

RĂZBOIUL ELECTRONIC și INTELIGENȚA ARTIFICIALĂ

Nicolae Sfetcu

MultiMedia Publishing

Războiul electronic și inteligența artificială

PREVIZUALIZARE CARTE

RELAȚIA RĂZBOIULUI ELECTRONIC CU ALTE CAPACITĂȚI DE LUPTĂ

Nicolae SFETCU
nicolae@sfetcu.com¹

Sfetcu, Nicolae (2024), *Războiul electronic și inteligența artificială*, MultiMedia Publishing, ISBN 978-606-033-824-6, DOI: [10.58679/MM88277](https://doi.org/10.58679/MM88277), <https://www.telework.ro/ro/e-books/razboiul-electronic-si-inteligenta-artificiala/>

© 2024 Nicolae Sfetcu.

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

Cuprins

Războiul electronic și inteligența artificială	1
Războiul electronic și inteligența artificială	3
Electronic Warfare and Artificial Intelligence.....	3
Abstract	3
Rezumat	3
Relația războiului electronic cu alte capacități de luptă.....	4
Războiul electronic cibernetic.....	8
Cuprins.....	10
Cartea	11
De ce este această carte esențială.....	12
Caracteristici principale ale cărții	12
Cui se adresează această carte?	12
Teme abordate.....	13
Puncte unice de vânzare.....	13
Ce vor învăța cititorii	13
Aprecieri pentru carte	14
Bibliografie	14

Războiul electronic și inteligența artificială

Ing. fiz. Nicolae SFETCU, MPhil

Electronic Warfare and Artificial Intelligence

Abstract

Electronic warfare is a critical component of modern military operations and has undergone significant advances in recent years. This article provides an overview of electronic warfare, its historical development, key components, and its role in contemporary conflict scenarios. It also discusses emerging trends and challenges in electronic warfare and its contemporary relevance in an era of advanced technology and cyber threats, emphasizing the need for continued research and development in this area.

The book explores the burgeoning intersection of artificial intelligence and electronic warfare, highlighting the evolving landscape of modern conflicts and the implications of integrating advanced technologies. The multifaceted roles of artificial intelligence in electronic warfare are highlighted, examining its potential advantages, ethical considerations, and challenges associated with its integration.

Keywords: electronic warfare, artificial intelligence, machine learning, cognitive warfare, asymmetric warfare, electromagnetic spectrum

Rezumat

Războiul electronic este o componentă critică a operațiunilor militare moderne și a suferit progrese semnificative în ultimii ani. Acest articol oferă o privire de ansamblu asupra războiului electronic, a dezvoltării sale istorice, a componentelor cheie și a rolului său în scenariile de conflict contemporane. De asemenea, se discută tendințele și provocările emergente în războiul electronic și și relevanța sa contemporană într-o eră a tehnologiei avansate și a amenințărilor cibernetice, subliniind necesitatea cercetării și dezvoltării continue în acest domeniu.

Cartea explorează intersecția în plină dezvoltare dintre inteligența artificială și războiul electronic, evidențiind peisajul evolutiv al conflictelor moderne și implicațiile integrării tehnologiilor avansate. Se evidențiază rolurile cu mai multe fațete ale inteligenței artificiale în

războiul electronic, examinând avantajele sale potențiale, considerentele etice și provocările asociate cu integrarea acestora.

Cuvinte cheie: războiul electronic, inteligența artificială, învățarea automată, războiul cognitiv, războiul asimetric, spectrul electromagnetic

Relația războiului electronic cu alte capacități de luptă

Războiul informațional și cibernetic²: În epoca modernă, războiul se extinde și în spațiul cibernetic, unde serviciile de informații joacă un rol vital în apărarea împotriva amenințărilor cibernetice. Ele monitorizează activ activitățile digitale, identifică potențiale atacuri cibernetice și evaluează capacitățile actorilor cibernetici ostili. În plus, serviciile de informații se angajează în război informațional, contracarând propaganda inamicului și influențând percepția publicului pentru a câștiga puterea în conflict. Una dintre provocările semnificative din războiul ruso-ucrainean a fost utilizarea pe scară largă a campaniilor de dezinformare atât de către Rusia, cât și de către Ucraina. Informațiile false și propaganda au fost folosite pentru a influența opinia publică, a manipula percepțiile și a crea confuzie în rândurile inamicului. Serviciile de informații sunt nevoite să se adapteze și să investească în combaterea dezinformării, asigurând în același timp credibilitatea și acuratețea propriilor rapoarte.

