

Zoperstavljanje grožnjam brezpilotnih letalnih sistemov skozi koncept elektronskega bojevanja

Countering the Threat of Unmanned Aircraft Systems Through the Concept of Electronic Warfare

Povzetek

V prispevku je predstavljen sodoben način vojskovanja, pri katerem predstavlja elektronsko bojevanje kot »omogočevalec« najpomembnejšo zmogljivost v boju proti brezpilotnim letalnimi sistemom. Prispevek z različnimi raziskovalnimi metodami odgovori na raziskovalni vprašanji, in sicer, kako zagotoviti zaščito sil in kritične infrastrukture pred brezpilotnimi letalnimi sistemi ter kako z elektronskim bojevanjem zagotoviti zaščito pred brezpilotnimi letalnimi sistemi v Slovenski vojski. V okviru tega se prispevek osredotoča predvsem na razvoj predloga koncepta zaščite pred brezpilotnimi letalnimi sistemi z izvajanjem elektronskega bojevanja v Slovenski vojski. Izpostavljene so grožnje iz zraka, ki predstavljajo izziv tako Slovenski vojski kot civilnemu področju. Obravnavano področje je svojstven izziv tudi za slovenski jezik, ki se je s terminološkimi zadregami in različnimi prevodi iz angleškega jezika pokazal kot zelo živ. Prispevek spodbuja bralca k nadaljnjemu raziskovanju morebitnih vrzeli.

Ključne besede: *brezpilotni letalni sistem, brezpilotni letalnik, daljinsko voden letalni sistem, daljinsko voden letalnik, protidronska zaščita, zaščita pred brezpilotnimi letalnimi sistemi, elektronsko bojevanje, Slovenska vojska.*

Abstract

This paper presents a new approach to warfighting and electronic warfare capabilities as a key enabler to counter Unmanned Aircraft Systems (UAS). Two core questions are answered through different research methods: how should we secure our units and critical infrastructure in countering UAS, and how should the Slovenian Armed Forces (SAF) counter UAS conducting electronic warfare. In this context the focus of the paper lies in the development of a proposed

concept for the SAF to counter UAS conducting electronic warfare. Countering UAS is a challenging task for both the SAF and the civilian domain; it is therefore very important to explore the vulnerabilities of UAS, and the advantages and disadvantages of the new C-UAS tactics, techniques and procedures. This paper seeks to provide a detailed definition of various terms used for Unmanned Aircraft Systems in the Slovenian language, and last but not least seeks to address the reader on possible further research of gaps.

Keywords: *Unmanned Aircraft System (UAS), Unmanned Airship (UA), Unmanned Aircraft (UA), Unmanned Aerial Vehicle (UAV), Remotely Piloted Aircraft System (RPAS), Counter Drone, C-UAS, Counter Unmanned Aircraft System, Electronic Warfare, Slovenian Armed Forces.*

1 Uvod

V preteklosti so tehnološki napredek predstavljala letala in letenje, danes pa ga zastopajo brezpilotni letalni sistemi. Etičnost uporabe in morebitna zloraba brezpilotnih letalnih sistemov je predmet razprav v svetovnem merilu. Kljub velikemu mogočemu doprinosu najnaprednejših tehnologij in umetne inteligence smo ponovno pred dilemo, kako preprečiti zlorabe in njihovo uporabo. Kot je bilo v prejšnjem stoletju veliko nasprotujočih si mnenj glede uporabe letal, jedrskega orožja ipd., se danes krešejo mnenja glede uporabe brezpilotnih letalnih sistemov. Pri tem ne moremo spregledati dejstva, da je kljub hitro rastoči komercialni uporabi zaznati predvsem negativne posledice z vidika varnosti. Zakaj je tako, ni treba posebej navajati, saj sodobno bojevanje zaznamuje prav uporaba brezpilotnih letalnih sistemov. Kljub široki uporabi brezpilotnikov v Afganistanu in drugod po svetu je glavni mejnik in način uporabe v združenem bojevanju predstavljal armensko-azerbajdžanski konflikt leta 2020, v katerem so z brezpilotnimi letalnimi sistemi poskrbeli za načelo presenečenja, kot ga do takrat še ni bilo.

Novim doktrinarnim izhodiščem uporabe brezpilotnih letalnih sistemov in posledično zaščite sil ter kritične infrastrukture pred nizko letečimi, počasnimi in majhnimi grožnjami iz zraka se ne moremo več izogniti. Večina držav kupuje svoje brezpilotne letalne sisteme in razvija zaščito pred njimi v vojaške namene. Hkrati pa ne smemo zanemariti proliferacije komercialnih brezpilotnih letalnih sistemov. Slovenija bo morala kljub svoji majhnosti slediti tem trendom, razvoj oboroženih sil pa se bo moral prilagoditi novemu načinu vojskovanja. Zastarele metode in tehnologije bodo sčasoma zamenjale nove.

»Bojmo se dronov, vse drugo je lažji izziv,« je izjava slovenskega podjetnika Iva Boscarola (M. Z., 2022), ki danes še kako drži za vojake na ukrajinsko-ruski fronti. Četudi z droni oziroma brezpilotnimi letalnimi sistemi izvajamo natančnejše delovanje po ciljih in se zato zmanjšujejo žrtve med civilnim prebivalstvom, je psihološki učinek na bojišču teh majhnih in poceni naprav neznansko velik. Občutek nenehnega nadzora iz zraka, ne da bi vedeli zanj, in grožnje iz zraka vsako minuto, celo sekundo, je nekaj, česar se verjetno ne da razumeti, dokler tega v resnici ne izkusimo.

Prispevek s sistematičnim zbiranjem virov, analizo vsebine pisnih virov, deskriptivno in komparativno metodo predstavlja, kako se je z elektronskim bojevanjem mogoče zaščititi pred brezpilotnimi letalnimi sistemi in kako se zoperstaviti tovrstnim grožnjam na taktični ter operativno-strateški ravni. Odgovorjeno je na raziskovalni vprašanji, kako zagotoviti zaščito sil in kritične infrastrukture pred brezpilotnimi letalnimi sistemi ter kako z izvajanjem elektronskega bojevanja zagotavljati zaščito pred brezpilotnimi letalnimi sistemi v Slovenski vojski. Zaradi varovanja tajnih podatkov ter poslovnih skrivnosti ni bilo mogoče pridobiti oziroma opisovati nekaterih taktično-tehničnih podatkov in taktik, tehnik ter postopkov zaščite pred brezpilotnimi letalnimi sistemi in načinov elektronskega bojevanja.

2 Opredelitev temeljnih pojmov

Neurejeno področje uporabe temeljnih pojmov nas zavezuje, da se opredelimo glede uporabe izrazja ter opozorimo na problematiko in netransparentnost uveljavljenih terminov za nekatere strokovne izraze v slovenskem jeziku: dron, trot, brezpilotni letalnik (BPL) (angl. *Unmanned Aircraft* – UA, in *Unmanned Aerial Vehicle* – UAV), brezpilotni letalni sistem (BLS) (angl. *Unmanned Aircraft System* – UAS), brezpilotni zrakoplov (BPZ) (angl. *Unmanned Airship*), sistem brezpilotnega zrakoplova (SBZ), daljinsko voden letalnik – (DVL)¹ (angl. *Remotely Piloted Aircraft* – RPA), daljinsko voden letalni sistem – (DVLS) (angl. *Remotely Piloted Aircraft System* – RPAS). V prispevku bosta kljub različni uporabi izrazov v Natu in na novo predpisani rabi, ki jo je predstavila Civilna agencija za letalstvo, uporabljena izraza, brezpilotni letalnik in brezpilotni letalni sistem. Menim, da so tako brezpilotni letalnik kot brezpilotni letalni sistem, dron, daljinsko voden letalnik, daljinsko voden letalni sistem in zrakoplov povsem sprejemljivi termini,

¹ Pogačnik (2017, 6) opredeli *Remotely Piloted Aircraft* kot daljinsko voden letalnik in *Remotely Piloted Aircraft System* kot daljinsko voden letalni sistem.

ki se vsak dan uporabljajo v različnih strokovnih publikacijah. Kadar govorimo o dronih, se v strokovnih publikacijah termin enači z majhnimi komercialnimi različicami brezpilotnih letalnikov. Po vojaškem razumevanju se sem uvrščajo še brezpilotni letalni sistemi razreda I po Natovi klasifikaciji (Willis, 2021, 28). Treba je omeniti, da se v Natu uporabljajo vsi prej naštetni termini, vendar so v strokovnih publikacijah jasno opredeljene razlike med izrazi dron, brezpilotni letalnik, brezpilotni letalni sistem, daljinsko voden letalnik, daljinsko voden letalni sistem itn. Zaznati je tudi opuščanje angleškega termina Unmanned Aerial Vehicle – UAV (Schmidt in Haider, 2021c, 31). Dejstvo je, da kot pripadniki Slovenske vojske in država članica Nata moramo, za potrebe interoperabilnosti ter skupnega razumevanja in smotrne uporabe različnih terminov, poznati njihovo raznovrstno uporabo, in da je glede na dosedanje oblike uporabe terminov ter različnih definicij skoraj nemogoče pričakovati poenotenje mnenj in posledično enotno rabo.

2.1 Zaščita pred brezpilotnimi letalnimi sistemi

Grožnjam iz zraka se je mogoče zoperstaviti z različnimi sistemi za boj proti brezpilotnim letalnim sistemom – angl. *Counter – Unmanned Aircraft System/C-UAS*.² To so sistemi ali naprave, s katerimi lahko zakonito in varno zaznamo, identificiramo ter po potrebi onemogočimo in nevtraliziramo delovanje, motimo ali prevzamemo nadzor nad brezpilotnim letalnikom oziroma brezpilotnim letalnim sistemom (Wang, Liu, Song, 2020, 1).

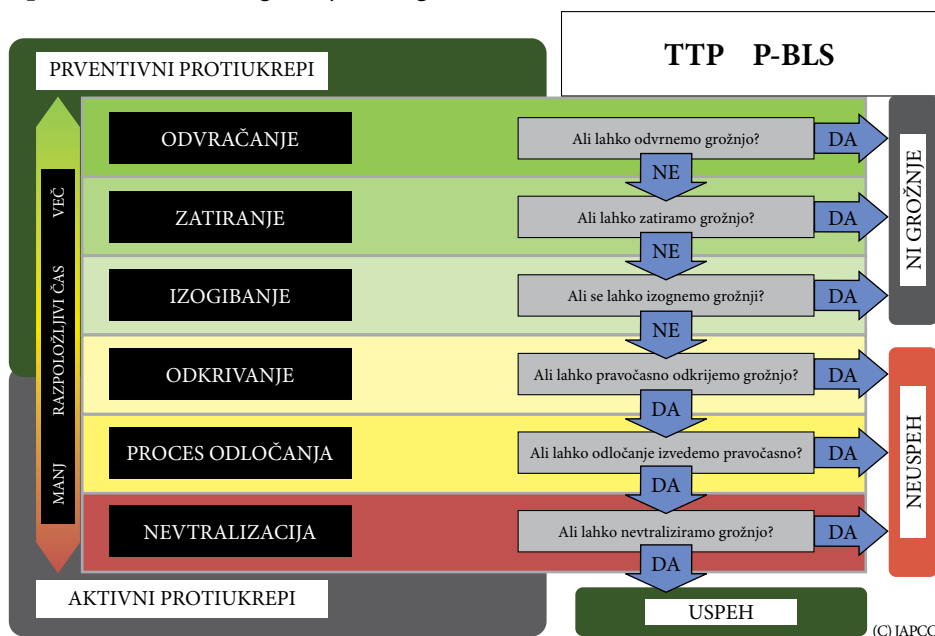
2.2 Elektronsko bojevanje, elektronska zaščita, napad in podpora

Elektronsko bojevanje (EB) je vsaka vojaška akcija, v kateri se uporablja elektromagnetna in usmerjena energija za izvajanje nadzora in prevlado v elektromagnetnem spektru ali za napad na sovražnika (ATP 3-12.3, 2019). Po slovenski Vojaški doktrini (Furlan idr., 2006, 52) je elektronsko bojevanje vrsta informacijskega delovanja. Lahko ga opredelimo tudi kot enega izmed načinov zoperstavljanja grožnjam pred brezpilotnimi letalnimi sistemi. Elektronsko bojevanje ali danes vse pogostejši izraz elektromagnetno bojevanje po ATP 3-12.3 (2023) sestavljajo elektronska zaščita (angl. *EP – Electronic Protection*), elektronski napad (angl. *EA – Electronic Attack*) in elektronska podpora (angl. *ES – Electronic Support*).

