so v zavezniških silah razumljene kot ofenzivne aktivnosti, so kljub vsemu to obveščevalne aktivnosti, ki so identične tistim, ki jih uporabljajo naše enote za elektronske bojevanje.

5 SISTEMATIZACIJA SODOBNIH SISTEMOV ZA EB

V tem poglavju bom predstavil sisteme in njihovo sistemizacijo. Uporabil bom že predhodno sistematizacijo, ker se mi zdi za to raven poznavanja najboljša možna oblika predstavitve. V nadaljevanju so še predstavljeni nekateri pojmi, ki so za samo razumevanje zelo pomembni.

> Sistemi za EB so se skozi zgodovino razvijali bistveno počasneje, kot to poteka v zadnjih nekaj letih – namen in cilji pa ostajajo isti, in to je imeti nadzor na uporabo EMS - nasprotniku preprečiti ali onemogočiti uporabo EMS ter s tem zagotoviti varno in učinkovito uporabo lastnih komunikacijsko informacijskih (računalniške povezave, komunikacijske povezave, senzorji) ter ne- komunikacijskih sredstev (NKS) (radarji, GPS) - ostalim enotam omogočiti varno izvajanje namenskih nalog. Vsaka tehnologija, ki je v uporabi na komercialnem trgu ali boju, od računalniških čipov, brezžičnih omrežij do digitalnih radarjev, je odvisna od komponent, ki delujejo v specifičnem področju EMS. Težava je v tem, da je EMS en sam – ne da si ga lastiti je pa mogoče imeti prevlado v EMS. Nasprotnik spoznava vedno nove načine apliciranja komercialnih tehnologij s ciljem napredka v njegovih vojaških zmogljivosti – predstavlja dodaten pritisk na razvijanje in uporabo novih tehnologij (Golob 2009a, 7).

5.1 Delitev in karakterizacija sodobnih sistemov za EB

Kaj sploh je sistem?

Definicij in razlag je kar nekaj, izpostavil pa bom najboljšo in sicer tisto, ki najbolj ustreza nadaljevanju poglavja – »sistem je celovitost urejene in omejene množice elementov, med katerimi obstajajo odnosi ali pa jih je mogoče vzpostaviti. Odnosi označujejo zveze, odvisnosti in vplive med elementi sistema ali okolja« (Kljajič v Golob 2009a, 7).

Sistem za elektronsko bojevanje predstavlja informacijsko močno podprt sklop oborožitvenih podsistemov - tehničnih sredstev za EB - in lahko deluje samostojno kot celota ali pa (predvsem to) je povezan v oborožitveni sistem, ki omogoča upravljanje na mestu samem ali z določenega prostora (daljinsko) (povzeto po Golob 2009a, 7) .

5.2 Delitev sodobnih sistemov za EB

Sodobne sisteme za elektronsko bojevanje lahko gledamo z različnih vidikov – podsistemov in sistemov, ki bodo prikazani v nadaljevanju, kjer se zopet navezujem na terminologijo predhodnikov in njihovo razdelitev, ker se mi zdi popolnoma smiselna.

> Primarna delitev sodobnih sistemov za EB je v naravi delovanja, in sicer na pasivne in aktivne. Osnovna razlika med navedenima je v tem, da v primeru pasivnega delovanja s sistemi za EB sprejemamo EME, ki jo oddajajo ciljna komunikacijska ali nekomunikacijskih sistemov (NKS) (izvajamo element EB, elektronski nadzor, s ciljem pridobivanja podatkov in informacij o nasprotniku), med tem ko v primeru aktivnega delovanja s sistemi EB oddajamo EME proti ciljnim komunikacijskim in NKS (izvajamo element EB, elektronski napad – elektronsko motenje ali elektronsko zavajanje, s ciljem onemogočiti ali otežiti njih uporabo). Sodobni sistemi za EB se v odvisnosti od posameznih sklopov sistema uporabljajo za določena frekvenčna področja in so vedno prilagojeni frekvenčnem področju ciljne skupine. Posledično različnim frekvenčnim področjem, se razlikuje tudi globina delovanja sodobnih sistemov EB (od nekaj 100m do nekaj 1000km). Ločimo predvsem naslednja aktualna frekvenčna področja: HF (1MHz do 30 MHz), VHF (30 MHz do 300 MHz), UHF (300 MHz do 3 GHz), SHF (3 GHz do 300 GHz). V navedenih frekvenčnih področjih se nahaja vrsta komunikacijskih in NKS, ki (lahko) predstavljajo grožnjo, slabost oz. težava pa je pogosto v tem, da se področje civilne in vojaške uporabe (pre)pogosto prepletata. Sodobni sistemi za EB se lahko uporabljajo v vseh prostorskih komponentah bojevanja, in sicer kopno, zrak, vesolje, morje (pod in nad morsko gladino) (Golob 2009a, 8–9).

»Vezano na prostorsko komponento bojevanja, se sodobni sistemi za EB lahko uporabljajo na različnih platformah, kot npr. prenosni, vozila, letala, helikopterji, brezpilotna letala, ladje, podmornice in konec koncev tudi sateliti« (Golob 2009a, 9).

»Sodobni sistemi za EB se v osnovnem načelu z vidika mobilnosti praktično vedno uporabljajo kot mobilni sistemi. Z razliko od izvajanja nalog v okviru Republike Slovenije (usposabljanje enot SV) se sodobni sistemi za EB (v OKO) lahko uporabljajo tudi v stacionarni izvedbi (konzola v objektu), v kolikor to omogoča učinkovitost izvedbe oz. »optična vidljivost« nasprotnika« (Golob 2009a, 9).

5.3 Karakterizacija sodobnih sistemov za EB

Tehnična sredstva, ki jih uporabljajo operaterji elektronskega bojevanja, se ločijo po namenu, zakaj in kako se jih uporablja in kateri elektronski ukrep izvajajo. Vsak elektronski ukrep namreč različno izrablja dogajanje v EMS, skupne so jim odvisnost od EMS in sprejemanje in oddajanje EM valov, signalov (energije). Sistemi se namreč karakterno močno razlikujejo, (zato je poleg sistema pripisan še elektronski ukrep, ki je zanj še posebej značilen), podsistemi pa so naslednji:

Tabela 5.1: Podsistemi elektronskih tehničnih sredstev

Podsistemi elektronskih tehničnih sredstev	**Opis podsistema**	**Vrsta elektronskega ukrepa**
Sprejemniki	*Sprejemniki so osnovno sredstvo za izvajanje pasivnih ukrepov EB, v okviru kateri izvajajo iskanje, prestrezanje, identifikacijo, spremljanje EME. Sprejemniki delujejo v določenem frekvenčnem področju, bistvena značilnost pa je, da so sodobni sprejemniki izredno hitri (prestrezanje signala v nekaj mikro sekundah) . Sprejemniki morajo biti izredno občutljivi, sposobni prestrezanja zelo šibkih signalov. Sprejemnike lahko upravljamo ročno (preko sprednje plošče), s programsko podporo – dvojnost uporabe je nujna, saj v primeru izpada ali težav s programsko opremo le - ta lahko postane neuporaben ali pa (kar je tudi trend)*	- podporni ukrepi elektronskega bojevanja

	daljinsko. Sprejemniki morajo biti sposobni prestrezanja t.i. »hooping signalov« - zelo hitra menjava oddajne frekvence, kar naj bi otežilo prestrezanje	
Motilci EMS	*Motilci EMS so osnovno sredstvo za izvajanje aktivnih ukrepov EB, v okviru katerih izvajajo elektronsko motenje ali/in elektronsko zavajanje. Motilci EMS delujejo v določenem frekvenčnem področju, z različnimi oddajnimi močmi, bistvena značilnost pa je, da so sodobni motilci EMS integrirani s sprejemniki, saj je osnovni predpogoj za izvajanje E napada predhodna detekcija tarče. Motilci EMS morajo biti zmogljivi izvajanja naprednih obliki E napada (različnih obliki elektronskega motenja/zavajanja. Konstruirani so v različnih dimenzijah, kar je vzročno povezano z namenom – npr. za zaščito baze, za zaščito vozila (posadke), za zaščito posameznika*	- elektronski protiukrepi
Spektralni analizatorji	*Spektralni analizatorji so osnovno sredstvo za analizo EMS s ciljem prikaza (selekcioniran ozkopasoven do širokopasoven pregled frekvenčnega spektra), selekcije, obdelave (meritve, de-moduliranje, dekodiranje) kompleksnih signalov. Delujejo v različnih frekvenčnih področjih, po principu »on – line« ali »off – line«, statično ali daljinsko, tudi v prenosni »man – pack« verziji*	- podporni ukrepi elektronskega bojevanja
Goniometri	*Goniometri so osnovno sredstvo za določanje izvora oddajnika (spremljanega signala) na (zelo širokem) področju 300 Hz do 3GHz. Goniometrski sistem zajema anteno,*	- podporni ukrepi elektronskega bojevanja

