RĂZBOI ELECTRONIC – LECȚII ÎNVĂȚATE DIN ATACUL RUSIEI ASUPRA UCRAINEI

ELECTRONIC WARFARE – LESSONS LEARNED FROM RUSSIA'S ATTACK ON UKRAINE

Comandor. (r) dr. Sorin TOPOR*

Rezumat*: Conflictele hibride devin tot mai dese şi mai suprinzătoare. Este tot mai greu să încerci să faci o previziune pentru viitoarele operații militare. Analizând declanşarea Operației militare speciale a Rusiei, la un an de desfăşurare, putem observa că, de la o etapă la alta, strategiile, formele şi metodele de acțiune se diversifică extrem de rapid prin introducerea de noi tehnologii şi tactici. În prezenta lucrare ne propunem să stabilim locul şi rolul războiului electronic în acest conflict şi să identificăm unele repere pentru reforma concepției de dezvoltare a războiului electronic în Armata României.*

Cuvinte cheie: *război electronic, război în Ucraina, operația militară specială a Rusiei.*

Abstract: *Hybrid conflicts are becoming more frequent and surprising. It is increasingly difficult to try to make a forecast for future military operations. Analyzing the launch of Russia's Special Military Operation, one year after its implementation, we can see that, from one stage to another, the strategies, forms and methods of action are diversifying extremely quickly through the introduction of new technologies and tactics. In this paper, we propose to establish the place and role of electronic warfare in this conflict and to identify some benchmarks for the reform of the concept of electronic warfare development in the Romanian Army.*

Keywords: *electronic warfare, war in Ukraine, Russian special military operation.*

Introducere

La un an de la debutul Operației speciale militare a Rusiei asupra Ucrainei ne propunem să analizăm locul și rolul războiului electronic în cadrul concepției de război hibrib desfășurat de Rusia asupra Ucrainei. Rezultatele obținute constituie repere pentru modernizarea forțelor și pentru estimarea unor ipotetice modele de pregătire pentru apărare a țării.

După cum se cunoaște, Rusia a acordat întotdeauna o mare importanță războiului electronic. În abordările sale despre „războiul noii generații” războiul electronic este caracterizat de o serie de sisteme noi și tactici inovative, în strânsă relație cu dezvoltarea sistemelor UAV, focul

* Institutul Național de Cercetare-Dezvoltare în Informatică, membru asociat al Academiei Oamenilor de Știință din România, sorin.topor@ici.ro

masiv cu sisteme avansate de dirijare și submuniții, reforma marilor unități tactice în grupuri de luptă, mobile și combinate, precum brigăzi mobile de arme combinate, brigăzi de asalt aerian și operații speciale, unități mobile și avansate de apărare antiaeriană etc. Un grup de luptă este capabil să desfășoare operații combinate, cu lovituri kinetice și cibernetice.

Până la declanșarea Operației speciale militare, Rusia a dezvoltat elemente sofisticate de război electronic care integrează tehnologii și aplicații pentru război electronic, pentru tot spectrul războiului informațional și cibernetic. Industria de apărare a prezentat realizări științifice remarcabile și tehnologii care au permis modernizări ale echipamentelor existente și de crearea de noi sisteme de luptă care să sprijine acțiunea forțelor armate.

Nu în ultimul rând, participarea Rusiei în misiuni din diverse teatre de război precum Siria, Georgia, Ucraina (2014), dar și în aplicații cu parteneri externi (de regulă cu Bielorusia) a permis forțelor armate ruse să testeze noile echipamente, să studieze și să indentifice noi tactici de utilizare a lor.

Detalii experimentale

Prezentăm cele mai relevante secvențe care caracterizează operațiile de război electronic desfășurate în perioada februarie 2022 – februarie 2023. De departe, se observă că ambii actori implicați au utilizat drone aeriene de diverse dimensiuni, civile și militare, în scopul culegerii de informații, monitorizarea manevrelor de forțe și targeting-ului loviturilor cu foc. Poate fi considerat un război al dronelor.

Analiza tacticilor de război electronic desfășurate de Rusia

Debutul invaziei forțelor ruse (24.02.2022) a fost precedat de puternice acțiuni de bruiaj și de dezinformare electronică. În prima fază a războiului, Rusia a acordat un interes scăzut capacităților ucrainene de război electronic cunoscând foarte bine capabilitățile de luptă, majoritatea fiind fabricate în Rusia. Diferențele tehnologice provin din faptul că Rusia, după criza financiară din 2008, și-a continuat strategia de dezvoltare și de modernizare a tuturor capabilităților de luptă. Ucraina s-a concentrat pe alte obiective pe care le-a considerat prioritare la nivel național. După 2013, Rusia a implementat ample reforme și modernizări în cadrul forțele armate dispuse în zona de vest a țării, iar după 2014 a creat noi trei armate[1]. Acestea erau echipate cu sisteme moderne de luptă, în special, pentru apărare CBRN, operații speciale, război electronic, vehicule blindate și JISR.

