

DROONID JA TARKVARARAADIOD EHK VÄIKERIIGI ÕPPETUNDE ELEKTROONILISEST VÕITLUSEST

Kaarel Piip, Haldo-Rait Harro, Ivo Müürsepp, Toomas Ruuben



DRONES AND SOFTWARE DEFINED RADIOS: WHAT A SMALL STATE COULD LEARN ABOUT ELECTRONIC WARFARE. Abstract. Electronic warfare (EW) has already spread to the air, the land, the sea, and even space. Today, software defined radio (SDR) technologies that can easily be interfaced with computers are available to anyone for only a few dozen euros. In a software defined radio, signals are usually processed on the software level. Enthusiasts of SDR can independently store large quantities of signals, process these with powerful processors and, when adding the capabilities of AI, they have great resources at hand.

We know that the armed forces of the Russian Federation (RF) have great EW capabilities, at least in theory, but we know nothing about the level of military training of their EW units. It is too early to come to any final conclusions about the current conflict, but it is evident that the RF uses all elements of EW.

Experience from the war in Ukraine has shown that one can build well-functioning systems from readily available devices. The proficient use of existing capabilities may be the most cost-effective approach to enhancing electronic warfare capabilities.

Võtmesõnad: elektrooniline võitlus, tarkvararaadio, elektromagnetspekter

Keywords: electronic warfare, software defined radio (SDR), electromagnetic spectrum

1. Sissejuhatus

Kellelegi ei tule enam üllatusena, et sidesüsteemid on tänapäeval peaaegu kogu ühiskonna toimimise alus. Moodne lahinguväli ei ole selles mõttes erand. Peaaegu ükski tänapäevane relvasüsteem maal, meres, õhus või kosmoses ei toimi ilma sidelahenduseta. Suur osa lahinguväljasüsteeme kasutab sidepidamiseks mingil kujul raadiolaineid. Seejuures on kasutusvaldkond ülimalt lai, ulatudes krüpteerimata käsiraadiojaamadest keeruliste ja salajaste satelliitsidesüsteemideni. Lisaks sidele kasutatakse raadiolaineid seiresüsteemides, ennekõike radarites, millega saab tuvastada huvipakkuvaid objekte suurelt distantisilt. Samuti on laialdaselt levinud satelliitnavigatsioonisüsteemid, mis põhinevad satelliitidelt raadiosignaalide vastuvõtmisel, nt GPS, GLONASS,

BeiDou, Galileo ja analoogsed süsteemid. Raadioside on oma eri vormides tihti asendamatu, sest annab võimaluse pidada sidet liikudes ja keskkonnas, kus puudub sidepidamist toetav taristu. Viimased konfliktid on näidanud, et militaar- ja tsiviilside lahendused ei ole teineteisest eraldi – tsiviillahenduste kasutamine lahinguväljal on laialt levinud¹.

Teisest küljest teeb raadiosageduslike, ruumis vabalt levivate signaalide kasutamine meid vastasele vähem või rohkem haavatavaks. Esiteks on võimalik neid signaale tuvastada ning hankida seadmete, üksuste ja nende tegevuse kohta erinevat infot. Teiseks saab vastane tekitada signaale, mis meie side-, navigatsiooni- ja radarisignaale segavad.

Kõike seda kokku võttes peetakse elektromagnetspektrit mõnikord isegi eraldiseisvaks sõjapidamise domeeniks, kus vaenupooled teineteisele oma tahet peale suruvad². Võitlust elektromagnetspektris nimetatakse elektrooniliseks võitluseks ehk elektrooniliseks sõjapidamiseks (ingl *electronic warfare*; edaspidi EV). EV ei hõlma mitte ainult raadiolaineid, vaid ka teisi elektromagnetspektri sagedusvahemikke (ennekõike optilist). Veidi kitsam on Venemaa Föderatsioonis (edaspidi VF) kasutatav termin *raadiaoalektroniline võitlus* (vn *радиоэлектронная борьба*), mis jääb raadiosageduslikku vahemikku. Ka siinses artiklis on käsitletud EV-d pigem raadiosageduslikus raamis. Toome esmalt ära EV definitsiooni.

EV on sõjaline tegevus, mis hõlmab elektromagnet- (sh suunatud) energia kasutamist elektromagnetspektri kontrollimiseks või vastase ründamiseks³ või kasutab elektromagnetenergiat olukorratadlikkuse loomiseks ning ründe- ja kaitseefektide saavutamiseks⁴. Liidestades küber-, info-, side- ja luureoperatsioonid ühisele platvormile, on võimalik EV-valdkonnas saavutada ühendrelvaliikidega samaväärne efekt⁵.

¹ **Horbyk, Roman** 2022. "The war phone": mobile communication on the frontline in Eastern Ukraine. – Digital War, Vol. 3, pp. 9–24. <https://link.springer.com/article/10.1057/s42984-022-00049-2> (15.07.2024).

² **Willis, Matthew; Stathopoulos, Panagiotis** 2020. Cyber-Electromagnetic Domain: The Necessity of Integrating the Electromagnetic Spectrum's Disciplines Under a Single Domain of Operations. – The Journal of the JAPCC, Edition 30, pp. 72–77. <https://www.japcc.org/articles/cyber-electromagnetic-domain/> (15.07.2024).

³ **JP 3-13.1**. 2012. Joint Publication 3-13.1. Electronic Warfare. Washington, D.C.: U.S. military, February 8. [JP 3-13.1, 2012]

⁴ **NATO** 2019. The 107th NATO Electronic Warfare Advisory Committee (NEWAC) convenes in Brussels. https://www.nato.int/cps/en/natolive/news_171280.htm (13.09.2023).

⁵ **Lockheed Martin** 2022. Spectrum Convergence. <https://www.lockheedmartin.com/en-us/capabilities/spectrum-convergence.html> (25.09.2023).

Lennart Meri on öelnud 18. septembril 1997:

Kaitserelvastus, olgu ta kui tahes kaasaegne, on surnud raud, kui seda usaldaks ilma väljaõppeta meeskonna kätte. Kõige võimsam relv, kõige keskem tegur mis tahes väeliigis, mis tahes demokraatlikus riigis on kõigepealt sõdur. Inimene ja tema tahe. Inimene ja tema oskus. Inimene ja tema oskus teostada oma kaitsetahet tõhusalt oma riigi nimel.⁶

Sellest põhimõttest tuleb lähtuda ka väikeriigi EV-võime arendamisel. Seega peab iga kaitseotstarbelise varustuse planeerimise ja hankimisega kaasnema ka väljaõppe analüüs, planeerimine, täiendamine ja kontrollimine.

2. Tegevused, sagedusalad ja seadmed

EV jaotus erineb riigiti ja ka NATO piires. Muu hulgas räägitakse tegevustest (ingl *actions*) ja meetmetest (ingl *measures*). Tegevuste ja meetmete vahel ei ole üksühest vastavust. Siiski on iga tegevuse all mingit tüüpi meetmed, mida kõige rohkem kasutatakse. Järgnevalt toomegi need paarid ära.

Üldjoontes võib EV jagada kolmeks:

- 1) elektrooniline rünnak (ingl *electronic attack*; EA) – elektroonilised vastu-meetmed (ingl *electronic countermeasures*; ECM);
- 2) elektrooniline kaitse (ingl *electronic protection*; EP) – elektroonilised vastu-vastumeetmed (ingl *electronic counter-countermeasures*; ECCM);
- 3) elektrooniline toetus (ingl *electronic support*; ES) – elektroonilised toetus-meetmed (ingl *electronic support measures*; ESM)⁷.

EV-seadmed on nagu sideseadmedki piiratud kasutamiseks mingis kindlas sagedusvahemikus. Sagedusalade jaotus ja nimetamine erinevad veidi riigiti, valdkonniti ja organisatsiooniti. Siinses artiklis lähtume raadioside puhul Rahvusvahelise Telekommunikatsiooni Liidu (International Telecommunication Union; ITU) jaotistest⁸ ning kasutame ingliskeelseid lühendeid HF (ingl *high frequency* – kõrgsagedus, 3–30 MHz), VHF (ingl *very high*

⁶ Meri, Lennart 1997. Vabariigi President miiniveeskajate „Kalev“ ja „Olev“ kojusaabumise ja Saksa miinieskaadri külaskäigu puhul Tallinna sadamas 18. septembril 1997. – Vabariigi Presidendi kõned 1992–2001. Vabariigi Presidendi kantselei.

⁷ Poisel, Richard A. 2002. Introduction to Communication Electronic Warfare Systems. London: Artech House.

⁸ ITU-R 2015. Nomenclature of the frequency and wavelength bands used in telecommunications. – Recommendation ITU-R V.431-8, pp. 2–3. International Telecommunication Union. https://www.itu.int/dms_pubrec/itu-r/rec/v/R-REC-V.431-8-201508-I!!PDF-E.pdf (15.07.2024).

frequency – ülikõrgsagedus, 30–300 MHz), UHF (ingl *ultra high frequency* – ultrakõrgsagedus, 300 MHz – 3 GHz) ja SHF (ingl *super high frequency* – superkõrgsagedus, 3–30 GHz). Radarite puhul kasutatakse enamasti veidi teistsugust sagedusribade (ingl *band*) jaotust, mis samuti varieerub. Militaar-rakendustes on radarite töösageduste jaotus enamasti järgmine: L (1–2 GHz), S (2–4 GHz), C (4–8 GHz), X (8–12 GHz), Ku (12–18 GHz), K (18–27 GHz) ja Ka (27–40 GHz). Veel kõrgematel sagedustel on tegu millimeeter-laineradariga.

Tänapäeval on leidnud üha enam kasutust globaalsed navigatsioonisüsteemid ja muud satelliidipõhised rakendused. Globaalsete satelliit-navigatsioonisüsteemide (ingl *global navigation satellite systems*; GNSS) satelliidid asuvad keskmise kõrgusega geotsentrilisel orbiidil (ingl *medium Earth orbit*; MEO), ligikaudu 20 000 km kõrgusel maapinnast. Globaalse positsioneerimissüsteemi (ingl *global positioning system*; GPS) kui kõige tuntuma GNSS-i satelliitide orbiidi kõrgus on näiteks 20 180 km. Kasutatavad sagedused jäävad UHF-sagedusvahemiku keskele suurusjärku 1,5 GHz (L-sagedusriba). GPS-i puhul on madalaim kasutatav sagedus 1176,45 MHz (L5-signaal) ja kõrgeim 1575,42 MHz (L1-signaal).

Merehäda ja -ohutuse ülemaailmne süsteem (ingl *global maritime distress and safety system*; GMDSS) on mõeldud merel seilavate laevade hädaabikutsungite automaatseks edastamiseks. Süsteem kasutab hädaabikutsungite edastamiseks eri sagedusalasid ja raadiosidesüsteeme, muu hulgas lühilaine- ja satelliitsidet. Viimase jaoks kasutatakse erinevaid satelliitsidesüsteeme ja konstellatsioone.