	sprejemnik in strojno opremo. Določanje izvora (lokacije na V/UHF področju) bazira na principu triangulacije (potrebujemo vsaj 3 goniometerske sisteme za določitev presečišča posameznih smeri), na področju HF pa se lahko izvor določi z enim samim goniometrom (regulirano s pogoji v ionosferi). Goniometri so lahko stacionarni ali mobilni (samostojni ali kot del integriranega sistema) – v obeh primerih tudi daljinsko krmiljeni	
Antenski sistemi	*Antenski sistemi so osnovno sredstvo (kot izhodni element) za sprejemanje ali oddajanje EME. Antenski sistemi so različnih oblik, delujejo na različnih frekvenčnih področjih (ozkopasovni, širokopasovni), usmerjeni ali neusmerjeni, nameščeni na antenskih stolpih (objekti, različne platforme), preko vodnikov povezanih na krmilne naprave, ki omogočajo rotiranje le-teh po azimutu ali elevaciji (tudi daljinsko). Področju, kjer so postavljeni antenski sistemi, pravimo antensko polje*	- vsi trije elektronski ukrepi
Delovne postaje	*Delovne postaje (strojna oprema) predstavljajo specifične računalniške sisteme, prilagojene delovnim razmeram, zahtevnih konfiguracij, saj to predstavlja osnovo za krmiljenje (tudi daljinsko) posameznih segmentov sistema. V terenskih razmerah se uporabljajo t.i. »military« prenosni računalniki, odporni na tresljaje, vlago, vodo, blato, pesek, ...*	- vsi trije elektronski ukrepi
Programska oprema	*Učinkovitost delovanja sodobnih sistemov za EB je močno pogojena z ustrezno programsko opremo, aplikativnimi rešitvami, ki*	- vsi trije elektronski ukrepi

	omogočajo: obdelavo in analizo (selekcija, klasifikacija, filtriranje), dekodiranje, demoduliranje in dešifriranje, selekcioniranje po ključnih besedah in barvi glasu, ipd	
Snemalni sistemi	*Snemalni sistemi imajo dvojno vlogo – snemanje širokopasovnih digitalnih signalov namenjenih za nadaljnjo analizo (v kombinaciji z vektorskim analizatorjem je npr. mogoče identificirati frekvence, ki jih uporablja sredstvo zvez v načinu frekvenčnega skakanja), druga vloga snemalnih sistemov pa je v hranjenju enormnih količin zvočnih zapisov za nadaljnjo analizo*	- podporni ukrepi elektronskega bojevanja - elektronski protiukrepi
Komunikacijski sistemi	*Komunikacijski sistemi (ustrezno zaščiten in širokopasoven) za komuniciranje z nadrejenim in podrejenimi ter daljinsko krmiljenje sistema. Stopnja zaščite komunikacijskih poti mora biti najvišjih stopenj tajnosti, t.j. strogo tajno (po nacionalni zakonodaji) v NATO pa CTS-B (cosmic top secret – bohemia). Vzrok navedenemu izhaja iz specifičnosti in pomembnosti podatkov*	- elektronski zaščitni ukrepi
Elektronski nevtralizatorji	*Elektronski nevtralizatorji so oborožitveni sistemi, ki z uporabo usmerjene EM energije in EM pulza uničujejo ali delno trajno poškodujejo EM naprave in EM sredstva, ki delujejo v EMS (radarji, optoelektronske naprave, termične naprave, sredstva zvez in poveljevanja (C2 in sodobnejši)*	- elektronski protiukrepi

Vir: Golob (2009, 9–11).

5.4 Lastnosti in kazalci sistemov

Operativne sposobnosti zelo pomembne pri opravljanju nalog elektronskega bojevanja. Operativno izvajanje elektronskega bojevanja ni zagotovljeno (v kolikor ne gre za mobilne sisteme za elektronsko bojevanje) brez ustreznih platform, ki morajo biti prostorsko in funkcionalno prilagojena (2-3 delovni mesti). Vozila s sistemi za elektronsko bojevanje se delijo na kolesnike (4 x 4, 6 x 6, 8 x 8) in goseničarje, ki so prilagojena geografskemu področju delovanja (povzeto po Golob 2009a, 11). Trend uporabe je bil takšen, da je prenesel sisteme za elektronsko bojevanje v zračno ter pomorsko komponento, s katerim so povečali območje delovanja oziroma učinka elektronskega bojevanja.

Element operativne sposobnosti z vidika funkcionalnosti ni dovolj, sistemi za elektronsko bojevanje morajo doseči standarde NATO (prilagajanje tehnike ektremnim razmeram, ki so odraz vremenskih vplivov na EMS, popačenost), katerim smo priča na severu Evrope - mraz, Bližnji vzhod - puščava oziroma Afrika - tropsko okolje) (povzeto po Golob 2009a, 11). Zato morajo imeti sodobni sistemi naslednje lastnosti:

- zanesljivost,
- učinkovitost,
- robustnost,
- enostavnost in varnost uporabe,
- primerljivost in interoperabilnost z ostalimi NATO članicami,
- ekonomičnost,
- sistemi morajo biti med seboj združljivi ter povezani s pomočjo širokopasovnih in ustrezno zaščitenih komunikacijsko informacijskih sistemov (KIS) (krmiljenje, prenos podatkov, skupne podatkovne baze, …) v več smereh (RS – OKO, na OKO in v RS),
- možnost avtomatskega načina dela na čim več segmentih delovanja sistema,
- čim večji del sodobnih sistemov za EB mora biti grajen modularno, z možnostjo hitrega premeščanja tehničnih sredstev za EB med različnimi nosilnimi platformami,
- tehnična sredstva, namenjena delovanju tudi v mobilnih platformah, morajo izpolnjevati tudi ustrezne standarde za delovanje v zahtevnejših pogojih (glede na pogoje delovanja v posameznih mobilnih platformah) ter standarde za delovanje v specifičnih mobilnih platformah (npr. standarde za delovanje v zračnih ali vodnih plovilih),
- tehnična sledljivosti izvajanja nalog (gre za element, ki je izredno pomemben, in je vezan na nadzorno funkcijo – v vsakem trenutku mora biti jasno določljivo, kateri delovni kanali so bili v določenem časovnem obdobju v obdelavi) (Golob 2009a, 11–12).

5.5 Vloga sodobnih sistemov za EB pri izvajanju nalog v okviru OKO

Osnovna naloga delovanja sistemov EB v okviru operacij kriznega odzivanja (v nadaljevanju OKO) je zagotavljanje pogojev enotam na terenu za varno in učinkovito izvajanje namenskih nalog – skozi zagotavljanje verodostojnih, ažurnih in pravočasnih obveščevalnih podatkov in informacij o nasprotniku (grožnji) ter onemogočanje ali oteževanje uporabe EMS (povzeto po Golob 2009a, 14).

Sodobni sistemi za elektronsko bojevanje se kljub majhni razliki v priemrjavi z nalogami doma se pri izvrševanju nalog v okviru OKO prilagajajo:

- taktiki delovanja lastnih enot in združenih enot katero podpirajo ter skupni taktiki,
- terenskim razmeram (verjetna uporaba prenosnih kompletov),
- lokalnim grožnjam (frekvenčnem področju – GSM, SATKOM, ipd.),
- komponenti delovanja-čas (nekaj ur, nekaj dni),
- velikosti skupin za elektronsko bojevanje,
- komunikacijsko informacijski infrastrukturi za prenos vseh vrst podatkov,
- ter, kar bo v bližnji prihodnosti bistvenega pomena, interoperabilnosti (v tehničnem in aplikativnem smislu – analitična orodja, podatkovne baze) (povzeto po Golob, 2009a, 14).

»Elektronski napad, kot element zaščite sil, je z razliko od elektronskega nadzora »vidna« aktivnost, tako v smislu sprememb v EMS kakor tudi fizično (antenski sistemi na vozilu) in zaradi tega tudi bistveno bolj ranljiv segment – tudi za lastne in prijateljske sile, saj lahko »tehnična težava« vodi (najmanj) v omejitve delovanja elektronskih sredstev, v najhujšem primeru pa žrtve« (Golob 2009a, 14).

Zavezništvo NATO in naše obveznosti do zavezništva nas vodita v skupno sodelovanje na področju kolektivne obrambe. Lastne sile se morajo znati prestrukturirati v že naprej znane vzorce struktur NATO-a. Združene sile (Joint forces, štabna oznaka služb J-2, J-3, J-6) so sile sestavljene iz več nacionalnih oboroženih sil za skupno sodelovanje na operacijah kriznega odzivanja. Skupne enote sestavljajo tudi enote za elektronsko bojevanje (Electronic warfare units), ki pa morajo znati, zaradi uporabljene različne tehnologije in metod dela in aktivnosti, mednacionalno sodelovati med seboj. To pomeni ustvarjanje novih kanalov obveščevalnega ciklusa, novih filtrov, novih komunikacijskih poti ter močne kompatibilnosti elektronske opreme, kajti če se oprem na doktrinarne dokumente ZDA in posledično NATO-ve

dokumente, spoznam, da je veliko težišče elektronskega bojevanja prevzelo vojno letalstvo ZDA v vseh svojih komponentah, kar pomeni ogromno prilagajanje programske opreme, elektronskih sistemov, načina dela s strani zavezništva oziroma širših zaveznikov znotraj NATO-a.