Deși bugetul alocat apărării era destul de mic în comparație cu alte state membe NATO, Rusia a reușit ca prin implementarea de noi concepte

[1] Muzyka, K. (2021), *Russian Forces in the Western military District*, the CNA Occasional Paper, disponibil la https://www.researchgate.net/publication/350313637_Russian_Forces-_in_the_Western_Military_District, accesat la 18.01.2023.

de dezvoltare, de coordonare și de stimulare a capacităților industriei de apărare să se poziționeze destul de bine față de majoritatea statelor europene și să suporte bine efectele pandemiei Covid 19.

Anterior începerii războiului, în cadrul forțelor armate ruse au fost implementate primele măsuri bazate pe „doctrina Gherasimov". Generalul Valeri Gherasimov, șeful Statului Major General, atrăgea atenția într-un discurs din 2013 la Academia Statului Major asupra faptului că există „forme și metode de operații asimetrice... care fac posibilă nivelarea superiorității unui inamic într-o luptă armată"[2] referindu-se la tacticile informaționale. Gherasimov estima că vor fi înființate un corp cibernetic în 2013, forțe operaționale informaționale în 2017 și Fundația pentru Cercetare Avansată (Echivalentul US Defence Advanced Research Projects Agency). Nu sunt informații despre existența acestor noi structuri. Analiza lui Shelhorst despre percepția Rusiei asupra conceptului de război, bazat pe lecțiile învățate în Estonia și Georgia, aplicate în Ucraina (2014), prezintă importanța convergenței dintre războiul cibernetic și electronic[3], fără a le nominaliza în mod direct.

Într-o analiză privind modul de implementare a doctrinei Gherasimov în cadrul forțelor armate ruse Lt.col. Timothy Thomas[4], sublinia că noua viziune de desfășurare a războiului aduce profunde schimbări în conținut și nu în forma de desfășurare a operațiilor militare. Calitatea luptei armate va fi determinată de calitatea armamentului și de metodele de angajare a acestora. O luptă de calitate trebuie să includă lovitura cu foc, lovirea electronică, robotizată, aerospațială, mobilitate aeriană, asalt aerian, lovitura de informare-recunoaștere, operațiuni de contrainformații și alte acțiuni, în care converg acțiunile de luptă și cele non-combat. Operațiunile ruse se vor caracteriza prin efecte indirecte, fără contact direct și cu lovituri active preventive. Concepția rusă stabilește că războiul electronic este parte a strategiei Anti-Acces/Area-Denial (A2/AD) adaptată pentru combaterea sistemelor C4ISR ale NATO. Acțiunile de război electronic sunt parte integrantă ale operațiilor kinetice și non-kinetice desfășurate atât în sprijinul forțelor cât și prin conducere independentă[5].

---

[2] Gherasimov, V. (translated by Dr.Harold Orenstein), *Thoughts on Future Military Conflict – March 2018*, disponbil la https://www.armyupress.army.mil/Portals/7/Army-Press-Online-Journal/documents/2019/Gerasimov-2019.pdf, accesat la 12.01.2023.

[3] Shelhorst A.J.C. (2016), *Russia's Perception Warfare*, Militaire spectator, disponibil la https://militairespectator.nl/artikelen/russias-perception-warfare, accesat la 12.02.2023.

[4] Thomas, T., *Russian Forecasts of Future War*, in Military Review (May-June 2019), disponibil la https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2019/Thomas-Russian-Forecast/, accesat la 22.02.2023.

[5] Thomas T. (2018), *Russia's Forms and Methods of Military Operations, The Implementers of Concep*t, disponibil la https://www.armyupress.army.mil/Journals-/Military-Review/English-Edition-Archives/May-June-2018/Russias-Forms-and-Methods-of-Military-Operations/, accesat la 20.01.2023

În prima fază a invaziei, mare parte din sistemele de război electronic au fost dispuse pe avioane pentru a asigura o concentrare a efortului electronic asupra țintelor din adâncimea teritoriului ucrainean și să sprijine acțiunea forțelor de la sol. O problemă majoră a utilizării excesive a atacului electronic a condus la realizarea bruiajului fratricid în numeroase sectoare de luptă. Semnalul de bruiaj emis nu poate discrimina receptorul țintă al inamicului de cel identic al forțelor proprii și amice. Constatând că sistemul ucrainean de apărare antiaeriană era încă operativ după atacul masiv eletronic efectuat, riscul de bruiaj fratricid i-a obligat pe ruși la o foarte atentă planificare, organizare și control al executării loviturilor electronice asupra sistemelor ucrainene. Ulterior, atacurile electronice au fost executate pe domenii concentrate pe misiuni distincte asupra comunicațiilor radio sol-aer și aer-aer, precum și asupra sistemelor radar și de navigație.

O altă problemă a fost determinată de sprijinul logistic în raport cu dislocarea forțelor. Dispozitivul de luptă inițial respecta organizarea ierarhică a forțelor. Problemele au apărut atunci când fluxurile logistice au avut întârzieri excesive în asigurarea cu echipamente, carburant, muniție și alimente pentru trupe. În mod implicit, pe timpul manevrelor de reorganizare a dispozitivelor de luptă și unitățile de război electronic au fost influențate.

În faza a doua a invaziei, Rusia a schimbat organizarea ofensivei pe aliniamente și a combinat echipamentele unităților strategice cu cele de nivel tactic.