Vene-Ukraina sõjas palju tähelepanu pälvinud Starlink on USA ettevõttele SpaceX kuuluv satelliitsidesüsteem. 2024. aasta jaanuari seisuga koosneb konstellatsioon 5289 satelliidist 340–1200 km kõrgustel orbiitidel. Sideks kasutatakse Ku-, Ka- ja E-sagedusriba. Viimane hõlmab ülikõrgeid sagedusi vahemikus 60–90 GHz.

EV-s kasutatavate seadmete tööpõhimõtted on samad mis sideseadmetel, kuid erinevad on rõhuasetused ja parameetrid. Mõnel juhul saabki side-seadmeid kasutada EV-vahendina. Kui näiteks teame vastase käsiraadio-jaamades kasutatavat sagedust, saame seda võimsama autoraadiojaamaga segada. Vastase krüpteerimata raadiosidet saame oma sarnase raadiojaamaga pealt kuulata. Lisaks on hakatud rääkima raadiojaamade kasutamisest vastase side segamiseks. Sellised jaamad töötavad kolmes režiimis: sideseade, seire-seade ja segamiseade. Seirest ja segamisest on lähemalt juttu allpool.

Sideseadmed jagunevad kõige üldisemalt saatjateks ja vastuvõtjateks (peaaegu kõik tänapäevased sideseadmed sisaldavad mõlemat). Sama jaotus kehtib ka EV-vahendite puhul.

Elektroonilise rünnaku vahendid on saatjad, nende eesmärk on saata signaal, mis takistab vastasel elektromagnetspektri kasutamist või selles toimuvast õigete järelduste tegemist. Segamine on rünnak, mis seisneb sidekanali tahtlikus või tahtmatus häirimises, hoides seda hõivatuna või rikkudes edastatavaid andmeid, põhjustades teenuse katkemise⁹. Harilikest raadio-saatjatest eristab segajaid ennekõike väga suur saatevõimsus. Tüüpilise VHF-käsiraadiojaama väljundvõimsus on kuni 10 W, kuid tüüpilise VHF-segaja võimsus võib ulatuda 1000 W-ni. Elektroonilise rünnaku tegevusraadiuse suurendamiseks on segajatel tihti suundantennid ja kõrged mastid või on nad monteeritud lennuvahenditele.

Teine erinevus raadiosaatjatest on võime saata segavaid signaale korraga mitmel sagedusel või laias sagedusvahemikus, et segada mitut vastase sidekanalit või sagedusvahemikku tervikuna. Erinevalt raadiojaamast pole niivõrd oluline saadetava signaali kvaliteet, sest eesmärk ongi tekitada häireid. Siiski ei tohi segaja signaal olla päris kontrollimatu, et ei häiritaks tahtmatult oma sidekanaleid.

Elektrooniline pettetegevus ehk elektrooniline pete (ingl *electromagnetic deception*; ED) on elektromagnetenergia tahtlik kiirgamine, tagasi-kiirgamine, muutmine, mahasurumine, neelamine, takistamine, võimendamine või peegeldamine viisil, mille eesmärk on edastada vastasele või tema elektromagnetenergia abil juhitavatele relvadele eksitavat infot, vähendades või neutraliseerides sellega vastase võitlusvõimet¹⁰. Tüüpiline näide on pette-radar – seade, mille kiirguspilt matkib radarit ja loob sedasi vastasele radari asukohast vale mulje¹¹. Esmapilgul tundub see lihtne ülesanne, kuid tegelikult on signaalil palju parameetreid, mida tuleb matkida: sagedus, võimsus, polarisatsioon, kasutatav ribalaius, modulatsioon, impulsside pikkus ja kordussagedus, antenni suunadiagramm. Tõsi, olenevalt sellest, mida vastane on võimeline tuvastama, ei pruugi olla tarvis kõiki parameetreid matkida.

⁹ **Bout, Emilie; Loscri, Valeria; Gallais, Antoine** 2020. Energy and Distance evaluation for Jamming Attacks in wireless networks. – IEEE/ACM 24th International Symposium on Distributed Simulation and Real Time Applications (DS-RT), pp. 1–5. <https://hal.science/hal-02933418> (15.07.2024).

¹⁰ **JP 3-13.1**, 2012.

¹¹ **Annunli, Massimo** (*sine anno*). Spoofing in Radar ECM. – Emsopedia. <https://www.emsopedia.org/entries/spoofing-in-radar-ecm/> (23.09.2023).

Kõige selle juures peaks pettesüsteem olema ideaalis palju odavam kui süsteem, mida matkitakse.

Elektroonilise toetuse jaoks kasutatavad seadmed on vastuvõtjad. Harilik raadiovastuvõtja võtab vastu signaale ühel kindlal sagedusel, kuid elektroonilise toetuse puhul tuleb esmalt leida sagedus, mida vastane kasutab. Selleks kasutatavad seadmed jagunevad laias laastus kaheks.

Esimest tüüpi, skaneerivad seadmed häälestavad vastuvõtusageduse kiiresti ümber, luues nii pildi kiirgusvõimsuse jaotumisest laias sagedusvahemikus. Selliste süsteemide eelis on võime katta väga suuri sagedusvahemikke. Kaasnev puudus on piiratud tundlikkus ehk võime tuvastada nõrku signaale. Skaneerimiskiirust vähendades saab tundlikkust suurendada, kuid sellisel juhul võivad lühikese kestusega signaalid jääda märkamata. Lähtetasemel skaneerimisvõimet pakuvad ka tänapäevased raadiovastuvõtjad. Nende kasutamine eeldab aga, et huvipakkuvad sagedused on teada.

Teist tüüpi, monitoorivad seadmed suudavad haarata küllaltki laia sagedusvahemikku korraga. Eelis on kogu signaali kvaliteetne ja pidev vastuvõtmine, puudus reaajas nähtava sagedusvahemiku võrdlemisi väike ulatus (nt R&S PR200-l maksimaalselt 40 MHz¹²). Selliste seadmetega saab signaali ka kohe kogu vaadeldavas vahemikus salvestada ja järeltöötlusse suunata. Üsna soodsat võimalust laia sagedusvahemikku korraga vaadelda pakuvad tarkvara-raadiod. Ka alla 1000-eurosed lahendused (nt Red Pitaya SDR¹³) võimaldavad korraga analüüsida 60 MHz suurust vahemikku. Tarkvararaadiotest on lähemalt juttu allpool. Tänapäeval muutuvad ka raadiojaamades kasutatavad sagedusvahemikud järjest suuremaks, mis seab suuremad nõudmised ka EV-seadmetele. Näiteks VF-i moodsamaid raadiojaamasid Azart töötab sagedusvahemikus 27–520 MHz¹⁴. Konkreetsed sagedusvahemikud on määranud asukohariigi sagedusregulaator (Eestis Tarbijakaitse ja Tehnilise Järelevalve Amet)¹⁵, kuid EV seisukohalt pole nendest enamasti abi, kuna me ei pruugi teada, mis sagedusi vastane kasutama hakkab. Probleemi leevendamiseks võidakse kasutada samal ajal töötavaid monitooringuvastuvõtjaid,

¹² **R&S®PR200 Portable monitoring receiver.** Rohde & Schwarz.com. https://www.rohde-schwarz.com/us/products/aerospace-defense-security/handheld/rs-pr200-portable-monitoring-receiver_63493-594881.html (13.09.2023).

¹³ **SDRlab 122-16 Standard Kit.** Redpitaya.com. <https://redpitaya.com/product/sdr122-16-standard-kit/> (13.09.2023).

¹⁴ **Rosoboronexport** (*sine anno*). Military Communications Equipment and Automated Control Systems. Azart. <https://roe.ru/eng/catalog/land-forces/military-communications-equipment-and-automated-control-systems/radiocomms/azart/> (13.09.2023).

¹⁵ **Eesti raadiosagedusplaan.** – RT I, 01.12.2023, 8.

millest igaüks jälgib kindlat spektrivahemikku. Lisaks saab kahte, monitoorivat ja skaneerivat seadmetüüpi kombineerida, muutes pidevalt monitooritavat sagedusvahemikku.

Eriliigilisteks vastuvõtjateks on suunamäärajad, mille eesmärk on määrata huvipakkuva raadiosignaali saabumise suund. Kui soovime määrata peale suuna ka huvipakkuva saatja asukohta, vajame vähemalt kahte suunamäärajat: kummastki saab tõmmata ühes punktis lõikuvad kiired. Kuna suunamääraja näidul on määramatus (tüüpiliselt 1–10 kraadi), tuvastatakse tegelikkuses kindla punkti asemel ala, kus signaallikka asumine on tõenäoline. Et vältida süsteemseid vigu ja vähendada määramatust, on soovitatav kasutada vähemalt kolme suunamäärajat.

Suunamäärajaid on erineva tööpõhimõttega. Kõige primitiivsem lahendus on mehaaniliselt pööratav suundantenn, mis mõõdab suuna, kust saabuv signaal on kõige tugevam. Sellised suunamäärajad ei ole militaarkasutuses üldiselt sobivad, kuna ei suuda tuvastada lühikese kestusega signaalide suunda (antenn ei pöörle piisavalt kiiresti). Teine liik on Watson-Watt-tüüpi suunamäärajad, mis võrdlevad erinevate suundantennide signaali tugevust ja leiavad selle põhjal signaali suuna.¹⁶

Kolmas suunamääraja tüüp on dopplersuunamääraja ja pseudodopplersuunamääraja, mis tekitavad kas reaalselt (dopplersuunamääraja) või elektrooniliste lülitustega (pseudodopplersuunamääraja) pöörleva antennivõre. Viimane lahendus on mehaaniliselt liikuvate osade puudumise tõttu tänapäeval eelistatud. Olenevalt sellest, kas antenn liigub saatja poole või saatjast eemale, muutub veidi vastuvõetav sagedus (Doppleri efekt) ja signaali suund on võimalik välja arvutada.

Neljas tüüp on interferomeetrilised suunamäärajad, mis kasutavad ära üldteada asjaolu, et raadiosignaali levib valguse kiirusega ning jõuab eri positsioonides paiknevatesse antennidesse erineval ajal ja eri faasiga. Kui antennid on lähedikkude ja mõõtepunkte on vähemalt kolm, on signaalide faasinihke järgi võimalik välja arvutada signaali suund. Selliste seadmete üks suurimaid keerukusi on täpne ja sünkroniseeritud faasinihete mõõtmine, kuid need seadmed on viimastel aastatel üha rohkem levinud ja soodsamaks muutunud.¹⁷

¹⁶ Read, W. 1989. Review of Conventional Tactical Radio Direction Finding Systems. – Defence Research Establishment Ottawa. Technical Note 89-12, pp. 2–21. <https://apps.dtic.mil/sti/pdfs/ADA212747.pdf> (15.07.2024).