Războiul cibernetic³ este o componentă a confruntării dintre Rusia și Ucraina de la prăbușirea Uniunii Sovietice în 1991. În timp ce primele atacuri asupra sistemelor informaționale ale întreprinderilor private și ale instituțiilor de stat din Ucraina au fost înregistrate în timpul protestelor în masă din 2013, arma cibernetică rusă Uroburos exista din 2005. Războiul cibernetic rusesc a continuat cu penetrarea rețelei electrice din Ucraina din 2015 la Crăciun, și din nou în 2016 prin paralizarea Trezoreriei de stat a Ucrainei în decembrie 2016, un atac în masă al hackerilor din iunie 2017 și atacuri asupra site-urilor web guvernamentale ale Ucrainei în ianuarie 2022.

Războiul psihologic⁴: Activitatea de informații poate juca, de asemenea, un rol în războiul psihologic, unde diseminarea informațiilor elaborate cu atenție poate influența moralul și luarea deciziilor inamicului. Prin diseminarea strategică a anumitor informații sau dezinformare,

² Sfetcu, „Rolul serviciilor de informații în război”.

³ Sfetcu.

⁴ Sfetcu.

serviciile de informații pot crea confuzie, neîncredere și incertitudine în rândul forțelor opuse, subminându-le potențial hotărârea și coeziunea.

În ultimul secol, și în special în a doua jumătate, EW s-a alăturat altor capacități de luptă și a devenit una dintre competențele majore ale războiului. Cele cinci competențe de bază împreună, PSYOP, CNO, EW, MILDEC și OPSEC, sunt esențiale pentru modelarea mediului informațional⁵.

Operațiuni de rețea de calculatoare (CNO) și EW: Cu cât EW și CNO sunt mai integrate, cu atât colectarea, manipularea și diseminarea informațiilor sunt mai ușoare, deoarece există o creștere a dependenței de spectrul EM în utilizarea rețelelor de calculatoare, în special a rețelelor wireless.

SUA definește un atac de rețea de computere (CNA) ca incluzând „operațiuni de perturbare, negare, degradare sau distrugere a informațiilor rezidente în computer și rețele de calculatoare, sau computerele și rețelele înseși”⁶. Există beneficii potențiale într-o realiniere a terminologiei, doctrinei și chiar sistemelor CNW, cu lecțiile învățate din războiul electronic⁷.

Decepția militară (MILDEC) și EW: Decepția militară este constituită din acele „acțiuni care sunt executate în mod deliberat pentru a induce în eroare adversarul. factorii de decizie militari cu privire la capacitățile, intențiile și operațiunile militare prietenești, determinând astfel adversarul să întreprindă acțiuni specifice care vor contribui la îndeplinirea misiunii prietenoase”⁸. Această relație este în creștere datorită faptului că armatele folosesc mai des spectrul EM în scopuri de decepție.

Securitatea operațiunilor (OPSEC) și EW: Securitatea operațiunilor este procesul de identificare a informațiilor esențiale și de refuzare a acestora factorilor de decizie adversi pentru a-i determina să calculeze greșit forțele, cursurile de acțiune și intențiile prietene⁹. Misiunile militare care pot evita detectarea de către radarul inamicului se dovedesc de obicei a fi mai eficiente. ES oferă OPSEC informații despre capacitățile adversarului și intențiile de a colecta informații despre elementele esențiale ale informațiilor prietenoase prin intermediul spectrului

⁵ Army, *Joint Publication JP 3-13 Information Operations Change 1 November 2014*, II-1.

⁶ Army, *Joint Publication JP 3-13 Information Operations Change 1 November 2014*.

⁷ Smith și Knight, „Applying Electronic Warfare Solutions to Network Security - Canadian Military Journal”.

⁸ Army, „Joint Pub 3-58 Joint Doctrine for Military Deception”, I-1.

