

INTELLIGENCE INFO

ISSN 2821 - 8159, ISSN – L 2821 – 8159, Volumul 3, Numărul 1, Martie 2024

Evoluția modernă a războiului electronic/electromagnetic

Nicolae Sfetcu

Sfetcu, Nicolae (2023), Evoluția modernă a războiului electronic/electromagnetic, *Intelligence Info*, 3:1, 39-47, DOI: 10.58679/II27427, <https://www.intelligenceinfo.org/evolutia-moderna-a-razboiului-electronic-electromagnetic/>

Publicat online: 02.01.2024

© 2024 Nicolae Sfetcu. Responsabilitatea conținutului, interpretărilor și opiniilor exprimate revine exclusiv autorilor.

Evoluția modernă a războiului electronic/electromagnetic

Ing. fiz. Nicolae SFETCU, MPhil¹
nicolae@sfetcu.com

The modern evolution of electronic/electromagnetic warfare

Abstract

Electronic warfare is a critical component of modern military operations and has undergone significant advances in recent years. Electronic warfare is a multifaceted field of warfare that involves manipulating the electromagnetic spectrum to gain a tactical advantage. The recent explosive development of emerging technologies has radically changed war strategies. As the modern battlespace has become more sophisticated, military operations are executed in an increasingly complex electromagnetic environment.

Keywords: electronic warfare, electromagnetic warfare, electromagnetic spectrum, information environment, electronic intelligence, ELINT

Rezumat

Războiul electronic este o componentă critică a operațiunilor militare moderne și a suferit progrese semnificative în ultimii ani. Războiul electronic este un domeniu cu mai multe fațete al războiului care implică manipularea spectrului electromagnetic pentru a obține un avantaj tactic. Dezvoltarea explozivă din ultimul timp a tehnologiilor emergente a schimbat radical strategiile de război. Pe măsură ce spațiul de luptă modern a devenit mai sofisticat, operațiunile militare sunt executate într-un mediu electromagnetic din ce în ce mai complex.

Cuvinte cheie: război electronic, război electromagnetic, spectrul electromagnetic, mediul informațional, inteligența electronică, ELINT

¹ Cercetător - Academia Română - Comitetul Român de Istoria și Filosofia Științei și Tehnicii (CRIFST), Divizia de Istoria Științei (DIS), ORCID: 0000-0002-0162-9973

INTELLIGENCE INFO, Volumul 3, Numărul 1, Martie 2024, pp. 39-47

ISSN 2821 - 8159, ISSN – L 2821 – 8159, DOI: 10.58679/II27427

URL: <https://www.intelligenceinfo.org/evolutia-moderna-a-razboiului-electronic-electromagnetic/>

© 2024 Nicolae Sfetcu. Responsabilitatea conținutului, interpretărilor și opiniilor exprimate revine exclusiv autorilor.



Articol în Acces Deschis (Open Access) distribuit în conformitate cu termenii licenței de atribuire Creative Commons CC BY SA 4.0 (<https://creativecommons.org/licenses/by-sa/4.0/>)

Introducere

Războiul electronic (EW) este o componentă critică a operațiunilor militare moderne și a suferit progrese semnificative în ultimii ani. Războiul electronic este un domeniu cu mai multe fațete al războiului care implică manipularea spectrului electromagnetic (EM) pentru a obține un avantaj tactic.

Războiul electronic (EW) ajută forțele aeriene, terestre, navale și spațiale la mai multe niveluri de conflict prin limitarea utilizării spectrului de frecvență radio (RF)². Sistemul de apărare al unei țări se bazează pe EMS pentru infrastructura sa de comandă și control (C&C), legăturile de comunicații, sistemele de arme și tehnologiile de asistență.

EW permite războiul cinetic, care este pur și simplu ineficient în războiul modern fără EW³.

Definiții

Războiul electronic (EW) include „orice acțiune militară care implică utilizarea energiei electromagnetice și direcționate pentru a controla spectrul electromagnetic sau pentru a ataca inamicul”⁴.

Războiul electronic (EW): În operațiunile militare, termenul EW se referă la ”orice acțiune militară care implică utilizarea EM sau a energiei dirijate pentru a controla spectrul EM sau pentru a ataca inamicul”. Războiul electronic include trei subdiviziuni majore: atac electronic (EA), protecție electronică (EP) și suport de război electronic (ES)⁵.