¹⁷ Ibid. Vt ka **KrakenSDR: A phase-coherent software-defined radio with five RTL-SDRs**. CrowdSupply.com. <https://www.crowdsupply.com/krakenrf/krakensdr> (13.09.2023). [KrakenSDR]

Viies tüüp on suunamäärajad, mille antennid asetsevad üksteisest kaugel ja millega mõõdetakse antennidesse saabuvate signaalide ajalist hilistumist. Seda nimetatakse TDOA-meetodiks (ingl *time difference of arrival method*). Selle meetodi puhul on oluline väga täpne ajaline sünkroniseerimine (1 ns viga ajas vastab 30 cm veale asukohas).

Samal põhimõttel töötavad ka kõigile veebis vabalt kättesaadavad süsteemid, mis võimaldavad määrata HF-sagedusalas signaali suunda ja arvutada piisava arvu vastuvõtjate olemasolul saatja asukohta¹⁸. Märkimist väärib, et selleks kasutatakse raadioamatööride üle maailma paigaldatud seadmeid ja kasutajal endal ei olegi vastavat riistvara vaja.

EV-süsteemides on riistvaraga sama oluline tarkvara, eriti elektroonilise toetuse puhul. Spektrist saadav infohulk on tohutu, ulatudes ka küllalt piiratud võimega lahenduste puhul terabaitidesse. Toorandmete väärtus on aga üsna väike, väärtuse luureteabena omandavad need pärast analüüsimist ja süstematiseerimist. Tänapäeval on järjest rohkem sidesüsteeme digitaalsed (isegi kui kasutatakse häälsidet), mistõttu on tarkvara vaja kinnipüütud andmete dekodeerimiseks. Kuigi lihtsam dekodeerimine on mõeldav ka riistvara abil, on tarkvaralahendused märksa paindlikumad, võimaldades kiireid uuendusi ja uute standardite lisamist. Suurte andmemahutudega seotud probleeme vaadeldakse artiklis lähemalt tarkvararaadioid käsitlevas osas.

3. Infotehnoloogia arengu mõju elektroonilise võitluse arengule

Nii nagu paljudes teistes valdkondades, on siingi olnud suur mõjutaja esmalt pooljuhtelektroonika ja seejärel infotehnoloogia kiire areng. Tarkvaralahendused on kiirendanud iseäranis elektroonilise luure eri distsipliinide arengut. Lisaks on seadmete füüsilised mõõtmed tunduvalt vähenenud, mis teeb need paremini transporditavaks ja avab uusi kasutusvõimalusi. Veel 20. sajandi lõpus olid lahendused raadiospektri seiramiseks, lindistamiseks, töötlemiseks jms kättesaadavad üksnes professionaalidele või pühendunud asjaarmastajatele, kuid tänapäeval on lihtsamad personaalarvuti või isegi mobiiltelefoniga ühendatavad lahendused kättesaadavad vaid paarikümne euro eest. Võtmesõna on siin tarkvararaadio (ingl *software defined radio*; SDR), kus suur osa signaale töödeldakse tarkvara tasemel, kasutades signaali-protssoreid (ingl *digital signal processor*; DSP) või programmeeritavatest

¹⁸ KiwiSDR. <http://kiwisdr.com/public/> (15.09.2023).

loogikakomponentidest koosnevaid kiipe (ingl *field-programmable gate array*; FPGA). Kui lisada siia veel võimalus salvestada suures mahus signaale, töödelda neid võimsate protsessoritega ning kasutada näiteks kõnetuvastuseks tehisaru (AI)¹⁹, on hobikasutajate käsutuses vahendid, mis olid mõned kümnendid tagasi ka professionaalidele kättesaamatud. Tarkvararaadiod võimaldavad küllaltki kättesaadavate vahenditega koostada interferomeetrilisi suunamäärajaid²⁰, mille täpsus sõltub peale keskkonna parameetrite (ennekõike signaali sumbumine ja peegeldumine) mõistagi kasutatava riistvara kvaliteedist, kuid mis on siiski mitu hinnaklassi soodsamad²¹ kui senised riistvaral põhinevad lahendused. Tarkvararaadiod on leidnud Vene-Ukraina sõjas laialdaselt kasutust, teadaolevalt just Ukraina poolel.

Siiski tuleb arvestada, et kuigi prototüübi tasemel seadme koostehind on väike, nõuab lahinguväljal kasutatav lahendus töökindluse ja kasutusmugavuse saavutamiseks arendustööd, mis tõstab väikeste tootmismahude puhul märgatavalt lõpptooto hinda.

Üks tarkvararaadiote probleeme on ka vastuvõtja tundlikkus. See parameeter määrab, kui nõrka signaali on võimalik tuvastada, vastu võtta ja töödelda. Mida tundlikum on vastuvõtja, seda suurema tegevusraadiusega on seadmed ja seda kaugemalt saab signaali tuvastada. Tarkvararaadiotele saab tundlikkuse suurendamiseks lisada riistvaralisi madala müratasemega eelvõimendeid, kuid need tõstavad tunduvalt soodsate seadmete hinda.

Tarkvararaadiote kogu potentsiaali kasutamisel seavad piirangu andmemahud ning andmeedastuse ja -töötluse kiirus. Olukord on samasugune kui paljudes teistes valdkondades (ka luures), kus küsimus ei ole mitte niivõrd andmete saamises, kuivõrd nende töötlemises inimesele hoomatavaks teabeks. Näiteks töötab laialt levinud tarkvararaadio HackRF One²² diskreetimissagedusega 20 MSa/s (20 miljonit mõõtmist sekundis), 8-bitise signaali puhul tekib igas sekundis 20 MB andmeid (suurema bittide arvu puhul vastavalt rohkem). See tähendab, et 1 TB kõvaketta täitmiseks kulub

¹⁹ Rockbach, Jonas D.; Bluhm, Luka-Franziska; Schlangen, Isabel; Over, Laura; Apfeld, Sabine; Henneke, Lukas; Wilkinghoff, Kevin 2022. Towards Human-Machine Integration for Signals Intelligence Applications. – 2022 Sensor Data Fusion: Trends, Solutions, Applications (SDF), pp. 1–6. <https://doi.org/10.1109/SDF55338.2022.9931698>.

²⁰ Skinner, Sam; Patel, Kishan; Pittman, Jeremiah; Lebiednik, Brian; Vassallo, Frank; Duncan, Kate J. 2019. Direction Finding System using an N-Channel Software Defined Radio Implemented with a Phase Interferometry Algorithm. – 2019 SoutheastCon. Huntsville, Alabama, USA, pp. 1–5. <https://doi.org/10.1109/SoutheastCon42311.2019.9020650>.

²¹ KrakenSDR.

²² HackRF One. <https://greatscottgadgets.com/hackrf/one/> (15.09.2023).

umbes 50 000 sekundit ehk veidi alla 14 tunni. See võimaldab aga salvestada vaid 20 MHz riba spektrist, kuid tegelikult on isegi taktikalise häälside salvestamiseks vaja vähemalt 80 MHz ehk neli korda rohkem andmeid.

Elektromagnetspektris toimuva salvestamiseks kasutatakse spetsiaalseid formaate, mis jätavad järeltöötamiseks alles peaaegu kogu signaalis olnud info. Sel viisil salvestatud signaali on võimalik digitaalselt erinevate võtetega reaajas või hiljem salvestisena töödelda (nt filtreerida ja demoduleerida) ning teha sisuliselt kõiki operatsioone, mida varem tehti raadiojaama analoog-elektroonikas. Lihtsate matemaatiliste tehete abil on võimalik arvutada kõik signaali peamised parameetrid: ennekõike amplituud, faas ja sagedus.²³ Levinud operatsiooniks andmetöötlemises on Fourier' kiirteisendus (ingl *fast Fourier transform*; FFT), mis võimaldab luua tervikpildi sellest, milline on signaali amplituud eri sagedustel²⁴.

Suure andmemahu korral on juba andmeid salvestades vaja teha eelvalik, mida salvestatakse. Piisavalt võimekate algoritmide ja eelinfo põhjal on võimalik salvestada ainult see osa spektrist, kus toimub meid huvitav andmevahetus²⁵. Järeltöötamise käigus väheneb andmemahut vajadus veelgi, kuna üle 90% esmalt huvi pakkunud salvestistest ei ole tegelikku väärtust. Arvestada tuleb ka seda, et taktikalises olukorras vananeb informatsioon väga ruttu. Aktiivsema tegevuse ajal võib info olla väärtuslik vaid 15 minutit alates saamishetkest. Seega ei ole salvestiste pikaajaline säilitamine taktikalises olukorras mõistlik. Küll aga on see oluline pikema tsükliga elektroonilise toetuse korral.

Järeltöötlemises on kindlasti järjest suurem abi kõnetuvastusalgoritmidest. Algoritmide võimaliku rakenduse saab jagada mitmesse järjestikusesse etappi, mille keerukus üha suureneb. Esmalt saab algoritm automaatselt otsustada, kas salvestises on arusaadav inimkõne või on see juhuslik sahin vms. Teiseks

²³ Xue, R.; Xu, Q.; Chang, K. F.; Tam, K. W. 2005. A new method of an IF I/Q demodulator for narrowband signals. – 2005 IEEE International Symposium on Circuits and Systems, Vol. 4. Kobe, Japan, pp. 3817–3820. <https://doi.org/10.1109/ISCAS.2005.1465462>. Ziomek, Christopher D.; Corredoura, Paul 1995. Digital I/Q demodulator. – Proceedings Particle Accelerator Conference, Vol. 4. Dallas, TX, USA, pp. 2663–2665. <https://doi.org/10.1109/PAC.1995.505652>.

²⁴ Cheng, Chi-Hao; Lin, David M.; Liou, Lihyeh L.; Tsui, James B. 2012. Electronic Warfare Receiver with Multiple FFT Frame Sizes. – IEEE Transactions on Aerospace and Electronic Systems, Vol. 48, Issue 4, pp. 3318–3330. <https://doi.org/10.1109/TAES.2012.6324709>.

²⁵ Oliveira, Abel; Figueira, Nina 2021. An Application of Command, Control, Computing, Communication, Intelligence, Surveillance and Reconnaissance Systems in the Protection of the Amazon Rainforest. – 2021 International Conference on Electrical, Computer and Energy Technologies (ICECET). Cape Town, South Africa, pp. 1–5. <https://doi.org/10.1109/ICECET52533.2021.9698538>.

saab algoritm tuvastatud kõne transkribeerida ja vajadusel tõlkida. Kolmandaks saab algoritm anda hinnangu kõneluse prioriteetsusele ja sünteesida mitme kõneluse põhjal olukorrapildi, mida inimesele esitada.