⁹ Army, *Joint Publication JP 3-13 Information Operations Change 1 November 2014*, II-3.

EM. Într-o campanie de decepție militară, decepția electromagnetică și OPSEC trebuie să fie integrate, sincronizate și coordonate.

Operațiuni psihologice (PSYOP) și EW: Influențarea adversarului trebuie să fie întotdeauna obiectivul final al operațiunilor informaționale. Progresele tehnologice recente permit competențe precum PSYOP și MILDEC să ofere un număr mai mare de capabilități îmbunătățite, necesitând o mai mare implicare a EW în aceste domenii. EW ajută PSYOP prin degradarea capacității inamicului de a observa activitățile din teatru, de a raporta acele activități și de a lua decizii în consecință¹⁰.

Competențele de sprijin ale IO sunt securitatea fizică, atacul fizic, contrainformațiile (CI), asigurarea informațiilor (IA) și camera de luptă (COMCAM), acestea contribuind direct sau indirect la eficacitatea IO.

Securitatea fizică și EW: Utilizarea unui dispozitiv de bruij pentru convoaiele militare poate fi considerată securitate fizică. Măsurile de securitate fizică sunt utilizate oriunde este prezent echipamentul EW¹¹.

Atacul fizic și EW: Atacul fizic perturbă, distruge sau deteriorează ținte de orice fel folosind puterea cinetică distructivă, oferind un mijloc eficient de a ataca sistemele EW adverse și, prin urmare, sprijină superioritatea operațiunilor EW prietenoase.

Contraspionajul (CI) și EW: CI este compus din informații colectate și activități desfășurate pentru a contracara informațiile adverse, spionaj, sabotaj, asasinate etc¹². CI sprijină EP și ES prin furnizarea de contramăsuri electronice¹³, iar mijloacele EW pot fi folosite pentru a distruge sau degrada capacitățile de informații ale inamicului. Informațiile electronice colectate prin capabilitățile SIGINT și ES sunt folosite pentru a evalua, analiza și actualiza capacitățile de informații inamice.

Măsurile de contrainformații urmăresc să împiedice adversarii să se infiltreze și să culeagă informații sensibile de la forțele prietene. Acest aspect este esențial pentru menținerea securității operaționale și pentru asigurarea faptului că strategiile și tacticile cuiva rămân confidentiale. Serviciile de informații monitorizează protejarea informațiilor sensibile și a operațiunilor militare

¹⁰ Kucukozyigit, „Electronic Warfare (EW) Historical Perspectives and Its Relationship to Information Operations (IO) - Considerations for Turkey”.

¹¹ Army, *Joint Publication JP 3-13 Information Operations Change 1 November 2014*, B-2.

¹² Army, II-7.

¹³ Army, B-3.

pentru a nu fi compromise de agenți ostili. Identificarea și neutralizarea spionilor inamici poate avea un impact semnificativ asupra capacității inamicului de a colecta informații și de a le perturba planurile. Războiul ruso-ucrainean este caracterizat de utilizarea pe scară largă a dezinformării și a tacticilor hibride de război de către Rusia. Serviciile de informații joacă un rol esențial în detectarea și contracararea acestor eforturi. Ele monitorizează rețelele sociale, forumurile online și mass-media tradiționale pentru a identifica narațiunile false și propaganda difuzate de actori ostili. Informațiile false sunt folosite pentru a provoca indignarea publicului în timpul războiului. În aprilie 2014, canalele de știri ruse Russia-1 și NTV au arătat un bărbat spunând că a fost atacat de o bandă ucraineană fascistă pe un canal, și pe celălalt canal spunând că finanțează formarea radicalilor de dreapta anti-ruși. În mai 2014, Rusia-1 a difuzat o poveste despre atrocitățile ucrainene folosind imagini ale unei operațiuni rusești din 2012 în Caucazul de Nord. În aceeași lună, rețeaua de știri rusă Life a prezentat o fotografie din 2013 a unui copil rănit în Siria ca victimă a trupelor ucrainene care tocmai recuceriseră Aeroportul Internațional Donețk. Înțelegând peisajul dezinformării, serviciile de informații pot informa guvernele și publicul cu privire la tacticile înșelătoare folosite de Rusia, asigurându-se că dezinformarea nu influențează opinia publică sau nu compromite autoritățile naționale¹⁴.

