

# INTELLIGENCE INFO

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

---

## Tehnici și tactici utilizate în războiul electronic

Nicolae Sfetcu

Sfetcu, Nicolae (2023), Tehnici și tactici utilizate în războiul electronic, *Intelligence Info*, 3:1, 22-29, DOI: 10.58679/II49637, <https://www.intelligenceinfo.org/tehnici-si-tactici-utilizate-in-razboiul-electronic/>

Publicat online: 10.01.2024

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

## Tehnici și tactici utilizate în războiul electronic

Ing. fiz. Nicolae SFETCU, MPhil<sup>1</sup>  
nicolae@sfetcu.com

### Techniques and tactics used in electronic warfare

#### Abstract

The main activities used in EW include the following: countermeasures, EM battle management (EMBM), EM compatibility; EM fraud; EM hardening, EM interference resolution, EM intrusion, EM jamming, EMP, EM spectrum control, electronic intelligence gathering, electronic cloaking, electronic probing, electronic reconnaissance, electronic security, EW reprogramming, emission control, JEMSO, JEMSMO, low observability/stealth, signal interception and retransmission, wartime navigation (NAVWAR), precision geolocation, and wartime backup modes.

**Keywords:** electronic warfare, electromagnetic warfare, techniques, tactics, countermeasures, electromagnetic measures

#### Rezumat

Principalele activități utilizate în EW includ următoarele: contramăsuri, managementul de lupte EM (EMBM), compatibilitatea EM; înșelăciune EM; întărirea EM, rezoluție interferență EM, intruziune EM, bruij EM, EMP, control spectru EM, colectare de inteligență electronică, mascare electronică, sondare electronică, recunoaștere electronică, securitate electronică, reprogramare EW, control emisii, JEMSO, JEMSMO, observabilitate/ascundere scăzută, interceptarea și retransmiterea semnalelor, navigație război (NAVWAR), geolocalizare de precizie și moduri de rezervă în timp de război.

**Cuvinte cheie:** război electronic, război electromagnetic, tehnici, tactici, contramăsuri, măsuri electromagnetice

---

<sup>1</sup> 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. 22-29

ISSN 2821 - 8159, ISSN – L 2821 – 8159, DOI: 10.58679/II49637

URL: <https://www.intelligenceinfo.org/tehnici-si-tactici-utilizate-in-razboiul-electronic/>

© 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

Principalele activități utilizate în EW includ următoarele<sup>2</sup>: contramăsuri, managementul de lupte EM (EMBM), compatibilitatea EM; înșelăciune EM; întărirea EM, rezoluție interferență EM, intruziune EM, bruijă EM, EMP, control spectru EM, colectare de inteligență electronică, mascare electronică, sondare electronică, recunoaștere electronică, securitate electronică, reprogramare EW, control emisii, JEMSO, JEMSMO, observabilitate/ascundere scăzută, interceptarea și retransmiterea semnalelor, navigație război (NAVWAR), geolocalizare de precizie și moduri de rezervă în timp de război.

## Sisteme EW

O configurație tipică pentru un sistem EW depinde de aplicația particulară, dar în general include următoarele elemente<sup>3</sup>:

**Controlul sistemului:** poate fi realizat cu un singur computer (control centralizat) sau mai multe computere.

**Antene:** folosite pentru a extrage energia electromagnetică (EM) din mediul de propagare, sau pentru conversia energiei electrice în energie electromagnetică care poate fi propagată prin atmosferă.

Antenele convertesc semnalele electrice în unde EM care se propagă și invers, convertesc undele EM care se propagă în semnale electrice. De obicei, antenele pentru EW trebuie să fie în bandă largă, și prezintă aceleași caracteristici, indiferent dacă sunt utilizate pentru transmitere sau recepție. Cele mai importante caracteristici ale antenelor sunt răspunsul în frecvență (determină lățimea de bandă), direcționalitatea (determină modul

---

<sup>2</sup> (Army 2020)

<sup>3</sup> (Poisel 2008)

în care o antenă concentrează energia în anumite direcții) și caracteristicile de impedanță (să se potrivească cu cea a antenei). Cele mai populare tipuri de antene utilizate pentru EW în gamele de frecvență inferioare sunt dipolul, monopolul și log periodic. Pe măsură ce frecvențele de interes cresc, sunt folosite alte tipuri de antene.