Üldiselt on tänapäevased kõnetuvastusprogrammid teksti transkribeerimises ja tõlkimises piisavalt usaldusväärsed, kuid militaarrakenduste puhul tuleb arvestada, et raadioside keelekasutus erineb suuresti igapäevasest. Kasutatakse tahtlikult koodsõnu, et kõneluse mõistmist vastasele keerulisemaks teha, aga ka slängi, mille tõlkimine tavakeelest lähtudes võib viia väärtõlgendusteni.

Tehisaru ja masinõpet rakendatakse tänapäeval paljudes eluvaldkondades, erand ei ole siin ka EV. USA relvajõud sõlmisid 2019. aasta märtsis Northrop Grummaniga lepingu summas 982 miljonit dollarit, et moderniseerida küber- ja EV-vahendid tehisaru ja masinõppe meetoditega. Kognitiivne EV-süsteem on võimeline tajuma oma keskkonda, sellest õppima ning tegema varem õpitu ja hiljuti tajutu põhjal keerulistes olukordades otsuseid.²⁶

Nii või teisiti on selge, et tehisaru hakkab EV-vallas ja ka muudes valdkondades luureinfo töötlemisel järjest suuremat rolli mängima²⁷. Kuigi praegu jääb tulemuse kvaliteet inimese tehtule kohati veel alla, on tehisaru info-töötlemise kiiruses inimesest juba praegu väga suurel määral üle. See tähendab aga seda, et on võimalik töödelda ka sellist infot, millega tegelemiseks praeguste vahendite suutlikkusest ei piisa. Näiteks võib tuua hüpoteetilise stsenaariumi, kus tehisaru tuvastab raadiosidet kuulates, mobiililiikluse aktiivsust skaneerides ning liikumismustrit analüüsides vastase üksuste võitlusmoraali tuntava raugemise ning teeb ettepaneku alustada selle võimenduseks infooperatsiooni, pakkudes sõnumeid, mida raadioetrisse paisata.

Areng kõnetuvastuse, masintõlke ja tehisaru vallas võimaldab avatud kõne transkriptsiooni, vajadusel arusaadavasse keelde tõlkimist ning analüüsi lihtsustamiseks huvipakkuvate märksõnade või isegi fraaside otsingut.

Vastupidisel suunal on võimalik rakendada etteantud teemal teksti genereerimist ja kõnesünteesi eksitava informatsiooni suunamisel avatud kõne-sidevõrku. Masinõpe võimaldab lühikeste kõnenäidete põhjal sünteesida

²⁶ **Xiao, Qinghan** 2020. Cognitive Electronic Warfare: Conceptual Design and Architecture. – International Journal of Artificial Intelligence and Expert Systems (IJAE), Vol. 9, Issue 3, pp. 48–65. <https://www.cscjournals.org/manuscript/Journals/IJAE/Volume9/Issue3/IJAE-198.pdf> (15.07.2024).

²⁷ **Szabadföldi, István** 2021. Artificial Intelligence in Military Application – Opportunities and Challenges. – Land Forces Academy Review, Vol. 26, No. 2, pp. 157–165. https://www.researchgate.net/publication/352801264_Artificial_Intelligence_in_Military_Application_-_Opportunities_and_Challenges (15.07.2024).

suvalise inimese häält, mis suurendab lisaks eksliku informatsiooni tõesena võtmise võimalust. Üks olulisi märksõnu on sensorsulamil (ingl *sensor fusion*) põhinev lähenemine, kus mitme, tihti vähese kvaliteediga sensori signaalist pannakse kokku kvaliteetne koondpilt²⁸.

Tehnoloogia areng on pakkunud ruumandmete haldamise lahendusi, millest on elektroonilise toetuse valdkonnas olukorra visualiseerimisel suur abi. Siiski ei ole see lõpuni lahendatud probleem, sest sageduste dimensiooni lisamine neljamõõtmelisele aegruumile sel viisil, et koondpilt oleks inimesele hoomatav, on keeruline ülesanne, mille puhul standardlahendusi veel ei ole.

Elektroonilise rünnaku valdkonnas on põhimõttelised muutused olnud väiksemad: vastase raadiosignaali segamiseks vajatakse endiselt (suhteliselt) suuri väljundvõimsusi, milleks on tarvis spetsiifilisi ja kalleid pooljuhtlülitusi. Siiski leidub ka siin uusi lahendusi, mis kasutavad intelligentseid segamisalgoritme (nt vastase enda sidesignaali tagasisaatmine), vähendades nii võimsuse vajadust. Omaette tehniline proovikivi on segamise efektiivsuse hindamine. Tavapärased seiremeetodid ei võimalda sellal, kui võimas segaja töötab, kindlaks teha, kas segatavas raadiosidevõrgus side toimub või mitte. Sel puhul on kasutatud tavaliselt meetodit, kus segaja lülitatakse lühikeseks ajaks välja, et spektrit seirata²⁹. Tänapäeval arendatakse selleks laia dünaamilise diapasoniga seiresüsteeme, mis võimaldavad eristada nõrka sidesignaali tugevast segaja signaalist.

Küll aga on märkimisväärselt muutunud ja mitmekesisestunud sagedusvahemikud, mida on vastase mõjutamiseks vaja segada. Madalama taseme militaarside toimub paljuski VHF-sagedusalas, kuid kõrgema taseme side, aga ka tsiviillahenduste jaoks on vaja järjest kõrgemaid sagedusi. Näiteks Vene-Ukraina sõjast tuntuks saanud Starlink kasutab isegi üle 50 GHz sagedusi. See seab uusi nõudmisi ka segamishahenditele. Nii nagu muudes lahinguväljasüsteemides, tuleb vältida eelmise sõja sõdimist: tuleb olla valmis segama neid vahendeid, mida võimalik vastane järgmises konfliktis kasutab.

²⁸ **Chmielewski, Mariusz; Kukielka, Marcin; Pieczonka, Paweł; Gutowski, Tomasz** 2020. Methods and analytical tools for assessing tactical situation in military operations using potential approach and sensor data fusion. – *Procedia Manufacturing*, Vol. 44, pp. 559–566. <https://doi.org/10.1016/j.promfg.2020.02.255>.

²⁹ **Blanding, Wayne; Koch, Wolfgang; Nickel, Ulrich** 2006. Tracking Through Jamming Using Negative Information. – 9th International Conference on Information Fusion. Florence, Italy, pp. 1–8. <https://doi.org/10.1109/ICIF.2006.301813>. **Vardhan, Shesh; Garg, Anubhav** 2014. Information jamming in Electronic warfare: Operational requirements and techniques. – 2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE). Hosur, India, pp. 49–54. <https://doi.org/10.1109/ICECCE.2014.7086634>.

Vastupidi laialdaselt levinud arvamusele on tsiviillahendused kohati küllaltki segamiskindlad, kuid see ei tähenda, et neil ei võiks olla muud liiki haavatavusi. Näiteks kasutatakse Eestis 4G-mobiilsideks nelja sagedusriba (kõik neli riba on kasutatavad siiski vaid piirkondades, kus tugijaamu on palju). Praegu lisanduvad veel 5G-sagedusribad ja kuigi 3G-võime peagi kaob, jäävad 2G-sagedusribad, mis võimaldavad kõnesidet (2G protokollis on siiski turvanõrkusi).

Teisest küljest saab elektroonilise kaitse valdkonnast esile tuua arendusi, mis muudavad signaalide tuvastamise, pealtkuulamise ja segamise tunduvalt keerulisemaks. Kõige laiemalt levinud meede pealtkuulamise vastu on signaali krüpteerimine. Kuigi ajalooliselt on kasutatud ka analoogsignaali krüpteerimise lahendusi³⁰, on digitaalelektronika kasutuselevõtt muutnud signaali krüpteerimise märksa lihtsamaks. Tänapäeval on signaali krüpteerimine üldiselt standard nii militaar- kui ka tsiviilsektoris. Erandiks on vaid väga lihtsad laiatarbesüsteemid või ka sellised sidelahendused, mille signaal peabki kõigile avalik olema. Ka laiatarbe-tsiivilraadiojaamad lubavad kasutada näiteks AES-256 krüpteeringut, mida võib praeguse teadmise põhjal hinnata taktikatasandil kasutamiseks piisavalt turvaliseks. Samuti on tarkvararaadiote kasutuselevõtt muutnud märgatavalt kättesaadavamaks sagedushüplusega seadmete kasutamise.

Samas on keeruliste krüpteerimissüsteemide kasutamine muutnud järjest olulisemaks usalduse tootja vastu. On näiteid, kus ilma tootja teadaoleva paha-tahtlikkuseta on riist- või tarkvaravea tõttu dekrüpteerimisvõtme efektiivne pikkus tunduvalt vähenenud. Hästi teada on Eesti ID-kaartide turvaintsident³¹, kuid väidetavalt on sama laadi nõrkus leitud ka Motorola raadiojaamades³².

Arendatud on ka lai- ja ülilairibatehnoloogiat (ingl *ultra wideband* (UWB) *technology*), mis ühest küljest võimaldab kasutada suuremat andmemahu ja teisest küljest teeb sidesignaali avastamise tavapäraste meetoditega keeruliseks, kui mitte võimatuks. Näiteks võimaldab ülilairibatehnoloogia signaali laiali jagada 500 MHz ribale (mobiilses andmesides kasutatakse üldjuhul näiteks 10–20 MHz riba, ringhäälingu raadiojaamadel on kanali laius

³⁰ **Gersho, Allen** 1984. Perfect Secrecy Encryption of Analog Signals. – IEEE Journal on Selected Areas in Communications, Vol. 2, Issue 3, pp. 460–466. <https://doi.org/10.1109/JSAC.1984.1146071>.

³¹ **Parsovs, Arnis** 2020. Estonian Electronic Identity Card: Security Flaws in Key Management. – SEC'20: Proceedings of the 29th USENIX Security Symposium, pp. 1785–1802.

³² **Zetter, Kim** 2023. Code Kept Secret for Years Reveals Its Flaw—a Backdoor. – Wired.com. Security, July 24. <https://www.wired.com/story/tetra-radio-encryption-backdoor/> (15.07.2024).

ligikaudu 0,1 MHz), muutes selle eristamise taustamürast äärmiselt raskeks. Ülilairibatehnoloogiat kasutavad näiteks ka uuemad Apple'i telefonid ja käekellad rakenduse AirTag jaoks, mis võimaldab määrata asukohta väga täpselt, aga väikesel kaugusel. Ülilairibatehnoloogia miinus on tõsiasi, et piisava ribalaiuse saavutamiseks vajatakse kõrget sagedust, mis piirab leviulatust nii signaali sumbumise tõttu keskkonnas kui ka seetõttu, et levi on võimalik vaid otsenähtavusega.³³

Radaritehnoloogias kasutatakse avastamise raskemaks muutmise eesmärgil keerulise struktuuri ja heade korreleeruvate omadustega skaneerivaid signaale. Nende signaalide tööprintsip seisneb selles, et signaali energia jaotatakse pikema aja peale laiali, mis võimaldab vähendada signaali võimsust ja muudab selle vastase EV-seadmetele raskemini avastatavaks. Sellist tüüpi radareid nimetatakse madala avastusläävega radariteks (ingl *low probability of intercept* (LPI) *radar*).³⁴

4. Elektroonilise võitluse valdkonna perspektiivsed teadussuunad

On ilmne, et edukus EV-valdkonnas sõltub suurel määral kasutatavate tehniliste vahendite uudsusest. Nagu ka muudes valdkondades toimub võidujooks kaitse- ja ründevahendite vahel. Kui üks pool on välja töötanud näiteks parema segamiskindlusega sidevahendid, siis töötab vastane oma elektrooniliste ründevahendite täiustamise kallal, et teise eelist neutraliseerida. Kui vastasel see õnnestub, ei jää teisel poolel muud üle kui oma kaitsemeetmeid veelgi täiendada.