Camera de luptă (COMCAM) și EW: COMCAM oferă liderilor imagini pentru a sprijini cerințele operaționale și de planificare¹⁵. Capacitățile ES care susțin informații contribuie, de asemenea, la misiunea COMCAM pe tot spectrul conflictelor. COMCAM poate fi utilizat pentru a evalua eficacitatea țintirii EW, iar EP contribuie la misiunea COMCAM prin transmiterea în siguranță a imaginilor COMCAM.

Asigurarea informațiilor (IA) și EW: IA este compusă din măsuri care protejează și apără informațiile și sistemele informaționale. EW oferă protecție operațională împotriva eforturilor adverse și de informații care vizează informații electronice și sisteme de informații prietenoase¹⁶, și sprijină IA prin protejarea informațiilor, a sistemelor informaționale și a activelor¹⁷.

¹⁴ Sfetcu, „Rolul serviciilor de informații în război”.

¹⁵ Army, *Joint Publication JP 3-13 Information Operations Change 1 November 2014*, II-7.

¹⁶ Army, II-6.

¹⁷ Army, B-3.

Războiul electronic cibernetic

La începutul anilor 2000, războiul cibernetic a început să apară ca un nou concept. Avantajele acestuia au fost confirmate în al doilea război din Golf, în Estonia în 2007 când aceasta a fost expusă unui atac cibernetic de către Rusia¹⁸, și în Georgia în timpul războiului din Oseția de Sud din 2008¹⁹.

Războiul cibernetic implică utilizarea atacurilor ciberneticе la nivel statal, provocând daune comparabile războiului real și/sau perturbând infrastructura și sistemele inamice²⁰. [

Taddeo a oferit următoarea definiție a războiului cibernetic, în 2012:

”Războiul bazat pe anumite utilizări ale TIC în cadrul unei strategii militare ofensive sau defensive susținute de un stat și care vizează perturbarea sau controlul imediat al resurselor inamicului și care se desfășoară în mediul informațional, cu agenți și ținte variind atât pe plan fizic, și domenii non-fizice și al căror nivel de violență poate varia în funcție de circumstanțe.”²¹

Securitatea cibernetică și războiul cibernetic au devenit aspecte esențiale într-o lume din ce în ce mai interconectată. Securitatea cibernetică (practica de salvagardare a sistemelor digitale și a datelor de activități rău intenționate), este indisolubil legată de războiul cibernetic, care implică utilizarea tehnologiilor digitale pentru a perturba, deteriora sau câștiga controlul asupra sistemelor informatice ale adversarilor. Granița dintre acestea două domenii este neclară, deoarece strategiile de securitate cibernetică au adesea dublă utilizare ca aplicații în războiul cibernetic și invers.

Securitatea cibernetică și războiul cibernetic sunt împletite într-o relație complexă care modelează lumea noastră digitală. Pe măsură ce amenințările ciberneticе evoluează continuu, și statele-națiune se angajează în acțiuni ciberneticе ofensive, nevoia de măsuri solide de securitate cibernetică și cooperare internațională este mai critică decât oricând. Pentru a naviga eficient în acest nexus complicat, părțile interesate trebuie să se adapteze continuu la natura dinamică a domeniului cibernetic, recunoscând că lupta digitală este la fel de importantă ca oricare câmpul de luptă fizic în secolul XXI.

În era digitală, peisajul amenințării evoluează constant, necesitând măsuri adaptive de securitate cibernetică. Amenințările ciberneticе cuprind o gamă largă de activități, inclusiv furturi

¹⁸ Dunn Cavelty, „Cyber-Allies”.

¹⁹ Yasar, Yasar, și Topcu, „Operational advantages of using Cyber Electronic Warfare (CEW) in the battlefield”.

²⁰ Singer și Friedman, *Cybersecurity*.

²¹ Taddeo, „An analysis for a just cyber warfare”.

de date, atacuri malware, atacuri denial-of-service și inginerie socială. Aceste amenințări pot viza indivizi, organizații sau chiar națiuni întregi. Pe măsură ce amenințările cibernetice cresc în complexitate, la fel și provocarea de securizare a infrastructurii critice și a informațiilor sensibile.