Din punct de vedere a războiului electronic au organizat următoarele aliniamente:

1) Primul aliniament, la aproximativ 1 – 3 km față de linia de contact, era format preponderent din sisteme tactice de război electronic, sisteme mobile sau portabile, combinate cu echipamente SIGINT. Cu echipamente de tipul Benthos, Mercury-BM, Lille-2, Roland-Jet-AD etc., au executat misiuni de interceptare, localizare și blocarea comunicațiilor mobile (VHF și GSM) ale adversarului.

2) Al doilea aliniament, la aproximativ 15 – 30 km față de aliniamentul de contact, era format din echipamente de tipul Lille-3, Rexident, R-943UM, Borisogrebsk-2 cu misiunea de a intercepta comunicațiile radio ale adversarului și a produce bruiaj de dezinformare și de inducere în eroare.

3) Al treilea aliniament era dispus la 60 – 240 km fiind format din echipamente de tipul Moscova-1 și Krasuha-4 cu misiuni de asigurare a sprijinului electronic, supraveghere și suprimarea interferențelor electromagnetice ale adversarului.

4) Echipamente ale structurilor strategice precum Murmansk-BN și Auto Yard erau dispuse mult în adâncime, pe teritoriul Rusiei și asigurau

monitorizarea traficului radio de nivel strategic, în special comunicațiile strategice ale Ucrainei cu diverse componente NATO. Aceste dispozitive de luptă fiind fixe sau puțin mobile executau misiuni active de bruiaj numai în momente critice, atunci când considerau că erau încălcate limitele stabilite, așa cum ar fi raiduri aeriene ale NATO peste frontiera de stat.

Această reorganizare a permis:

- Optimizarea controlului asupra sistemului de comandă și control (C2) a armatei ucrainene în afara contactului. Spre exemplu, bruiajul radio din regiunea Dombass a blocat complet comunicațiile radio. De regulă, pentru această sarcină erau destinate stații de tipul Borisogrebsk-2, R-300KMW și Boris Glebsk-2. Interesant este faptul că rușii au folosit și echipamente anterior scoase din uz. Stația de bruiaj radio R-330ZH a fost folosită pentru bruierea receptoarelor rachetelor de croazieră ucrainene, a rachetelor dirijate prin radio, a sistemelor UAV și a altor stații radio aflate în dotarea structurilor tactice de nivel brigadă.

- Bruiaj de navigație asupra sistemelor GPS. Înainte de declanșarea operațiunii militare specială, Rusia a efectuat bruiaj GPS pe scară largă, de-a lungul graniței ucrainene-belaruse, la nord de Cernobîl, precum și în regiunea Dombas. Pentru aceasta a utilizat sistemul Shipovnik-Aero care lansează semnale false de navigație pentru GPS pentru inducerea în eroare a radarelor de navigație, a radarelor sistemelor de trageting ale țintelor aeriene și a radarelor sistemelor de dirijare a rachetelor. În plus, Rusia a lansat bruiaj GPS și asupra zonelor geografice din Crimeea/Marea Neagră și Marea Baltică pentru a perturba libertatea de mișcare a aeronavelor de recunoaștere și de supraveghere ale NATO.

- Încercări de bruiaj a legăturilor satelitare cu sistemul Tianye-21 și alte echipamentele instalate pe piloni și antene de comunicație.

- Bruiajul împotriva radarelor sistemelor de apărare antiaeriană ucrainene a sprijinit foarte mult efortul forțelor aeriene pe timpul executării loviturilor aeriene. Sistemele aeropurtate de bruiaj Beech, Viespa și Khibiny pot detecta și bloca automat radarul sistemului de apărare antiaeriană dispus la sol. Dar poate bloca și radarul unui avion amic dacă funcționează în același spectru de frecvențe.

Alte acțiuni de război electronic executate pe timpul misiunilor de tip SEAD au implicat rachete anti-radiație care au scos din luptă numeroase radare ucrainene de avertizare timpurie și instalații de tragere cu rachete. Numai în data de 13 iunie 2022, 338 instalații de rachete antiaeriene ucrainene au fost distruse cu rachete de tipul KH-31 lansate de pe avioane SU-35.

- Dezinformarea electronică executată de ruși a avut două obiective și anume: 1) Dezinformarea vectorilor de lovire și a sistemelor lor de control; și 2) Dezinformarea personalului uman. Pentru dezinformarea sistemelor de identificare a țintelor au fost folosite numeroase tipuri de momeli active și pasive, manevre de înșelare, aeriene sau terestre, precum și

unele forme de bruiaj activ. Cu stația Krasuha-4 au generat ținte false pentru radarele sistemului de apărare antiaeriană ale Ucrainei și NATO. Eficiența bruiajului a fost destul de bună determinând forțele ucrainene să lanseze numeroase atacuri electronice și riposte fizice fapt care a determinat deconspirarea poziției forțelor și, ulterior, atacarea lor.

- Bruiaj asupra emisiilor posturilor radio ale mass-mediei naționale. Chiar dacă echipamentele aveau sisteme de protecție împotriva diverselor tipuri de interferențe specialiștii ruși au reușit să spargă aceste protecții și să execute bruiaj asupra unor emisii relevante.