Mida vähem teab võimalik vastane sinu EV-vahendite tööpõhimõtteid ja parameetreid, seda raskem on tal vajalikke vastumeetmeid välja töötada. Seega on selge, et avalikult kättesaadav teave EV-valdkonna teadus- ja arendustööst on kas juba vananenud või peetakse seda väheoluliseks. Lugeja peaks seetõttu arvestama, et alltoodu ei kajasta valdkonna kõige uuemaid saavutusi, vaid annab heal juhul ainult ülevaate üldistest suundumustest.

³³ **Rahayu, Yusnita; Rahman, Tharek Abt; Ngah, R.; Hall, P. S.** 2008. Ultra-wideband technology and its applications. – 2008 5th IFIP International Conference on Wireless and Optical Communications Networks (WOCN '08). Surabaya, Indonesia, pp. 1–5. <https://doi.org/10.1109/WOCN.2008.4542537>.

³⁴ **Pace, Philip E.** 2009. Detecting and Classifying Low Probability of Intercept Radar. 2nd ed. Artech House.

Sidesüsteeme saab rünnata kas EV- või küberründevahenditega³⁵. Mõlemal juhul on võimalik saavutada sama lõpptulemus – vastase jaoks katkenud või häiritud side ja juhtimine. Esimesel juhul kasutatakse soovitud tulemuse saavutamiseks elektromagnetkiirgust, teisel juhul aga rünnatakse seadmete tarkvara. Mõlema ohu eest kaitsmiseks peab järjepidevalt sidesüsteeme arendama. Võimaliku vastase mõjutamiseks tuleb aga oma elektroonilise rünnaku vahendeid pidevalt uuendada.

Elektrooniliste vastumeetmete arengu tõttu ei pruugi senised, elektromagnetkiirgusel põhinevad sensorid olla enam piisavalt töökindlad. Seega on uueks arengusuunaks mitme erinevat tehnoloogiat kasutava sensori kombineerimine. Näiteks võib rakett lukustuda sihtmärgile radari abil, kui aga vastane seda segab, võib süsteem võtta automaatselt kasutusele hoopis infrapunakiirgusel põhineva lukustuse. Sellise kombineeritud lähenemise üks ilmselgeid miinuseid on süsteemi suurem keerukus ja hind.

Väheste intensiivsusega konfliktide asemel on lähitulevikus põhjust oodata suuremaid, konventsionaalsemaid konflikte, kuhu on kaasatud üks või mitu globaalset suurjõudu. Näiteks Vene-Ukraina sõja eskaleerumine, võimalik Hiina-Taiwani või Vene-NATO konflikt. Taolistes konfliktides on võimalik ka elektromagnetimpulsi (ingl *electromagnetic pulse*; EMP) kasutamine relvana, seega tuleb tähelepanu pöörata piisavate elektrooniliste kaitsemeetmete väljatöötamisele ja rakendamisele. EMP iseenesest ei ole relvana midagi uut, kuid kuna tegu on kõrgtehnoloogilise vahendiga, mis on kättesaadav ainult suurjõududele, ei ole seda väheste intensiivsusega konfliktides kasutatud.

Galliumnitriidi (GaN) kasutamine pooljuhina tavapärase räni (Si) asemel võimaldab valmistada pooljuhtseadmeid, millel on suurem kasutegur, mis taluvad kõrgemat temperatuuri ja juhivad varasemast paremini soojust. Kirjeldatud omadustega pooljuhtmaterjal võimaldab valmistada senisest kompaktsemaid raadio- ja EV-seadmeid. Muu hulgas saab valmistada täisdigitaalselt tüüritavaid antennivõresid, mida võib vaadelda tarkvararaadio kontseptsiooni edasiarendusena signaalide ruumilise filtreerimise suunas. Varem on selliseid tüüritavaid antennivõresid kasutatud näiteks lennukitele monteeritud radarites, kus ruum on piiratud ning seega klassikalise pööratava radariantenni kasutamine ei ole mõeldav.³⁶

³⁵ **Topor, Sorin** 2014. Approach about joint cyber and electronic warfare and futures of the military operations. – Proceedings: The 10th International Scientific Conference Strategies XXI “Strategic Changes in Security and International Relations”, Vol. 3, pp. 72–76.

³⁶ **Brukiewa, Thomas F.** 2016. First flight of a high power software defined electronic warfare system. – 2016 IEEE International Symposium on Phased Array Systems and Technology (PAST). Waltham, MA, USA, pp. 1–6. <https://doi.org/10.1109/ARRAY.2016.7832655>.

Taolise antenniga varustatud raadio võib täita laias vahemikus erinevaid ülesandeid, nii otseselt EV-ga seotud kui ka muid. Näiteks signaaliluure, elektrooniline toetus, elektrooniline rünnak, signaalliallikate suuna ja asukoha määramine, navigeerimine ja täpse aja määramine, side jms. Kombineerituna kognitiivse tehisaruga võib kindla ülesande valik olla automatiseeritud.

Taktikalises olukorras on aina olulisem signaaliluure ulatus. Kuna tavaliselt on kasutusel VHF- või UHF-sagedusala, on siin piirav tegur antennimastide kõrgus ja sellega seotud otsenähtavusala. Arvestamata kindlat maastikku ja pealtkuulatava raadio antenni kõrgust, on otsenähtavuse maksimaalne ulatus ehk optilise horisondi kaugus D_L (km) hinnatav järgmise valemiga³⁷:

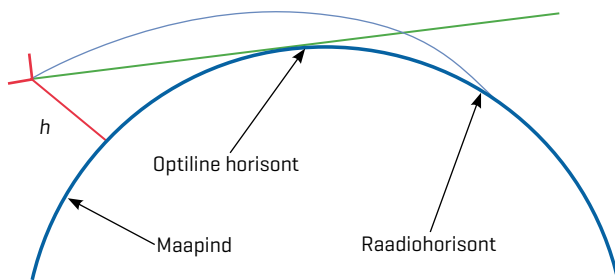
$$D_L \approx 3,57 \cdot \sqrt{h},$$

kus h tähistab antenni kõrgust (m).

Arvestades raadiolainete levi iseärasusi, kasutatakse ka terminit *raadiohorisont*, mis on Eesti oludes tavaliselt optilisest otsenähtavusest suurem. Üks lihtsamaid variante hinnata raadiohorisondi D_R (km) kaugust mastist on kasutada järgmist valemit.

$$D_R = 4,12 \cdot \sqrt{h}.$$

Optilist ja raadiohorisonti illustreerib alljärgnev joonis.



Joonis. Optiline ja raadiohorisont

Võib tuua näite, et kui luuresensori masti kõrgus oleks 10 m, võiks see ideaaljuhul (valemi järgi) aidata pealt kuulata radiojaamu, mis asetsevad kuni 13 km kaugusel. Reaalsuses on see ulatus siiski väiksem, sõltudes konkreetsest

³⁷ **Everything RF.** <https://www.everythingrf.com/rf-calculators/line-of-sight-calculator> (25.09.2023).

sagedusest, seejuures on täpsemate hinnangute saamiseks vaja kasutada spetsiifilisemaid levimudeleid. Üldiselt kehtib reegel, et mida kõrgem mast, seda suurem on luuresensori tegevusraadius.

Tänapäeval ulatuvad taktikatasandil kasutatavad mastisüsteemid sellise kõrguseni, mis tagab minimaalselt vajaliku seireulatuse. Tavaliselt vajavad need eraldi toetust ja nende paigaldamine on aeganõudev. Automaatsed teleskoopmastid on üldjuhul väga kallid ja rasked. Mõistliku suurusega teleskoopmastid suudavad ilma toetuseta toimida kuni 20 m kõrguseni. Arvestada tuleb ka seda, milline on masti otsa paigaldatava seadmestiku kaal ja tuule tugevus. Miniaturiseerimise ja täisdigitaalsete antennivõrede koostamisega saab tulevikus antennivõrede moodustamiseks ja signaali-luure ulatuse suurendamiseks kasutada väikeste mõõtmetega mehitamata õhusõidukisüsteeme (ingl *unmanned aerial systems*; UAS). Sellisel juhul kannaks iga UAS mitte tervet antennivõret, vaid ühte antennivõre elementi ning antennivõre moodustuks UAS-ide parve alusel. Selline lahendus võimaldaks vajadusel muuta ka antennivõre konfiguratsiooni (elementide arvu, sagedust, suunadiagrammi kuju jm). Siiaamaani on selle lahenduse teostamist raskendanud antennivõre elementide omavaheline sünkroniseerimine läbi õhu, kuid probleemile on hakatud leidma lahendust ülilairibatehnoloogia või kommunikatsiooniprotokolli tasandil³⁸.

Suunatud elektromagnetenergia kasutamine relvana (ingl *directed energy weapon*; DEW) on üks elektroonilise rünnaku vahenditest, mis on võimeline teatud sihtmärke ka füüsiliselt kahjustama ja hävitama. Peamiselt on tegemist laserrelvade kasutamisega UAS-ide vastu ehk C-UAS-i (ingl *counter-unmanned aircraft systems*) rakendustega. Arengusuundadeks on suunatud energiaga relvade ja nende energiaallikate miniaturiseerimine ning osaliselt sel viisil ka nende relvade mobiilsuse suurendamine. Iisrael on juba mõnda aega tagasi demonstreerinud lennukile paigutatud energiarelva Iron Beam. VF-i strateegiliste raketivägede teenistuses on aga teadaolevalt viis või kuus Peresveti (vn Пересвет) süsteemi, mis on väidetavalt võimelised hävitama selge ilma korral mitme kilomeetri kaugusel lendavaid UAS-e³⁹.

³⁸ **Prager, Samuel; Haynes, Mark S.; Moghaddam, Mahta** 2020. Wireless Subnanosecond RF Synchronization for Distributed Ultrawideband Software-Defined Radar Networks. – IEEE Transactions on Microwave Theory and Techniques, Vol. 68, Issue 11, pp. 4787–4804. <https://doi.org/10.1109/TMTT.2020.3014876>.

