Sistemi za elektronsko bojevanje

Gal Likar, Boštjan Batagelj

Univerza v Ljubljani, Fakulteta za elektrotehniko, Laboratorij za sevanje in optiko, Tržaška cesta 25, 1000 Ljubljana, Slovenija

E-pošta: likar.gal.likar@gmail.com

Electronic warfare systems

Abstract. *This paper is an overview of the field of electronic warfare and it's different areas and systems used. It paints a broad picture of what this field of warfare covers while also pointing out a few typical and exciting technologies, some of which are in combat use today. The purpose of this paper is to show the field of electronic warfare, which needs a lot of attention, as technologies and methods of work are continually changing, and the obsolescence of systems can mean a significant weakness in conflict with the enemy.*

1 Uvod

Vojna spremlja človeka že vse od njegovega začetka. Z razvojem človeške družbe in njenim tehnološkim napredkom, so se vzporedno spreminjale tudi oblike vojskovanja. V vojnem konfliktu tehnologija predstavlja pomembno utež, ki lahko prevesi tehtnico razmerja sil v tisto stran, katera jo zna bolje uporabiti. Ob začetku uporabe elektromagnetnega valovanja se je odprla nova dimenzija vojskovanja. Če se je prej vojna bila na zemlji, vodi in v zraku, se je kasneje konflikt razširil še na področje elektromagnetnega spektra (EMS), ki je postal pomembna dobrina, uporaben sprva predvsem za komunikacije, pozneje pa tudi za radarske in namerilne sisteme. Tako kot je raba radijskih komunikacij in drugih naprav, ki uporabljajo elektromagnetni spekter, nepogrešljiva v civilnem svetu, lahko ohromitev takih sistemov povzroči zlom celotne vojaške organizacije, ki je svoje delovanje prilagodila uporabi tovrstnih modernih tehnologij.

2 Elektronski sistemi in elektronsko bojevanje

V NATO slovarju je termin elektronsko bojevanje definiran kot vojaška aktivnost, s katero raziskujemo elektromagnetni spekter in obsega iskanje, prestrezanje, identifikacijo signalov v elektromagnetnem spektru, uporabo elektromagnetne energije (vključno z usmerjeno energijo), s ciljem zmanjšati in preprečiti uporabo elektromagnetnega spektra s strani sovražnika in aktivnosti, ki zagotavljajo učinkovito uporabo elektromagnetnega spektra s strani lastnih sil. [1]

Sodobno elektronsko bojevanje lahko razdelimo v tri večje podskupine; elektronske protiukrepe, elektronske zaščitne ukrepe in podporne ukrepe elektronskega bojevanja. V tem članku so predstavljene posamezne podskupine kot tudi njihove glavne značilnosti. Namen članka je predstaviti sisteme za elektronsko bojevanje in izpostaviti nekaj sistemov, ki so trenutno v uporabi.

3 Elektronska komunikacija

Ena prvih oblik uporabe elektromagnetnega spektra v vojaške namene je bila elektronska komunikacija med enotami in poveljstvom s pomočjo radijskih valov v elektromagnetnem spektru. Elektromagnetne valove, ki jih oddaja radijska postaja, je mogoče prestrezati in motiti, hkrati pa iz njih izluščiti posredovano informacijo. Poleg tega lahko določimo sovražnikove elektronske zmožnosti iz modulacije, smeri sprejema signala, njegove moči in sorodnih parametrov radijske komunikacije.

Sodobne vojaške operacije zahtevajo izmenjavo velike količine informacij med sodelujočimi enotami. Najpomembnejša tipa komunikacij za namene elektronskega bojevanja so taktične komunikacije, kjer so naprave v mreži hkrati oddajniki in sprejemniki, navadno delujejo na isti frekvenci, prenos informacij pa večinoma poteka od nadrejenega k podrejenemu in pa podatkovne zveze med brezpilotnimi letali in nadzornimi centri ali med letali, ki si delijo informacije o letu, po njih pa lahko prenašamo podatke senzorjev, statusne informacije in podatke za določanje lokacije. [2]

4 Radar

Radar (angl. radio detection and ranging) je bil razvit za sledenje zrakoplovov in plovil. Danes jih uporabljamo tudi v civilni sferi za sledenje potniškim in tovornim letalom, določanje vremenskih pogojev, izrisovanje terena, itd.