- Monitorizare și bruiaj GSM. Tactica bruiajului radio intermitent le-a permis rușilor să concentreze monitorizarea comunicațiilor prin GSM în spațiu și timp. Militarii ucraineni care păstrau legătura cu familiile sau civilii care utilizau telefoane mobile puteau vorbi numai atunci când era posibilă monitorizarea GSM din parte rușilor. Multe informații despre armata ucraineană și despre manevrele lor au fost obținute din serviciile rețelelor sociale. Cu echipamentul Lille-3 rușii au trimis numeroase mesaje text către telefoanele mobile ale ucrainenilor pentru a-i convinge să se predea și pentru a slăbi moralul trupelor. În plus, zona de emisie a unui telefon mobil GSM devenea țintă pentru focul artileriei.

Privind apărarea electronică a forțelor ruse, o mare vulnerabilitate a fost dotarea limitată cu stații radio protejate și utilizarea și de militarii ruși a telefoanelor mobile civile GSM. Observând aceasta, încă din prima fază a operației speciale, rușii au limitat folosirea serviciilor sociale prin impunerea unei discipline radio foarte strictă. Analiza streemurilor video din Internet, aferente spațiului de luptă, ne demostrează că doar ucrainenii și, uneori, forțele cecene, au postat imagini și materiale filmate.

În această operație militară, rușii au creat o nouă utilitate războiului electronic, bruiajul fiind implicat pentru combaterea dronelor ucrainene. Cu sistemele Krasuha au lovit cu bruiaj senzorii și sistemul radio de control al dronei, ceea ce a condus la uzura prematură și/sau doborârea ei. Bruiajul radio produce blocarea receptorului GPS sau inducere de ținte false fapt care împiedică drona să identifice ruta normală. Nu în ultimul rând se poate bruia radioaltimetrul dronei făcând-o să iasă din zona de securitate aeriană și să o expună combaterii cu sistemele anti-dronă de tipul Armor, Pishchal-PRO, Taran-PRO, Sapsan-Bekas, Luch și Kupol. Numărul extrem de mare de drone consumate demostrează eficiența bruiajului. Numai în data de 20 iunie 2022, 1260 de drone ucrainene au fost doborâte de armata rusă. Numeroase epave găsite la sol nu aveau urme de gloanțe sau de arsuri fiind evident că au fost scăpate de sub control prin bruiaj radio.

Analiză critică a războiului electronic desfășurat de către armata ucraineană

Din punct de vedere al dotării armatei ucrainene cu echipamente de război electronic apreciem că Ucraina nu mai are sisteme funcționale, cele deținute fiind rapid detectate și neutralizate de armata rusă.

Ucrainenii bruiază emisiile radio ale comunicațiilor ruse prin suprapunerea propriilor emisii radio peste cele ale legăturilor de comunicații ruse. Pentru informare și apărare electronică au folosit servicii proprii de interceptare și localizare, precum și sprijinul de informații din partea NATO, în special pentru monitorizarea sistemelor de atac electronic a rușilor.

Pentru protecția forței ucrainenii au implementat rapid principiul descentralizării comenzii și controlului (C2) evitând bruiajul radio total executat de către ruși. Cea mai mare vulnerabilitate a acestei strategii a fost scăderea moralului luptătorilor, aflați în dispozitive descentralizate, prin lipsa informațiilor. La început, mass-media ucraineană și occidentală au scăzut în mod deliberat numărul de informații despre manevrele reale de forțe și despre evoluția conflictului, în unele situații acuzând armata rusă că nu folosește acțiuni de război electronic. Pentru a stimula voința de a lupta a populației ucrainene au fost difuzate o serie de programe prin care se dorea motivarea luptătorilor să nu se predea. Însă, datorită numărului copleșitor de atacuri electronice executate de ruși, modul de comunicare a guvernului cu cetățenii săi a trebuit modificat. Pe 6 martie 2022, ministul apărării al Ucrainei, Oleksii Reznikov, a cerut poporului să caute și să distrugă echipamentele rusești de război electronic și de informații. Acesta afirma că „*sarcina tuturor cetăţenilor cărora le pasă de asta (armata noastră n.a.) este să distrugă coloanele de aprovizionare şi sisteme EW/REB... Acest lucru va slăbi semnificativ trupele ruseşti şi va oferi un avantaj soldaţilor noştri. Ocupatorii vor deveni neputincioşi*”[6]. După acest moment, în presă au început să apară tot mai multe imagini cu echipamente de război electronic rusești avariate sau distruse cu ample referiri la modul în care au fost capturate de către ucraineni.

Unele dintre puținele acțiuni de succes care aparțin războiului electronic ucrainean țin de exploatarea unei mari vulnerabilități a avioanelor rusești. Acestea, în fața atacului cu rachete aer-aer care se dirijează în infraroșu, nu pot riposta cu capcane și momeli specifice combaterii acestei amenințări electonice. Majoritatea avioanelor rusești sunt ținte facile pentru rachetele Stinger, 9K38 Needle și alte rachete aer-aer puse la dispoziție de NATO.