² Poznana tudi kot C-UAV – *Counter Unmanned Aircraft Vehicle*.

3 Taktike, tehnike in postopki zoperstavljanja brezpilotnim letalnimi sistemom in elektronsko bojevanje

Številni incidenti s komercialno razpoložljivimi brezpilotnimi letalnimi sistemi, ki jih nismo posebej obravnavali, so bili glavni povod za raziskave in razvoj na področju zaščite pred majhnimi brezpilotnimi letalnimi sistemi. V ATP 3-01.81 (2017, 1–2) je bilo že pred leti zapisano, da bodo prav brezpilotni letalni sistemi I, II in deloma razreda III predstavljali največjo grožnjo, celo večjo kot razreda IV in V.³ Odgovore, zakaj majhni brezpilotni letalni sistemi predstavljajo tako veliko grožnjo, lahko najdemo tako v nadzoru zračnega prostora, zračni obrambi in nezmožnosti delovanja na take cilje kot tudi v proliferaciji brezpilotnih letalnih sistemov ter v številnih incidentih oziroma napadih na kritično infrastrukturo, politične osebnosti in letališča. Sistemi za zaščito pred brezpilotnimi letalnimi sistemi se razvijajo po principu zaznavanja grožnje in delovanja po njej. Namen sistema boja proti brezpilotnim letalnimi sistemom ni le v njihovi detekciji in nevtralizaciji, temveč so vredni naše pozornosti tudi preventivni ukrepi. V kolikor so preventivni ukrepi uspešni, protiukrepi niso več nujni. Polkovnik Andree Haider (2021b) je razvil metodologijo zoperstavljanja brezpilotnim letalnimi sistemom po principu preventivnih in aktivnih protiukrepov. To je nazorno predstavljeno na sliki 1. Preventivne ukrepe je mogoče načrtovati vnaprej, in če so uspešni, se odziv na grožnjo ne zgodi.



Slika 1: Taktike, tehnike in postopki zoperstavljanja brezpilotnim letalnimi sistemom (vir: prirejeno po Haider, 2021b, 76)

³ Natova klasifikacija se razlikuje od uporabljene ameriške.

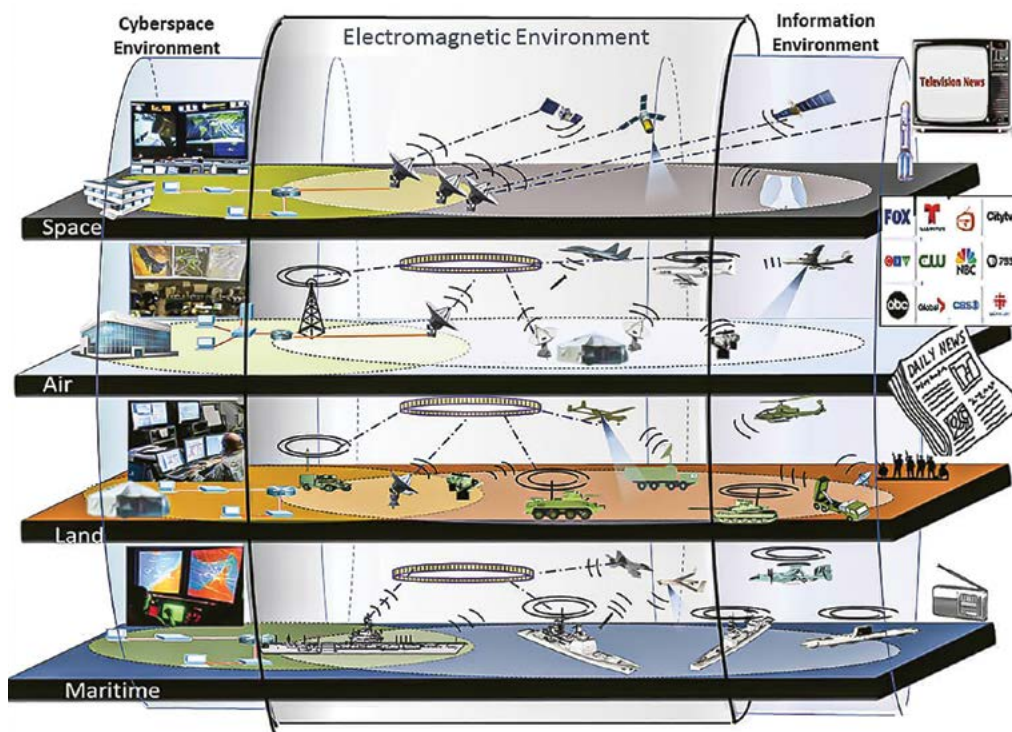
Odvračanje (angl. *Deterrence*) temelji na predpostavki, da so posledice za uporabnika brezpilotnih letalnih sistemov tako hude, da je bolje, če jih sploh ne uporablja. K odvračalni drži spada tudi strateško komuniciranje oziroma Stratcom s širjenjem točno določenih sporočil (Haider, 2021b, 78–79). Z **zatiranjem** (angl. *Suppression*) se izvaja preprečevanje dostopa do zaščenega območja z zračno obrambo in elektronskim bojevanjem, kot enim izmed najučinkovitejših sredstev. Kibernetski napad se lahko izvede na zemeljske upravljalne postaje in tako prepreči uporabo brezpilotnih letalnih sistemov. Elektronsko bojevanje je uspešno tudi ob zoperstavljanju komercialnim brezpilotnim letalnim sistemom, ki pa je v mirnodobnem času zakonsko zelo omejeno (Haider, 2021b, 75–82). Če brezpilotnih letalnih sistemov ni mogoče odvrniti ali zatreti, je naslednja stopnja razmislek o tem, kako se **izogniti** (angl. *Avoidance*) njegovim senzorjem oziroma kinetičnim učinkom. Kot odzivni ukrep lahko omenimo predvsem detekcijo oziroma **odkrivanje** (angl. *Detection*), ki omogoča nadaljnje aktivne protiukrepe. Detekcija mora biti seveda dovolj zgodnja in na čim daljših razdaljah (Haider, 2021b, 80–82). **Reakcijski čas za odločanje** (angl. *Decision Making*) lahko včasih pri majhnih brezpilotnih letalnih sistemih traja manj kot minuto in takrat lahko govorimo le še o avtomatiziranem odzivanju sistemov za boj proti brezpilotnim letalnim sistemom. Ob prestrezanju in nevtralizaciji navadnih letal ali večjih brezpilotnih letalnih sistemih se odloča na višjih ravneh, v Sloveniji bi bil to minister za obrambo (Haider, 2021b, 81). Odločitvi sledi še **nevtralizacija** (angl. *Neutralization*), ki je predmet razprave, kadar se je treba odločiti, s čim delovati po cenovno zelo ugodnih brezpilotnih letalnih sistemih. V tem delu je treba izpostaviti elektronsko in kibernetsko bojevanje, še posebno, če so rakete zemlja–zrak cenovno nesprejemljive (Haider, 2021b, 81–82).

3.1 Elektronsko bojevanje in sistemi za zaščito pred brezpilotnimi letalnimi sistemi

Elektromagnetni spekter povezuje celoten ustroj, ki nadvlada delovanju sistemov, ki jih uporabljamo v sodobni informacijski družbi in v sodobno opremljenih vojskah. Vse je povezano znotraj elektromagnetnega spektra, ki dominira nad vsako operacijo in znotraj vseh domen delovanja, kot je prikazano na sliki 2 (Spreckelsen, 2018).

Sinhronizacija elektronskega bojevanja, kot so elektronski napad, elektronska zaščita ter elektronska podpora, med seboj in z vsemi aktivnostmi hkrati, ki se na bojišču izvajajo, lahko omogoči izvajanje konkretnih protiukrepov kot zaščito

pred grožnjami iz zraka. Nenazadnje je s svojo izjavo temu pritrdil tudi general Mark Kelly, ki je na konferenci Air, Space and Cyber leta 2021 dejal: »Če izgubimo vojno v elektromagnetnem spektru, izgubimo vojno v zraku, in izgubimo jo zelo hitro.« Delovanje znotraj elektromagnetnega spektra lahko prevlada nad nasprotnikovimi sistemi, tudi nad brezpilotnimi letalnimi sistemi. Metodološko se lahko elektronsko bojevanje izvaja v vseh fazah zoperstavljanja brezpilotnim letalnim sistemom. V prvi fazi odvrčanja se s posedovanjem sistemov za boj proti brezpilotnim letalnim sistemom že izvaja neke vrste odvrčanje. V vseh naslednjih pa je pomembna predvsem zmožnost pravočasne detekcije ter nevtralizacije.



Slika 2: Operacije v elektromagnetnem prostoru (vir: Von Spreckelsen, 2018)

Idealni sistemi za zaščito pred brezpilotnimi letalnimi sistemi bi razpolagali z možnostjo detekcije in nevtralizacije. Najboljši sistemi za detekcijo pa bi omogočali sledenje, identifikacijo brezpilotnih letalnih sistemov oziroma vseh podsistemov brezpilotnih letalnih sistemov, imeli bi zelo majhen odtis v elektromagnetnem spektru ter visoko avtonomnost operacij. Idealni podsistemi za nevtraliziranje brezpilotnih letalnih sistemov bi zakonito in varno onemogočili, motili ali prevzeli nadzor nad brezpilotnimi letalniki oziroma brezpilotnimi letalnimi

sistemi s čim manjšo kolateralno škodo ter nizkimi stroški delovanja (Wang, Liu in Song, 2020, 1). V vojaške namene bi morali sistemi za boj proti brezpilotnim letalnim sistemom zagotavljati tudi robustnost, mobilnost, avtonomnost in vremensko vzdržljivost. Tehnologije detekcije oziroma zaznavanja so utemeljene na podlagi detekcije zvoka, toplote, slike, radijskih signalov, odbojev signalov (radar) ter fuzije ali združevanja podatkov.⁴ Tehnologije, uporabljene za nevtralizacijo, pa vključujejo motenje C2-sistemov, motenje in »spoofing« globalnega navigacijskega satelitskega sistema (angl. *Global Navigation Satellite System* – *GNSS*), uničenje oziroma nevtralizacijo brezpilotnih letalnikov oziroma brezpilotnih letalnih sistemov z visoko energijskimi laserskimi sistemi, elektromagnetnim pulzom, mrežami ali elektromagnetnim prenosnim orožjem oziroma puškami ter drugimi (Willis, 2021), (Wang, Liu in Song, 2020).

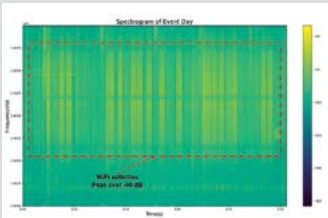
3.1.1 Detekcija brezpilotnih letalnih sistemov v elektromagnetnem spektru

Wang, Liu in Song (2020) so v svoji raziskavi ugotavljali tehnološki razvoj detekcije brezpilotnih letalnih sistemov po letu 2014. Ugotovili so, da so bili najpopularnejši pristopi s pomočjo fuzije podatkov. Najmanj poudarka so dajali tehnologijam na podlagi detekcije zvoka. V nadaljevanju bodo v preglednici 1 na kratko predstavljene prednosti in slabosti vsake posebej ter ugotovitve, zakaj so nekatere tehnologije obetavnejše od drugih.

Taktike, tehnike in postopki:	Prednosti:	Slabosti:
Akustična tehnologija 	– omogoča identifikacijo, – omogoče sledenje cilju, – analizira in loči zvok brezpilotnih letalnikov od avtomobilskega in zaznava nizkoleteče brezpilotne letalne sisteme, – omogoča preprosto uporabo in mobilnost sistema, ima nizko težo, – locira izvor zvoka (TDOA),⁵ – detektira tudi avtonomno vodene brezpilotne letalne sisteme, – ima pasiven sistem, – stroški so nizki	– ima omejen domet, – odkriva le brezpilotne letalne sisteme do razreda I, – omejena je na nekaj 100 metrov v urbanem okolju do enega kilometra v zelo tihem urbanem okolju, – slabša učinkovitost, – odvisna je od vremenskih vplivov (veter ter vibracije vetra)

⁴ Angl. *Data Fusion* – gre za tehnike združevanja podatkov, ki združujejo podatke iz več senzorjev z informacijami iz podatkovnih baz. Tako izboljšamo natančnost določanja ciljev (Castanedo, 2013).