³⁹ **Hendrickx, Bart** 2020. Peresvet: a Russian mobile laser system to dazzle enemy satellites. – The Space Review, June 15. <https://www.thespacereview.com/article/3967/1> (29.09.2023).

Üks viimase aja keskseid teemasid on UAS-ide segamine ja tõrjumine⁴⁰. UAS-ide leidmiseks, tuvastamiseks ja asukoha määramiseks saab kasutada nii akustilisi, optilisi kui ka raadiotehnilisi meetodeid. Tarkvararaadio abil saab UAS-e nende raadiosignatuuri põhjal tuvastada või nende asukohta määrata. Tuvastatud lennuvahendi saab füüsiliselt hävitada, segada selle raadiosidet või üritada juhtimist üle võtta. Segamiseks vajalik signaali võimsus on üldjuhul suurem, kui on võimalik saada tarkvararaadio väljundist, seega on vaja lisa-võimendit või koguni eraldi seadet, nn droonitõrjepüssi. Neid valmistavad ka Eesti kohalikud ettevõtted⁴¹.

Siingi puutume kokku järjest enamate sagedusribade segamise vajadusega. Suurem osa tänapäevaseid tsiviilkasutuses UAS-e on võimelised kasutama vähemalt kahte sagedusribade sagedust (2,4 GHz ja 5,8 GHz). Hiljuti on lisandunud ka kolmas sagedusala⁴², nt 5,2 GHz, aga ka 900 MHz (sageduskasutust reguleerivate õigusaktide tõttu on siin olukord USA-s ja Euroopas märgatavalt erinev). Nii mõnigi UAS on võimeline lendama ka 4G-andmesidet kasutades. Militaar- ja kahetise kasutusega UAS-idel on sagedusribade kasutamisel veelgi mitmekesisemad, näiteks kõrgema hinnaklassi UAS-idel laialt levinud Silvuse raadiolink⁴³ võimaldab kasutada sagedusvahemikke 1,35–1,44 GHz, 2,2–2,5 GHz ja 4,4–4,94 GHz (üldjuhul mitte kõiki vahemikke ühes seadmes). Sealjuures kasutatakse korraga 1,25–5 MHz laiusega sidekanalit, mis võimaldab ühe sagedusvahemiku segamise korral üle minna teisele sagedusele.

Siiski on paljude UAS-ide haavatavuseks sõltuvus globaalsest satelliitnavigatsioonisüsteemist (GPS, GLONASS, Galileo, Beidou). GNSS-i segajad on järjest laiemalt kättesaadavad, see võime on ka praegu turul saadaval nn droonitõrjepüssidel. Eriti mõjus on GNSS-i segamine, kui seda tehakse õhuvahendilt. Maapinnal paiknevate GNSS-i segajate vastumeetmena on võimalik kasutada navigeerimissignaali vastuvõtmiseks suundantenne ja varjestust segava signaali eest. GNSS-i segamise vastumeetmeks on ka alternatiivsete navigeerimissüsteemide (nt inertsiaalne, visuaalne, stellaarne) kasutamine, kuid need tõstavad märgatavalt UAS-i hinda.

⁴⁰ Wang, Jian; Liu, Yongxin; Song, Houbing 2021. Counter-Unmanned Aircraft System(s) (C-UAS): State of the Art, Challenges, and Future Trends. – IEEE Aerospace and Electronic Systems Magazine, Vol. 36, Issue 3, pp. 4–29. <https://doi.org/10.1109/MAES.2020.3015537>.

⁴¹ Vt nt PJ-2458G-3. <https://rantelon.ee/toode/pj-2458g-3/> (13.09.2023).

⁴² Autelpilot. <https://www.autelpilot.com/products/autel-robotics-evo-nano-plus-drone-premium-bundle?variant=39550210768942> (15.09.2023).

⁴³ Silvus Technologies. <https://silvustechologies.com/products/streamcaster-radios/> (15.09.2023).

Nagu mainitud, on UAS EV kontekstis lisaks ohule, millega tuleb võidelda, ka platvorm, mis pakub võimalusi. Juba varasemast on teada, et elektrooniline toetus on õhuvahenditelt märksa tõhusam kui maapinnal. Lennukeid on EV-s kasutatud juba Teisest maailmasõjast alates. Nii jääb signaaliallika ja EV-vahendi vahele vähem sumbumust, peegeldusi ja häireid tekitavat keskkonda (taimestik, pinnavormid, inimtekkelised objektid jm). Madalamatel sagedustel taandub signaali sumbumine sisuliselt vaba ruumi (ingl *free space path loss*; FSPL) kaole ja võimalikud tuvastuskaugused (kõrgused) on suured. EV UAS-idelt eeldab kahe tehnoloogilise tingimuse täidetust: piisava kandevõimega UAS ning piisavalt kompaktsed ja kerged EV-seadmed. Praegu on USA-l ja Austraalia käsil vananenud AN/ALQ-99 EV-süsteemi väljavahetamine moodsa NGJ-süsteemi (ingl *Next Generation Jammer*) vastu. UAS-ide kandevõime on olnud juba mõnda aega piisavalt suur, et neid saab kasutada ka EV-platvormina. Näiteks kasutab VF EV ülesannete täitmiseks laialdaselt mehitamata lennuvahendit Orlan-10. USA-s kannab EV-süsteemi NERO (ingl *Networked Electronic Warfare Remotely Operated*) UAS MQ-1C Gray Eagle⁴⁴. Nüüdseks oleme jõudnud nii kaugele, et isegi kommertstoodete puhul on mõlemad tingimused täidetavad. On kujunenud olukord, kus varem pigem riikide pärusmaaks olnud EV õhust on kindlate teadmiste ja oskuste korral kättesaadav ka hobikasutajatele.

Varitseva õhuründemoona (VÕRM) laialdane kasutuselevõtt on tekitanud suure nõudluse aktiivsete kaitsesüsteemide järele. VÕRM on väga sarnane UAS-idega, paljudel juhtudel ongi tegemist kommerts-UAS-i külge kinnitatud lõhkelaenguga. Kuna UAS-ide kasutamine on olnud probleem juba mõnda aega, on töötatud välja meetodeid nende vastu võitlemiseks. Osal juhtudel saab C-UAS-i meetodeid kasutada ka VÕRM-i vastu, kuid mitte alati. Seega jääb vajadus kohendada EV-vahendeid kaitseks VÕRM-i vastu.

Üks huvitavaid suundi on EV kosmosest. Suured kosmoseriigid alustasid seda juba möödunud sajandi teisel poolel. Nagu eespool õhuvahendite kohta esile sai toodud, on signaali sumbumine kosmoses minimaalne (takistav asjaolu on teatud sagedustel siiski maa atmosfääri, ennekõike ionosfääri läbimine). Sel juhul ei ole suur kaugus takistus. Ühelt satelliidilt kaetav ala on määratult suurem kui maapinnalt ühe seirejaamaga kaetav. Nagu kõik, mis seostub satelliitluurega, on seegi valdkond olnud suuresti salastatud. Praeguseks on aga turule ilmunud eraettevõtted, mis pakuvad teenusena satelliidipõhist

⁴⁴ Moudy, Adrienne 2014. Army tests putting NERO electronic warfare jammer on UAVs. – U.S. Army, July 11. https://www.army.mil/article/129608/army_tests_putting_nero_electronic_warfare_jammer_on_uavs (13.09.2023).

elektroonilist toetust. Näiteks USA ettevõtte HawkEye 360 pakub nii kiirgusallikate tuvastamist, asukoha määramist kui ka mõõtmistulemuste analüüsi, seejuures suudetakse väidetavalt tuvastada ka käsiraadiojaamu⁴⁵. Selline võime paneb proovile elektroonilise kaitse, sest muudab kiirgusmustrite varjamise väga keeruliseks.

5. Venemaa Föderatsiooni elektroonilise võitluse võime ja esmajärelused Vene-Ukraina sõjast

VF loeb oma raadioelektroonilise võitluse alguseks Vene-Jaapani sõda aastatel 1904–1905⁴⁶. Nagu eespool käsitletud, on EV ja raadioside ajalugu lahutamatud ning järgivad sama loogikat, mis ülejäänud lahinguväljasüsteemide areng: mingi süsteemi ja meetme arengule järgneb peagi vastumeede, millele leitakse omakorda vastumeede. See põhimõte kehtib mõistagi ka väljaspool EV-d.

Autorite hinnangul võib öelda, et Nõukogude Liidu keskkond oli EV-võime arenguks mitmeti soodne. Nõukogude ühiskond soosis inseneriteadusi paljuski sõjalise rakenduse tõttu. Raadiotehnilisi uurimisinstituute oli nii tsiviil- kui ka militaarsfääris palju ja nende tase oli korralik. Teisest küljest hakkas pärast Nõukogude Liidu sõjajärgset esmast tehnoloogilist edu ilmnema üha tugevam mahajäämus USA-st. EV-d võib siin pidada vastumeetmeks, mis sarnaneb õhutõrjega: kergem on segada ja hävitada vastase kõrgtehnoloogilisi lahendusi (õhuvahendid, side- ja radarisüsteemid) kui endale samasugust võimet luua. Üldjuhul on elektroonilise rünnaku süsteemid tehnoloogiliselt lihtsamad ja soodsamad kui side- ja seirelahendused, mida nad häirivad ja hävitavad. Nõukogude Liit kasutas elektroonilise rünnaku meetmeid ka omaenda tsiviilühiskonna vastu, takistades lääne raadio- ja teleasaadete vastuvõttu⁴⁷.

Avalike allikate kaudu kättesaadavate koosseisutabelite ja seadmete kirjelduse põhjal on VF-i relvajõudude EV-võime väga hea. Motolaskurbrigaadi kui vähima enam-vähem iseseisvalt tegutseva üldvägede üksuse koosseisus

⁴⁵ **HawkEye 360**. <https://www.he360.com/> (15.09.2023).

⁴⁶ **Иванов, О.** 2009. Радиоэлектронная борьба: вчера, сегодня и завтра. – Российское военное обозрение, № 7 (66).

⁴⁷ **Trapans, Jan Arveds** 1988. The Baltic States and Western radio broadcasts: The role and estimated impact of radio free Europe. – Journal of Baltic Studies, Vol. 19, Issue 2, pp. 93–100. <https://doi.org/10.1080/01629778800000011>.

on ette nähtud EV-rood (lääne mõistes kompanii), mille koosseisu kuuluvad erinevate sagedusalade segajad. Need hõlmavad lühilainet, GNSS-i (GPS jms), lihtsamat satelliitsidet ja raadiolaineid kasutavaid sütikuid.⁴⁸ Teadaolevalt on VF allutanud EV-üksusi viimastel aastatel laialdaselt kasutatud pataljoni taktikaliste gruppide (PTG) koosseisu⁴⁹. Lisaks on brigaadi luurepataljonis raadiotehniliste luurevahendite rood, kus on erinevad raadiospektri seireseadmed. Kasutusele on võetud uusi süsteeme. Suuremat avalikku tähelepanu on pälvinud kompleksi Borisoglebsk-2 kasutuselevõtt⁵⁰, millega vahetati välja vanemad süsteemi R-330 seadmed. Motolaskurbrigaadis on ka UAS-i rood, kuhu kuuluvad näiteks mehitamata õhusõidukid Orlan-10, mida kasutatakse EV-süsteemis Leer-3⁵¹. Kaudselt võib siia nimekirja lisada veel radarid, mis avastavad sihtmärke nii õhus kui ka maismaal, sealjuures tuvastavad laskekehade trajektoori järgi kaudtulesüsteemide asukoha.