O altă tactică a forțelor ucrainene a fost mare mobilitate a forțelor combatante sub efectul tăcerii electromagnetice. Scoaterea lor rapidă de sub efectul loviturilor directe a produs pierderi destul de mari dar într-un timp mult mai mare decât își planificase armata rusă. Mai mult decât atât, sistemele de comunicații ale forțele speciale pătrunse în adâncimea dispozitivului de apărare rus au folosit numai linii criptate și numai în momente critice. Echipamentele puse la dispoziție de NATO sunt de ultimă

[6] Radio Svoboda, *Міністр оборони закликав українців знищувати російські системи радіоелектронної боротьби і розвідки*, disponibil la https://www.radiosvoboda.-org/a/news-inistr-oborony-reznikov-ukraintsi/31745048.html, accesat la 20.02.2023.

generație. Forțele ucrainene au primit accesul și au început să folosească Sistemul radio terestru și aerian cu un singur canal al NATO (SINCGARS)[7].

În domeniul radar, ucrainenii au fost foarte atenți la organizarea și la realizarea dispozitivelor de luptă în relație cu cantitatea resurselor de mascare din teren pentru camuflaj și dezinformare electronică. Cu toate acestea pierderile au fost considerabile. Numai în prima zi de luptă au pierdut 36 radare, 13 posturi de comandă și stații radio, precum și 14 instalații de rachete de apărare antiaeriană. Totuși, utilizarea limitată a radarului și a bruiajului radio doar în momente critice a fost o măsură extrem de eficientă care a fost confirmată prin încercările eșuate ale rușilor de a încercui așezări urbane cheie din nordul Ucrainei, așa cum ar fi Kiev sau Harkov. Acțiunea forțelor ucrainene, cumulată cu o serie de factori precum logistica limitată rusă cu combustibil, muniție și provizii împreună cu accesul pe un teren dificil au oprit înaintarea coloanelor blindate rusești pe mai multe direcții cheie, făcând inutile atacurile electronice în tot spectrul electromagnetic ale sistemelor rusești.

Cu privire la sprijinul Ucrainei de către NATO cu sisteme și tehnologii destinate apărării țării observăm că forțele ucrainene au început să opună rezistență atunci când au primit echipamente de comunicații criptate din SUA și Turcia.

Privind furnizarea de echipamente de război electronic nici o țară nu dă detalii.

Nu în ultimul rând, serviciul Starlink oferit de Elon Musk asigură un sprijin incontestabil pentru Ucraina. Îngrijorarea lui Musk privind creșterea efortului rușilor pentru bruirea legăturilor de comunicații satelitare l-a determinat să-i avertizeze pe ucraineni că ar trebui să țină terminale oprite atunci când este posibil deoarece sunt vulnerabile la geolocalizare și pot reprezenta indicii pentru planificarea loviturilor cu foc.

Alte observații privind desfășurarea războiului electronic în acest război

Rusia este capabilă să integreze capabilitățile de război electronic și cibernetic la toate nivelurile ierarhice, tactic, operațional și strategic. Rusia are numeroase echipamente de război electronic și suficient know-how în domeniu.

La nivel strategic și operațional, Rusia are în subordinea forțelor terestre cinci brigăzi de război electronic, dintre care două brigăzi de război electronic în Districtul Militar de Vest[8]. La nivelul forțelor navale există

[7] Clark, B., *The Fall and Rise of Russian Electronic Warfare*, IEEE Spectrum, disponibil la https://spectrum.ieee.org/the-fall-and-rise-of-russian-electronic-warfare, accesat la 22.02.2023.

[8] Spring-Glace, M., *Return of Ground-base Electronic Warfare Platforms and Force Structure*, in Military Review (July-August 2019), disponibil la https://www.armyupress.-army.mil/Journals/Military-Review/English-Edition-Archives/July-August-2019/Spring-Glace-Electronic-Warfare/, accesat la 22.02.2023.

cinci centre de război electronic (de nivel brigadă), câte unul pentru flotele din parte eruropeană și două pentru flota din Oceanul Pacific[9]. Forțele aeriene au batalioane independente de război electronic (echivalente batalioanelor din brigăzile EW a forțelor terestre) în cel puțin patru din cele cinci armate aeriene și de apărare antiaeriană. Acestea sunt adaptate să lucreze cu brigăzile EW ale forțelor terestre.

Fiecare brigadă EW este formată din patru batalioane EW care pot îndeplini misiuni de nivel operativ și strategic sau pot sprijini activitatea structurilor de nivel tactic – operativ ale forțelor terestre. Acestea au în dotare: complexele RL257 Krasukha-4, L260 Krasukha-2, Murmansk-BN, Borisoglebsk-2, stațiile RB-341V Leer-3, Svet-KU, Infauna, Lesocek, Jitel, Dziudoist, Zaslon-REB și multe altele[10].

Aceste echipamente pot fi folosite independent sau conjugat cu altele. În Siria, un sistem Krasukha-4 a lucrat cu sistemul aeropurtat TK-25 pentru detectarea și blocarea semnalele radar de la sistemele terestre și aeriene de tragere, precum și contra rachetelor anti-navă[11]. Primul sistem detectează ținta iar cel de-al doilea suprimă activitatea radarului.

Sistemul RB-341V Leer-3 își poate extinde raza de acțiune prin utilizarea unui UAV de tip Orlan-10. Cu aceste sisteme se realizează urmărirea utilizatorilor de telefoane mobile, distribuirea de mesaje text false către abonații rețelei și targeting pentru executarea loviturilor cu foc de artilerie.