⁵ *Time Delay Of Arrival (TDOA)* – tehnologija lociranja izvora zvoka na podlagi merjenja časovnih razlik sprejetega signala na več lokacijah.

Taktike, tehnike in postopki:	Prednosti:	Slabosti:
Optoelektronska in IR-tehnologija 	– razločuje brezpilotne letalnike od ptic (IR-kamere in algoritmi nevronske mreže), – ima nižjo porabo, – prepozna frekvenco propelerja, – shranjuje slikovni material, – detektira tudi avtonomno vodene brezpilotne letalne sisteme, – je lahko namestljiva na brezpilotne letalne sisteme, – ima nizke stroške, nizko težo, majhno velikost	– učinkovito ločuje cilje od ozadja, – možne so napake pri razločevanju s prikazom slike, – odvisna je od vremenskih vplivov (padavine, vlaga, mrak, megla itn.), – ima omejen domet, – identifikacija je omejena, – pojav lažnih alarmov
Radiofrekvenčna (RF) tehnologija 	– doseg, – hitra detekcija, mogoča je identifikacija, – zaznava majhne brezpilotne letalne sisteme, – določa lokacije operatorja in drugih podsistemov (lahko več hkrati), – učinkovito locira, – je pasivni sistem, – stroški so nizki	– zaznava komercialne in šifrirane podatkovne povezave, – zaznava avtonomno vodene brezpilotne letalne sisteme, – tipično kratek domet, – manj učinkovita na zasičenih RF-območjih
Radarska tehnologija 	– deluje podnevi in ponoči, – neodvisna je od vremena, – meri razdaljo do cilja in hitrost cilja, – detektira roje, več ciljev hkrati, in sicer ne glede na avtonomnost leta, – identicira, – lociranje je učinkovito, natančno in konstantno, – ima daljši domet	– klasični radarji ne zaznavajo manjših brezpilotnih letalnikov, ki imajo radarski presek oziroma odboj (RCS)⁶ manjši od 1 m² – zaznavanje nizko letečih in počasi premikajočih se ciljev, – znanje operatorjev, – potrebnih več sistemov, – minimalna razdalja za detekcijo, – visoki stroški
Fuzija podatkov 	– združuje več vrst senzorjev hkrati, – združuje različne algoritme	– stroški so visoki

Preglednica 1: Prednosti in slabosti posameznih tehnologij detekcije (vir: povzeto po Butterworth-Hayes, 2022, in Wang, Lui in Song, 2020)

⁶ Angl. *Radar Cross Section (RCS)* – radarski presek oziroma odboj je mera odbojnosti radarskega signala od cilja v smeri radarskega sprejemnika.

3.1.1.1 Akustična detekcija

Akustična detekcija deluje z uporabo mikrofонов, s katerimi se zaznava specifičen zvok brezpilotnih letalnikov. Njihova detekcija je odvisna od številnih dejavnikov. Pri tem lahko izpostavimo veter, saj so akustični senzorji zelo občutljivi na vibracije, ki jih ta povzroča. Način izdelave propelerjev in njihova nizka hitrost vrtenja lahko močno zmanjšata hrup, ki ga povzroča brezpilotni letalnik. Podobno lahko hrup, ki ga oddaja brezpilotni letalnik, zmanjšamo z jadranjem. Kot je bilo že omenjeno, zvočno zaznavo močno zmanjša hrupno okolje, kar je še posebej značilno za mestna območja in konfliktna žarišča. Do neke mere se lahko akustična zaznava izboljša s postavitvijo mikrofонов na primerni razdalji, s čimer se nadomesti kratek doseg sistemov za detekcijo z zvokom (Udin in dr., 2020).

Številna podjetja, ki ponujajo rešitve za akustično detekcijo, to navadno kombinirajo z drugimi sistemi detekcije. Kot stacionarne možnosti se sistemi v kombinaciji z drugimi senzorji uporabljajo predvsem za zaščito kritične infrastrukture, kot so letališča, pristanišča, elektroenergetski sistemi, telekomunikacijski sistemi itn. Omenimo lahko tudi možnosti zaznave brezpilotnih letalnikov do razreda I po mikrofону in aplikacijo na mobilnem telefonu. Aplikacijo je predstavilo ameriško podjetje Northrop Grumman pod oznako MAUI (angl. *Mobile Application for UAS Identification*) (Ball, 2016).

3.1.1.2 Optoelektronska in IR-detekcija

Detekcija z optoelektronskimi in infrardečimi (IR) svetlobnimi senzorji je pasivna metoda, ki vključuje spekter valovnih dolžin vidne svetlobe ter IR-svetlobe. Detekcija in klasifikacija brezpilotnih letalnikov je močno odvisna od odbojnosti ter ločevanja od ozadja oziroma okolja. Več o tem sta v svojem delu analizirala Dong in Zou (2017). IR-senzorji so primerni za delovanje v okoljih, v katerih je malo vidne svetlobe, torej ponoči. Nasprotno so v okoljih z vidno svetlobo primernejši optoelektronski senzorji, ki se uporabljajo podnevi. Čeprav smo kot prednosti v preglednici 1 navedli razločevanje brezpilotnih letalnikov od ptic, gre za dejavnik, ki močno vpliva na delovanje sistema. V kolikor sistem ni opremljen s potrebnimi algoritmi za prepoznavo in ločevanje ptic od brezpilotnih letalnikov, je lahko stopnja lažnih alarmov previsoka za učinkovito delovanje sistema. Najšibkejša točka optoelektronske detekcije ostajajo vreme in vremenski vplivi, kot so megla, padavine, vlaga, onesnaženost zraka itn. Optoelektronski senzorji lahko, odvisno od proizvajalca, zaznavajo brezpilotne letalnike na več deset kilometrov razdalje (Stathopoulos, 2021, 174–176).

3.1.1.3 Radiofrekvenčna detekcija

Radiofrekvenčni analizatorji zaznavajo radiofrekvenčne signale v radiofrekvenčnem spektru. Z radiofrekvenčnimi analizatorji lahko zaznavamo signale, ki jih oddajajo različni podsistemi brezpilotnih letalnih sistemov. Med detektiranjem in identificiranjem frekvenc se s triangulacijo določajo tudi lokacija brezpilotnih letalnikov ali drugih podsistemov. V okoljih, v katerih je uporaba radijskih frekvenc zelo nasičena, se lahko učinkovitost zaznave zelo zmanjša. Detekcija brezpilotnih letalnikov je seveda mogoča z zaznavanjem vzpostavljene komunikacije med operatorjem in brezpilotnim letalnikom. Najpogosteje se za njegov nadzor uporabljajo frekvence 2,4 GHz, 5,8 GHz, 433 MHz in 868 MHz. Komunikacija se vzdržuje tudi po GSM-komunikaciji (Al-Sa'd in dr., 2019).

3.1.1.4 Radarska detekcija

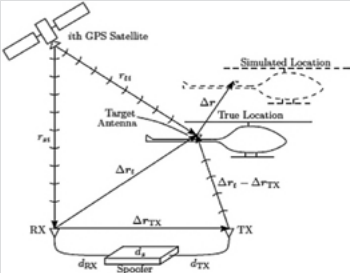
Detekcija z radarji je lahko pasivna ali aktivna. Aktivni radarski sistemi oddajajo signale in tako razkrivajo svojo lokacijo, kar pa ne velja za pasivne radarske sisteme. Trenutno je radarska detekcija v Natu glavna izbira za nadzor zračnega prostora. Radarski sistemi imajo v primerjavi z drugimi prednosti predvsem z vidika delovanja tako podnevi kot ponoči ter v vseh vremenskih razmerah in ne glede na avtonomnost leta. Pri tem je treba omeniti, da je to cenovno najdražja izbira in da je za upravljanje radarja treba usposobiti posadko in tehnike (Stathopoulos, 2021, 168–180).

Klasični radarji, ki zaznavajo letala z radarskim presekom oziroma odbojem nad enim kvadratnim metrom, ne morejo hkrati zaznavati tudi manjših ciljev, kot so brezpilotni letalniki razreda I ter komercialni brezpilotni letalniki, saj delujejo na prenizkih frekvencah. Seveda se je z novonastalimi grožnjami pospešil razvoj radarjev, ki delujejo na frekvencah, višjih od šest GHz. Primer za to je lahko X-band radar, ki deluje na frekvenci 8,75 GHz in zaznava mikro brezpilotne letalnike na razdalji dveh kilometrov (Quevedo, 2018). Omeniti je treba še način delovanja radarjev, pri čemer ima pomembno vlogo lokacija postavitve sistema, še posebno, ker lahko brezpilotni letalniki letijo izjemno nizko nad tlemi in zavzemajo kritje za grmovjem in drugim rastlinjem. Treba je upoštevati tudi minimalno razdaljo med radarjem in ciljem, ki jo radar še lahko zaznava. Izraelsko podjetje ELTA je podobno kot drugi ponudniki razvila sistem, ki poleg radarja obsega še druge senzorje in efektorje ter z radarsko tehnologijo deluje na različnih razdaljah do 30 kilometrov (EDR, 2021).

3.1.2 Nevtralizacija/uničenje brezpilotnih letalnih sistemov v elektromagnetnem spektru

V preglednici 2 so predstavljene prednosti in slabosti sistemov zoperstavljanja brezpilotnim letalnim sistemom, ki so v nadaljevanju podrobneje opisane.

Taktike, tehnike in postopki:	Prednosti:	Slabosti:
Fizični ulov z mrežo 	– je prenosen, – omogoča montažo na brezpilotni letalni sistem, – fizično zajame brezpilotni letalnik	– lahko povzroči stransko škodo, – stroški so visoki, – mreže, izstreljene s tal, imajo kratki doseg
RF-motenje 	– nekinetično deluje – nevtralizacija, – motenje več brezpilotnih letalnih sistemov hkrati, – strošek je nizek do srednji	– ima kratek doseg, – lahko vpliva in moti druge radijske zveze, – deluje na komercialne brezpilotne letalne sisteme, – nepredviden odziv brezpilotnih letalnih sistemov
Elektromagnetna puška 	– je prenosna, – preprosta za uporabo, – stroški so nizki	– ima ozek spekter delovanja, – velika poraba energije, – ni toliko učinkovita
EMP – elektromagnetni pulz 	– je majhen, lahek sistem, – učinkovito zaustavlja brezpilotne letalne sisteme	– uničuje oziroma moti druge naprave na območju delovanja, – povzroči nepredviden padec brezpilotnih letalnih sistemov, – ima visoko porabo, – ima srednje stroške

Taktike, tehnike in postopki:	Prednosti:	Slabosti:
Spoofing 	– je neuničujoč, – ima nizke stroške, – zaseže baze podatkov na brezpilotnih letalnih sistemih, vključujoč posnetke ter zgodovino leta	– mogoča je interferenca z drugimi napravami, – omejeno deluje ob šifriranih povezavah, – zahteva znanje operaterjev, – ne locira operatorja leta
Visokoenergetski laserski žarek 	– povzroči uničenje brezpilotnih letalnih sistemov	– povzroči uničenje brezpilotnih letalnih sistemov, – velikost sistema, – so večinoma eksperimentalni sistemi, – poraba energije in stroški so visoki
Hekanje 	– nekinetično deluje, – mogoče je zavajanje, – ima nizke stroške	– vpliva na druge sisteme, – deluje le v določenih operacijskih sistemih

Preglednica 2: Prednosti in slabosti sistemov zoperstavljanja brezpilotnim letalnim sistemom (vir: povzeto po Willis (2021), Butterworth-Hayes, 2022, in Wang, Lui in Song, 2021, idr.)