**Distribuția semnalului:** se realizează în mod normal la ieșirea antenelor și înaintea receptorilor.

**Receptor de căutare:** caută în spectrul de frecvență semnale de interes.

*Receptorul conectat:* pentru analiza pe termen relativ lung a semnalelor detectate prin alte mijloace.

Receptoarele pentru interceptarea semnalelor de comunicație depind de tipul de semnal care urmează să fie interceptat. Pentru semnalele în bandă îngustă, cel mai popular tip de receptor a fost superhetrodina. Acolo unde frecvența instantanee de funcționare a emițătorului este necunoscută, sunt necesare receptoare de bandă largă. Funcția fundamentală a unui receptor este de a converti un semnal de la antenă într-unul care se poate utiliza, de obicei demodulat, prin conversie și demodulare.

**Procesarea semnalului:** detectarea prezenței energiei la o anumită frecvență și într-o lățime de bandă specificată, determinarea modulației unui semnal și măsurarea vitezei de transmisie a unui semnal de comunicație digitală.

*Procesarea semnalului de căutare a direcției:* localizarea sursei de emisie a semnalelor de comunicație, de obicei prin triangulare.

Procesarea semnalelor în EW implică procesarea semnalelor pentru a extrage informații din ele.

**Geolocalizarea (fixarea poziției):** determinarea locației unei ținte emitente, pe baza unor parametri temporali asociați cu semnalul de intrare.

Ca metode se folosesc ora de sosire și/sau diferența de frecvență de sosire sau efectul Doppler diferențial, cu doi sau mai mulți senzori prin triangulație.

**Excitator:** un amplificator de mare putere, filtre și o antenă, în esență un generator de semnal RF cu capacitatea de a modula semnalele generate.

**Amplificator de putere:** amplifică semnalul de la excitator.

Excitatoarele și amplificatoarele de putere sunt incluse într-un sistem EW atunci când se apelează la EA. Semnalele generate astfel interferează cu comunicațiile

adversarului. De cele mai multe ori este necesar să se injecteze mai multă energie decât cea a emițătorului vizat. Excitatorul generează semnalul care este apoi mărit în putere de amplificatorul de putere.

**Filtre:** limitează energia în afara canalului (nedorită) pe care o emite sistemul.

**Comunicații:** subsistemul de comunicații poate fi compus din mai multe tipuri de capabilități, pentru comanda și controlul sistemului.

### **Radar**

„RADAR” este un acronim pentru RAdio Detection And Ranging, bazat pe reflexia undelor electromagnetice. În 1903, reflexia undelor radio a fost folosită în Germania pentru a demonstra detecția navelor pe mare. Dezvoltarea practică a radarului cu puls a început în anii 1930, în principal în Statele Unite, Marea Britanie și Germania. Radarul poate „vedea” mai departe decât ochiul uman și poate evalua cu mai multă precizie distanța sau distanța unui obiect. Sistemele radar trebuie să utilizeze discriminatori țintă pentru a izola returul dorit de țintă: intervalul, viteza și unghiul. Prezența unui ecou indică detectarea țintei<sup>4</sup>.

Sistemele radar sunt concepute pentru a furniza avertizare de atac, informații despre implicarea țintei, și pentru a furniza informații suficient de precise privind raza de acțiune, azimutul și altitudinea țintei.

Un radar transmite și primește radiații electromagnetice, denumite radiații de radiofrecvență (RF). Frecvența RF transmisă afectează capacitatea unui sistem radar de a analiza ținta, capacitatea antenei de transmisie de a focaliza energia RF într-un fascicul îngust, și propagarea semnalului prin atmosferă.