Radar sestavljata sprejemnik in oddajnik, kot prikazuje slika 1. Oddan signal se odbije od površine katerekoli ovire in se vrne v sprejemnik, kjer je ta signal analiziran. Pogosto sta oddajnik in sprejemnik na isti lokaciji, lahko pa uporabljata tudi isto anteno. Skoraj vedno se uporabi zelo usmerjene antene saj se tako lahko azimut ovire, od katere se je signal odbil, natančneje določi. Razdalja do tarče (d) se izračuna iz časa med oddajo in sprejemom odboja (Δt). Enačba je:

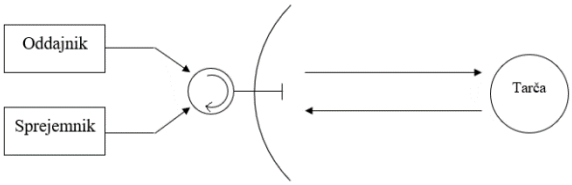
$$d = \frac{c\Delta t}{2} \tag{1}$$

pri kateri je

d = razdalja do ovire (m);

c = hitrost svetlobe (3×10^8 m/s);
Δt = čas med oddajo in sprejemom signala (s).

Če lokacija tarče ni znana, se radarski snop vrti v nekem vzorcu, da pokrije prostor v katerem bi se tarča lahko nahajala. V primeru da je tarča odkrita, ji lahko radar sledi ali pa nadaljuje s skeniranjem prostora.



Slika 1: Poenostavljen koncept delovanja radarja.

Največji sodoben radarski sistem, ki ga uporablja Slovenska vojska je Ground Master GM-403 proizvajalca Tales Raytheon in je sposoben detekcije letal, helikopterjev, manevrirnih raket, brezpilotnih letal in taktičnih balističnih raket na razdaljah do 470 km. Eden izmed takih sistemov se nahaja na Ljubljanskem vrhu. [3]

5 Elektronski podporni ukrepi

Sistemi elektronskih podpornih ukrepov (EPU) zaznavajo signale iz EMS ter določajo njihove lastnosti in možne lokacije oddajnikov. Sistemi EPU so torej tisti, ki 'poslušajo' kaj se na spektru dogaja, da se lahko ostali sistemi elektronskega bojevanja na to pravilno odzovejo. Sisteme EPU delimo na več tipov, med katerimi so najpomembnejši radarski detektorji, sistemi za določanje ciljev (angl. threat targeting sistem) in sistemi za nadzor bojišča (angl. battlefield surveillance systems).

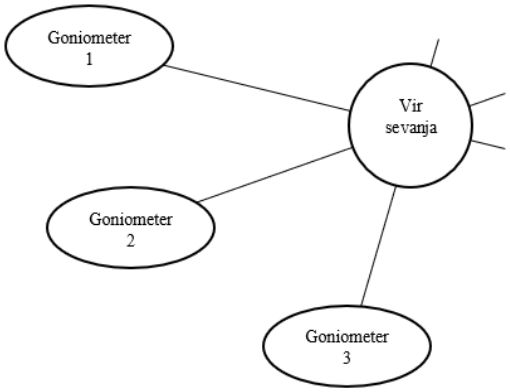
5.1 Radarski detektorji

Kot že samo ime pove, radarski detektorji opozorijo, da je vozilo (najpogosteje letalo) v območju sevanja radarja, kar omogoči pravočasno uporabo protiukrepov ali manevrov za izogib nevarnosti. Z analizo zajetih signalov lahko javljalnik določi tudi tip sovražnega radarja, ali je vir radarskega signala na primer drugo letalo ali pa protiletalski raketni sistem.