Kljub detekciji brezpilotnega letalnega sistema nam to ne koristi, če se grožnji ne moremo zoperstaviti ali se kakor koli drugače pred njo zaščititi. Zato številna podjetja in vojske hkrati s sistemi za detekcijo razvijajo tudi sisteme za nevtralizacijo brezpilotnih letalnih sistemov. Podobno kot velja za različne sisteme detekcije, tudi nevtralizacije niso stoodstotno učinkovite. Najučinkovitejša je vzpostavitev optimalne mreže različnih taktik, tehnik in postopkov, s katerimi se lahko zoperstavljamo brezpilotnim letalnim sistemom.

3.1.2.1 Fizični ulov

Pri fizičnem ulovu se podjetja poslužujejo različnih mrež, ki se izstreljuje iz puške, kombiniranih modulov sistema za boj proti brezpilotnim letalnim sistemom

ali drugega brezpilotnega letalnega sistema. Fizičnega ulova ne uvrščamo neposredno pod elektronsko bojevanje, čeprav postaja del sistemov za boj proti brezpilotnim letalnim sistemom. Za uspešen ulov brezpilotnih letalnih sistemov je treba zagotoviti povezavo z navigacijo in sledenjem tarči (Wang, Liu in Song, 2020, 10).

3.1.2.2 Radiofrekvenčno motenje

K aktivnim ukrepom elektronskega bojevanja spadata motenje in zavajanje. Radiofrekvenčni motilci so lahko statični, mobilni ali prenosni. Z radiofrekvenčno energijo, ki jo z motilci oddajamo proti brezpilotnim letalnim sistemom, se prekine povezava z zemeljsko upravljalno postajo, kar lahko vodi v več različnih scenarijev. Brezpilotni letalni sistem lahko nadzorovano pristane na poziciji, na kateri je. Brezpilotni letalni sistem se vrne na izhodiščno pozicijo, ki je lahko ponastavljena na ciljno pozicijo. Lahko se nenadzorovano spusti na tla ali odleti neznan kam. Ker navadno ne vemo, kako bo brezpilotni letalni sistem odreagirala na motenje, se to izvaja premišljeno in glede na grožnjo, ki jo predstavlja. Ob avtonomiji leta je motenje brezpilotnega letalnega sistema omejeno, izvaja se predvsem do brezpilotnega letalnega sistema razreda II (Stathopoulos, 2021, 168–180). Številna podjetja razvijajo taktične puške, ki delujejo na različnih frekvenčnih območjih. V Sloveniji puške že uporablja Policija, so pa cenovno dostopne, vendar ne tako učinkovite, da bi lahko le z njimi opremili vojake in tako zagotavljali popolno zaščito pred brezpilotnimi letalnimi sistemi. Za učinkovito delovanje puške je treba natančno meriti na brezpilotni letalni sistem. V praksi se je pokazalo, da je merjenje s puško zelo oteženo v urbanem okolju in na gozdom poraslem območju. Uporabnike je treba dodatno usposablјati.

3.1.2.3 Elektromagnetni pulz (EMP)

Z elektromagnetnim pulzom lahko onesposobimo ali uničimo elektronske komponente brezpilotnega letalnega sistema. Glavna prednost elektromagnetnega pulza, glede na prihodnost, je nedvomno boj z roji brezpilotnih letalnih sistemov, ki jih lahko z elektromagnetnim pulzom onesposobimo. Zelo pomembna je pravilna uporaba, ob upoštevanju, da z elektromagnetnim pulzom lahko hkrati onesposobimo tudi svoje naprave. Sistemi, kot je Thor in Leonidas, so še v fazi testiranj (Wang, Liu in Song, 2020, 13–14).

3.1.2.4 Visokoenergetski laser

Ena izmed tehnologij zoperstavljanja in nevtralizacije brezпилotnih letalnih sistemov je laserska. Visokoenergetski laserski žarki so se izkazali za zelo učinkovite v dobrih vremenskih pogojih. Laserski žarki se v megli ali ob padavinah razpršijo na vodnih molekulah in izgubijo moč. Nevtralizacija brezпилotnih letalnih sistemov z laserjem je lahko neprimerna zaradi nenadzorovanega pristanka oziroma padca brezпилotnega letalnega sistema, po drugi strani pa z laserjem lahko delujemo tudi po roju brezпилotnih letalnih sistemov (Stathopoulos, 2021, 170–180). Raytheon in številna druga podjetja razvijajo HEWLS,⁷ ki jih je mogoče uporabiti kot stacionarne, mobilne ali prenosne sisteme. Pri Raytheonu je 50 kW HEWLS kratkega dosega lahko nameščen na vojaškem vozilu. 100 kW HEWLS lahko deluje tudi po rojih brezпилotnih letalnih sistemov in podpira mobilne sisteme kratkega dosega zračne obrambe. Omenjeni sistemi so prototipi v fazi testiranja (Chanakya, 2022).

3.1.2.5 »Spoofing« in hekanje

Z eno besedo bi lahko »spoofing« opisali kot prevaro. Gre za pojem, ki se uporablja predvsem v kibernetnem bojevanju, vendar se ga lahko poslužujejo tudi izurjeni operaterji na sistemih za elektronsko bojevanje. »Spoofing« globalnega navigacijskega satelitskega sistema je najpogosteje uporabljen za prevaro brezпилotnih letalnikov, pri čemer se mu pošiljajo napačni podatki o položaju. S spreminjanjem koordinat globalnega navigacijskega satelitskega sistema v realnem času se lahko s »spoofingom« nadzira položaj brezпилotnih letalnih sistemov, s čimer ga je mogoče preusmeriti na t. i. varno območje (Robin, 2022). Številni sistemi za boj proti brezпилotnim letalnim sistemom imajo tudi možnost izvajanja »spoofinga« kot ene izmed komponent sistema. Tudi hekanje se vse bolj uporablja, glede na uporabo WiFi in mobilnih omrežij, s katerim upravljamo brezпилotne letalne sisteme. »Spoofing« je ena izmed metod hekanja (Wang, Liu in Song, 2020, 15).

Tako kot je treba danes povezovati vse domene vojskovanja, rodove in zvrsti za zagotovitev uspeha pri izvajanju vojaških operacij, so sistemi za zaščito ter zoperstavljanje brezпилotnim letalnim sistemom združili različne tehnologije znotraj posameznega sistema. Prej smo podrobneje opisali prednosti in slabosti vsakega posebej. In res je, da se zgolj z uporabo enega sistema ne moremo zoperstaviti brezпилotnim letalnim sistemom, še posebej ne majhnim

⁷ *High Energy Weapon Laser Systems.*

komercialnim ali rojem. Razvijalci posameznih sistemov so kmalu ugotovili, da lahko z združitvijo različnih senzorjev in efektorjev povečajo učinkovitost zoperstavljanja ter verjetnost uničenja letelih groženj. Podjetja danes v ospredje postavljajo sisteme za boj proti brezpilotnim letalnim sistemom, ki združujejo tako radarje, RF-senzorje, mikrofone in optoelektronske naprave za detekcijo kot tudi efektorje, ki delujejo na cilje v zraku. V Sloveniji so varnostne službe kritičnih infrastruktur kot prve pokazale zanimanje za opremljanje s sistemi za boj proti brezpilotnim letalnim sistemom, vendar bolj zaradi pritiskov nadrejenih evropskih ustanov kot zaradi občutka ogroženosti in preteče nevarnosti iz zraka. Tako se za sisteme aktivno zanimajo Luka Koper, civilno mednarodno letališče Jožeta Pučnika v Ljubljani ter Uprava RS za izvrševanje kazenskih sankcij. Odprto ostaja vprašanje zaščite preostale kritične infrastrukture v Republiki Sloveniji. Za Slovensko vojsko trenutno poteka projekt razvoja sistema za boj proti brezpilotnim letalnim sistemom. Za skupno situacijsko zavedanje bo nujno treba združiti situacijsko sliko nadzora zračnega prostora, nadzora pomorskega okolja, kopna ter elektromagnetnega spektra, v katerem poteka kibernetško, informacijsko ter elektronsko bojevanje.

4 Koncept zaščite pred brezpilotnimi letalnimi sistemi in elektronsko bojevanje v Slovenski vojski

Številni analitiki potrjujejo dejstvu, da se elektronsko bojevanje s sodobnim načinom vojskovanja prebujajo iz predolgega spanca. Grožnje in način bojevanja, kot ga lahko spremljamo danes v Ukrajini ter drugod po svetu, zahtevajo razvoj novih zmogljivosti oziroma posodabljanje tistih, ki so bile v zadnjih dveh desetletjih vse manj pomembne. Elektronsko bojevanje in zračna obramba sta bila zagotovo taka. Odgovor, zakaj je bilo tako, je zelo preprost, saj so grožnje Natu v tem času predstavljale predvsem manj razvite države in nedržavni akterji, kot je bila na primer Al Kaida. V ospredju sta bila terorizem in stabilizacijsko delovanje. Tudi v Slovenski vojski je bilo zaznati podobno situacijo, ki pa se zaradi vojne v Ukrajini naglo spreminja. Vse bolj se izpostavljajo pomen zračne obrambe, rodovsko bojevanje in med drugim tudi elektronsko bojevanje. Vprašanje o tem, kako uspešni bomo pri zoperstavljanju novim grožnjam iz zraka, bi si morali zastavljati tako na civilnem kot vojaškem področju. Grožnje brezpilotnih letalnih sistemov, ki jih lahko koristijo tako teroristične skupine, kriminalne združbe, zgolj naključne skupine ali posamezniki, niso neznanka. Kaj uporaba brezpilotnih letalnih sistemov pomeni za sodobno vojskovanje, so nam pokazale lekcije iz Gorskega Karabaha, Sirije, Libije ter drugih kriznih žarišč, v

najobsežnejši obliki pa jih vsak dan prejemamo iz Ukrajine. Da brezpilotni letalni sistemi ne bodo grožnja le na civilnem področju, se zavedajo tudi v Slovenski vojski. Kako razviti sodobno vojsko z brezpilotnimi letalnimi sistemi in hkrati dovolj močnim elektronskim bojevanjem, zračno obrambo in obveščevalno prvine, ki se bo sposobna braniti proti takim sistemom, pa je vprašanje, ki si ga poleg vzpostavitve Natovih zmogljivosti trenutno zastavlja vrh Slovenske vojske (Willis, 2021).

Tematika zaščite pred brezpilotnimi letalnimi sistemi je zelo razširjena tako na civilnem kot vojaškem področju. Civilno področje se s proliferacijo brezpilotnih letalnih sistemov srečuje s številnimi incidenti, nekatere smo že omenjali. Podobno zaradi brezpilotnih letalnih sistemov in zaščite pred njimi v vojskah po svetu spreminjajo doktrinarna izhodišča ter posodablajo svoje sisteme. Številne vojske pospešeno razvijajo sisteme za zaščito pred njimi, vse več pa se jih spoprijema z vprašanji, kako jih optimalno uporabiti, jih vpeljati v strukturo, kakšen kader zagotoviti, koliko sredstev ter katera izbrati. Glede na proliferacijo brezpilotnih letalnih sistemov lahko z gotovostjo trdimo, da bodo sistemi za boj proti brezpilotnim letalnim sistemom lahko igrali dvojno vlogo,⁸ in sicer tako v mirnem času kot v vojni. Še podrobneje bo treba razdelati pooblastila, pravila delovanja in uporabe sistemov za boj proti brezpilotnim letalnim sistemom ter možnosti prestrezanja brezpilotnih letalnih sistemov tako v mirnem kot kriznem času. Poleg klasičnega nadzora zračnega prostora bo nujno še širše zavedanje o elektromagnetnem spektru. V mislih moramo imeti hitro razvijajoče se roje brezpilotnih letalnih sistemov in možnosti njihove različne uporabe.