Fiecare radar produce un semnal de radiofrecvență (RF) cu caracteristici specifice care îl diferențiază de toate celelalte semnale și îi definesc capacitățile și limitările. Lățimea pulsului (durata pulsului), timpul de recurență a pulsului (interval de repetare a pulsului), frecvența de repetare a pulsului și puterea sunt caracteristicile semnalului radar determinate de transmițătorul radar, oferind o semnătură unică pentru a identifica un anumit semnal radar. Timpul de ascultare, timpul de odihnă și timpul de recuperare sunt caracteristicile receptorului radar. Componentele individuale ale unui radar determină capacitățile și

---

<sup>4</sup> (\* \* \* 2000)

limitările unui anumit sistem radar. Caracteristicile acestor componente determină și contramăsurile care vor fi eficiente împotriva unui anumit sistem radar.

Scopul principal al sistemelor radar este de a determina intervalul, azimutul, elevația sau viteza unei ținte. Capacitatea unui sistem radar de a determina și rezolva acești parametri depinde de caracteristicile semnalului radar transmis.

Funcția antenei în timpul transmisiei este de a concentra energia radar de la transmițător într-un fascicul modelat spre direcția dorită. În timpul recepției sau a timpului de ascultare, funcția antenei este de a colecta energia radar care revine prin ecou, transmițând aceste semnale la receptor. Metoda folosită de antenele radar pentru eșantionarea mediului este o caracteristică critică de proiectare a sistemului radar. Orizontul radar, mascarea directă a terenului și mascarea indirectă a terenului sunt limitări pentru toate scanările radar.

Un radar de urmărire a țintei (TTR) furnizează informațiile necesare pentru a ghida o rachetă sau pentru a ținti cu o armă pentru a distruge o țintă. Un TTR obișnuit are bucle de urmărire individuale pentru a urmări o țintă în rază, azimut, altitudine sau viteză. Antena TTR este îndreptată către o singură țintă. Odată ce o țintă a fost identificată, etapa finală a angajării este de a ghida o rachetă sau proiectil pentru a distruge ținta.

Bruiajul radar este radiația sau re-radierea intenționată a semnalelor de radiofrecvență pentru a interfera cu funcționarea unui radar prin saturarea receptorului acestuia cu ținte false sau informații false despre ținte. Cele mai utilizate tipuri de bruij radar sunt zgomotul și decepția. Raportul semnal-zgomot al radarului de victimă determină vulnerabilitatea receptorului radar la bruij, în timp ce raportul bruij-semnal este un indiciu al capacității sistemului de bruij de a bloca eficient radarul victimei.

### Tehnici și tactici

EW include o serie de tehnici și tactici, inclusiv<sup>5</sup>: bruij, falsificare, energie direcționată (DE), război electronic cibernetic (CEW) și înșelăciune electronică.

- **Bruiaj:** radiația deliberată EM pentru a preveni sau reduce utilizarea eficientă a EMS de către un inamic<sup>6</sup>.

---

<sup>5</sup> (Duke 2023)

<sup>6</sup> (Army 2020)

- **Falsificarea:** transmiterea de informații false către senzorii sau sistemele de comunicare ale adversarului, provocând confuzie și potențial să-i determine să ia decizii incorecte<sup>7</sup>.
- **Energie direcționată:** este „un termen umbrelă care acoperă tehnologiile care se referă la producerea unui fascicul de energie electromagnetică concentrată sau a particulelor atomice sau subatomice”<sup>8</sup>. O armă cu energie direcționată folosește „energia dirijată în primul rând ca mijloc direct de a deteriora sau distruge echipamentul, instalațiile și personalul inamicului”<sup>9</sup>. Energia direcționată folosește tehnologiile care produc energie EM concentrată și particule atomice sau subatomice, ca mijloc de a incapacita, deteriora, dezactiva sau distruge echipamentele, instalațiile și/sau personalul inamic.
- **Război electronic cibernetic:** îmbină capacitățile spațiului cibernetic cu metodele tradiționale EW, prin infiltrarea în computerul sau în sistemele de comunicații ale unui adversar pentru a fura sau manipula informații și pentru a-i perturba operațiunile<sup>10</sup>.
- **Decepția electronică:** folosirea mijloacelor electronice pentru a induce în eroare un adversar să creadă ceva neadevărat, prin tehnici precum crearea de ținte false pe ecranele radar, utilizarea contramăsurilor electro-optice, infraroșu sau frecvență radio și transmiterea de semnale false pentru a deruta senzorii adversarului<sup>11</sup>.
- **Armele antiradiație:** folosesc energia radiată emisă de țintă ca mecanism de ghidare către un emițător vizat (de exemplu, sistemul de rachete antiradiații de mare viteză [HARM - high-speed antiradiation missile]).