² (Lazarov 2019)

³ (Duke 2023)

⁴ (Army 2016)

⁵ (Army 2000, sec. I–I)

Războiul electronic (EW): se referă la utilizarea mijloacelor electronice în EMS pentru a perturba, nega, degrada sau înșela sistemele de informare sau comunicații ale unui adversar fără a provoca daune fizice⁶.

Informații: Fapte, date sau instrucțiuni în orice mediu sau formă. Informațiile se referă, de asemenea, la sensul pe care un om îl atribuie datelor prin intermediul convențiilor cunoscute utilizate în reprezentarea lor⁷.

Operațiunea de informare (IO): IO sunt descrise ca angajarea integrată a războiului electronic (EW), a operațiunilor de rețea de calculatoare (CNO), a operațiunilor psihologice (PSYOP), a decepției militare (MILDEC) și a securității operațiunilor (OPSEC), împreună cu suportul specificat și capacități aferente, pentru a influența, perturba, corupe sau uzurpa luarea deciziilor umane adverse și automatizate, protejându-ne în același timp pe noi⁸.

Războiul informațional (IW): Operațiuni de informare care se desfășoară în timpul unei crize sau conflict pentru a atinge sau promova obiective specifice asupra unui adversar.

Superioritatea informațională: O stare de echilibru în favoarea cuiva în domeniul informațional⁹ sau avantajul operațional derivat din capacitatea de a colecta, procesa și disemina un flux neîntrerupt de informații în timp ce exploatează sau neagă capacitatea unui adversar de a face la fel¹⁰.

Mediul informațional: Agregatul de persoane, organizații și sisteme care colectează, procesează, difuzează sau acționează asupra informațiilor¹¹.

Mediu electromagnetic: produsul rezultat al distribuției de putere și timp, în diferite intervale de frecvență, a nivelurilor de emisii electromagnetice radiate sau dirijate care pot fi întâlnite de o forță militară, un sistem sau o platformă atunci când își îndeplinește misiunea atribuită în mediul operațional prevăzut. Este suma interferențelor electromagnetice; impuls electromagnetic; pericolele radiațiilor electromagnetice pentru

⁶ (Army 1996)

⁷ (Army 2016)

⁸ (Army 2020b)

⁹ (Army 2020a, 8)

¹⁰ (Army 2016, 257)

¹¹ (Army 2016, 257)

personal, artileria și materialele volatile; și efectele fenomenelor naturale ale fulgerelor și statică a precipitațiilor¹². (Publicația comună 1-02, 175).

Energia electromagnetică operațională: o combinație a puterii, frecvenței și duratei emisiilor electromagnetice care pot fi întâlnite de o forță militară în timp ce își îndeplinește misiunea atribuită¹³.

Energie direcționată: un termen general care definește tehnologiile legate de producerea unui fascicul de energie electromagnetică concentrată, particule atomice sau particule subatomice. Este folosit pentru a deteriora sau distruge echipamentele, personalul și instalațiile unui adversar¹⁴.

Inteligența electronică (ELINT): este inteligența obținută din radiațiile EM străine noncomunicative. Inteligența electronică poate fi tehnică, geolocațională sau ambele¹⁵.

Securitatea electronică: este activitatea menită să interzică accesul persoanelor neautorizate la informații valoroase, având ca rezultat protecția sistemelor prietenoase împotriva activităților precum interceptarea sau radiațiile non-comunicații¹⁶.

Reprogramarea electronică: reprezintă modificări ale sistemelor EW și sensibile la țintă pentru a adopta schimbările în echipamente, tactici și mediul EM. Aceste schimbări se pot datora unor activități prietenoase sau ostile. Rezultatul dorit al reprogramării electronice este de a susține și de a crește eficiența sistemelor și dispozitivelor sensibile EW și vizate utilizate în armele defensive sau ofensive și în sistemele de colectare a informațiilor¹⁷.

Controlul emisiilor (EMCON): este utilizarea selectivă și controlată a emițătorilor EM, acustici și a altor emițători pentru a obține capabilități optime de C&C¹⁸.

Managementul spectrului: este planificarea, coordonarea și gestionarea spectrului EM. Obiectivul este de a crea un mediu EM în care sistemele electronice prietenoase să își poată îndeplini funcțiile fără interferențe sau confuzii¹⁹.