5.2 Sistemi za nadzor bojišča

Sistemi za nadzor bojišča sprejemajo in analizirajo vse vrste signalov na bojišču in tako določijo sovražnikove zmožnosti elektronskega bojevanja ter pomagajo pri določanju tarč. Takšni sistemi se lahko namestijo na vse vrste vozil, zrakoplovov in vodnih plovil. V uporabi so tudi prenosni sistemi, katere se lahko prenaša v nahrbtniku, kot je na primer Wolfhound. [4]

Goniometriranje je določanje lokacije vira elektromagnetnega sevanja, med tem ko le-ta oddaja signal. Najosnovnejši način goniometriranja je triangulacija, kjer s pomočjo najmanj dveh goniometrov, ki poznata svojo lokacijo in smer iz katere signal prihaja, lahko določimo območje, kjer se snop križa. S tremi ali več goniometri, kot prikazuje slika 2, je mogoče dobiti natančnejše meritve. Na natančnost določanja lokacije vpliva veliko dejavnikov, med drugim tudi frekvenca na kateri vir oddaja. Pri nižjih frekvencah je točno lokacijo težje določiti, ker se taki elektromagnetni valovi poslužujejo različnih vrst razširjanj, medtem ko je večina visokofrekvenčnih zvez omejena na zvezo z neposredno vidljivostjo (angl. line of sight communications).



Slika 2: Goniometriranje vira sevanja s triangulacijo.

Za določanje lokacije virov, ki oddajajo v kratkovalovnem (HF) območju, je bila razvita metoda SSL (angl. single site location), ki s pomočjo merjenja kota, pod katerim se elektromagnetni valovi odbijejo od ionosfere in znane višine plasti ionosfere lahko poleg smeri določi razdaljo do izvora signala. [5] Za goniometriranje s to metodo zadostuje le en goniometer, ki je po navadi stacionaren. Eden izmed predstavnikov premičnih goniometrov v nemški vojski je KWS RMB (nem. Kampfwertsteigerung Radio Multiband), osnovan na šest kolesnem transportnem vozilu Fuchs. Uporablja se za goniometriranje lokacije radarskih sistemov. [6]

6 Elektronski protiukrepi

Glavni namen elektronskih protiukrepov je aktivno motenje, zavajanje ali uničenje sovražnikovih elektronskih naprav ali sistemov. Nadpomenka elektronskih protiukrepov je elektronski napad, pod katerega štejemo tudi orožja, ki uporabljajo usmerjeno energijo in protiradiacijske izstrelke. Med orožji, ki uporabljajo usmerjeno energijo je še posebej kontroverzen tako imenovani Active denial system, ki ga je razvila vojska Združenih držav in v usmerjenem snopu oddaja signal s frekvenco 95 GHz z močjo 100 kW, ki v koži povzroči podoben učinek kot mikrovalovna pečica – vzburi molekule vode in maščobe, ter jo tako segreje, kar je pri testirancih povzročilo zelo neprijeten občutek. Nihče od tistih, na katerih so preizkusili ta sistem, ni zdržal dlje kot 5 sekund. Pri testirancih pa sistem ni imel

negativnih posledic na njihove oči, splošno zdravje kože ali pa na moške reprodukcijske organe. Prav tako izpostavljenost žarkom na tej frekvenci ni povečala možnosti za raka. [7]

Elektronsko motenje je načrtno sevanje elektromagnetne energije v sovražnikove sprejemnike, z namenom da bi mu otežili ali celo popolnoma onemogočili sprejemanje tistih signalov, ki dejansko nosijo informacijo. Motnje so lahko elektromagnetni šum, neželeni signal ali pa sprememba lastnosti prenosnega medija.

Učinkovitost motilcev komunikacij se meri z razmerjem med močjo motilnega in močjo motenega signala v sprejemniku (angl. jamming-to-signal ratio – J/S). Večje kot je to razmerje, bolj učinkovito je motenje. Moč signala in motenj na sprejemniku je odvisna od izhodne moči oddajnika in motilca, njune oddaljenosti od sprejemnika in terena, ki ga morajo signali premostiti. V praksi je faktor motenja okrog 10 zadosten za učinkovito motenje komunikacij.