6 SODOBNO BOJIŠČE 21. STOLETJA

6.1 Odraz tehnologije in asimetričnega bojevanja

Situacije in grožnje, s katerimi se srečujejo vojaki na modernem bojišču, niso več takšne kot so bile nekoč. Vojaška in nevojaška oprema se je razvila do te mere, da je nasprotnik postal optično neviden, kar pa še en pomeni, da ga ni. Največja grožnja in varnostni izziv na sodobnem bojišču je postala uporaba improviziranih eksplozivnih sredstev, katera so radijsko prožena. In ravno zaradi uporabe radijskih valov, sovražnik postane viden. Ker so radijski valovi del elektromagnetnega spektra, postanejo vidni enotam elektronskega bojevanja, ki nenehno skenirajo elektromagnetni spekter (EMS) v operativni coni delovanja. Poleg IES je potrebno razumeti in kot grožnjo šteti tudi nenehno nasprotnikovo uporabo elektronskih oborožitvenih sistemov za nadzor, oborožitvenih sistemov poveljevanja in kontrole in ne le spremljanje komunikacijskega toka in na njem izvajati elektronsko izvidovanje in bojevanje.

Prve uporabe improviziranih eksplozivnih sredstev segajo že nekaj desetletij v zgodovino, vendar do takšne masovne uporabe IES je prišlo šele v zadnjih nekaj letih, odkar je postalo uničevalno orožje številka ena, še posebej v operacijah kriznega odzivanja (OKO), kjer sama optična nevidnost, poleg uničevalne moči, predstavlja nov način psihološkega bojevanja. Predstavlja nov način asimetričnega bojevanja. Oborožene sile sprva niso bile pripravljene na tak način bojevanja, kar se je odrazilo v številu žrtev IES. Povečanje žrtev je sililo vojske, da se uspešno spoprimejo z novo obliko grožnje. Z nenehnim izpopolnjevanjem znanja o IES in pridobljenih obveščevalnih podatkih, o načinu in vrstah proženja IES, uporabi frekvenc radijsko vodenih IES (RV IES), o sami napravi IES, ki ji predstavlja omejitev le domišljija, trg elektronskih naprav in z njo tehnične značilnosti in omejitve uporabe. Veliko vlogo pri odkrivanju groženj in nevtralizaciji le teh ima elektronsko izvidovanje, ki nenehno izviduje in skenira EMS in pridobiva informacije, ki jih preoblikuje v podatke s pomočjo širšega konteksta, ki ga pridobiva z različnimi obveščevalnimi disciplinami, kot so na primer SIGINT, COMINT, HUMINT, ELINT, MASINT, IMINT, RADINT, TEHINT, OSINT. Enote elektronskega bojevanja in izvidovanja izvajajo metodo napada na mrežo, ki

predstavlja višjo strukturo in je načeloma pod okriljem elektronskega izvidovanja in predstavlja strateški in operativni pristop napada, kjer se prestreza, identificira, evidentira, locira komunikacijske in nekomunikacijske signale ter analizira informacije in podatke skozi uporabo analitičnih metod s ciljem napada na mrežo IES. S temi podatki želijo zagotoviti informacijsko prednost pred nasprotnikom, ugotoviti njegovo ranljivost in omogočiti lastnim silam ofenzivno delovanje in varnost. Pridobivanje informacij poteka preko celotnega spektra elektromagnetnega valovanja z željo po pridobitvi informacij in podatkov o mednarodnih povezavah in vodenju, usposabljanjem, lokalnem vodenju, rekrutiranju, izbiranjem tarč in načrtovanje, premikih nasprotnikovih sil, izdelovanju IES, infrastrukturi shranjevanja in skladiščenja, celic skupin, ki izvajajo tovrstno delovanje (povzeto po Golob 2009b 6). Tako enote elektronskega izvidništva posedujejo in dajo v obdelavo informacije kot so na primer »ključne besede, besedne zveze, analiza pogostosti komuniciranja, analiza kodnih nazivov udeležencev, lokacij, določanje barv glasu in elektronskih (prstnih) odtisov« (Golob 2009b, 6). S takimi informacijami oblikujejo elektronsko sliko dogajanja na sodobnem bojišču in z uspešnim sodelovanjem med sektorji na vseh ravneh (S-2 in S-3, G-2 in G-3, J-2 in J-3) lahko prepoznajo bodoče grožnje in v skladu z njimi sodelujejo pri načrtovanju in pripravi načina in taktike bojevanja lastnih sil ter taktiko bojevanja enot za elektronsko bojevanje. Pri tem je vsekakor pomembna določitev lastnih delovnih frekvenc, ki morajo biti različne od tistih, kjer se izvaja elektronsko izvidovanje in še posebno tistih, kjer se izvaja elektronsko bojevanje ter uporaba vseh elektronskih ukrepov, od podpornih, zaščitnih in protiukrepov. Z odličnim načrtovanjem in taktiko izvajanja elektronskih protiukrepov s pomočjo mobilnih EMS motilcev na vozilih izvajajo metodo napada na napravo, s katero se lahko uspešno spopadejo z RV IES. Predpriprava sistemov omogoča dva načina motenja, ki predstavljata napad na napravo, »aktivni EMS motilci motijo neprestano - na določenih prednastavljenih frekvenčnih področjih, kjer se pričakuje delovanje IES ter reaktivnih, ki z nenehnim skeniranjem elektromagnetnega spektra iščejo delujoče frekvence in jih ob aktivaciji oziroma pojavu motijo« (Golob 2009b, 9) (glej prilogo J). Vendar je sama uspešnost takšnega načina zoperstavljanja grožnjam in zaščiti lastnih sil odvisna od ažurnosti informacij in podatkov enot elektronskega izvidovanja, ki s svojim delovanjem narekujejo menedžment uporabe elektromagnetnega spektra, ki ga nato izvajajo bojne enote in enote elektronskega bojevanja. Kajti napaka pri določanju delovnih frekvenc, aktivnih frekvenc za elektronsko izvidovanje in elektronsko bojevanje in njihova zamenjava vodi v kolaps komunikacij in nadzor ter spremljanju elektromagnetnega spektra.

Tehnološki napredek v elektrotehniki je prinesel tudi veliko sprememb na področju nadzora bojišča preko oborožitvenih sistemov poveljevanja in kontrole, na področju kontrole ognja, spremljanja lastnih sil... Varnost lastnih sil kot najpomembnejši dejavnik v modernem vojskovanju, predstavlja preskok, kjer sta pomembna podatek in informacija in-time, je prinesla s seboj razvoj tehnologije, ki omogoča spremljanje lastnih in nasprotnikovih sil preko digitalnih vmesnikov in nepogrešljivega elektromagnetnega spektra, s pomočjo GPS povezave s satelitom, telekomunikacijskih linij med uporabniki. Poveljevanje in kontrola se je tako premaknila do točke, kjer poveljnik lažje, hitreje in varneje odloča o nadaljnjih aktivnostih lastnih sil. Sistemi poveljevanja in kontrole so se v zadnjih letih razvili od primitivnih C2 (command and control), C3 (command, control, communications), do C4 (command, control, communications, computerization) sistemov, ter njihovih nadgradenj. S svojo kompatibilnostjo se lahko povežejo z vsemi znanimi komunikacijskimi aparati, in tako omogočajo prednost v informacijah in podatkih. Vendar pa kot IES oddajajo elektromagnetni pulz in uporabljajo elektromagnetni spekter. Tako postanejo občutljivi na delovanje skupin za elektronsko izvidovanje in enot za elektronsko bojevanje. Kljub temu da so nekateri sistemi C4 opremljeni z moduli zaščitnih ukrepov, so ti sistemi vseeno tarča elektronskega bojevanja. Tako zopet elektronsko izvidovanje s podpornimi ukrepi pridobi informacije in posreduje podatke enotam elektronskega bojevanja, ki izvajajo vse vrste podpornih ukrepov elektronskega bojevanja, protiukrepov in zaščitnih ukrepov. Ker prenos informacij in sprejem le-teh omogoča prednost na bojišču, je zelo pomembno, da se ustvari lastna prednost, da se ne dovoli nasprotniku, da bi med seboj komuniciral. To enote elektronskega bojevanja izvajajo z metodami protiukrepov elektronskega bojevanja in podpornih ukrepov elektronskega bojevanja.