¹² (Army 2016, 175)

¹³ (Army 2000, sec. I-1)

¹⁴ (Army 2000, sec. I-4)

¹⁵ (Kucukozyigit 2006)

¹⁶ (Kucukozyigit 2006)

¹⁷ (Kucukozyigit 2006)

¹⁸ (Kucukozyigit 2006)

¹⁹ (Army 2000, sec. I-6-7)

Evoluția istorică

Războiul electronic își are rădăcinile în tehnologiile radio și radar timpurii. Ele pot fi regăsite încă din Războiul Civil din S.U.A. din 1861. Odată cu izbucnirea Războiului Civil în 1861, firele telegrafice au devenit una dintre cele mai importante ținte. Traficul telegrafic militar era schimbat către destinații greșite, s-au transmis ordine false comandanților Uniunii, și s-au tăiat firele pentru a stopa informațiile către forțele Uniunii²⁰. Acestea pot fi considerate aplicații timpurii ale comenzii, controlului, comunicațiilor și inteligenței (C3I), exemple timpurii de inteligență, bruiaj și înșelăciune²¹.

Cea mai veche utilizare documentată a EW a fost în timpul războiului boer (1899-1902), când armata britanică a folosit un reflector pentru semnalele codului Morse de pe nori. Boerii au observat acest lucru și au folosit unul dintre propriile lor reflectoare în încercarea de a bloca semnalele britanice²².

Primul caz cunoscut de bruiaj intenționat nu a fost, surprinzător, în scopuri militare, ci în scopuri civile, în timpul curselor de iahturi de la Cupa Americii din 1901, în Statele Unite. În acel an, Marconi a obținut un contract de la Associated Press. O altă companie, Wireless Telegraph Company of America, a obținut și ea un contract. O a treia companie, American Wireless Telephone and Telegraph Co., nu a reușit să obțină un sponsor, astfel încât a decis să bruieze pe ceilalți folosind un transmițător mai puternic²³.

Prima utilizare intenționată a bruiajului radio de către armată a avut loc în 1902, în timpul exercițiilor flotei marinei britanice în Marea Mediterană, apoi în 1903, în timpul manevrelor flotei marinei americane²⁴.

În timpul războiului ruso-japonez din 1904–1905, japonezii au localizat flota rusă în strâmtoarea Tsushima și au transmis informația „wireless” cartierului general al flotei japoneze. La 13 iulie 1904, stațiile rusești de telegrafie fără fir au întrerupt cu succes comunicarea între un grup de nave de luptă japoneze. Acesta a fost și primul exemplu de contramăsuri electronice. Ulterior, căpitanul navei de război rusești Ural a cerut permisiunea să perturbe comunicațiile japoneze cu un semnal radio mai puternic, dar

²⁰ (Price 1984, 1–2)

²¹ (Browne și Thurbon 1998, 3)

²² (Judd și Surridge 2013)

²³ (Price 1984, 3)

²⁴ (Price 1984, 4)

amiralul rus Zinovy Rozhstvensky a refuzat, permiând astfel japonezilor să câștige o bătălie decisivă la Tsushima²⁵.

În timpul Primul Război Mondial și al Doilea Război Mondial, EW a implicat în primul rând bruiaj radio și decepție radar. În 1939, chiar înainte de declanșarea celui de-al Doilea Război Mondial, o primă misiune ELINT a fost efectuată de dirijabilul german Graf Zeppelin de-a lungul coastei de est a Marii Britanii²⁶.

În al Doilea Război Mondial, Aliții au apelat la EW în „Bătălia Grinzilor” [10], folosind radarele de navigație pentru a dirija bombardierele, adversarii încercând să învingă acele radare de navigație²⁷. Pleava” a fost folosită de Royal Air Force (nume de cod Window) în timpul celui de-al Doilea Război Mondial pentru a învinge sistemele radar de urmărire²⁸. În primul exemplu de ECCM, germanii și-au mărit puterea emițătorului radio în încercarea de a „trece prin” sau de a depăși bruiajul britanic, aceasta fiind și azi una dintre metodele principale ale ECCM.

Epoca Războiului Rece a cunoscut progrese substanțiale în războiul electronic, deoarece superputerile s-au angajat într-o cursă tehnologică a înarmărilor pentru a depăși reciproc sistemele de supraveghere și comunicații ale altora. {4}Evoluțiile Războiului Rece au inclus rachete anti-radiații concepute pentru a se concentra pe transmițătoarele radar inamice²⁹.

În primul exemplu de ECCM, germanii și-au mărit puterea emițătorului radio în încercarea de a „trece prin” sau de a depăși bruiajul britanic, aceasta fiind și azi una dintre metodele principale ale ECCM.

Epoca Războiului Rece a cunoscut progrese substanțiale în războiul electronic, deoarece superputerile s-au angajat într-o cursă tehnologică a înarmărilor pentru a depăși reciproc sistemele de supraveghere și comunicații ale altora. Evoluțiile Războiului Rece au inclus rachete anti-radiații concepute pentru a se concentra pe transmițătoarele radar inamice³⁰.