Brigăzile de manevră ale forțelor terestre au în dotare o companie de război electronic, o companie de sisteme aeriene fără pilot (UAV) și un pluton de sprijin de informații. În cadrul unei companii de război electronic sunt 12 platforme mobile și 15 sisteme individuale portabile. Pentru bruiaj radio în VHF rușii au mai folosit preponderent stațiile R-934B și SPR-2 VHF/UHF. Pentru misuni de bruiaj radio HF, companiile EW au în dotare sistemele Murmansk-BN, Pole-21 sau R-330H Zhitel[12]. Acestea au acționat asupra comunicațiilor radio dintre aeronave, nave și sateliți în scopul degrădării acurateții armamentului dirijat prin radio și GPS.

Prin combinarea acțiunilor în mediile cibernetic și informațional, structurile terestre au ca principale misiuni protejarea structurilor de nivel

---

[9] Copcea I., *Războiul electronic devine componentă esențială în doctrina pentru operații a Forțelor Navale ruse*, Desense Romania, disponibil la https://www.defenseromania.ro-/razboiul-electronic-devine-componenta-esentiala-in-doctrina-pentru-operatii-a-fortelor-navale-ruse_606497.htm, accesat la 21.02.2023

[10] Tass, Чем армия России может "ослепить" и "подавить" противника, https://tass.ru/armiya-i-opk/6328905 visited by 22.02.2023

[11] Cranny-Evans, S., *Fields of silence and broke cycles: Russia's electronic warfare*, in Global Defence Technology, disponibil la https://defence.nridigital.com/global_-defence_technology_mar22/russia_electronic_warfare, accesat la visited by 22.02.2023

[12] Pravda, *Nurmansk-BN systems turn F-35 figters into scarp metal near Russian borders*, disponibil la https://english.pravda.ru/news/world/149839-murmansk_f_35/, accesat la 21.02.2023;

operativ și interzicerea accesului inamicului aerian, prin integrarea capacităților de apărare aeriană ca parte a strategiei A2/AD.

Anterior războiului, strategii militari ruși au testat diverse tactici în condiții de război (Georgia și Siria) sau pe timp de pace. Evenimentul în care a fost implicat distrugătorul american USS Donald Cook atunci când a intrat în apele Mării Negre pentru a executa o misiune de patrulare de rutină este un bun exemplu. Pe data de 15.04.2014 deasupra lui USS Donald Cook a evoluat un avion Su 24 rusesc și a executat mai multe treceri care simulau atacul navei. Problema a apărut când s-a constat că sistemul rusesc aeropurtat Khibiny a reușit să oprească toate sistemele electronice de la bordul navei, inclusiv cele care aparțin sistemului Aegis[13].

Echipamentele rușești de bruiaj GPS au determinat includerea în sistemele de navigație prin GPS ale NATO de algoritmi antiblocare și adaptarea lor la regimul de dirijare inerțială, ca sistem secundar. În Siria numeroși vectori de lovire ai NATO dotați cu sisteme de dirijare de precizie au fost perturbați, fapt care a produs un consum sporit de muniție și concomitent cu scăderea efectelor unor lovituri cu rachete.

Indiferent de numărul pierderilor în drone acestea au fost cele mai intens utilizate. Pentru doborârea dronelor atât ucrainenii cât și rușii folosesc arme cu foc de calibru mic, mitraliere, rachete antieriene portabile și bruiaj electronic[1], iar pentru obținerea controlului asupra funcționării lor atacuri cibernetice[2]. Oficiali ai ambelor forțe implicate au recunoscut că sunt zone în care dronele nu au putut fi folosite pentru că adversarul folosește bruiaj radio asupra sistemelor GPS și asupra legăturilor radio de control al acestora. Sistemul rusesc antidronă Rosehip-AERO reprezintă un echipament de război electronic care înlocuiește erorile generate prin bruiaj cu coordonate dinamice ale spațiului de navigație obligând drona să aterizeze în locația stabilită de sistemul de război electronic.

Servicul de internet prin sateliți de orbită joasă, Starlink al SpaceX a permis armatei ucrainene să folosească comunicații în bandă largă și servicii Internet, conform acordurilor încheiate. Și alte companii comerciale au oferit servicii satelitare Ucrainei pentru monitorizarea raioanelor și manevrelor forțelor, pentru monitorizarea fluxurilor de refugiați etc. Dintre acestea amintim OneWeb, Planet și MDA. În momentul în care ucrainenii au folosit serviciul Starlink pentru a controla drone[6] Rusia a încercat să bruieze semnalele Starlink realizând întreruperi temporare. Pentru aceasta au utilizat sistemele Suha-2, Krasuha-4 și Jilada-2.

Armata rusă a mai utilizat avioane specializate de război electronic de tipul Il-22PP, în misiuni strategice și operative, pentru suprimarea electronică a țintelor terestre, aeriene, maritime și spațiale. Există informații

[13] Sharman, J., *Russia claims to have weapon that could cripple the US Navy, State new report surfaces three years after alleged o jammer against American destroyer*, disponibil la https://www.independent.co.uk/news/world/europe/russia-weapon-us-navy-cripple-electronic-signals-deactivate-defence-systems-a7693816.html, accesat la 16.01.2023.

că ar mai folosi și elicopterul Mi-8MTRP-1 Rychag, specializat în suprimare electronică a sistemelor de apărarea antiaeriană[14].