Managementul spectrului include „planificarea, coordonarea și gestionarea utilizării în comun a spectrului electromagnetic prin proceduri operaționale, de inginerie și administrative. Obiectivul managementului spectrului este de a permite sistemelor electronice să își îndeplinească funcțiile în mediul vizat, fără a provoca sau a suferi interferențe inacceptabile”<sup>12</sup>.

EW este folosit pentru a crea efecte decisive, autonome sau pentru a sprijini operațiunile militare prin generarea diferitelor niveluri de control, detecție, negare, înșelăciune, perturbare, degradare, exploatare, protecție și distrugere.

- În *războiul neregulat*, EW poate influența adversarul, populația prietenoasă și populația neutră, cu mesajul operațiunilor de informare (IO).

---

<sup>7</sup> (Army 2020, I–10)

<sup>8</sup> (Army 2016)

<sup>9</sup> (Army 2016)

<sup>10</sup> (Yasar, Yasar, și Topcu 2012)

<sup>11</sup> (Adamy 2001)

<sup>12</sup> (Army 2016)

- În *operațiunile informaționale*, EW contribuie prin folosirea tacticilor și tehnicilor ofensive și defensive pentru a modela, perturba și exploata utilizarea adversă a EMS, protejând în același timp libertatea de acțiune amicală.
- În *operațiunile spațiale*, manevrele fizice și colectarea EM necontestată implică o formă de EW.
- În operațiunile în *spațiul cibernetic* este necesară utilizarea EMS pentru activarea efectelor, prin coordonarea cu EW.
- În războiul *prin navigație*, EW produce efecte NAVWAR prin influențarea transmisiei sistemului global de navigație prin satelit sau a altor semnale radio.

Alte tehnici și tactici folosite în EW<sup>13</sup>:

- *Managementul bătăliilor electromagnetice (EMBM)*: monitorizarea dinamică, evaluarea, planificarea și conducerea operațiunilor.
- *Compatibilitate electromagnetica (EMC)*: capacitatea sistemelor, echipamentelor și dispozitivelor de a funcționa fără a suferi o degradare inacceptabilă sau a provoca o degradare neintenționată.
- *Decepția electromagnetică*: radiația deliberată, reradierea, alterarea, suprimarea, absorbția, negarea, îmbunătățirea sau reflectarea energiei EM într-o manieră menită să transmită informații deceptivă unui inamic.
- *Întărirea electromagnetică*: pentru a proteja împotriva efectelor nedorite ale energiei EM.
- *Rezoluția interferențelor electromagnetice*: procesul de diagnosticare sistematică a cauzei sau sursei interferențelor EM.
- *Intruziune electromagnetică*: inserarea intenționată a energiei EM în căile de transmisie pentru a înșela operatorii sau a provoca confuzie.
- *Blocaj electromagnetic*: modificarea energiei EM pentru a preveni sau reduce utilizarea eficientă a EMS de către un inamic.
- *Puls electromagnetic (EMP)*: un impuls electronic puternic produs de o explozie nucleară sau generat în mod convențional, care produce supratensiuni.
- *Controlul spectrului electromagnetic*: prin execuția coordonată a JEMSO cu alte operațiuni letale și neletale care afectează EMOE.
- *Inteligența electronică (ELINT)*: o subcomponentă a SIGINT
- *Mascarea electronică*: radiația controlată a energiei EM pe frecvențele prietenoase care să protejeze emisiile sistemelor electronice de comunicații prietenoase
- *Sondarea electronică*: radiația intenționată concepută pentru a fi introdusă în dispozitivele sau sistemele potențialilor inamici.
- *Recunoașterea electronică*: detectarea, localizarea, identificarea și evaluarea radiațiilor EM străine.
- *Securitatea electronică*: protecția împotriva persoanelor neautorizate în interceptarea și studiul radiațiilor EM.
- *Reprogramarea războiului electronic*: modificarea EW sau a sistemelor de detectare a țintei (TSS) ca răspuns la modificările validate ale echipamentelor, tacticilor sau EME.