Oluline on märkida, et VF on mõistnud tsiviillahenduste tähtsust ja samas haavatavust lahinguväljal. Lisaks süsteemidele, mis võimaldavad segada näiteks mobiilsidet ja GNSS-e, on ka mõned küllaltki teravmeelsed lahendused. Üks selliseid on spetsiaalsete mobiilside tugijaamade kasutamine, mille abil luuakse võltsitud sidevõrgud⁵². Telefon, millele on rünne suunatud, ühendub oma operaatori võrgu asemel tugijaamaga, mida kontrollib kolmas pool (siinses kontekstis VF-i EV-üksus). Nii tekib võimalus kuulata pealt kõnesid, lugeda sõnumeid, jälgida telefonide liikumist jms. Selline võime on näiteks UAS-il põhineval süsteemil Leer-3. Teisest küljest on Vene-Ukraina sõda

⁴⁸ **Grau, Lester W.; Bartles, Charles K.** 2016. The Russian Way of War: Force Structure, Tactics, and Modernization of the Russian Ground Forces. Foreign Military Studies Office (FMSO). Fort Leavenworth, USA, p. 289. <https://www.armyupress.army.mil/portals/7/hot%20spots/documents/russia/2017-07-the-russian-way-of-war-grau-bartles.pdf> (16.07.2024). [**Grau, Bartles** 2016]

⁴⁹ **Singh, Mandeep** 2023. Russian Electronic Warfare in Ukraine 2022–2023. – Indian Defence Review, Vol. 38, No. 2, July 7, pp. 15–19. <http://www.indiandefencereview.com/news/russian-electronic-warfare-in-ukraine-2022-2023/> (25.09.2023).

⁵⁰ **SP's Landforces** 2019. Russia's Borisoglebsk-2 electronic warfare complex enters service. Issue 1. <https://www.spslandforces.com/story/?id=599&s-Borisoglebsk-2-electronic-warfare-complex-enters-service> (15.09.2023).

⁵¹ **Nikolov, Boyko** 2022. Russian Leer-3 jams GSMs in Ukraine and sends SMS for provocation. Bulgarianmilitary.com, October 19. <https://bulgarianmilitary.com/2022/10/19/russian-leer-3-jams-gsms-in-ukraine-and-sends-sms-for-provocation/> (29.09.2023).

⁵² **Bhushan, Bharat; Sahoo, G.; Rai, Amit Kumar** 2017. Man-in-the-middle attack in wireless and computer networking – A review. – 2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA) (Fall). Dehradun, India, pp. 1–6. <https://doi.org/10.1109/ICACCA.2017.8344724>.

näidanud, et kõikide uute tsiviillahendustega ei suuda VF-i EV hakkama saada – hea näide on Ukrainas laialdaselt kasutatav Starlink.

Kõrgemal tasemel on sõjaväeringkondades EV-brigaadid (lääne sõjaväeringkonnas kaks, teistes üks)⁵³. Nende üksuste koosseisu kuuluvad kõrgema taseme süsteemid. Kõrgem tase võib ilmnedas kahes mõõtnes. Esiteks kuuluvad siia võimsamad süsteemid, mille tegevusraadius on märksa suurem kui motolaskurbrigaadis kasutatavatel süsteemidel. Tehnoloogiliselt huvipakkuvam on aga teine seadmete klass, mis on suunatud vastase (NATO riikide) operatsioonilis-strateegiliste sidesüsteemide vastu. Sellised süsteemid on erinevad satelliitside- ja seiresüsteemid, kuid ka õhuväe sidesüsteemid ning radarid. Konflikti algul pälvis tähelepanu ühe Krasuhha-2/4 süsteemi Ukraina kätte langemine Kiievi lähedal⁵⁴.

Oluline on tähele panna, et avalike allikate põhjal teame ennekõike seda, mida VF väidab endal olevat. Nende süsteemide tegelike tehniliste parameetrite ja suutlikkuse kohta on aga väga vähe infot. Peaaegu kogu kättesaadav materjal on pigem VF-i päritolu ja seega tõenäoliselt tugevasti propagandistlik. Puudub info selle kohta, milline on VF-i EV-üksuste väljaõppetase.

Autoritele on teada, et vähemalt mõnes üksuses oli Nõukogude Liidu ajastu lõpus väljaõppetase madal ja suur osa tehnikast polnud töökorras. Tegelikult ei ole ka selget ülevaadet, kui paljudes motolaskurbrigaadides on EV-roodud formeeritud, varustatud ja võitlusvõimelised. Lääne eksperdid rõhutavad, et nii nagu teiste relvaliikide puhul on ka EV väljaõpe ja koostöö teiste üksustega ülioluline⁵⁵.

Võib arvata, et siiani kestev Vene-Ukraina konflikt toob selles vallas mõneti selgust ka avalikesse allikatesse. Ukraina kätte langenud VF-i tehnika annab aga vähemalt luureteenistustele väga hea ülevaate selle tõelistest parameetritest ja võimest.

Kaugele ulatuvaid järeldusi on siiani kestva konflikti rohke infomüra tingimustes veel vara teha. Siiski võib öelda, et VF kasutab kõiki EV elemente,

⁵³ **McDermott, Roger N.** 2017. Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum. Report, September. – International Centre for Defence and Security, Estonia, pp. 1–36. https://icds.ee/wp-content/uploads/2018/ICDS_Report_Russia_Electronic_Warfare_to_2025.pdf (16.07.2024). [**McDermott** 2017]

⁵⁴ **Clark, Bryan** 2022. The Fall and Rise of Russian Electronic Warfare. – IEEE Spectrum, July 30. <https://spectrum.ieee.org/the-fall-and-rise-of-russian-electronic-warfare> (15.09.2023).

⁵⁵ **Fischer, Jeffrey H.** 2022. A Key Reason for Russia's Colossal Electronic Warfare Failure in Ukraine. – The Defense Post, April 13. <https://www.thedefensepost.com/2022/04/13/russia-electronic-warfare-failure-ukraine/> (15.09.2023).

kuid nende aktiivsus on eri rindelõikudes väga erinev. Palju saab tähelepanu UASi-vastane tegevus. On väidetud, et Ukraina kaotab 10 000 UAS-i kuus⁵⁶ ja seda ilmselt peamiselt VF-i EV-vahendite tõttu.

Üks olulisi aspekte on GNSS-ide segamine, mida VF teeb laialdaselt. Märke sellest, et VF ja talle sõbralikud riigid GNSSi-vastaseid tegevusi sooritavad, on juba varasemast, kuid täiemõõtmelises konfliktis on see eriti ulatuslik. Kuivõrd paljud lääne relvasüsteemid kasutavad GNSS-lahendusi nii navigeerimiseks kui ka täpseks aja määramiseks, annab GNSS-i segamine VF-ile võimaluse lääne relvastuse tehnoloogilist üleolekut veidi vähendada. Analüüsides GNSS-i häiringute paiknemist, on selge, et nii mõnigi neist on loodud VF-i enda territooriumil paiknevate oluliste objektide kaitseks⁵⁷.

Vastuoksusena tasub välja tuua, et kuigi VF-i doktriinide loojad ja tehnoloogiaarendajad on hästi mõistnud tsiviilsidesüsteemide ning loomulikult ka krüpteerimata sidesüsteemide haavatavust, ei tähenda see, et VF-i taktikalised üksused ise sellega arvestaks. Vene-Ukraina sõjast on arvukalt näiteid, kus VF-i üksused kasutavad krüpteerimata sidet ja Ukraina mobiilsidevõrku. Viimasel juhul saavad Ukraina mobiilioperaatorid kõnesid pealt kuulata ja kogu muud infot seirata. Kuivõrd VF-i kasutatav krüpteerimata lühilaineside levib väga kaugele (soodsatel juhtudel üle terve Maa), on VF-i üksuste lühilainesidet kuulanud ja salvestanud paljud raadioamatöörid. Sõja esimestel kuudel oli isegi internetikanaleid, mis võimaldasid VF-i sidekanaleid reaalsajas jälgida. Olgu märgitud, et teadaolevalt on VF-i relvajõudude kasutuses lühilainejaamad, mille sidet saab krüpteerida⁵⁸. See viitab eelmainitud võimalikele probleemidele: üksustes ei ole krüpteeringuga jaamasid, krüpteeringuseadmed ei ole töökorras või neid ei osata või ei soovita kasutada.

Eespool käsitletust nähtub, et tänapäevase EV keerukus ja efektiivsus peitub paljuski tarkvaras, eriti elektroonilise toetuse puhul. VF-i EV tarkvara-võime kohta on avalikes allikates usaldusväärseid andmeid vähe. Autorite

⁵⁶ **Watling, Jack; Reynolds, Nick** 2023. Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine. – Royal United Services Institute (RUSI) for Defence and Security Studies, May 19, p. 18 (pp. 18–19). <https://static.rusi.org/403-SR-Russian-Tactics-web-final.pdf> (16.07.2024).

⁵⁷ **GPS Jam.** <https://gpsjam.org/?lat=55.95752&lon=37.48060&z=4.8&date=2023-09-23> (25.09.2023).

⁵⁸ **Cranny-Evans, Sam; Withington, Thomas** 2022. Russian Comms in Ukraine: A World of Hertz. – Royal United Services Institute (RUSI), March 9. <https://rusi.org/explore-our-research/publications/commentary/russian-comms-ukraine-world-hertz> (15.09.2023).

hinnangul võib üks põhjusi olla ka see, et kasutatakse välismaiseid seadmeid ja tarkvara, mida ei taheta presenteerida.

Lisaks raadioside arengule on tähtis tegur VF-i üldine tehnoloogiline tase. Arvestades VF-ile kehtestatud sanktsioone, võib oletada, et ei suudeta taas-toota keerulisemaid EV-seadmeid ja pärsitud on ka EV arendustegevus. Seda valdkonda on mõjutanud kindlasti ka spetsialistide lahkumine Venemaalt. Teisest küljest tuleb arvestada, et EV ründe vahendid on tehnoloogiliselt küllaltki lihtsad ja neis kasutatakse paljusi samu komponente, mida näiteks tsiviilides, seejuures on paljud komponendid ka erasikutele vabalt kättesaadavad. Analoozkomponentide puhul on VF-il mingil tasemel riigisisene tootmisvõime ja oskusteave⁵⁹. Seetõttu on siinse artikli autorite esmahinnang, et VF säilitab ja taastoodab algtasemel EV-vahendeid, kuid keerulisemate lahenduste arendus on pärsitud. NATO riikide vaatepunktist on kahtlemata üks võimalikke ohte VF-i koostöö Hiinaga.