Rezultate

Apreciem că perioada analizată se caracterizează prin următoarele aspectele inovative și tipuri de vulnerabilități ale sistemelor de luptă:

1) Executarea loviturilor cu foc, de la mare distanță (cu artileria sau rachetele), concomitent cu acțiuni cibernetice, sprijin satelitar și de război electronic. Cele mai mari vulnerabilități a sistemelor de conducere (C2) au fost generate de dotarea precară cu echipamente moderne de comunicații. Introducerea în luptă a militarilor mobilizați, fără să parcurgă toate etapele de pregătire au sporit efectele negative. Necesitatea menținerii unei rezerve mari de forțe și de mijloace adaptate operațiilor în mediul electromagnetic și în spațiul cibernetic a determinat neimplicarea tuturor forțelor specializate din dotarea categoriilor de forțe.

2) Lipsa unei instruiri adecvate a operatorilor radio și radar a produs bruiaj fratricid și perturbarea informării despre situația electromagnetică în momente critice. Pe fondul stresului operatorii au folosit prea mult bruiajul activ.

3) Un mare avantaj al sistemului de război electronic rus este determinat de capabilitățile de mobilitate majoritatea sistemelor fiind montate pe vehicule pe șenile și pe roți. Terenul a creat mari probleme pentru unitățile de război electronic. Natura neomogenă a liniilor frontului într-un teren cu diverse forme de relief face dificilă utilizarea războiului electronic fără a afecta forțele proprii care acționează în vecinătatea lor. Când forțele ruse au încercat să distrugă antenele sistemelor de telefonie celulară 3G în regiunea Harkov au făcut inactive și serviciile propriei rețele de criptofonie militară pentru că și aceasta funcționa pe tehnologia 3G/4G. Mai mult decât atât, datorită utilizării aceleiași tip de tehnologie rușii nu au putut întrerupe complet infrastructura cibernetică prin lovituri cibernetice și kinetice.

Necunoașterea vulnerabilităților electromagnetice a permis forțelor ucrainene să contracareze avantajul numeric și tehnologic al armatei ruse. Grupuri de luptă dispersate și foarte mobile au desfășurat atacuri de hărțuire asupra coloanelor de blindate pe care rușii se bazau în operația lor specială.

4) Punerea la dispoziția ucrainenilor de către mai multe armate NATO a unei game variate de sisteme radio de comunicații a sporit nivelul de protecție electronică a comunicării grupurilor de luptă. În plus, în zone cu aglomerări urbane încă locuite de civili, militarii ucraineni au folosit servicii GSM, făcând foarte grea discreditarea emisiilor militarilor de către alte

[14] Copcea, I., *Rușii folosesc în Ucraina un model de elicopter extrem de rar-Mi-8MTPR-1 Rychag, specializat în războiul electronic*, Defense Romania, disponibil la https://www.defenseromania.ro/rusii-folosesc-in-ucraina-un-model-de-elicopter-extrem-de-rar-mi-8mtpr-1-rychag-specializat-in-razboiului-electronic_618745.html, accesat la 21.02.2023.

emisii a telefoanelor civile. Informațiile extrase din modul de comandă al sistemului Krasukha-4, capturată la periferia Kievului, la mijlocul lunii martie 2022, demonstrează interesul rușilor și limitele practice în soluționarea acestui aspect.

Concluzii

Războiul modern se bazează în mare măsură pe spectrul electromagnetic și spațiul cibernetic, iar mijloacele de război electronic sunt cheia pentru a profita de avantajul spectrului electromagnetic. Conceptul că victoria electronică înseamnă victoria în război devine din ce în ce mai reală.

Rigiditatea relativă a liniilor de front și utilizarea caracteristicilor de mascare electronică a terenului într-un dispozitiv de luptă cu structuri dispersate și neregulate vor constitui avantaje pentru organizarea apărării temporare în fața unui inamic care abordează o strategie ofensivă multi-domeniu.

Dotarea cu echipamente moderne și crearea unei rezerve adecvate reprezintă o cerință prioritară. Pentru aceasta instruirea operatorilor la echipamentele de război electronic trebuie făcută din timp având în vedere consumul extrem de mare de forțe și mijloace din cadrul conflictului. Totodată trebuie înființate linii tehnologice naționale pentru producția echipamentelor cu elemente proprietare pentru a se evita surprinderea și eventuale politici de embargou ale statelor care susțin acțiunea adversarului.

În contextul unui conflict de mare intensitate capacitățile de război electronic reprezintă o amenințare pentru sistemele ISR convenționale ale inamicului. Dacă acceptăm că majoritatea conflictelor viitoare vor fi în medii foarte urbanizate și digitalizate, sistemele de război electonic vor fi un real sprijin în combaterea unui număr extrem de mare de ținte complexe și diverse, multe putând să se ascundă printre semnăturile electronice ale infrastructurilor civile.

Tacticile de război electronic vor continua să aducă avantaje asimetrice grupurilor de luptă prin încetinirea sau confuzarea forțelor inamicului fără să provoace victime directe. Tehnologiile moderne de atac electronic cu unde electromagnetice de frecvențe foarte înalte și de mare putere pot afecta vehiculele adversarului făcându-le vulnerabile tacticilor de hărțuire și ambuscadelor.