S pomočjo podpornih ukrepov se locira oddajnike elektromagnetnega pulza, na podlagi katerih lahko sklepamo o razporeditvi in razmestitvi poveljniških mest centrov zvez, združevanju v skupine, razporeditvi sil, smereh uporabe in premikih nasprotnikovih sil (povzeto po Golob in drugi, 2006, 15). Z bolj natančno metodo triangulacije, ki jo opravi enota za elektronsko bojevanje, s katero locira cilj, sodeluje z drugimi enotami vojske (artilerija, letalstvo,...), ki uničijo cilje (glavne centre zvez in poveljniških mest), s katerih onemogočimo prenos podatkov in informacij na bojišču. Poleg klasičnega uničenja ciljev, enota za elektronsko bojevanje tudi samostojno izvaja elektronski napad na uporabnike in naprave (glej prilogo A), ki uporabljajo elektromagnetni spekter. Uporablja metode protiukrepov elektronskega bojevanja in sicer elektronskega motenja, zavajanja in

nevtralizacije. Prvo s pomočjo elektronskega izvidovanja, s skeniranjem EMS, določi frekvenčno območje nasprotnikovih enot, katerega bo motilo. To lahko počne na 3 načine. Ozkopasovno motenje, kjer napademo točno določeno frekvenco ali ožji frekvenčni pas, ki je značilen za uporabo nasprotnika, s tem je moč motilca koncentrirana in ni večje izgube moči. Naslednji način je širokopasovno motenje, kjer napademo širše frekvenčno območje naenkrat, vendar se pri tem zavedamo, da se moč motilca zmanjša na posamezno frekvenco, kar se potem izrazi v manjšem učinku elektronskega motenja. Vendar kljub širšemu pasu, lahko zavarujejo lastne delovne frekvence, če širši pas vključuje tudi lastne delovne frekvence. Kompromis med tema načinoma je način brišočega motenja, ki nam omogoča, da kljub večjemu frekvenčnemu pasu z motilcem napademo in prebrisujemo frekvence s čim hitrejšim prebrisom po frekvenčnem pasu, tako ohranimo moč motilca veliko, čeprav je razširjen čez celotni frekvenčni pas (povzeto po Žaže 2008, 21). Vendar se je potrebno zavedati, da lahko nastanejo interference elektronskega motenja z lastnimi delovnimi frekvencami ali pa z aktivnimi ter ažurnimi delovnimi frekvencami nasprotnika, ki so vir obveščevalnih podatkov. Tako lahko z lahkomiselnostjo ustvarimo vakuum informacij in podatkov, ki jih pridobivajo elektronski izvidniki.

Ena izmed metod elektronskih protiukrepov, ki jih enote za elektronsko bojevanje izvajajo, s katerimi želijo dezinformirati nasprotnika, je elektronsko zavajanje, kjer s pomočjo elektronskega izvidovanja določijo aktivne frekvence, kjer bodo delovali. S to metodo pa sami lahko dosežemo cilj, vdor v komunikacijsko mrežo nasprotnika. Z uspešnim vdorom se hitro doseže in prisili nasprotnika v nerazumna povelja in sklepe, ki niso v skladu s sliko bojišča. Ob enem se lahko doseže preobremenjenost in zasičenost nasprotnika z obveščevalnimi podatki. Tako mu ne pustimo počitka in ga zavedemo v proces pridobivanja fiktivnih obveščevalnih podatkov in informacij. Tako lahko zavedemo nasprotnika z uporabo njegovih frekvenc, lastne frekvence pa uporabimo pri zavajanju nasprotnika o lastnih silah, premikih lastnih sil ipd.

»Tretja metoda elektronskih protiukrepov je elektronska nevtralizacija, katere namen je absolutna uporaba elektromagnetne energije za začasno ali permanentno uničenje naprav, ki uporabljajo elektromagnetni spekter« (Žaže 2008, 25). Ta oblika je še posebno primerna pri elektronskem napadu na sisteme za nadzor (radarji, optoelektronske naprave, senzorji, nasprotnikovi sistemi za elektronsko bojevanje).

Zavedati se je potrebno, da tudi nasprotnik izvaja nadzor, nadzor zračnega prostora, elektromagnetnega spektra ipd. Zato smo prisiljeni uporabljati elektronske zaščitne ukrepe, ki nam omogočajo nemoteno uporabo elektromagnetnega spektra. Poznamo 2 obliki zaščitnih ukrepov, aktivni - pri čemer zagotavljamo nemoteno uporabo EMS s pomočjo spreminjanja parametrov oddajnika, komunikacijskih poti ter pasivni, kjer uporabimo vse prikrite ukrepe za nemoteno uporabo EMS, to pa zagotovimo s težje zaznavnimi parametri, kot so npr. tehnična značilnost opreme in načinom dela (povzeto po Golob in drugi 2006, 25). V primeru ostalih oborožitvenih sistemov, ki so namenjeni nadzoru, uporabljamo ofenzivne ukrepe, elektronske protiukrepe in podporne ukrepe elektronskega bojevanja, ker nas sama naravnanost sistemov sili in omogoča tovrstno obliko bojevanja.

Večina sistemov za nadzor deluje na elektromagnetnem pulzu in uporablja elektromagnetni spekter, zato tudi ti postanejo žrtev in čutijo vpliv elektronskega bojevanja. Radarji, kot revolucionarni oborožitveni obrambni sistemi 2. svetovne vojne, so postali glavne tarče napada klasičnega in elektronskega napada, pri čemer ima elektronski napad nalogo izvidovanja, lociranja, identificiranja in motenja ipd. Sodeluje pa tudi pri samem klasičnem napadu in to s podporo obveščevalne dejavnosti. Kakor pri radarjih, tudi pri optoelektronskih napravah in senzorjih, imajo enote elektronskega bojevanja prvotno nalogo izvidovanja in bojevanja, pri čemer minimizirajo učinke nasprotnikovega delovanja z uporabo elektronskih protiukrepov in njegovih metod.

Nujno sodelovanje med samimi enotami za elektronsko delovanje (razlikovanje po uporabljenih platformah) in sodelovanje enot za elektronsko bojevanje z drugimi klasičnimi enotami, specialnimi enotami in drugimi se odraža v večkomponentnosti sil elektronskega bojevanja (glej prilogo I), kompatibilnosti in nujne komplementarnosti enot ter več funkcionalnosti združenih sil.

7 ZAKLJUČEK

Nove oblike oborožene spopada so prišle do te točke, kjer samo klasično orožje in ognjena moč nista več zadosten kriterij za uspešnost bojnih aktivnosti. Potreben je razmislek tudi o dodani vrednosti elektronskega bojevanja, ki nadzira in se bojuje na nevidnem bojišču. S to obliko boja močno pripomore k skupnemu uspehu. Vendar pa sama potrošnja in nesmiselna uporaba elektromagnetnega spektra lahko naredi več škode kot koristi. Ob nepravilni rabi

elektronskih sredstev in sistemov se poruši vse dosedanje delo in lahko pride do izgube informacijsko - komunikacijske prednosti, ki je v današnji obliki boja ključna in predstavlja pomemben kriterij za uspešno izvedene akcije in operacije.

Kljub temu, da so sodobni sistemi elektronskega bojevanja zelo sofisticirani in ob enem lahko predstavljajo tudi tehnološko prednost, je ta včasih lahko tudi preveč kompleksna za določene oblike bojevanja. Posledica tega je neuspešen poskus izvajanja elektronskih ukrepov, uporabe tehnološke prednosti na področju komunikacij, ki lahko negativno vplivajo na nadaljnji potek bojevanja. Nasprotniku dopustimo, da ob spremljanju našega dela, ki poteka preko EMS, ugotovi pomanjkljivosti naših sistemov, načina delovanja sredstev zvez in elektronskega bojevanja. Sovražnik lahko te pomanjkljivosti kasneje uporabi proti nam, z uporabo nasprotnikovih elektronskih ukrepov pa dovolimo in omogočimo nasprotniku popoln nadzor EMS, ki je ključen za pridobivanje obveščevalnih podatkov in informacij. Največjo nevarnost bi predstavljal nasprotnikov vstop v naše lastne komunikacijske mreže, kjer bi se sam napajal z obveščevalnimi podatki in informacijami ter povzročal zmešnjavo znotraj komunikacijskega ciklusa. Ukrepi elektronskega bojevanja tako ne ščitijo lastnih sil samo posredno, ampak tudi neposredno.

Neposredna zaščita, ki jo opravljajo enote elektronskega bojevanja, se kaže predvsem v superiornosti in nadzoru nad EMS. Z zavedanjem novih oblik groženj, kot so IES, ki ogrožajo lastne sile, se je spremenil tudi način bojevanja, pri katerem imajo glavno nalogo pripadniki enot za elektronsko bojevanje. Z izvajanjem elektronskega izvidovanja namreč preiskujejo območje delovanja lastnih in opozarjajo na morebitne nove grožnje, nove lokacije, mesta detonacije, odkrivanje novo nastalih celic. Kljub nenehnemu skeniranju EMS, česar se nasprotnik zaveda, enote elektronskega bojevanja niso vedno učinkovite. Nasprotnik s hitrim razvojem tehnologije in elektronike še vedno lahko deluje, pri čemer ga omejuje le tržna vrednost komercialnih tehničnih sredstev in domišljija. Zato so enote vedno pod pritiskom iskanja inovacij, tehnike in taktike bojevanja. Kljub temu, da se je število napadov z IES zmanjšalo, to še ne pomeni, da grožnja ne obstaja, ker se posadke, zaradi nenehnega motenja EMS okolice, ne zavedajo napada, ki so ga uspešno blokirale. Tako taktika enot za elektronsko bojevanje sili nasprotnika, da spremeni obliko proženja (»proženje preko žice«) (povzeto po Golob 2009b, 9), ki jo je lažje zaznati in blokirati, obenem pa nasprotnika prisilijo v bližinski boj, ki bi pomenil številčno premoč lastnih sil. Ob tem obstaja možnost zajetja nasprotnika in nadaljnje pridobivanje obveščevalnih podatkov in informacij, ki bi jih lahko enote elektronskega bojevanja uporabile pri napadu na mrežo in posameznih ciljev. »V

operacijah kriznega odzivanja se cilji oz. ciljne skupine delijo na paravojaške skupine, lokalna policija, vojaške enote, kriminalne združbe ter teroristične celice« (Golob 2005, 16).