Sodobni trendi in Natove smernice so danes jasni in zahtevajo potrebo po razvoju in opremljanju z brezpilotnimi letalnimi sistemi ter sistemi za boj proti brezpilotnim letalnim sistemom. Kot je bilo večkrat omenjeno in tudi v medijih izpostavljeno, Slovenska vojska podpira projekt s podjetjem TIMTEC Defense d. o. o., še vedno pa nima skupnega in celovitega koncepta umestitve elektronskega bojevanja v posamezne strukture Slovenske vojske, ki bi zagotavljale zaščito v elektromagnetnem spektru. Kako vzpostaviti učinkovito elektronsko bojevanje na vseh ravneh Slovenske vojske ter zaščito pred brezpilotnimi letalnimi sistemi, pa zahteva temeljito in celostno razpravo, tako kopenskih, zračnih in pomorskih struktur kot kibernetike, informatike, nadzora zračnega prostora, zračne obrambe, obveščevalnih struktur in drugih. Elektromagnetni spekter in elektromagnetno okolje namreč obsegata vsa področja. Povezati vse bo

⁸ Večkrat uporabljen angleški izraz *dual use*.

umetnost, vendar le tako se bo mogoče zoperstaviti grožnjam današnjega časa. Deloma lahko trdimo, da bo prevlada v elektromagnetnem spektru odločala o prihodnjih zmagovalcih, in se pridružujemo mnenju Briana Clarka (Clark, 2022, 18), da prevlada v elektromagnetnem spektru ni enaka zmagi v vojni, vendar je nujna, da se omogoči delovanje preostalim strukturam. Številni se osredotočajo in izpostavljajo predvsem razvoj elektromagnetnega delovanja Rusije in Kitajske. Med drugim John Christianson (2022) navaja, da Kitajska in Rusija prav elektronskemu bojevanju namenjata veliko sredstev. To bo področje, ki bo prineslo pomembno asimetrično razliko v bojevanju in posledično zmago na bojišču. Tudi Marcus Clay (2021) opozarja v svojem delu, da se je treba zavedati, kako ranljivi smo v elektromagnetnem spektru, ki danes pokriva vsa področja našega življenja. Podrobneje je opredelil superiornost Kitajske na področju elektromagnetnega spektra. Z uspehi na področju elektronskega bojevanja, ki jih dosega Rusija po stabilizaciji fronte v Ukrajini, je jasno, da elektronsko bojevanje ima in bo tudi v prihodnosti imelo pomembno vlogo. Realistično pa ne moremo trditi, da je to edino področje, ki bo odločalo o zmagi. V tem primeru je treba omeniti, da Natove države že pospešeno vzpostavljajo zmogljivosti ter se odzivajo na nove grožnje in so se jim sposobne bolj ali manj zoperstaviti.

Prihodnost elektronskega bojevanja in izvidovanja je glede na grožnje perspektivna. V ReDPROSV35⁹ (UL RS št. 103/04, 2022) kot tudi v novem predlogu 2023 je večkrat izpostavljeno opremljanje s sredstvi elektronskega bojevanja do leta 2035 oziroma 2040. Kako vzpostaviti učinkovit sistem za zaščito pred brezpilotnimi letalnimi sistemi in tudi vse pogostejše uporabljenimi komercialnimi brezpilotnimi letalnimi sistemi, pa je izziv, ki si ga moramo v naslednjih letih zastaviti v sodelovanju z različnimi strukturami Slovenske vojske ter v sodelovanju z drugimi nacionalnovarnostnimi prvinami.

Kot smo že omenili, v Slovenski vojski še ni bilo oblikovanega koncepta izvajanja zaščite pred grožnjami brezpilotnih letalnih sistemov. Enota za elektronsko bojevanje poskuša slediti sodobnim tehnologijam in načinom sodobnega vojskovanja, vendar ker zaščita pred grožnjami pred brezpilotnimi letalnimi sistemi močno presega delovanje posamezne enote, je nujno povezovanje v širšem smislu. Zaščito pred grožnjami iz zraka bo treba zagotavljati vsem silam, tako na morju, v zraku kot na kopnem. Ameriška vojska je že leta 2017 izdala ATP 3-01.81 (Counter-Unmanned Aircraft System Techniques), ki natančno

⁹ Resolucija o splošnem dolgoročnem programu razvoja in opremljanja Slovenske vojske do leta 2035, ki je bila sprejeta tik pred rusko agresijo na Ukrajino, 2. 2. 2022. Trenutno je v obravnavi nova, s katero se časovnica zamika.

opredeljuje tehnike zoperstavljanja v operativnem okolju do ravni brigade. Pri tem so zelo poudarjeni situacijsko zavedanje in pravočasno opozarjanje, poročanje ter prenos informacij.

Glede na pospešen razvoj na področju elektronskega bojevanja je smiselno izpostaviti nekatera dejstva velikih držav, kot sta Rusija in Kitajska. Rusija in Kitajska sta v zadnjih desetih letih močno vlagali v sisteme elektronskega bojevanja v vseh zvrsteh. Poročilo, ki ga je pripravil Roger N. McDermott leta 2017 o razvoju ruskih zmogljivostih na področju elektronskega bojevanja do leta 2025, podrobneje opredeljuje dolgoleten razvoj z jasno opredeljenimi političnimi cilji, pri čemer sta tako predsednik Putin kot Medvedjev podpisovala odloke že od leta 2002, in sicer o vzpostavitvi radioelektronskega bojevanja (REB), kot ga poimenujejo v Rusiji. Omenimo lahko, da Rusija elektronsko bojevanje, za razliko od Nata, spoznava kot samostojno domeno poleg kopenske, zračne, pomorske in vesoljske. Nato je za razliko v ospredje postavil kibernetško bojevanje. Rusija, podobno kot Kitajska, elektronsko bojevanje močno povezuje s kibernetško in zračno obrambo, artilerijo, za doseganje svojih ciljev se prepleta tudi s SIGINT. Enote za elektronsko bojevanje so spustili na raven motoriziranih brigad, pri čemer s četo za elektronsko bojevanje zagotavljajo zaščito brigadi na razdalji do 50 km. Skupno je na ruskem ozemlju razporejenih pet brigad za elektronsko bojevanje, dve sta na zahodnem vojaškem območju. Vsi sistemi za elektronsko bojevanje, ki jih ima Rusija, so porazdeljeni znotraj posameznih struktur, da omogočijo t. i. »bubbles«-način zaščite, ki zagotavlja celovito pokritost na območju delovanja (Cranny-Evans, 2022).

Zaščito manevrskih enot in posameznih struktur s konceptom elektronskega bojevanja bi morala zagotoviti tudi Slovenska vojska. Ker enota za elektronsko bojevanje ne more pokrivati celotnega področja delovanja, je treba razmišljati o elementih elektronskega bojevanja znotraj posameznih struktur Slovenske vojske. V nadzoru zračnega prostora, letalstvu, mornarici in odredu za specialno delovanje elektronsko bojevanje ni neznanka, lahko pa rečemo, da se zaščita sil z elektronskim bojevanjem premalo uporablja v drugih kopenskih strukturah. Žal sodobno vojskovanje in prav zaščita pred brezpilotnimi letalnimi sistemi vse pripadnike sili k razmišljanju, kako ukrepati, če se pojavi taka grožnja. Kot Natova članica napotujemo pripadnike na krizna žarišča, zato bi bilo treba začeti opremljati in usposabljamati enote v takih pogojih delovanja. Opremljanje enot s sistemi za boj proti brezpilotnim letalnim sistemom bi bilo potrebno po sistemu lažje prenosne do ravni voda ali čete, prevozne do ravni brigade in za posamezne

zmogljivosti, ki predstavljajo cilj visoke vrednosti za nasprotnika. Stacionarne sisteme bi se lahko razporejalo za zaščito kritične infrastrukture, kot so na primer pristanišča, letališča, različna skladišča ipd.

4.1 Taktična raven

Na taktični ravni v Slovenski vojski govorimo o zaščiti pred brezpilotnimi letalnimi sistemi do ravni brigade. Slovenska vojska v zadnjem obdobju pridobiva pozitivne izkušnje na mednarodnih vojaških vajah in v mednarodnih operacijah ter na misijah. V okviru teh aktivnosti se seznanja in usposablja z različnimi koncepti delovanja znotraj Natovih struktur. Tako so na primer spoznali, da brigada za svoje uspešno delovanje potrebuje tudi koordinacijsko celico elektronskega bojevanja (angl. *Electronic Warfare Coordination Cell – EWCC*), ki podpira poveljstvo in delovanje manevrskih struktur z elektronskim bojevanjem ter nadzorom nad elektromagnetnim spektrom. Situacijsko zavedanje o elektromagnetnem spektru in načrtovanje zaščite pred brezpilotnimi letalnimi sistemi se začeta z namero ter usmeritvami poveljnika brigade.

Zaščita pred brezpilotnimi letalnimi sistemi v sodobnem načinu vojskovanja postaja prednostna naloga, ki zahteva poglobljeno usklajevanje s podrejenimi enotami, ohranjanje nenehnega zgodnjega opozarjanja ter dodatne oborožitvene sisteme za podporo delovanja. Razmestitev posameznih senzorjev je treba predhodno načrtovati. Vse večji pomen dobivajo pravočasno informiranje, skupna operativna slika in odzivnost enot na grožnje iz zraka. Zaradi vse hitrejšega razvoja in vedno boljših lastnosti brezpilotnih letalnih sistemov je pomembno razvijati hitro opozarjanje ter takojšnje reakcije. Treba se je zavedati zelo ozkega časovnega okvira, ki je namenjen odločanju in delovanju proti brezpilotnim letalnim sistemom. Davis Hambling (2016) je že leta 2016 navajal, da se reakcijski čas za nevtralizacijo oziroma uničenje brezpilotnih letalnih sistemov zmanjšuje in je padel že pod eno minuto, čemur potrjujejo tudi izračuni Arthurja Hollanda Michela (2019, 8). Seveda se hitrosti med brezpilotnimi letalnimi sistemi zelo razlikujejo kot tudi detekcija pri posameznih sistemih za boj proti brezpilotnim letalnim sistemom. V kolikor smo brezpilotne letalne sisteme zaznali ali že delovali po njih, pa je velika verjetnost, da je bil tudi že naš položaj kompromitiran. Uporaba sistemov za boj proti brezpilotnim letalnim sistemom se načrtuje glede na obveščevalno pripravo bojišča, pri čemer se z vojaškim procesom odločanja določijo protiukrepi na pričakovane grožnje.

Brigadno načrtovanje mora vključevati tehnike poročanja, identifikacijo, zgodnje opozarjanje in pravila delovanja (ATP 3-01.81, 2017).

Usposabljanje enot, ki ga izvajajo na podlagi učenja iz izkušenj ter zmogljivosti brezpilotnih letalnih sistemov, ki predstavljajo potencialno grožnjo, je na taktični ravni ključnega pomena. Na usposabljanjih bi bilo treba preverjati usklajeno delovanje in integracijo z nadzorom zračnega prostora nadrejenega poveljstva, ognjeno celico, celico elektronskega bojevanja ter zračno celico. Na vseh ravneh v brigadi bi se morali vzpostaviti pogoji za hitro prepoznavo in poročanje o kršitvah zračnega prostora. Vpeljati bi bilo treba standardizirano poročanje in dodatno usposabljanje opazovalcev zraka. Opazovalci bi se morali posebej urediti v prepoznavi silhuete vojaških kot tudi komercialnih brezpilotnih letalnih sistemov. Na določeni razdalji bi morali biti sposobni prepoznati vzorce in načine leta (ATP 3-01.81, 2017).

Poleg usposabljanja, načrtovanja in uporabe senzorjev bi bilo treba vzdrževati skupno operativno sliko ter povezave med posameznimi elementi. Brigade so običajno opremljene z digitalnim C2-sistemom, ki omogoča sprejemanje, obdelavo in distribucijo podatkov ter informacij o grožnjah na območju delovanja. V Slovenski vojski se uporablja sistem SitaWare, ki omogoča prenos podatkov za potrebe poveljevanja in kontrole, administracije, logistike ter ognjene in obveščevalne podpore. Vzporedno se vzpostavlja tudi sistem radijskih zvez. Nedvomno bo treba v prihodnosti poudarjati področji informacijske podpore in zvez.

Za lažjo dekonflikcijo med uporabniki v zračnem prostoru in elektromagnetnem spektru bo treba na ravni brigade zagotavljati sodelovanje med različnimi elementi oziroma celicami, in sicer elementom zračne podpore, celico zračne obrambe, celico ognjene podpore, kontrolo združenega ognja, celico S2 (ISR), celico S3 ter med častniki za povezavo podrejenih enot (ATP 3-01.81, 2017).