S prekrivnim motenjem se znižuje kvaliteta izhodnega signala, tako da se v prostor oddaja moduliran šum, kar znižuje razmerje signal-šum ter ustvarja območje, kjer je sprejem signala zelo otežen. Ta način motenja se skoraj vedno uporablja za motenje komunikacij. Najpreprostejše za izvedbo je širokopasovno motenje, s katerim se prekrije vse možne frekvence, ki bi jih komunikacijski ali radarski sistemi lahko uporabljali. Širokopasovno motenje ima slab izkoristek, saj se večina moči potroši na frekvencah, ki v tistem trenutku sploh niso v uporabi, vendar za učinkovito motenje pri tem ni potrebno vedeti katere frekvence sovražnik uporablja. Boljši izkoristek ima ozkopasovno motenje, pri kateremu se najprej analizira elektromagnetni spekter. S podrobno analizo spektra se pridobi frekvence, ki jih nasprotnik uporablja, nato pa se na teh frekvencah oddaja motilne signale. Seveda je nujno, da vsake toliko časa motenje prekine, ponovno analizira spekter in po potrebi spremeni frekvence na katerih se oddajajo motilni signali. Tretja možnost je tako imenovano brišoče motenje, pri katerem se ozek pas, na katerem se moti, pomika po širšem delu spektra. S tem se nasprotniku povsem ne onemogoči delovanje, lahko pa se ga moti dovolj, da npr. odpovedo avtomatizirani procesi sledenja tarč, tako da mora sledenje ročno izvajati izkušen operater. [8]

Elektronsko zavajanje radijskih komunikacij (angl. spoofing) je oddajanje lažnih informacij sovražniku na isti način kot da bi prihajalo iz njegovega lastnega omrežja. Potrebno je kopirati postopke avtentikacije, ki jih sovražnik uporablja, zavajanje pa postane še posebej zahtevno, če je v zvezah uporabljeno šifriranje. Ena izmed tehnik zavajanja temelji na snemanju govorne zveze določenega poveljnika, ki se mu s posebno programsko opremo kasneje premeče besede, spremeni njihovo intonacijo, doda motnje ipd. nato pa v kritični situaciji, ko operater pozabi na protokole avtentikacije, odda posnetek njegovega poveljnika v kričečem tonu, ki ukazuje določen manever ali ukrep.

Pri motenju radarjev je pomembno razmerje med močjo motenja in močjo odbitega radarskega signala od tarče (na primer od letala), ki doseže radarski sprejemnik. Pomembno je tudi, da upoštevamo nekatere posebnosti radarjev, na primer smernost radarske antene, ki radarju omogoči da bolje sprejema signale iz določene smeri, medtem ko jih sprejema slabše s tiste smeri, kamor antena ni usmerjena. V primeru da motilec ne seva v glavni snop radarske antene, je potrebno motiti z veliko večjo močjo, kot jo ima sprejeti signal. Druga posebnost pa je posledica razširjanja elektromagnetnih valov; moč odboja signala od tarče se namreč do radarskega sprejemnika zmanjšuje s četrto potenco razdalje do tarče, medtem, ko se moč motnje zmanjšuje le z drugo potenco razdalje motilca od radarja. [9]

Najpreprostejša oblika radarskega motenja je samozaščitno motenje, pri katerem se motilec nahaja na tarči sami. Prednost te oblike je, da motilec seva naravnost v glavni snop radarskega sprejemnika, kar pomeni da je motenje učinkovitejše. Na sodobnih nevidnih letalih se taka postavitev ne uporablja, saj se s tem izniči prednosti majhnega radarskega preseka. Alternativa temu je motenje z daljave (angl. standoff jaming), pri katerem se motilec nahaja na drugem letalu, ki ni v dosegu protiletalskih sistemov nasprotnika. Letala s takim tipom motilca so velika in oddajajo z visoko močjo, kar je nujno, če sevamo v enega od stranskih snopov radarske antene. [10]