²⁵ (Rambo 2009)

²⁶ (Kucukozyigit 2006)

²⁷ (Rambo 2009)

²⁸ (McArthur 1990)

²⁹ (Polmar 1979)

³⁰ (Polmar 1979)

În timpul războiului din Coreea (1950—1953) sub comanda generalului Mac Arthur, SUA au desfășurat 100 de avioane bombardiere grele B-29 Superfortress în teatrul de război. Nord-coreenii au instalat, radare de avertizare timpurie și artilerie antiaeriană (AAA) controlată de radar, astfel încât pierderile aeronavelor au devenit inacceptabile³¹.

Războiul electronic a jucat un rol major și în timpul războiului din Vietnam, unde avioanele se bazau adesea pe EW pentru a supraviețui bătăliei, deși ECCM vietnamez a funcționat cu succes³².

În Primul Război din Golf (Operațiunea DESERT STORM) din 1991, luptătorii stealth s-au aventurat în spațiul aerian inamic lansând momeli pentru a declanșa radarul inamic în acțiune; unele purtând rachete anti-radiații care s-au activat instantaneu pe măsură ce radarele au apărut³³.

În 2007, un atac israelian în timpul Operațiunii Outside the Box (sau Operațiunea Orchard) a folosit EW pentru a perturba apărarea aeriană a Siriei³⁴³⁵.

În primele zile ale invaziei rusești a Ucrainei din 2022, EW rusesc a perturbat radarele și comunicațiile adverse, perturbând sistemele de apărare aeriană de la sol dar și propriile lor comunicații³⁶. Capacitatea rusă de a perturba semnalele GPS este creditată cu reducerea succesului utilizării ucrainene a bombelor HIMARS și JDAM³⁷. Potrivit unui raport al Royal United Services Institute din 19 mai 2023, Ucraina pierduse aproximativ 10.000 de drone pe lună din cauza războiului electronic rusesc³⁸.

În războiul modern, războiul electronic a devenit o componentă critică. Odată cu integrarea unor senzori sofisticăți, sisteme de comunicații și rețele de informații, spectrul electromagnetic este aglomerat și contestat. EW joacă un rol vital în câștigarea avantajului în ceea ce privește conștientizarea situației și avantajul tactic.

EW în războiul asimetric: EW nu este exclusiv războiului convențional. A câștigat importanță în conflictele asimetrice, operațiunile de contrainsurgență și eforturile de

³¹ (Browne și Thurbon 1998, 26)

³² (Dickson 1987)

³³ (Campen 1992, XIV)

³⁴ (Fulghum și Wall 2007)

³⁵ (Katz 2010)

³⁶ (Bronk, Reynolds, și Watling 2022)

³⁷ (Mizokami 2023)

³⁸ (Jankowicz 2023)

EVOLUȚIA MODERNĂ A RĂZBOIULUI ELECTRONIC/ELECTROMAGNETIC

combateră a terorismului. Grupurile insurgente și actorii nestatali au adoptat, de asemenea, tehnici rudimentare de război electronic.

Convergența cibernetică-electronică: convergența războiului cibernetic și a războiului electronic a cunoscut o dezvoltare semnificativă. Adversarii folosesc din ce în ce mai mult atacurile cibernetice pentru a perturba sistemele electronice, estompând liniile dintre cele două domenii.

Dominanța spațiului și a spectrului electromagnetic: Pe măsură ce spațiul devine un domeniu critic pentru operațiunile militare, controlul spectrului electromagnetic în spațiu este primordial. Sateliții și activele spațiale sunt vulnerabile la atacurile EW.

Concluzie

Dezvoltarea explozivă din ultimul timp a tehnologiilor emergente a schimbat radical strategiile de război. Pe măsură ce spațiul de luptă modern a devenit mai sofisticat, operațiunile militare sunt executate într-un mediu electromagnetic din ce în ce mai complex. Operațiunile militare depind acum în mare măsură de controlul spectrului electromagnetic care poate perturba fluxul de date, prin țintirea, exploatarea, perturbarea, degradarea, înșelarea, deteriorarea sau distrugerea sistemelor electronice ale adversarilor. Porțiunea de spectru electromagnetic a mediului informațional este denumită mediu electromagnetic (EME).