---

<sup>13</sup> (Army 2020)



## EVOLUȚIA MODERNĂ A RĂZBOIULUI ELECTRONIC/ELECTROMAGNETIC

- *Controlul emisiilor*: utilizarea selectivă și controlată a emițătorilor pentru a optimiza capacitățile C&C minimizând în același timp detecția de către senzorii inamici, interferența reciprocă între sistemele prietenoase și interferența inamicului.
- *Operații comune cu spectrul electromagnetic (JEMSO)*: eforturile coordonate de a exploata, ataca, proteja și gestiona EMOE pentru a atinge obiectivele.
- *Operațiuni comune de gestionare a spectrului electromagnetic (JEMSMO)*: planificarea, coordonarea și gestionarea utilizării comune a EMS prin proceduri operaționale, de inginerie și administrative.
- *Observabilitate scăzută/Infiltrare*: EP cu observabilitate scăzută/stealth, pentru a opera prin reducerea posibilității de detectare de către adversari.
- *Meaconing*: recepționarea semnalelor de radiofar și redifuzarea lor pe aceeași frecvență pentru a încurca navigarea
- *Războiul naval (NAVWAR)*: acțiuni deliberate pentru asigurarea și prevenirea informațiilor specifice navale.
- *Geolocalizare de precizie*: planificarea, coordonarea și gestionarea activelor prietenoase pentru geolocalizarea sistemelor RF inamice.
- *Moduri de rezervă în timp de război (WARM)*: caracteristici și proceduri de operare care vor contribui la eficacitatea militară dacă nu sunt cunoscute sau înțelese greșit de comandanții oponenti înainte de a fi utilizate, dar ar putea fi exploatate sau neutralizate dacă sunt cunoscute dinainte.

### Concluzie

Războiul electronic a devenit o componentă integrală a operațiunilor militare moderne. Pe măsură ce tehnologia continuă să avanseze, războiul electronic va juca un rol din ce în ce mai important în modelarea rezultatelor conflictelor militare. Dezvoltarea constantă a noilor tehnici și tactici evidențiază natura dinamică a războiului electronic, necesitând adaptare și inovare continuă. Forțele militare trebuie să rămână la curent cu aceste progrese pentru a utiliza eficient capacitățile de război electronic și pentru a menține un avantaj competitiv în peisajul în continuă evoluție al războiului modern.

### Bibliografie

- \* \* \*. 2000. „Electronic Warfare Fundamentals”. <https://falcon.blu3wolf.com/Docs/Electronic-Warfare-Fundamentals.pdf>.
- Adamy, David. 2001. *EW 101: A First Course in Electronic Warfare*. Artech House.
- Army, United States Government US. 2016. „Joint Publication JP 1-02 Department of Defense Dictionary of Military and Associated Terms”. [https://irp.fas.org/doddir/dod/jp1\\_02.pdf](https://irp.fas.org/doddir/dod/jp1_02.pdf).
- . 2020. *Joint Publication JP 3-13 Information Operations Change 1 November 2014*. Independently Published.
- Duke, Audrey. 2023. „Harnessing Chaos: Unleashing Electromagnetic Warfare for Enhanced Joint Operations”. <https://apps.dtic.mil/sti/citations/AD1206172>.

- Poisel, Richard. 2008. *Introduction to Communication Electronic Warfare Systems*. Artech House.
- Yasar, Nurgul, Fatih Mustafa Yasar, și Yucel Topcu. 2012. „Operational advantages of using Cyber Electronic Warfare (CEW) in the battlefield”. În *Cyber Sensing 2012*, 8408:151–59. SPIE. <https://doi.org/10.1117/12.919454>.