Element za elektronsko bojevanje lahko najdemo na ravni brigade v celici za ognjeno podporo, čez katero se lahko načrtuje, koordinira ter izvaja elektronsko bojevanje. Brezpilotnim letalnim sistemom se lahko zoperstavljamo tudi z elektronskim napadom. Na raven brigade bi bilo smiselno umestiti sisteme za elektronsko bojevanje oziroma sisteme za boj proti brezpilotnim letalnim sistemom. Glede na sodobno vojskovanje bi bilo smotrno enote za zaščito pred brezpilotnimi letalnimi sistemi razporediti kot organske enote znotraj brigad (ATP 3-01.81, 2017).

Koncept zaščite pred brezpilotnimi letalnimi sistemi lahko poleg elektronskega bojevanja in zračne obrambe izvajamo tudi na druge načine. V osnovi lahko govorimo o ukrepih pasivne in aktivne obrambe. Med pasivne ukrepe zaščite pred brezpilotnimi letalnimi sistemi štejemo maskiranje, kritje in masko, utrjevanje položajev, premike enot ponoči, upoštevanje maskirne discipline, zatemnitev svetlečih se površin in uporabo različnih materialnih sredstev za prepoznavo vojaške tehnike. Med pasivne ukrepe štejemo tudi sistem za zgodnje opozarjanje, varnostno kulturo, zmanjševanje emisij v elektromagnetnem spektru, radijski molk, skrivanje, zlivanje z okolico, prikrivanje, uporabo vab ter zavajanje, razpršenost enot, odzivnost itn. Poleg elektronskega bojevanja k aktivnim ukrepom zaščite štejemo še uporabo sistemov zračne obrambe, lahkega pehotnega orožja ter različnih namerilnih naprav in druge zmogljivosti ter sisteme, ki lahko zaznajo nasprotnikove brezpilotne letalne sisteme.

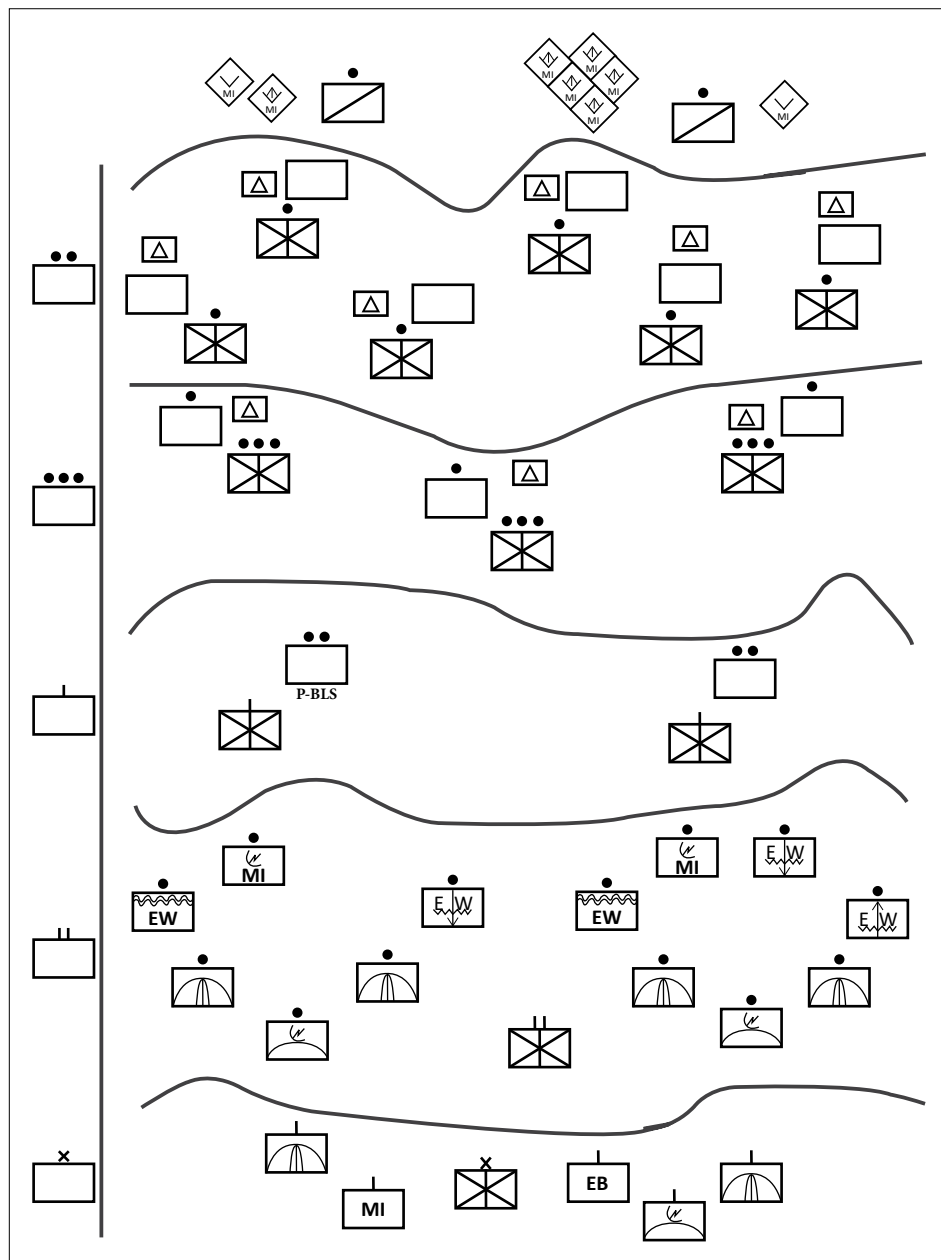
Na bataljonski ravni je treba podrobneje načrtovati multiplikatorje. Na ravni čete je poudarek predvsem na usposabljanju opazovalcev zraka, poročanju po standardiziranem obrazcu, upoštevanju pasivnih ukrepov zaščite pred brezpilotnimi letalnimi sistemi ter delovanju po njih s prenosnimi sistemi za boj proti brezpilotnim letalnim sistemom, kot so na primer elektromagnetna puška, pametno strelivo, fizični ulov z izstreljenimi mrežami itn. Delovanje po brezpilotnih letalnih sistemih mora biti seveda vnaprej določeno s Pravili delovanja (ATP 3-01.81, 2017).

V nadaljevanju bo sledil slikovni in tabelarni prikaz predloga koncepta zaščite pred brezpilotnimi letalnimi sistemi in elektronskim bojevanjem za potrebe Slovenske vojske. Na sliki 4 je predlog koncepta kot shematski prikaz umeščenosti različnih sistemov za boj proti brezpilotnim letalnim sistemom od ravni oddelka do brigade. Glede na velikost, premičnost in s ciljem lažje integracije v manevrske oddelke ter vode se do ravni čete za detekcijo razmeščajo opazovalci zračnega prostora. Za delovanje se do ravni čete opremlja z lahkimi, prenosnimi sistemi za boj proti brezpilotnim letalnim sistemom, kot je to prikazano v preglednici 3.

Na ravni čete lahko razvrščamo sisteme, ki omogočajo hkrati detekcijo in avtonomno delovanje zoper brezpilotne letalne sisteme. Sistemi se nameščajo na bojna vozila in predstavljajo sestavni del bojnega razporeda čete. Na bataljonski ravni se za potrebe zoperstavljanja brezpilotnim letalnim sistemom ter drugemu delovanju, ki obsega predvsem elektronsko izvidovanje, razporejajo zmogljivosti elektronskega bojevanja, elektronskega izvidovanja, zračne obrambe (SHORAD)¹⁰

¹⁰ Short Range Air Defence.

ter različni senzorji. Bataljonska bojna skupina (BBSk) v Slovenski vojski predstavlja stično točko sistemov za boj proti brezpilotnim letalnim sistemom najnižje taktične ravni, s kompleksnejšimi sistemi elektronskega bojevanja ter zračne obrambe, ki so prevozni in zmogljivejši ter namenjeni delovanju tudi po brezpilotnih letalnih sistemih višjih razredov in drugih grožnjah iz zraka.



Slika 4: Načelna shema koncepta zaščite pred brezpilotnim letalnim sistemom na taktični ravni – predlog (vir: lasten)

S predlagano razporeditvijo zmogljivosti detekcije in delovanja je treba vzpostaviti tudi sistem zgodnjega opozarjanja in poročanja ter mrežno pokritost zračnega prostora. Preglednica 3 v povezavi s shematskim prikazom na sliki 4 vključuje predstavnike zaščite pred brezpilotnimi letalnimi sistemi od ravni oddelka do brigade, upošteva možnosti umestitve in zmogljivosti posameznega sistema. Pomembno vlogo ima tudi povezljivost sistemov ter interoperabilnost z Natovimi članicami.

Enota	Sredstvo (primer)	Slika (primer)
ODDELEK - VOD	„Hand held neutralizer“ – EM-puška Teža puške: cca 7 kg Celotna teža: 18 kg RF-motilec: do ca. 2 km Bat.: 2 uri Antena: 2,4 GHz/5,8 GHz	
	(SMASH-Smartshooter) Detekcija: lock & track Delovanje: noč/dan Domet: do 250 m Način dela: drone mode Opcijsko: LRF (Laser Range Finder), Lock-Track-Hit	
ČETA	Mobilni P-BLS (sistemi za detekcijo ter nevtralizacijo) Radarski doseg: 15–30 km Akustika: do 300 m EO/IR: do ca. 1 km RF-sprejemnik: do ca. 5 km RF-motilec: do ca. 5 km	
BATALJON	Mobilni P-BLS Radarski doseg: 15–30 km Akustika: do 300 m EO/IR: do ca. 1 km RF-sprejemnik: do ca. 5 km RF-motilec: do ca. 5 km	
	Mobilni sistemi EI/EB RF-sprejemnik: do ca. 20 km RF-motilec: do ca. 10 km	

Enota	Sredstvo (primer)	Slika (primer)
BRIGADA	Sistemi z usmerjeno energijo, elektromagnetni pulz – EMP Različne moči Delovanje proti rojem brezпилotnih letalnih sistemov Prototipi	
	Visokoenergetski laserski sistemi Različne moči 50/100/300 kW Prototipi	

* Slike so simbolične. Slike in TT-podatki ne favorizirajo posameznih tehničnih sredstev oziroma proizvajalcev.

Preglednica 3: *Taktično-tehnična sredstva sistemov za boj proti brezпилotnim letalnim sistemom na taktični ravni** (vir: splet)

Po zelo splošnih ocenah bi v Slovenski vojski za pokrivanje elektromagnetnega spektra BBSk bilo treba zagotoviti približno 100 EM-pušk,¹¹ katerih okvirna cena znaša okoli 10.000 evrov. Na ravni čet bi bilo treba zagotoviti okoli štiri prevozne sisteme za boj proti brezпилotnim letalnim sistemom, katerih cene lahko nihajo od 100.000 evrov navzgor. Za bolj sofisticirane mobilne EI/EB-sisteme so cene še višje, tudi do desetkrat, pri laserskih sistemih ter sistemih z elektromagnetnim pulzom pa so še višje.¹² Tehnologija za boj proti brezпилotnim letalnim sistemom predstavlja zelo visoko investicijo v vsaki vojski. Pri tem je treba poudariti, da številni proizvajalci ne razkrivajo cen niti taktično-tehničnih podatkov. Znano je, da za zaščito kritične infrastrukture, kot je letališče, govorimo o večmilijonskih investicijah.¹³ Poleg osnovnih naložb je nujno upoštevati še stroške usposabljanja, vzdrževanja in plačilo posadki. Hitro se lahko vprašamo, ali je vlaganje sploh smiselno, če imamo na drugi strani komercialne brezпилotne letalne sisteme v vrednosti nekaj sto evrov. Poleg poceni brezпилotnih letalnih sistemov je vedno treba imeti v mislih tudi škodo, ki jo lahko povzročijo take majhne poceni naprave. Če pomislimo, da investicija v vozilo 8 x 8 znaša od sedem do deset milijonov evrov, lahko hitro izračunamo vrednost posamezne čete ali BBSk, ki lahko postane tarča majhnih in poceni brezпилotnih letalnih sistemov. Vprašanje, ali res lahko

¹¹ Lahko bi se kombiniralo s SMASH ali lovilci z mrežami.

¹² Razvoj še ni končan, investicija bi bila previsoka. Lahko pa se vloži v sisteme z usmerjeno energijo.