Da lahko protiletalski sistemi streljajo na tarčo, jim je potrebno najprej slediti preko radarja. Sled sestavljajo vrednosti kotov in razdalj iz katerih se lahko predvidi položaj tarče v prihodnosti. Elektronsko zavajanje radarskih sistemov ustvari lažno sled tarče, s čimer postanejo protiletalski sistemi neuporabni. Za zavajanje radarjev je potrebna natančnost v časovni resoluciji na nivoju manj kot mikrosekunda, zato so praktično uporabni le samozaščitni motilci, montirani na tarči sami. Eden izmed tipov elektronskega zavajanja je tako imenovani range gate pull-off (RGPO), pri katerem tarča sprejme radarski signal in ga odda s kratko zakasnitvijo, s čimer simulira odboj valov. V praksi namreč radarski signal z večjo zakasnitvijo pomeni bolj oddaljeno tarčo, ker pa dobiva več odbojev (prvi je pravi, ostali pa so emisije motilca) se lahko tarča nahaja kjerkoli v tem oknu razdalj. Radar tako ne more določiti točne lokacije tarče in izgubi njeno sled. [11]

Toplotno vodeni protiletalski izstrelki so eno najnevarnejših sodobnih orožij. Uporabljeni so lahko kot izstrelki zrak-zrak ali pa zemlja-zrak, pri slednjih so še posebej pomembni tisti, ki so izstreljeni iz relativno poceni lanserjev, za katere je velikokrat potreben le en operater. Taka orožja so pasivno vodena – senzor v glavi izstrelka sledi vročim delom motorja ali izpuha. Eden najpreprostejših protiukrepov za obrambo pred toplotno vodenim izstrelkom so toplotne vabe, ki jih letalo ali helikopter izstrelita in ki zaradi svojega vročega gorenja vodijo izstrelek stran od tarče. Poznani so tudi IR motilci, pri katerih laser v IR spektru meri v senzorsko glavo izstrelka in z utripajočimi pulzi spremeni preračunano pot izstrelka. Slovenska vojska za zaščito svojih helikopterjev Cougar uporablja sistem ISSYS (angl. Integrated Self-Protection System – ISSYS) Sestavljajo ga trije različni senzorji za zaznavanje valovanja, ki ga oddaja raketni motor, radar ali laserski namerilnik. Senzorji so vgrajeni v strukturo helikopterja tako, da

pokrivajo celotno območje okrog helikopterja. Del ISSYS je tudi sistem za izmet protiukrepov oziroma vab, tako toplotnih kot radarskih trakov. Sistem lahko ob zaznani grožnji avtomatsko spusti vabe, lahko pa le opozori posadko. [12]

Ena prvih oblik elektronskih protiukrepov so bili trakovi za motenje radarjev (angl. chaff), narejeni iz kovinskih lističev, žice ali steklene volne, prevlečene s kovino, ki odbijajo elektromagnetno energijo in tako ustvarjajo lažno radarsko sliko, običajno pa se odvržejo iz zračnega plovila ali pa se izstrelijo iz granat ali raket. Dolžina trakov je odvisna od frekvence, ki jo želijo optimalno odbijati. Če radarski sistem uporablja več frekvenc, se odvrže trakove različnih dolžin.

V široki uporabi so tudi imitacije ali vabe, ki imajo za namene elektronskega bojevanja podobno radarsko odbojno površino in vrnejo enak odbojni impulz, kot objekt ki ga poskušajo imitirati. To se lahko doseže pasivno z uporabo kotnih sejalcev, ki so neke vrste kresnice za radarske valove – signale iz katerekoli smeri, odbijejo nazaj proti viru, zaradi česar imajo tudi do sto krat večjo radarsko odbojno površino, kot bi jo imelo telo z isto fizično površino. Druga možnost so aktivne elektronske imitacije, ki ustvarjajo večjo navidezno radarsko površino s sprejemom in oddajo ojačenih radarskih signalov. Nasprotnik je lahko s tem zaveden, da na relativno poceni imitacijah iztroši svoje drage izstrelke, ob aktivaciji sovražnikovih obrambnih sistemov pa lahko s sistemi za nadzor bojišča določimo elektronske kapacitete in lokacije sovražnih položajev za elektronsko bojevanje.