6. Väikeriigi väljakutsed ja võimalused

Suurriigid suudavad katta kogu EV-vahendite spektri, kuigi fookus on riigiti erinev. Laias laastus saab öelda, et NATO suurriikide EV-võimed on keskendunud ennekõike õhusõjale: fookuses on radarid ning nendega seotud meetmed ja vastumeetmed. Paljusi on see tingitud sellest, et õhusõjas kasutatavad vahendid on kallid ja keerulised, mistõttu on nende kaitsmine oluline, ning teisest küljest võib nende ründamine EV-vahenditega anda väga kulutõhusa tulemuse. Vähetähtis ei ole seegi, et piloodi sisuliselt ainus väljapoole kokpitti ulatuv suhtlusviis on raadioside. Nagu eespool mainitud, paneb VF maa-vägede toetamisele EV-vahenditega suuremat rõhku⁶⁰.

Väikeriigil nagu Eesti ei ole võimalik ega ka mõistlik välja arendada kogu võimete diapasooni. Keskenduda tuleb ennekõike nendele võimetele, mis annavad konflikti korral võimaliku vastasega suurima efekti.

EV-vahendite väljatöötamine on aeganõudev ja kallis. Selles vallas tegutseb mujal maailmas palju suurettevõtteid, nagu Rohde & Schwarz, Keysight, Thales ja TCI. Neil on suured arendusmeeskonnad, tänu mastaabiefektile on neil arendusteks piisavalt ressursi. Ka Eestis on selles valdkonnas tegutsevaid

⁵⁹ **Веселова, Э.** 2015. Российская микроэлектроника: ренессанс или реанимация? – ЭКО, № 4, с. 36–49. <https://cyberleninka.ru/article/n/rossiyskaya-mikroelektronika-renessans-ili-reanimatsiya/viewer> (16.07.2024).

⁶⁰ **Grau, Bartles** 2016. Vt ka **McDermott** 2017.

või tegutsenud ettevõtteid. Tallinna Tehnikaülikoolis on tehtud EV-vallas uuringuid ja valmistatud EV-seadmete prototüüpe. Tartu Ülikool on loonud koostöös Kaitseväge Akadeemiaga Kaitsevägele mitu lahendust. Siiski on Eesti ettevõtete ressurss selles vallas piiratud.

Spetsiifiliste seadmete ja süsteemide nullist väljatöötamine ei pruugi olla nimetatud piiranguid arvestades jõukohane. Nii riist- kui ka tarkvara seisukohast oleks mõistlik kasutada olemasolevaid lahendusi ning piirduda peamiselt liidestamise ja optimeerimisega. Vene-Ukraina sõja kogemus on näidatud, et käepärastest laiatarbeseadmetest on võimalik ehitada tõhusaid süsteeme. Näiteks nutiseadmetel põhinev tulejuhtimisrakendus või tsiviil-otstarbeliste droonide kasutamine erinevate sõjaliste eesmärkide täitmisel. Tsiviilseadmetel on siiski vajakajäämisi, nagu vähene häirekindlus, võimalikud turvanõrkused ja piiratud vastupidavus välistingimustes. Seda kompenseerivad laialdane kättesaadavus, madal hind ja asjaolu, et nende kasutamiseks ei ole vaja eriväljaõpet.

Vajaliku riistvara saab enamasti realiseerida juba eespool kirjeldatud tarkvararaadioga, mida on võimalik hankida erineva suutlikkusega ja olenevalt sellest eri hinnaklassis. Ainuüksi raadioseadmest ei piisa, lisaks on tarvis nii antenne ja kõrgsageduskaableid kui ka toite- ja juhtseadmeid. Spetsiifilistes rakendustes võib vaja minna ka keerukamaid raadiosageduslikke komponente ja süsteeme, nagu antennivõred, kõrgsageduslülitid, suundhargmikud ning eel- ja võimsusvõimendid. Lihtsamaid tarkvararaadioid ning vähemalt mõnda eespool nimetatud kõrgsagedusseadet peaks olema võimalik toota ka Eestis. Meil on ka pikaajaline kogemus ja teadmised raadiosignaalide segajate vallast. Selle alusel oleks võimalik töötada välja keerukamaid süsteeme.

Moodsate sidevahendite puudus, olemasolevate vahendite halb seisukord ja kasutajate puudulik väljaõpe on võimalikud põhjused, miks VF-i relvajõud kasutavad Vene-Ukraina sõjas ohtralt mobiiltelefone ja krüpteerimata raadiosidet. Tarkvararaadioga on lahtise side pealtkuulamine lihtne.

Tarkvararaadio riistvarale ja vabatarkvarale tuginedes on võimalik luua eespool kirjeldatud mobiilside pettevõrke, mille abil saab pealt kuulata vastase sidet või mõjutada psühholoogiliselt tema isikkoosseisu. Koostöös kodumaiste mobiilsideoperaatoritega on ilmselt võimalik sama teha kommerts-kasutuses mobiilsidevõrkudes, mida näitab ka Ukraina kogemus.

Vastase kasutuses mobiilsideadmete asukoha määramine annab olulist informatsiooni nii vastase arvukuse, paiknemise kui ka liikumissuundade ja -aja kohta. Seadmete asukohta on võimalik määrata kas eraldi spetsiaalsete seadmetega või koostöös mobiilsideoperaatoritega.

Laiemas vaates saab tarkvararaadio abil rakendada kõiki võimeid, mida klassikalised side-, seire- ja EV-seadmed võimaldavad. Tarkvararaadio paindlikkusest tulenevat eelist saaks ära kasutada kombineerituna masinõppega. Tulemuseks võiks olla kognitiivne EV-süsteem, mis suudaks tajuda elektromagnetspektris toimuvat, analüüsida seda ja saadud tulemuste põhjal ennast optimaalselt ümber seadistada. Kaugemale ulatuva sammuna vääriks uurimist selliste süsteemide laiem automaatne koostöö. Näiteks laiale alale puistatuna, kuid omavahel sideühendustega seotud sensorite võrgu ehk vārk-vōrguna (ingl *Internet of things*; IoT).

Piiratud ressursside tõttu ei ole kõik nimetatud võimalused rakendatavad ja arengusuundi tuleb hoolikalt valida. Mōistlik on kasutada ära senised oskused ja olemasolevad vahendid ning tegelda nende arendamise ja mõju suurendamisega. Viimase aja areng tehisaru ja masinõppe vallas on näidanud selle tehnoloogia suurt potentsiaali paljudes valdkondades. Ilmselt ei ole ka EV erand. Masinõppe ja tehisaru mudelid ja tööriistad on muudetud kasutajale järjest mugavamaks ning vabamalt kättesaadavaks, samuti on Eestis vähemalt mõnetine pädevus nende rakendamises.

Üsiksikvōitleja ehk sõdur tähendab EV mõttes pigem haavatavust kui vōimet või vōimekordistajat. Vōitleja vōib reeta enda asukoha signaalide kaudu, mis kiirguvad tema mobiiltelefonist või raadiosaatjast. Vōitleja kehasoojus teeb ta mārगतavaks infrapunasppektris. Seda riski nāitlikustab Nodar Kharshiladze, endise Georgia asekaitseministri 2014. aastal jagatud tõdemus 2008. aasta sõja kohta Venemaaga: „Meie sõjavāel olid Ameerika sidesüsteemid, kuid me ei saanud neid kasutada. Me lihtsalt ei teadnud, kuidas teisele kanalile lūlituda, kui venelased hakkasid meie raadiolaineid segama.“

Nagu Lennart Meri 1997. aastal ütles, on vōtmetāhtsusega vāljaōpe, mis sūnnib tehnoloogia arendamise ja kasutuselevōtuga samas taktis. Oskused, mis vajavad täpsustamist ja vajadusel täiendamist, on nāiteks varukanalile ūleminek segamise korral, sagedushūplevate kanalite programmeerimine, raadiorežiimide või raadiovaikuse kehtestamine ja selle katkestamise kord, mobiiltelefonide ja teiste kiirgurite omadused ning ohud, keskkonna mõju oma jõudude ja vastase signaalidele ning antenni omadustega arvestamine. Hinnata tuleb ūksuste pūsivarustuse seadmete haavatavust ja kasutatavust EV kontekstis. Juba olemasolevate vōimete oskuslikum kasutamine vōib olla kõige kulutōhusam EV-vōime kasvatamise viis.

7. Kokkuvõte

Alates raadioside kasutuselevõtust on EV põhisuunad – elektrooniline rünnak, elektrooniline kaitse ja elektrooniline toetus – ning füüsikalised alusprintsipid püsinud paljuskki muutumatuna. Tehnilised vahendid on aga aja jooksul märgatavalt arenenud. Areng on käinud samas taktis üldiste tehnoloogiliste edusammudega. Viimaste kümnendite suurim läbimurre EV-valdkonnas on olnud tarkvararadio, mis on viinud seadmete keerukuse riistvarast tarkvarasse ning muutnud seeläbi uute lahenduste loomise kiiremaks ja soodsamaks. See on andnud võimaluse infotehnoloogia kiire arengu ülekandmiseks EV-valda.

EV on valdkond, mis on tulevastes sõjalistes konfliktides suure tõenäosusega oluline ja rohkem või vähem esiplaanil. Just elektromagnetspekter muudab tänapäevased sõjapidamise domeenid üheks tervikuks. Kõikide riikide armeed kasutavad elektromagnetspektrit järjest enam. Kõikvõimalikud relvasüsteemid kasutavad erinevaid raadiosageduslikke lahendusi, lisaks optilise spektri lahendusi. Ühest küljest on Eestile väikeriigina EV-valdkonnas konkurentsivõimelisena püsimine suur väljakutse, kuid teisalt ka võimalus kasutada ära vastasest suurem areng infotehnoloogia ja innovatsiooni vallas. Peale tehniliste lahenduste on ülioluline väljaõpe ja süsteemne lähenemine EV-valdkonnale.

Dr KAAREL PIIP

Kaitseväe Akadeemia elektroonilise võitluse kompetentsikeskuse juhataja-juhtivteadur

HALDO-RAIT HARRO, MSc

Ericsson Eesti Aktsiaseltsi koostamistehnoloogiate arendus- ja hooldusjuht

Dr IVO MÜÜRSEPP

Tallinna Tehnikaülikooli Thomas Johann Seebecki elektroonikainstituudi vanemlektor

Dr TOOMAS RUUBEN

Kaitseväe Akadeemia elektroonilise võitluse kompetentsikeskuse teadur ja Eesti Lennuakadeemia sidesüsteemide lektor