¹³ Letališče Gatwick je po incidentu s komercialnimi brezпилotnimi letalnimi sistemi namenil že več kot šest milijonov dolarjev za sistem za zaščito pred brezпилotnimi letalnimi sistemi.

dovolimo brezpilotnim letalnim sistemom uničiti sisteme, v katere smo vložili več sto milijonov evrov, je za današnji način vojskovanja zelo pomembno. Podobna vprašanja si zastavljajo v številnih vojskah, vendar lahko kmalu ugotovimo, da drugih možnosti, kot da preprosto poskrbimo za zaščito, ni. Kot podatek lahko navedemo ugotovitve, da je nesmiselno zoperstavljanje brezpilotnim letalnim sistemom z vojaškimi lovci, vrednimi več sto milijonov evrov, ali z raketami, vrednimi milijon evrov in več. Celo prestrezniki brezpilotnih letalnih sistemov v vrednosti 50.000 do 150.000 evrov so predraga investicija, še posebno, kadar govorimo o enkratni uporabi, kot to velja tudi za rakete. Smiselnost investiranja v sisteme za zaščito pred brezpilotnimi letalnimi sistemi, tako v okviru razvoja bataljonskih bojnih skupin, zračne obrambe, nadzora zračnega prostora, kibernetike ter elektronskega bojevanja, letalstva in mornarice, je vsekakor treba obravnavati celostno, kot je bilo že omenjeno, in ne ločeno, saj se področja dopolnjujejo ter le združeno lahko dosežejo zastavljene cilje (Holland Michel, 2019, 11 in EPIRUS, 2023).

Za vzpostavitev take zmogljivosti za boj proti brezpilotnim letalnim sistemom pa je treba poleg kadrovskega izziva omeniti tudi razvoj in s tem povezane razpise, testiranja, sprejemanja odločitev, pripravo pogodb, nabavo, usposabljanja, uvajanja v operativno uporabo, ki lahko tajajo tudi več let.

4.2 Operativno-strateška raven

Vodilna vloga pri vzpostavitvi novega koncepta, kot je zaščita pred brezpilotnimi letalnimi sistemi, bi morala pripadati operativno-strateški ravni. Z združitvijo pripadnikov z vseh ravni, tako s taktične, operativne kot strateške, bi lahko omogočili enotno usposabljanje s področja zaščite pred brezpilotnimi letalnimi sistemi. Operativno-strateška raven bi morala med drugim zagotavljati materialno-tehnična sredstva, opredeliti načine vzdrževanja ter vojaškega izobraževanja in usposabljanja kot tudi predlagati nacionalne in mednarodne vojaške vaje. Za lažje razumevanje bi bilo smiselno omeniti, da ima brigada Slovenske vojske, sicer taktična enota, glede na velikost Republike Slovenije in na številčnost Slovenske vojske v slovenskem vojaškem prostoru operativno in strateško odgovornost.

V nadaljevanju smo v preglednici analizirali dejanja, ki bi lahko služila kot priporočila pri uvajanju sistemov za boj proti brezpilotnim letalnim sistemom v Slovensko vojsko. Četudi ne govorimo o Natovih zmogljivostih, smo vseeno

uporabili orodje DOTMLPF-I,¹⁴ ki ga uporabljajo za njihovo vzpostavitev. I kot interoperabilnost je Natova posebnost, saj ima pomembno vlogo pri povezovanju članic. Ker se posebej nismo opredelili glede interoperabilnosti sistemov, naj omenimo le, da bi bilo treba upoštevati tudi to.

Na operativno-strateški ravni se bodo poveljniki zagotovo srečali tudi z vprašanjem primerne zaščite kritične infrastrukture. Pri zaščiti kritične infrastrukture, kot so skladišča, letalske baze in pristanišča, je smiselno analizirati način postavitve stacionarnih avtonomnih sistemov, ki zagotavljajo tako detekcijo, identifikacijo in nevtralizacijo, ob spremljanju konvojev pa se lahko poslužujemo predvsem RF-motilcev ter mobilnega spremstva. Visoko vredne cilje lahko zaščitimo s premičnimi sistemi.

DOTMLPFI		2 do 3 leta	do 10 let
Doktrina / Doctrine	Moramo narediti	Pregled Vojaške doktrine ter priprava predloga umestitve P-BLS.	Ponovno pisanje doktrine, ki bo opredeljevala spremembe v sodobnem vojskovanju.
	Morali bi narediti	Razvijanje koncepta uporabe BLS ter P-BLS skupaj z drugimi strukturami SV.	
	Dobro bi bilo narediti	Poudarjanje vloge obveščevalne dejavnosti za delovanje zaščite pred BLS.	
Organizacija / Organisation	Moramo narediti	EB ter P-BLS znova umestiti v strukturo SV.	P-BLS postane organski del vse do ravni oddelka.
	Morali bi narediti		Vpeljava modulov EI/EB na različnih ravneh od bataljona navzgor.
	Dobro bi bilo narediti	Vključitev posameznih EI-elementov v obveščevalno dejavnost strateške ravni, umestitev modulov EI/EB v vse strukture SV.	
Usposabljanje / Training	Moramo narediti	Uvedba usposabljanja P-BLS v načrte usposabljanj posameznih enot.	Usposabljanje vsakega vojaka o ukrepih pred BLS.
	Morali bi narediti	Uvedba usposabljanja prepoznavne BLS, usposabljanje inštruktorjev za zaščito pred BLS.	Usposabljanje posameznikov v vseh enotah oziroma ekipe za hitro odzivanje na grožnje pred BLS.
	Dobro bi bilo narediti	Sodelovanje na različnih mednarodnih vajah, ki vključujejo BLS, in usposabljanje za zaščito pred njimi.	Zaščita pred BLS, vključitev tematik o BLS na vseh ravneh VIU in DVSU.

¹⁴ Doctrine, Organization, Training, Material, Leadership, Personnel, Facilities, Interoperability.

DOTMLPFI		2 do 3 leta	do 10 let
Sredstva / Material	Moramo narediti	Opremljanje manevrske enote s sistemi za zaščito pred BLS (prenosni in prevozniki sistemi).	Oprema s kritično infrastrukturo z različnimi senzorji, radarji, OE-sistemi idr. z zmožnostjo detekcije, identifikacije in nevtralizacije ali uničenje BLS (stacionarni sistemi).
	Morali bi narediti	Podrobno spremljanje razvoja BLS in P-BLS.	Izgraditi sisteme za zgodnje opozarjanje.
	Dobro bi bilo narediti	Spodbujanje razvoja svoje industrije.	
	Moramo narediti	Usposabljanje vodstvenega kadra o zmogljivostih P-BLS.	
Vodenje / Leadership	Morali bi narediti		Usposabljanje ključnega kadra v okviru VIU o zmogljivostih P-BLS.
	Dobro bi bilo narediti	Povezovanje vodstvenega kadra z nevojaškimi institucijami, izobraževalnimi ustanovami, tako CAA kot amaterskimi klubi BLS, ter medresorsko sodelovanje.	
Kader / Personnel	Moramo narediti	Izdelava načrta pridobivanja kadra – zbiranje in združevanje različnih predlogov pridobivanja kadra, postati konkurenčni na trgu dela.	Pridobitev strokovnjakov s področij informatike, elektrotehnike, računalništva, mehatronike, robotike itn.
	Morali bi narediti	Povezovanje z izobraževalnimi ustanovami, sodelovanje na različnih projektih (civilno-vojaški, Natovi idr.).	Omogočanje razvoja obstoječega kadra v okviru večjih civilno-vojaških projektov.
	Dobro bi bilo narediti	Zaposlitev kadrovskih menedžerjev z vizijo in izkušnjami na področju slovenskega trga dela.	Povezovanje civilnih strokovnjakov z vojaško organizacijo, omogočanje dela po avtorskih ali podjemnih pogodbah.
Infrastruktura / Facilities	Moramo narediti	Zagotovitev kapacitet za simulatorje in delavnice.	Zagotovitev parkirne kapacitete za premične sisteme zaščite pred BLS.
	Morali bi narediti	Priprava in prilagoditev kritične infrastrukture za sisteme za zaščito pred BLS.	
	Dobro bi bilo narediti	Razmislek o podzemnih kapacitetah za zaščito.	

Preglednica 5: DOTMLPFI za zmogljivost sistemov za zaščito pred brezpilotnimi letalnimi sistemi (vir: prirejeno po Jbeli, 2019, posodobljeno 2023)

5 Sklep

Grožnje iz zraka, hitro rastoča proizvodnja brezpilotnih letalnih sistemov, njihova proliferacija in posledično razvoj sistemov za zaščito pred njimi so postali realnost sodobnega časa. Potrebe po sistemih za zaščito pred brezpilotnimi letalnimi sistemi obsegajo tako civilno kot vojaško področje. Številna podjetja, ki razvijajo nove tehnologije detekcije in nevtralizacije brezpilotnih letalnih sistemov, še ne izpolnjujejo pričakovanj uporabnika, vendar se iz dneva v dan izpopolnjujejo in združujejo. Kot je bilo zapisano že v uvodu, je bil namen odgovoriti na dve raziskovalni vprašanji. Prvo raziskovalno vprašanje se je glasilo: *Kako zagotoviti zaščito sil in zaščito kritične infrastrukture pred brezpilotnimi letalnimi sistemi?*

Ugotovili smo, da se ranljivost brezpilotnih letalnih sistemov glede na njihove različne lastnosti močno razlikuje. Nekatere je lažje zaznati s prostim očesom, nekatere slišati, spet druge odkrivati le z RF-senzorji, radarji itn. Raznolikost groženj je privedla do razvoja različnih tehnologij za detekcijo in nevtralizacijo, ki so bile podrobneje predstavljene. Upamo si postaviti trditev, da se v tem trenutku neke na svetu razvija sistem, ki bo kot novost na tržišču predstavljen na naslednji mednarodni razstavi EW Live v Tartuju. Zanimivo bo tudi spremljati tekmo med »mačko in mišjo« v naslednjih desetih letih ter momente, ko bo uporaba zaščitne tehnologije z iznajdljivostjo uporabnikov premagala brezpilotne letalne sisteme. In obratno, ko se bodo brezpilotni letalni sistemi znova prilagodili različnim algoritmom, poskušali zavesti umetno inteligenco ter različne senzorje in zaobiti detekcijo z novimi materiali, miniaturizacijo, moduli za elektronsko bojevanje, roji, novimi orožji itn. Če povzamemo, bodo na koncu ponovno odločilni človeški faktor, njegova inovativnost in do neke mere okolje, v katerem se bodo razvijale nove zamisli.

Kje se bo končala oboroževalna tekma z novimi brezpilotnimi letalnimi sistemi in sistemi za zaščito pred njimi, je nemogoče napovedati. Svetovno dogajanje in oboroževanje držav z omenjenimi sistemi ter drugo oborožitvijo zagotovo ne napovedujeta umiritve situacije. Ravno nasprotno, trendi napovedujejo njeno povečanje in zagotovo se novi tehnologiji ne da več izogniti. V prihodnosti bo prevlada na bojišču na strani, ki bo obvladovala združeno bojevanje ter hkrati zagotovila primerno zaščito lastnih sil na vseh področjih, tudi na področju elektromagnetnega spektra.