Skupno bojevanje enot je odvisno predvsem od medsebojnega komuniciranja, ki mora potekati hitro in brez motenj, zato so še posebej pomembne vaje, kjer se ocenjuje sodelovanje med enotami elektronskega bojevanja in ostalimi enotami, katere so odvisne in soodvisne med seboj. Če se osredotočimo bolj natančno, se zavemo, da so enote elektronskega bojevanja nepogrešljiv člen. S svojo predpripravo, ki vključuje elektronsko izvidovanje in elektronsko bojevanje, postavijo temelje bojišča in omogočajo nemoteno elektronsko komunikacijsko delovanje lastnih in lastnih združenih enot.

Metode in elektronske ukrepe, ki jih izvajajo enote elektronskega bojevanja, so zaenkrat nezadovoljivo učinkovite, še posebej v boju zoper IES, kar nam pove podatek, da se število napadov (glej prilogo K) in žrtev od prve uporabe takšnega ubojnega sredstva leta 2002 stalno povečuje. Leta 2008 je bilo 64 odstotkov več napadov in približno 7 odstotkov več žrtev v primerjavi z letom 2007 (povzeto po Golob 2009b, 10). Vendar se je kljub temu povečala tudi stopnja neeksplodiranih IES, ki se zadnje čase približuje 70 odstotkov glede na prejšnja leta (povzeto Golob 2009b, 10), kar pomeni premik k bolj učinkoviti rabi elektronskih ukrepov in delovanju enot za elektronsko bojevanje.

Čeprav so elektronski ukrepi in metode na področju IES še vedno nezadostne, tega ne moremo trditi za splošno oziroma klasično uporabo elektronskih ukrepov. Metode so preverjene, uporabljajo se dnevno. Učinkovitost metod je odvisna predvsem od znanja operaterja. Elektronski ukrepi sami po sebi zadostujejo potrebam elektronskega bojevanja. K učinkovitosti veliko pripomore tehnična oprema, kajti brez ustrezne tehnične podpore, kljub poznavanju metod, ne moremo uspešno delovati. Elektronskega motenja namreč ne moremo izvajati, če imamo preslab oziroma prešibak oddajnik, s katerim bi motili nasprotnikovo oddajanje EM energije. Sama učinkovitost se veže na znanje in tehnologijo. Metode in elektronski ukrepi bodo učinkoviti do trenutka, ko se bo pojavil nov način uporabe EMS in tehnologije, ki bo lahko podpirala takšen način. Zelo podobno se to kaže pri prestrezanju digitalnih paketnih podatkov, kjer sama hitrost in način prenosa podatkov onemogočata operaterju, da bi lahko prestregel ali pa motil EM signal.

Izboljšanje trendov učinkovitosti bi dosegli z več faktorji, nabavo najnovejših in najsodobnejših elektronskih sistemov in programov, ki bi zadovoljili potrebe enot za

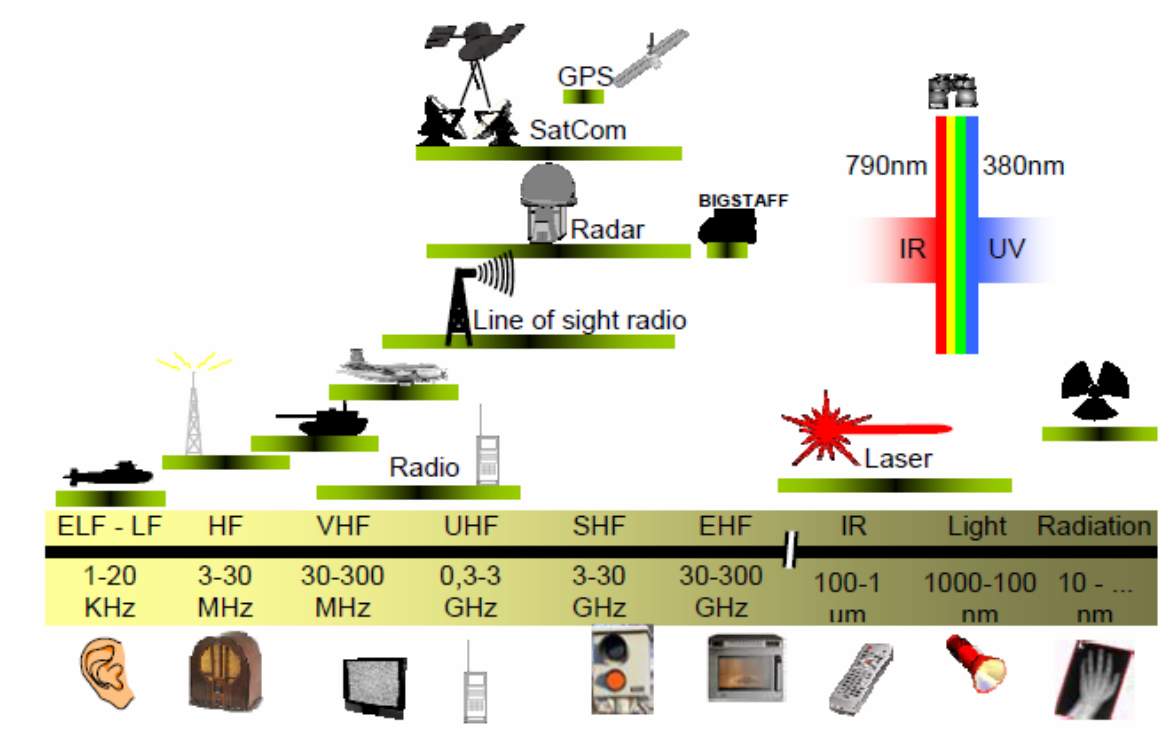
elektronsko bojevanje. Naslednji najpomembnejši faktor je usposobljenost in učinkovitost pripadnikov enot za elektronsko bojevanje, kjer je potrebna nadgradnja znanja s skupinskimi vajami, individualnim učenjem. Gledano zunaj okvirjev je vsekakor pomemben stik enot za elektronsko bojevanje z drugimi enotami, pri čemer mora priti do izmenjave izkušenj in napredka, pri čemer bi imela enota za elektronsko bojevanje nalogo inštruiranja drugih enot na področju zaščitnih ukrepov, ki se odražajo v širši varnosti lastnih komunikacij.

8 LITERATURA

- Adamy, David. 2001. *EW 101 - A first course in electronic warfare*. Boston, London: Artech house
- Berginc, Alojz. 2008. *Vloga enot za elektronsko bojevanje v obveščevalni dejavnosti.* Zaključna naloga. Ljubljana: Poveljstvo za doktrino, razvoj, izobraževanje in usposabljanje.
- Department of the army. 2009. *Electronic warfare in operations FM 3-36*, field manual. Washington D.C.: Department of the army.
- Furlan, Branimir. 2006. *Bojno delovanje*, skripta. Ljubljana: Poveljstvo za doktrino, razvoj, izobraževanje in usposabljanje.
- Golob, Damjan, Uroš Možina in Zdenko Frangež. 2006. *Elektronsko bojevanje*, skripta. Ljubljana: Poveljstvo za doktrino, razvoj, izobraževanje in usposabljanje.
- Golob, Damjan. 2005. *Vloga elektronskega bojevanja v zaščiti sil (Force protection).* Zaključna naloga. Ljubljana: Poveljstvo za doktrino, razvoj, izobraževanje in usposabljanje.
- --- 2009a. *Sodobni sistemi za elektronsko bojevanje*. Zaključna naloga. Maribor: Poveljstvo za doktrino, razvoj, izobraževanje in usposabljanje.
- --- 2009b. *Vloga elektronskega izvidovanja in elektronskega bojevanja v boju zoper sodobne grožnje – Improvizirane eksplozivne naprave*. Zaključna naloga. Maribor: Poveljstvo za doktrino, razvoj, izobraževanje in usposabljanje.
- --- 2010. *Vloga elektronskega izvidovanja in elektronskega bojevanja v boju zoper terorizem.* Seminarska naloga. Maribor: Poveljstvo za doktrino, razvoj, izobraževanje in usposabljanje.
- Steerly, Martin. 2001. *Electronic warfare systems*. Dostopno prek: http://www4.janes.com/subscribe/jrew/doc_view.jsp?K2DocKey=/content1/janesdata/yb/jrew/jrew0714.htm@current&Prod_Name=JREW&QueryText= (23. junij 2010)
- Žaže, Matej. 2008. *Elektronsko bojevanje s poudarkom na elektronskih protiukrepih*. Zaključna naloga. Ljubljana: Poveljstvo za doktrino, razvoj, izobraževanje in usposabljanje.