În acest context, obținerea și menținerea unui avantaj în războiul modern necesită o serie de soluții EW, soluții noi care pot viza și exploata vulnerabilitățile sistemului, și care pot modifica în mod semnificativ operațiunile de decepție militară (MILDEC), îmbunătățind operațiunile comune și războiul C&C.

Bibliografie

- Army, United States Government US. 1996. „Joint Pub 3-58 Joint Doctrine for Military Deception”.
https://webharvest.gov/peth04/20041021042923/http://www.dtic.mil/doctrine/jel/new_pubs/jp3_58.pdf.
- . 2000. „Joint Publication 3-51 Joint Doctrine for Electronic Warfare”.
https://irp.fas.org/doddir/dod/jp3_51.pdf.

———. 2016. „Joint Publication JP 1-02 Department of Defense Dictionary of Military and Associated Terms”. https://irp.fas.org/doddir/dod/jp1_02.pdf.

———. 2020a. „Joint Vision 2020: America’s Military - Preparing for Tomorrow”. <https://apps.dtic.mil/sti/citations/ADA526044>.

———. 2020b. *Joint Publication JP 3-13 Information Operations Change 1 November 2014*. Independently Published.

Bronk, Justin, Nick Reynolds, și Jack Watling. 2022. „The Russian Air War and Ukrainian Requirements for Air Defence”. <https://static.rusi.org/SR-Russian-Air-War-Ukraine-web-final.pdf>.

Browne, J. P. R., și Michael T. Thurbon. 1998. *Electronic Warfare*. Brassey’s.

Campen, Alan D. 1992. *The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War*. AFCEA International Press.

Dickson, John R. V. 1987. „Electronic Warfare in Vietnam: Did We Learn Our Lessons?”. În . <https://www.semanticscholar.org/paper/Electronic-Warfare-in-Vietnam%3A-Did-We-Learn-Our-Dickson/399e7323fb081cb95db35d3a9d3075154a0de068>.

Duke, Audrey. 2023. „Harnessing Chaos: Unleashing Electromagnetic Warfare for Enhanced Joint Operations”. <https://apps.dtic.mil/sti/citations/AD1206172>.

Fulghum, David A., și Robert Wall. 2007. „Israel Shows Electronic Prowess | Aviation Week Network”. 2007. <https://aviationweek.com/israel-shows-electronic-prowess>.

Jankowicz, Mia. 2023. „Ukraine Is Losing 10,000 Drones a Month to Russian Electronic-Warfare Systems That Send Fake Signals and Screw with Their Navigation, Researchers Say”. Business Insider. 2023. <https://www.businessinsider.com/ukraine-losing-10000-drones-month-russia-electronic-warfare-rusi-report-2023-5>.

Judd, Denis, și Keith Surridge. 2013. *The Boer War: A History*. Bloomsbury Academic.

Katz, Yaakov. 2010. „And They Struck Them with Blindness”. The Jerusalem Post | JPost.Com. 29 septembrie 2010. <https://www.jpost.com/magazine/features/and-they-struck-them-with-blindness>.

EVOLUȚIA MODERNĂ A RĂZBOIULUI ELECTRONIC/ELECTROMAGNETIC

Kucukozyigit, Ali. 2006. „Electronic Warfare (EW) Historical Perspectives and Its Relationship to Information Operations (IO) - Considerations for Turkey”.

Lazarov, Lazar. 2019. „Perspectives and Trends for the Development of Electronic Warfare Systems”. *2019 International Conference on Creative Business for Smart and Sustainable Growth (CREBUS)*, martie, 1–3.
<https://doi.org/10.1109/CREBUS.2019.8840074>.

McArthur, Charles W. 1990. *Operations Analysis in the United States Army Eighth Air Force in World War II*. American Mathematical Soc.

Mizokami, Kyle. 2023. „Why Ukraine’s GPS-Guided Bombs Keep Missing Their Targets”. *Popular Mechanics*. 20 aprilie 2023.
<https://www.popularmechanics.com/military/weapons/a43591694/russian-jamming-gps-guided-bombs/>.

Polmar, Norman. 1979. „The U. S. Navy: Electronic Warfare (Part 2)”. U.S. Naval Institute. 1 noiembrie 1979.
<https://www.usni.org/magazines/proceedings/1979/november/u-s-navy-electronic-warfare-part-2>.

Price, Alfred. 1984. *The History of US Electronic Warfare*. Association of Old Crows.

Rambo. 2009. „Information Warfare: History of Electronic Warfare”. *INFORMATION WARFARE* (blog). 7 decembrie 2009.
<https://ew30.blogspot.com/2009/12/such-is-reliance-on-electromagnetic-em.html>.