7 Elektronski zaščitni ukrepi

S pomočjo elektronskih zaščitnih ukrepov se poskuša nevtralizirati sovražnikove elektronske protiukrepe, oziroma elektronski napad, ter s tem zaščititi elektromagnetni spekter za lastno uporabo.

Radarji na primer lahko sledijo viru motenja ter tako sledijo tarči, ki poskuša oddati svoj lažni položaj. Pri radijskih komunikacijah se lahko uporabi katera izmed tehnik oddajanja z nizko verjetnostjo prestrezanja (angl. low probability of intercept), kot je na primer frekvenčno skakanje, ki signal razširi na širok spekter in je tako manj občutljiv na ozkopasovno motenje.

8 Zaključek

Področje elektronskega bojevanja je zelo široka tema, ki zahteva številne strokovnjake tako v civilnem kot vojaškem delu obrambne strukture. V tem članku so predstavljene posamezne podskupine kot tudi njihove glavne značilnosti elektronskega bojevanja. Namen članka je predstaviti sisteme za elektronsko bojevanje in izpostaviti nekaj takih sistemov v trenutni uporabi. Dimenziji elektronskega vojskovanja je potrebno posvečati veliko pozornost, saj se tehnologije in načini dela nenehno spreminjajo, zastarelost sistemov pa lahko pomeni veliko šibkost v konfliktu z nasprotnikom.

Literatura

[1] AAP-06(2019), "NATO glossary of terms", North Atlantic Treaty Organization NATO Standardization Office (NSO) 2019, dostopano 20. 7. 2020

[2] Golob D., Možina U., Frangež Z, Skripta elektronsko bojevanje, Poveljstvo za doktrino, razvoj, izobraževanje in usposabljanje, 2006, str. 19-24, ISBN 10-961-660-04-4

[3] Radarski sistem Ground master GM 403, dostopano dne 31. 8. 2020, dostopno na: http://www.slovenskavojska.si/oborozitev-in-oprema/zracna-obramba/tales-raytheon-ground-master-gm-403/

[4] Wolfhound Handheld Threat Warning System, dostopano 20. 7. 2020, dostopno na: https://www.definitive-design.com/project/wolfhound-handheld-threat-warning-system/

[5] Coetzee, P. J., and du Plessis, W. P. (2016), Definition of a quality factor for single site location estimates, Radio Sci., 51,str. 555– 562, doi:10.1002/2015RS005799.

[6] Transportpanzer Fuchs KWS-RMB, dostopano dne 31. 8. 2020, dostopno na: https://www.bundeswehr.de/de/ausruestung-technik-bundeswehr/landsysteme-bundeswehr/transportpanzer-fuchs-kws-rmb

[7] Patrick A. Mason, Thomas J. Walters, John DiGiovanni, Charles W. Beason, James R. Jauchem, Edward J. Dick, Jr, Kavita Mahajan, Steven J. Dusch, Beth A. Shields, James H. Merritt, Michael R. Murphy, Kathy L. Ryan, Lack of effect of 94 GHz radio frequency radiation exposure in an animal model of skin carcinogenesis, Carcinogenesis, Volume 22, Issue 10, oktober 2001, str. 1701–1708, doi:10.1093/22.10.1701

[8] Adamy D. L., Tactical Battlefield Communications Electronic Warfare, Artech House Inc., 2009, str. 251-256, ISBN-13: 978-1-59693-387-3

[9] D. Adamy, "Introduction to Electronic warfare Modeling and Simulation", Artech House Inc., 2003,str. 42-53, ISBN 1-58053-495-3

[10] S. Vardhan and A. Garg, "Information jamming in Electronic warfare: Operational requirements and techniques," 2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE), Hosur, 2014, str. 49-54, doi: 10.1109/ICECCE.2014.7086634.

[11] Neri F., Introduction to Electronic Defense Systems 2nd edition, Artech House Inc., 2001, str. 373- 435, ISBN 1-58053-179-2

[12] Podgoršek B., 2019, Sistem samozaščite helikopterja z metalci toplotnih in radarskih vab, Revija SV, številka 10, str. 16-17