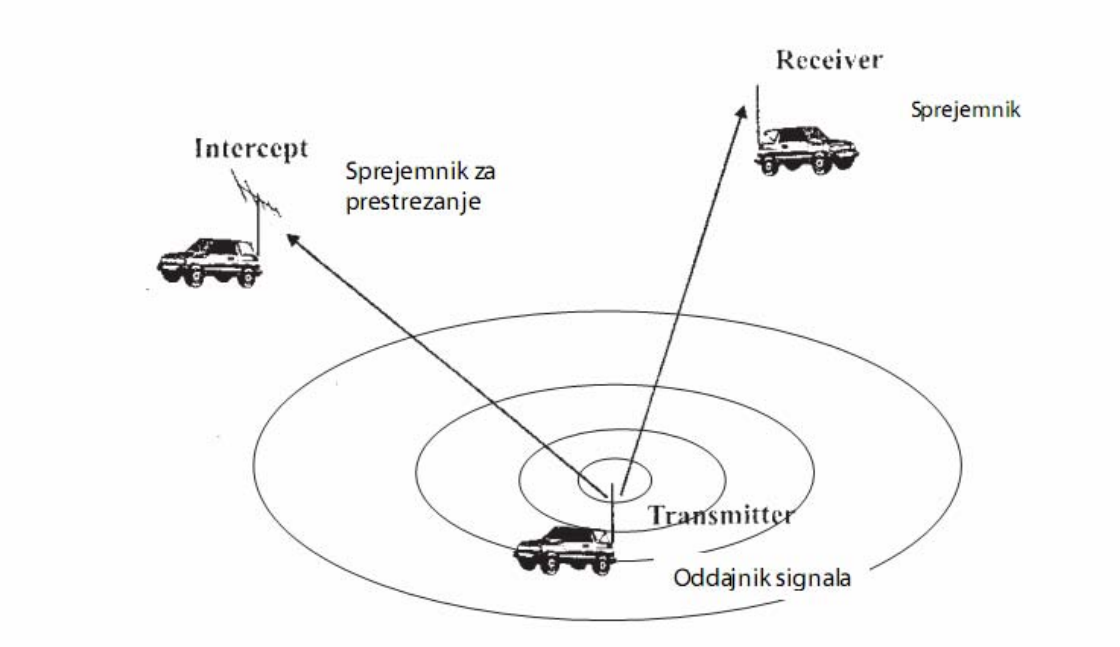
9 PRILOGE

Priloga A: Pregled civilne in vojaške uporabe elektromagnetnega spektra



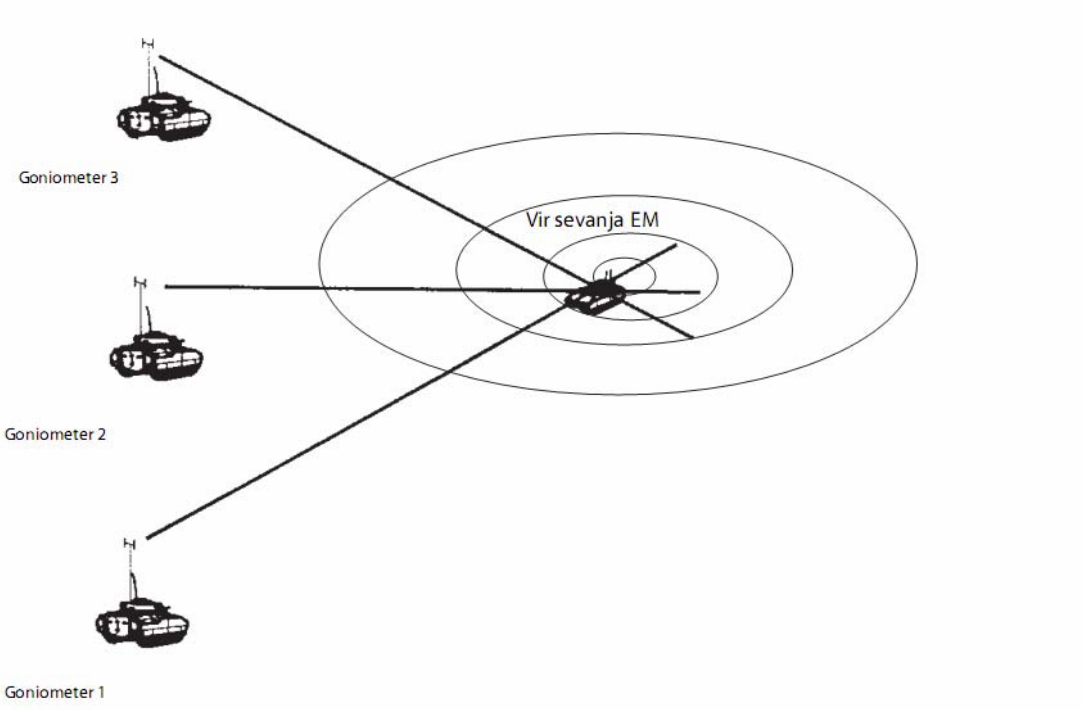
Vir: Golob (2009a, 8).

Priloga B: Osnove elektronskega prestrezanja



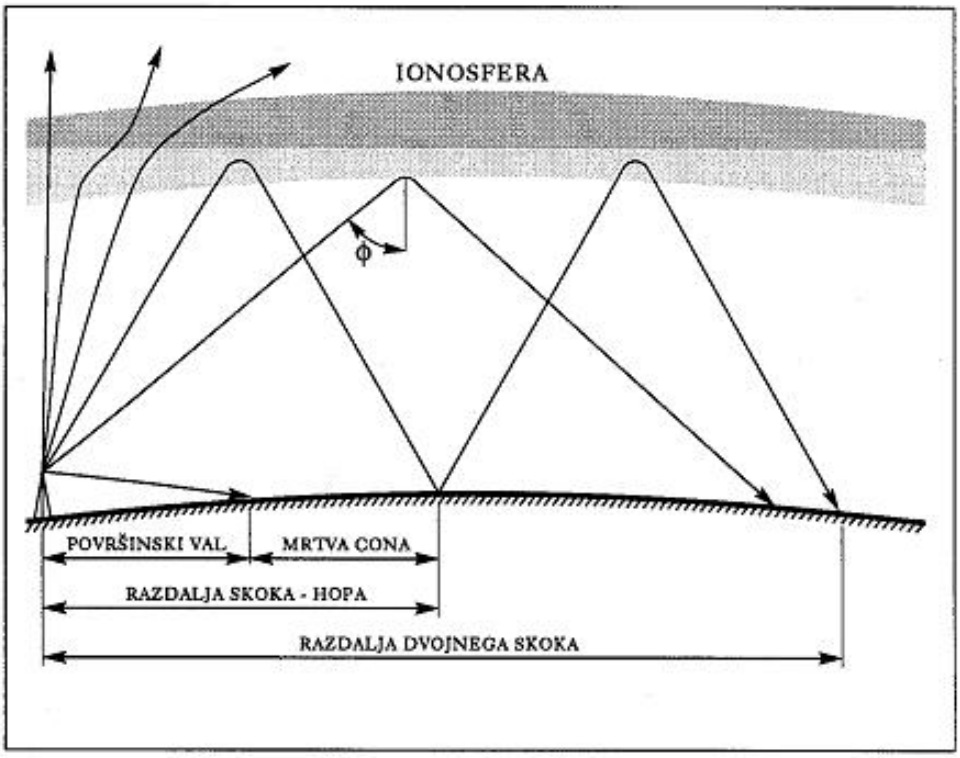
Vir: Golob in drugi (2006, 14).

Priloga C: Goniometriranje



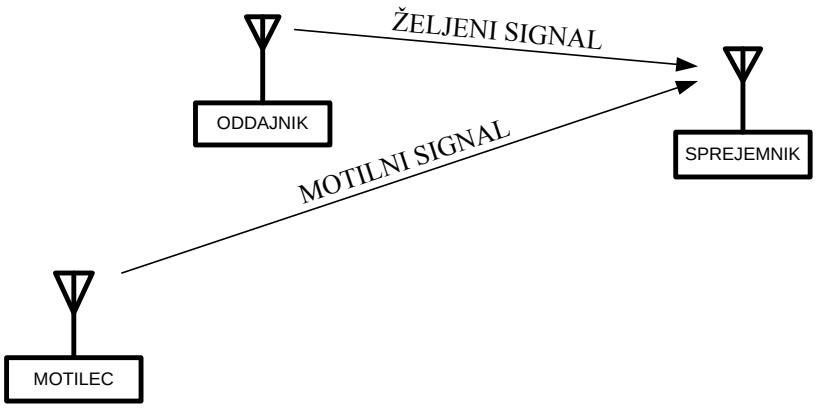
Vir: Golob in drugi (2006 , 16).