Poudarek v prispevku ni bil na zračni obrambi, kot bi sprva pomislili ob omembi grožnje iz zraka, temveč na grožnji v elektromagnetnem prostoru, ki ga kljub informacijski dobi, uporabi mobilne telefonije, interneta, navigacije ipd. še vedno

premalo poznamo. Dejstvo pa je, da se vse bolj kaže kot pomemben akter sodobnega vojskovanja. Ker je elektronsko bojevanje »sinonim« za elektromagnetni spekter, smo v drugem delu prispevka raziskovali elektronsko bojevanje v Slovenski vojski ter pripravili predlog koncepta zaščite pred brezpilotnimi letalnimi sistemi, ki ga danes vojske sveta na novo vpeljujejo ter izpopolnjujejo. V prispevku smo si zastavili še drugo raziskovalno vprašanje: *Kako z izvajanjem elektronskega bojevanja zagotavljati zaščito pred brezpilotnimi letalnimi sistemi v Slovenski vojski?*

Elektronsko bojevanje ni zgolj zaščita pred brezpilotnimi letalnimi sistemi, temveč je zmogljivost, ki nam omogoča nadzor ter delovanje v elektromagnetnem spektru. Brezpilotni letalni sistemi so poleg zračnega prostora tudi del elektromagnetnega spektra, saj v komunikaciji z zemeljsko upravljalno postajo ter z navigacijo oddajajo signale v prostor. Ob upoštevanju tega elektronsko bojevanje predstavlja ključno zmogljivost sodobnega vojskovišča. Države pospešeno prilagajajo svoje taktike, tehnike in postopke najnovejšim grožnjam iz zraka, kot so med drugim tudi majhni, nizkoleteči in počasni brezpilotni letalni sistemi. Tem se danes ne moremo več izogniti, vendar se jim lahko zoperstavimo tudi s podporo enot za elektronsko bojevanje in dopolnilnim usposabljanjem pripadnikov posameznih struktur v Slovenski vojski. Nenehno spremljamo nove publikacije ameriške vojske in Nata, ki zapolnjuje dolgoletne pomanjkljivosti na področju elektronskega bojevanja kot tudi zračne obrambe. Med pisanjem tega članka sta bili izdani s področja elektronskega bojevanja dve, in sicer ATP 3-12.3 in ATP 3-12.4, ki podrobneje urejata tehnike, taktike in postopke elektronskega bojevanja. Tudi na področju zračne obrambe je mogoče zaslediti prenovljene dokumente, ki na novo opredeljujejo grožnje brezpilotnih letalnih sistemov, prav tako to problematiko obravnavajo samostojne publikacije zaščite pred brezpilotnimi letalnimi sistemi. V ameriški vojski so po spoznanju, kako veliko grožnjo pravzaprav predstavljajo brezpilotni letalni sistemi, že pred časom sprejeli Strategijo za delovanje proti majhnim brezpilotnim letalnim sistemom. V Sloveniji se z omenjenimi grožnjami pod pritiski evropskih institucij srečujejo nekatere kritične infrastrukture, vse bolj pa se jih zavedata tudi Policija in Slovenska vojska.

Slovenska vojska je v fazi vzpostavljanja zaščite pred brezpilotnimi letalnimi sistemi. V nalogi smo s predstavitvijo predloga koncepta uporabe elektronskega bojevanja kot zaščite pred brezpilotnimi letalnimi sistemi vseskozi poudarjali tudi pomen združene situacijske slike in povezovanje z vsemi strukturami v

Slovenski vojski, saj bo le tako mogoče obvladovati kopenski, zračni, pomorski, kibernetski, informacijski in elektromagnetni prostor. Vsekakor bi naslednja raziskava lahko obravnavala analizo tržišča ali razvoj odločilnega modela za izbor sredstev za zaščito pred brezpilotnimi letalnimi sistemi ali izdelavo katerega izmed programov usposabljanja, ki bo potreben za urjenje in delovanje Slovenske vojske. Pri tem ne smemo zanemariti tudi elektronskega bojevanja posameznih zvrsti, kot sta mornarica in letalstvo, pri katerem se razvijajo specifični sistemi zaščite pred brezpilotnimi letalnimi sistemi, in jim v tem članku nismo namenili pozornosti, kot bi si jo zares zaslužili. Vsekakor gre za področje, ki ga lahko v prihodnosti poglobljeno raziščemo.

6 Literatura in viri

1. Al-Sa'd, A. S., Powell, K., Marojevic, V., in Geraci, G., 2020. UAV assisted attack prevention, detection, and recovery of 5G networks. *IEEE Wireless Communications*, 27(4). Str. 40–47. doi:10.1109/MWC.01.1900545. Dostopno na: https://www.researchgate.net/publication/342622466_UAVAssisted_Attack_Prevention_Detection_and_Recovery_of_5G_Networks/link/5f34febc92851cd302f15b73/download. [5. 2. 2023].
2. ATP 3-01.81. 2017. Counter-Unmanned Aircraft System Techniques. Washington DC. Headquarters-Department of the Army.
3. ATP 3-12.3. 2023. Electromagnetic Warfare Techniques. Washington DC. 30 January 2023. Headquarters – Department of the Army.
4. ATP 3-13.3. 2019. Electronic Warfare Techniques. Washington DC. 16. July 2019. Headquarters-Department of the Army.
5. Ball, M., 2016. Northrop Grumman Demonstrates Counter – UAS Technologies. UST. Dostopno na: <https://www.unmannedsystemstechnology.com/2016/10/northrop-grumman-demonstrates-counter-uas-technologies/>. [27. 2. 2023].
6. Butterworth-Hayes, P., 2022. Cyber takedown – the next generation of more effective counter-UAS technology. Unmanned Airspace. September 2022. A White Paper from <http://www.unmannedairspace.info>. [11. 12. 2022].
7. Castanedo, F., 2013. A Review of Data Fusion Techniques. Vol. 2013, ID 704504, *The Scientific World Journal*. Dostopno na: <https://doi.org/10.1155/2013/704504>. [28. 1. 2023].
8. Chanakya Team, 2022. Drone Killers: Raytheon's Laser Weapon Systems. Chanakya Geopolitics and National Security. [online]. India. Dostopno na: <https://chanakyaforum.com/drone-killers-raytheons-laser-weapon-systems/>. [5. 2. 2023].
9. Christianson, J., 2022. Fighting and Winning in the Electromagnetic Spectrum. War on the Rocks. [online]. 5. december 2022. Texas National

- Security Review. Dostopno na: <https://warontherocks.com/2022/12/fighting-and-winning-in-the-electromagnetic-spectrum/>. [31. 1. 2023].
10. Clark, B., 2022. The Fall and Rise of Russian Electronic Warfare. The Ukraine invasion has become an old-fashioned slog, enabling Russia to unleash its electronic weapons. War on the Rocks. [online]. 30. julij 2022. Texas National Security Review. Dostopno na: <https://spectrum.ieee.org/the-fall-and-rise-of-russian-electronic-warefare/>. [5. 2. 2023].
 11. Clay, M., 2021. The Rule of Invisible Battlefield: The Electromagnetic Spectrum and Chinese Military Power. War on the Rocks. [online]. 22. januar 2021. Texas National Security Review. Dostopno na: <https://warontherocks.com/2021/01/to-rule-the-invisible-battlefield-the-electromagnetic-spectrum-and-chinese-military-power/>. [5. 2. 2023].
 12. Cranny Evans, S., 2022. Fields of Silence and Broken Cycles: Russia's Electronic Warfare. Global Defence Technology. [online]. Dostopno na: <http://www.defence.nridigital.com>. [1. 3. 2023].
 13. Dong, Q., in Zou, Q., 2017. Visual UAV detection method with online feature classification. Technology, Networking, Electronic and Automation Control Conference (ITNEC). Chengdu, China. Str. 429–432. IEEE.
 14. EDR, 2021. Israel Aerospace Industries Sells Dozen of Drone Guard Systems to South Asian Country. European Defence Review. [online]. 2. 7. 2021. Dostopno na: <https://www.edrmagazine.eu/israel-aerospace-industries-sells-dozens-of-drone-guard-systems-to-south-asian-country>. [15. 2. 2023].
 15. EPIRUS. 2023. Correcting the cost imbalance in counter unmanned aerial system solutions. Epirus Product Markets. Dostopno na: Correcting the Cost Imbalance in Counter-Unmanned Aerial System Solutions — Epirus, Inc. (epirusinc.com). [26. 3. 2023].
 16. Furlan B., idr., 2006. Vojaška doktrina. Ljubljana: Defensor.
 17. Haider, A., 2021a. The Vulnerabilities of Unmanned Aircraft System Components. V M. Willis (US AF) A Comprehensive Approach to Countering Unmanned Aircraft Systems. Kalkar Germany. The Joint Air Power Competence Centre. Str. 55–72.
 18. Haider, A., 2021b. A Methodology for Countering Unmanned Aircraft Systems. V M. Willis (US AF) A Comprehensive Approach to Countering Unmanned Aircraft Systems. Kalkar Germany. The Joint Air Power Competence Centre. Str. 75–82.
 19. Haider, A., 2021c. Unmanned Aircraft System Threat Vectors. V V M. Willis (US AF) A Comprehensive Approach to Countering Unmanned Aircraft Systems. Kalkar Germany. The Joint Air Power Competence Centre. Str. 11–52.
 20. Hambling, D., 2016. »Drones Fight Back Against Laser Weapons« Popular Science. [online]. 4. november 2016. Dostopno na: <http://www.popsci.com/laser-guns-are-targeting-uavs-but-drones-are-fighting-back>. [6. 12. 2022].

21. Holland, M. A., 2019. Counter – Drone Systems 2nd edition. December 2019. Center for the Study of the Drone at Bard College. Dostopno na: <https://dronecenter.bard.edu/files/2019/12/CSD-CUAS-2nd-Edition-Web.pdf>. [15. 11. 2022].
22. Jbeli, J., 2019. Drones Proliferation: Should We Worry?. Master's Thesis. US Army Command and General Staff College. Fort Leavenworth. Kansas.
23. M. Z., 2022. Boscarol ob podpisu pogodbe z ministrstvom: »Bojmo se dronov, vse drugo je lažji izziv«. Intervju MMC RTV SLO. 14. september 2022 ob 13.19. STA.
24. McDermott, R., 2017. Russia's electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum. Report. RKK, ICDS. Republic of Estonia.
25. Pogačnik, R., 2017. Uporaba brezpilotnih letalnikov za zaščito kritične infrastrukture. Magistrsko delo. Celje: UM, Fakulteta za logistiko.
26. Quevedo, A. D., Urzaiz, F. I., Menoyo, J. G., Lopez, A. A., 2018. Drone Detection with X-Band Ubiquitous Radar. 19th International Radar Symposium (IRS). Junij 2018. Dostopno na: <https://www.semanticscholar.org/paper/Drone-Detection-With-X-Band-Ubiquitous-Radar-Quevedo-Urzaiz/e0a3026d83f574859369da27a67d865ae505ad6c>. [3. 2. 2023].
27. Resolucija o splošnem dolgoročnem programu razvoja in opremljanja Slovenske vojske do leta 2035 – ReDOPSV (Uradni list RS, št. 16/22).
28. Resolucija o strategiji nacionalne varnosti Republike Slovenije (ReSNV-2) (Uradni list RS, št. 59/19).
29. Robin, Robin Systems, 2022. 10 Counter Drones Technologies to Detect and Stop Drones Today. Dostopno na: <https://www.robinradar.com/press/blog/10-counter-drone-technologies-to-detect-and-stop-drones-today>. [3. 2. 2023].
30. Schmidt, A., in Haider, A., 2021. The Differences Between Unmanned Aircraft, Drones, Cruise Missiles and Hypersonic Vehicles. V M. Willis (US AF) A Comprehensive Approach to Countering Unmanned Aircraft Systems. Kalkar Germany. The Joint Air Power Competence Centre. Str. 27–31.
31. Udin, Z., in dr., 2020. Amateur Drones Detection: A machine learning approach utilizing the acoustic signals in the presence of strong interference. Computer Communications. [online]. Vol. 154, 15. marec 2020, str. 236–245. Dostopno na: <https://www.sciencedirect.com/science/article/abs/pii/S0140366419318341>. [5. 2. 2023].
32. Von Spreckelsen, M., 2018. Electronic Warfare – The Forgotten Discipline. Why is the Refocus in this Traditional Warfare Area Key for Modern Conflict?. The Journal of the JAPCC. Transforming Joint Air and Space Power. [online]. Journal Edition 27. JAPCC. Dostopno na: <https://www.japcc.org/articles/electronic-warfare-the-forgotten-discipline/>. [13. 12. 2022].

33. Stathopoulos, P., 2021. Electromagnetic Operations. V M. Willis (US AF) A Comprehensive Approach to Countering Unmanned Aircraft Systems. Kalkar Germany. The Joint Air Power Competence Centre. Str. 168–180.
34. Wang, J., Liu, Y., Song, H., 2020. Counter-Unmanned Aircraft System(s) C-UAS): State of the Art, Challenges and Future Trends. IEEE AEES Systems Magazine. [online]. Dostopno na: https://www.researchgate.net/publication/343986630_Counter-Unmanned_Aircraft_Systems_C-UAS_State_of_the_Art_Challenges_and_Future_Trends. [15. 12. 2022].
35. Willis in dr., 2021. A Comprehensive Approach to Countering Unmanned Aircraft Systems. Kalkar Germany. The Joint Air Power Competence Centre.