Atacurile convergente electronice și cibernetice asupra elementelor logistice și de infrastructură ale adversarului pot încetini manevrele de forțe prin perturbarea rețelelor IT utilizate pentru a gestiona stocurile de aprovizionare și pentru deplasările din depozite. Este puțin probabil ca aceste rețele să fie la fel de bine protejate ca și rețelele operaționale de conducere. Lovirea lor nu ar presupune tactici foarte performante precum cele aferente unui sistem de comandă și control al trupelor.

În acest context, războiul electronic își redefinește rolul de componentă de bază de sprijin a luptei armate contemporane, iar lecțiile

învățate din analiza conflictului dintre Rusia și Ucraina, pentru structurile de planificare și dezvoltare a forțelor armate din România trebuie să reprezinte o bază solidă a reformelor pentru toate categoriile de forțe.

BIBLIOGRAFIE

BBC, *How are kamikaze ‚drones' being uded by Russia and Ukraine?*, disponibil la https://www.bbc.com/news/world-.62225830;

BURRIDGE, T.S., *Inside Ukraine's critical drone warfare campaign against Russia*, disponibil la https://abcnews.go.com/-International/inside-ukraines-counteroffensive-drone-warfare-small-group-hackers/story?id=91104098;

CLARK, B., *The Fall and Rise of Russian Electronic Warfare*, IEEE Spectrum, disponibil la https://spectrum.ieee.org/the-fall-and-rise-of-russian-electronic-warfare;

COPCEA I., *Războiul electronic devine componentă esențială în doctrina pentru operații a Forțelor Navale ruse*, Desense Romania, disponibil la https://www.defenseromania.ro/razboiul-electronic-devine-componenta-esentiala-in-doctrina-pentru-operatii-a-fortelor-navale-ruse_606497.html;

COPCEA, I., *Rușii folosesc în Ucraina un model de elicopter extrem de rar-Mi-8MTPR-1 Rychag, specializat în războiul electronic*, Defense Romania, disponibil la https://www.defenseromania.ro/rusii-folosesc-in-ucraina-un-model-de-elicopter-extrem-de-rar-mi-8mtpr-1-rychag-specializat-in-razboiului-electronic_618745.html;

COȘLEA A., *„Trebuie să alegeți o tabără".SpaceX interzice Kievului să folosească tehnologia Starlink pentru controlul dronelor*, disponibil la https://www.hotnews.ro/stiri-razboi_ucraina-26073054-trebuie-alegeti-tabara-spacex-interzice-kievului-foloseasca-tehnologia-starlink-pentru-controlul-dronelor.htm;

CRANNY-EVANS, S., *Fields of silence and broke cycles: Russia's electronic warfare*, in Global Defence Technology, disponibil la https://defence.nridigital.com/global_defence_technology_mar22/russia_electronic_warfare;

GHERASIMOV, V. (translated by Dr.Harold Orenstein), *Thoughts on Future Military Conflict – March 2018*, disponibil la https://www.armyupress.army.mil/Portals/7/Army-Press-Online-Journal/documents/2019/Gerasimov-2019.pdf;

MUZYKA, K. (2021), *Russian Forces in the Western military District*, the CNA Occasional Paper, disponibil la https://www.-researchgate.net/publication/350313637_Russian_Forces_in_the_Western_Military_District;

PRAVDA, *Nurmansk-BN systems turn F-35 figters into scarp metal near Russian borders*, disponibil la https://english.pravda.ru/news/-world/149839-murmansk_f_35/;

Radio Svoboda, *Міністр оборони закликав українців знищувати російські системи радіоелектронної боротьби і розвідки*, disponibil la https://www.radiosvoboda.org/a/news-inistr-oborony-reznikov-ukraintsi/31745048.html;

SHARMAN, J., *Russia claims to have weapon that could cripple the US Navy, State new report surfaces three years after alleged o jammer against American destroyer*, disponibil la https://www.-independent.co.uk/news/world/europe/russia-weapon-us-navy-cripple-electronic-signals-deactivate-defence-systems-a7693816.html;

SHELHORST A.J.C. (2016), *Russia's Perception Warfare*, Militaire spectator, disponibil la https://militairespectator.nl/artikelen-/russias-perception-warfare;

SPRING-GLACE, M., *Return of Ground-base Electronic Warfare Platforms and Force Structure*, in Military Review (July-August 2019), disponibil la https://www.armyupress.army.mil/Journals-/Military-Review/English-Edition-Archives/July-August-2019/Spring-Glace-Electronic-Warfare/;

TASS, *Чем армия России может "ослепить" и "подавить" противника*, disponibil la https://tass.ru/armiya-i-opk/6328905;

THOMAS T. (2018), *Russia's Forms and Methods of Military Operations, The Implementers of Concep*t, disponibil la https://www.-armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2018/Russias-Forms-and-Methods-of-Military-Operations/;

THOMAS, T., *Russian Forecasts of Future War*, in Military Review (May-June 2019), disponibil la https://www.armyupress.army.-mil/Journals/Military-Review/English-Edition-Archives/May-June-2019/Thomas-Russian-Forecast/.