Priloga Č: Metoda SSL



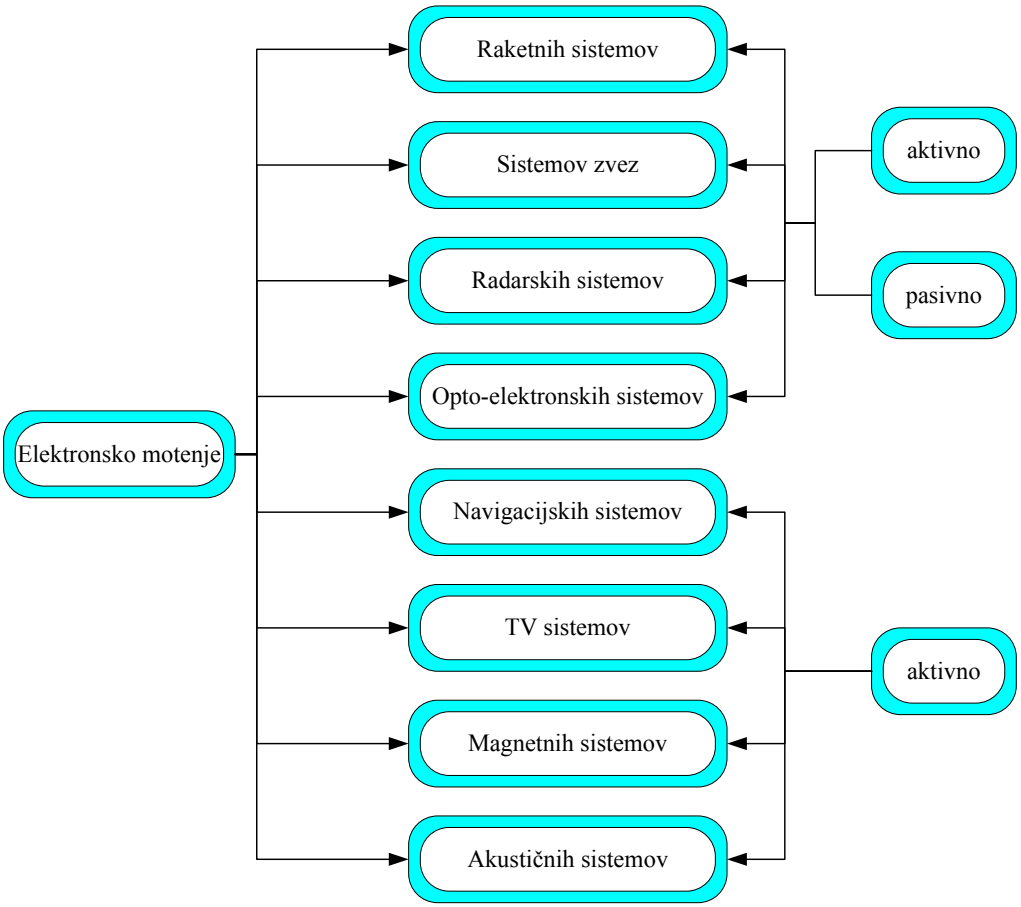
Vir: Grabenšek v Berginc (2008, 19).

Priloga D: Osnovna geometrija elektronskega motenja komunikacij



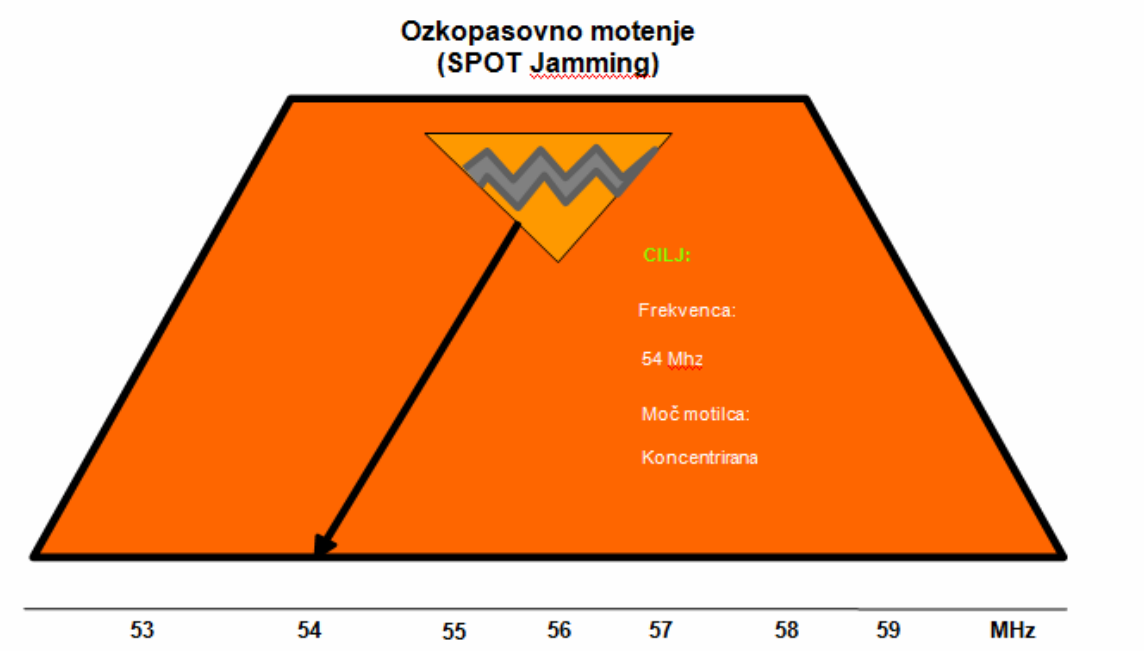
Vir: Adamy v Žaže (2008, 19).

Priloga E: Delitev elektronskega motenja glede na sisteme in sredstva katere motimo ter način nastanka motnje



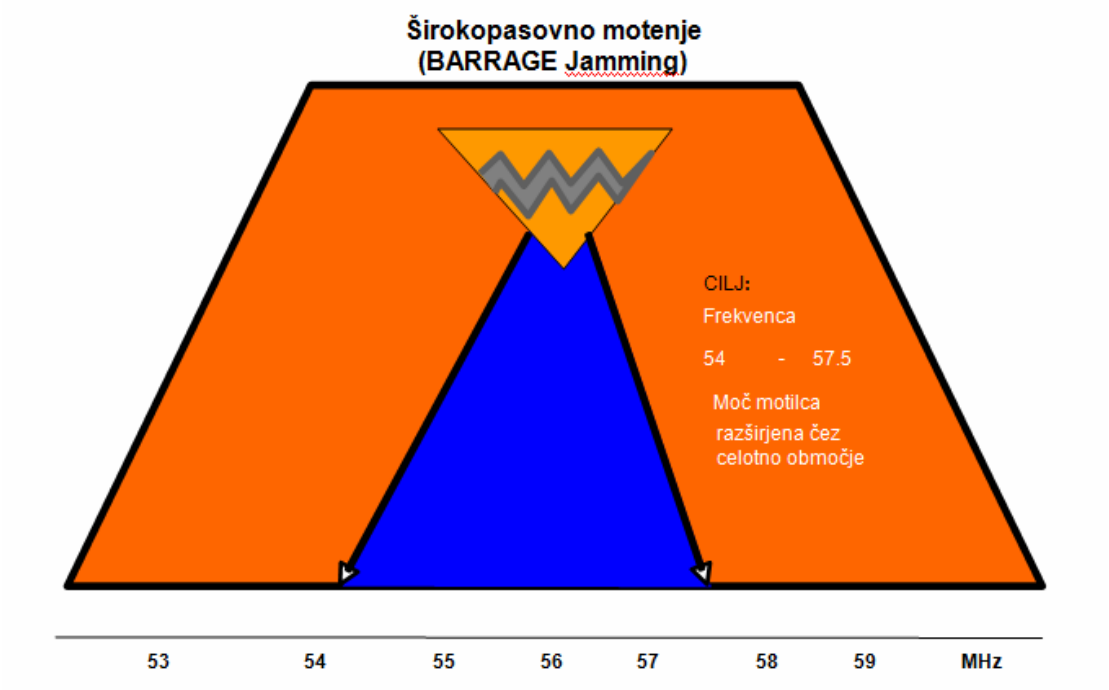
Vir: Žaže (2008, 20).

Priloga F: Ozkopasovno motenje



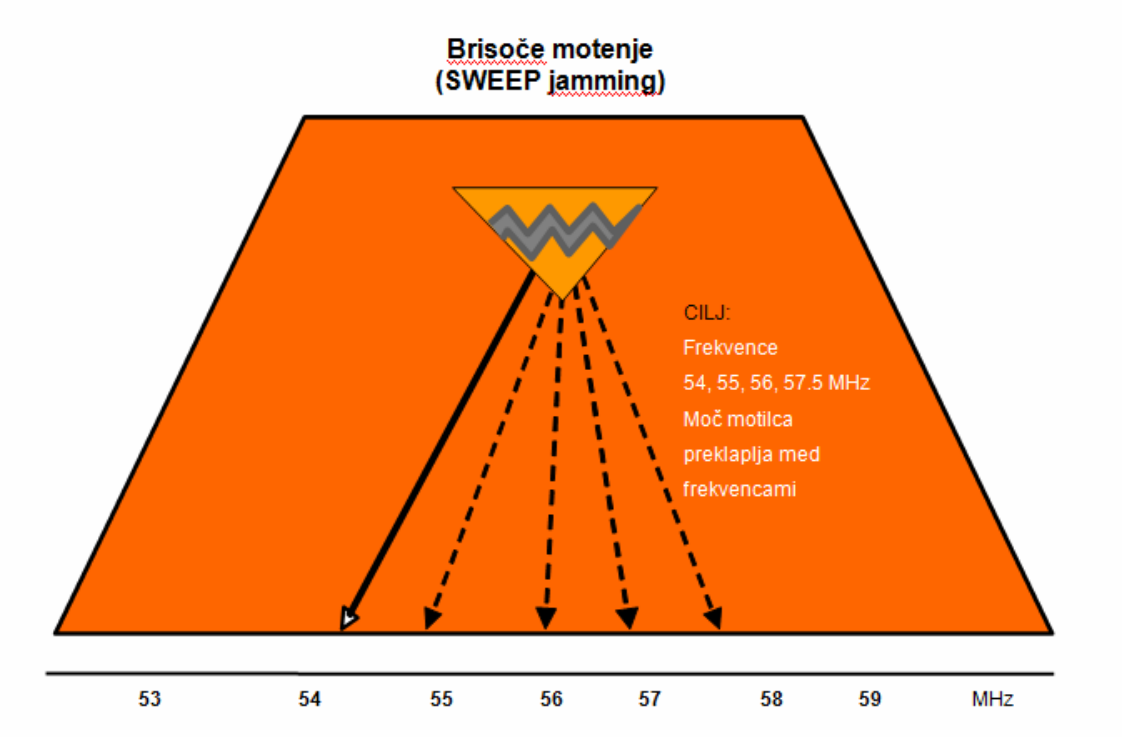
Vir: Žaže (2008, 21).

Priloga G: Širokopasovno motenje



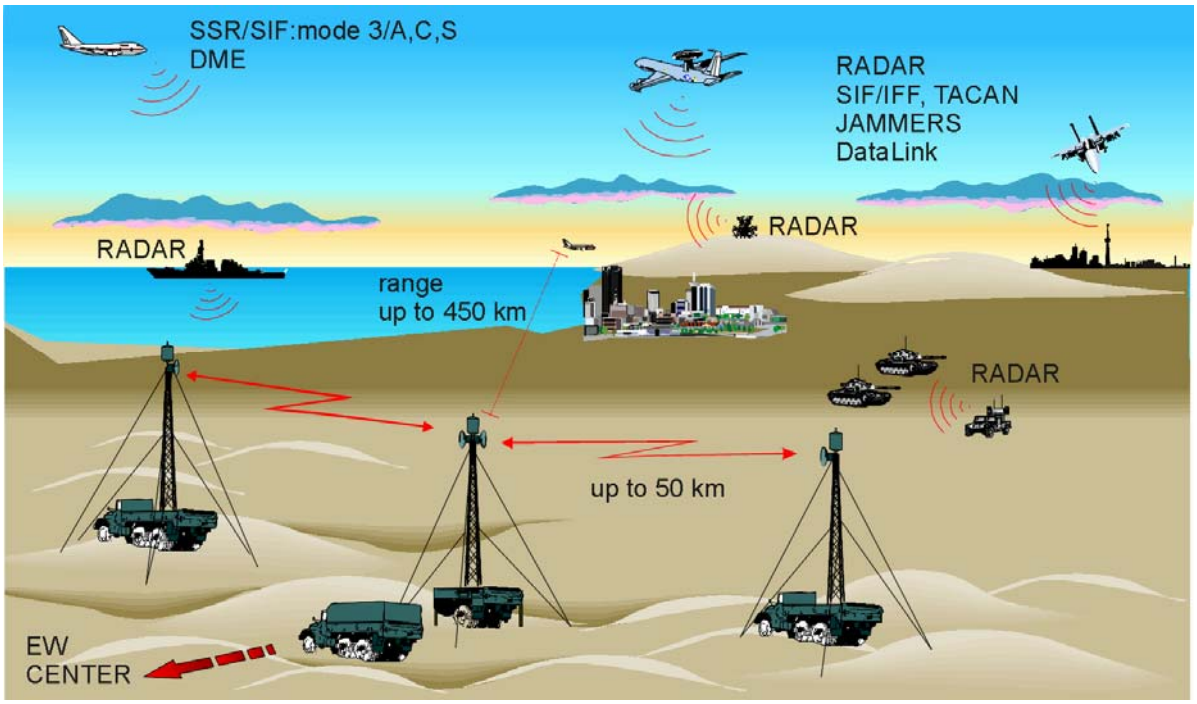
Vir: Žaže (2008, 22).

Priloga H: Brisoče motenje



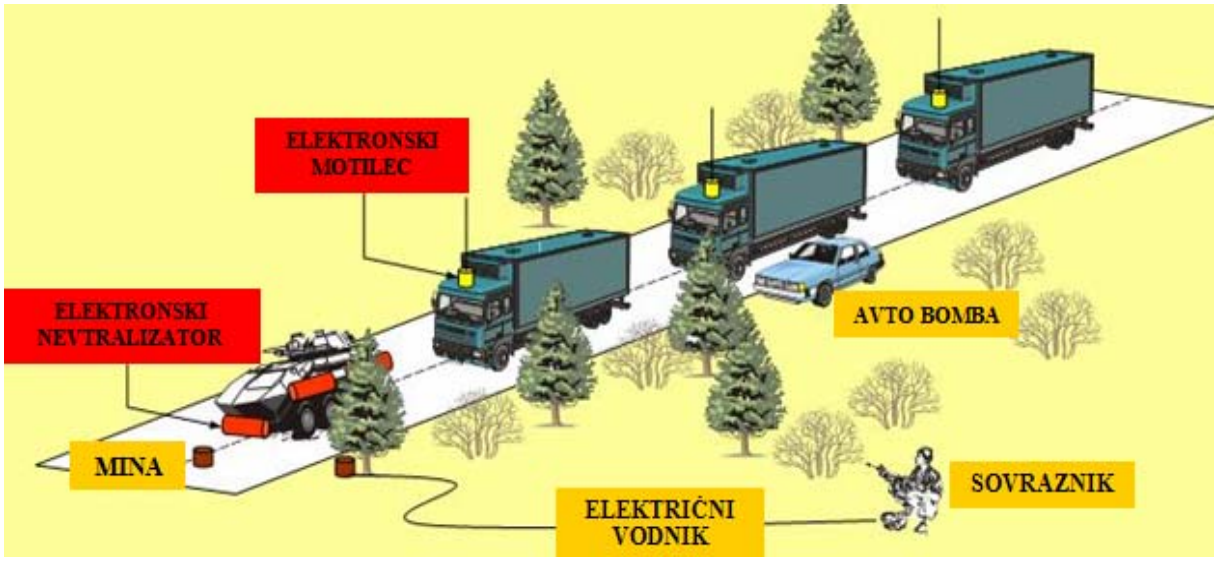
Vir: Žaže (2008, 23).

Priloga I: Večkomponentnost elektronskega bojevanja



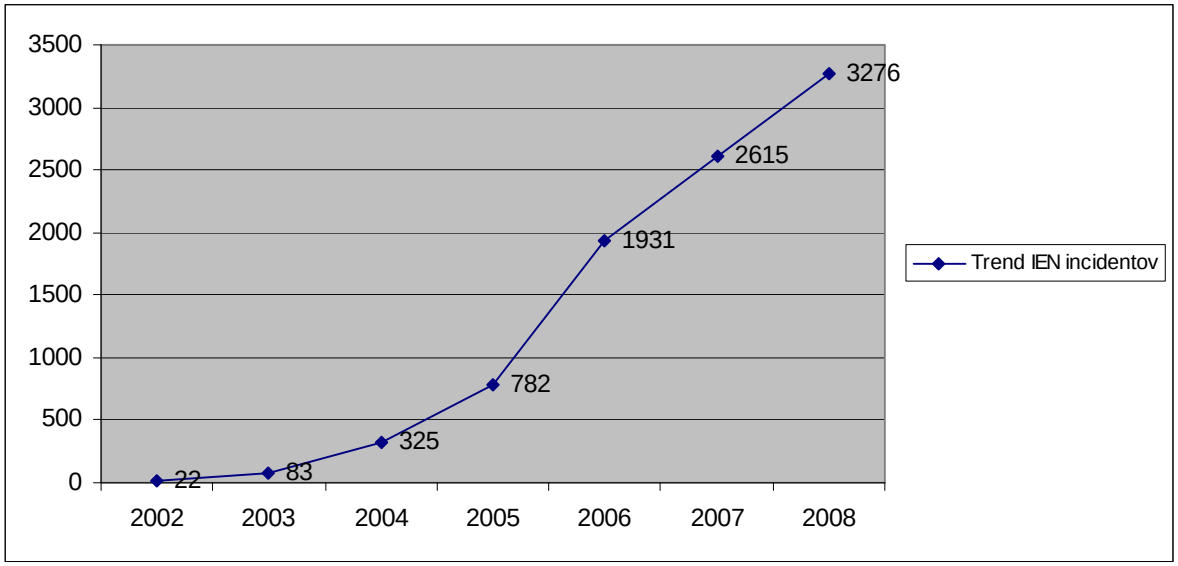
Vir: Golob (2005, 16).

Priloga J: Aktivni in pasivni napad na RV IES



Vir: Golob (2005, 17).

Priloga K: Trend števila IES incidentov v obdobju 2002-2008



Vir: povzeto po Cordesman v Golob (2009b, 10).