Relația dintre CW și EW poate fi considerată ca relația dintre războiul asimetric și cel simetric. CW și EW au fost folosite împreună pentru prima dată în războiul dintre Rusia și Georgia în 2008²².

În timp ce războiul electronic folosește spectrul electromagnetic și CW utilizează elemente ale spațiului cibernetic, războiul electronic cibernetic propune integrarea acestor două capacități de luptă. Avantajul CEW este că, în timp ce atacul electronic poate fi detectat, atacul electronic cibernetic este aproape imposibil de detectat.

Yasar, Yasar, și Topcu²³ fac o analiză SWOT a CEW, concluzionând că, deși este fezabil din punct de vedere tehnologic să se aplice conceptul CEW într-un atac, există câteva provocări, precum complexitatea sistemului de amenințări, necesitatea apelării la intelligence, și utilizarea diferitelor tipuri de firewall-uri și parole.

Internetul Obiectelor Militare (IoMT)

Internetul Obiectelor Militare (IoMT) este o rețea complexă de entități interconectate, sau „obiecte” cu beneficii recunoscute²⁴, care comunică între ele pentru a coordona, învăța și interacționa cu mediul pentru o gamă largă de activități într-un mod mai eficient și mai informat²⁵. Ideea de bază este că viitoarele bătălii militare vor fi dominate de inteligența mașinilor și războiul cibernetic²⁷.

Dispozitivele („obiectele”) din IoMT posedă capacități fizice inteligente de detectare, învățare și acționare prin interfețe virtuale sau cibernetice integrate²⁸. În general, dispozitivele IoMT formează o „țesătură de date”²⁹ pentru *transport de date, captare a datelor, detectare și de*

²² Yasar, Yasar, și Topcu, „Operational advantages of using Cyber Electronic Warfare (CEW) in the battlefield”.

²³ Yasar, Yasar, și Topcu.

²⁴ Silicon Labs, „The Evolution of Wireless Sensor Networks”.

²⁵ Rowlands, „The Internet of Military Things & Machine Intelligence: A Winning Edge or Security Nightmare? | Australian Army Research Centre (AARC)”.

²⁶ Cameron, „Internet of Things Meets the Military and Battlefield”.

²⁷ Kott, Alberts, și Wang, „Will Cybersecurity Dictate the Outcome of Future Wars?”

²⁸ Kott, „Challenges and Characteristics of Intelligent Autonomy for Internet of Battle Things in Highly Adversarial Environments”.

²⁹ Sydney J. Freedberg Jr, „Project Rainmaker”.

acționare, și un dispozitiv general cu capacități de procesare și comunicare care poate face schimb de informații cu rețeaua mai mare³⁰. S-a sugerat și posibilitatea de a încorpora în sistem obiecte neînsuflețite, cum ar fi plante și roci, prin dotarea acestora cu senzori care le vor transforma în puncte de colectare a informațiilor³¹. (e-Plants³²).

Cuprins

Abstract

Rezumat

Abrevieri

Introducere

Războiul electronic

- Definiții

- Dezvoltarea istorică

- Componentele cheie

- - Atacul electronic (EA)

- - Protecția electronică (EP)

- - Suport electronic (ES)

- Tehnici și tactici

- Sisteme EW

- - Radar

- Relația EW cu alte capacități de luptă

- - Războiul electronic cibernetic

- EW la nivel național și internațional

- - SUA

- - China

- - Rusia

- - NATO

- - Uniunea Europeană

- Provocări și tendințe

³⁰ Russell și Abdelzaher, „The Internet of Battlefield Things”.

³¹ Parker, „The Internet of Battlefield Things Is Coming. Are IT Pros Ready?”

³² Saxena, „Researchers Create Electronic Rose Complete with Wires and Supercapacitors”.

- Războiul asimetric

Inteligența artificială

- Contextul istoric al războiului electronic

- Rolul inteligenței artificiale în războiul electronic

- - Aplicații specifice

- Tehnici AI

- - Învățarea automată

- - Sisteme fuzzy

- - Algoritmul genetic

- Tendințe

- Provocări și riscuri

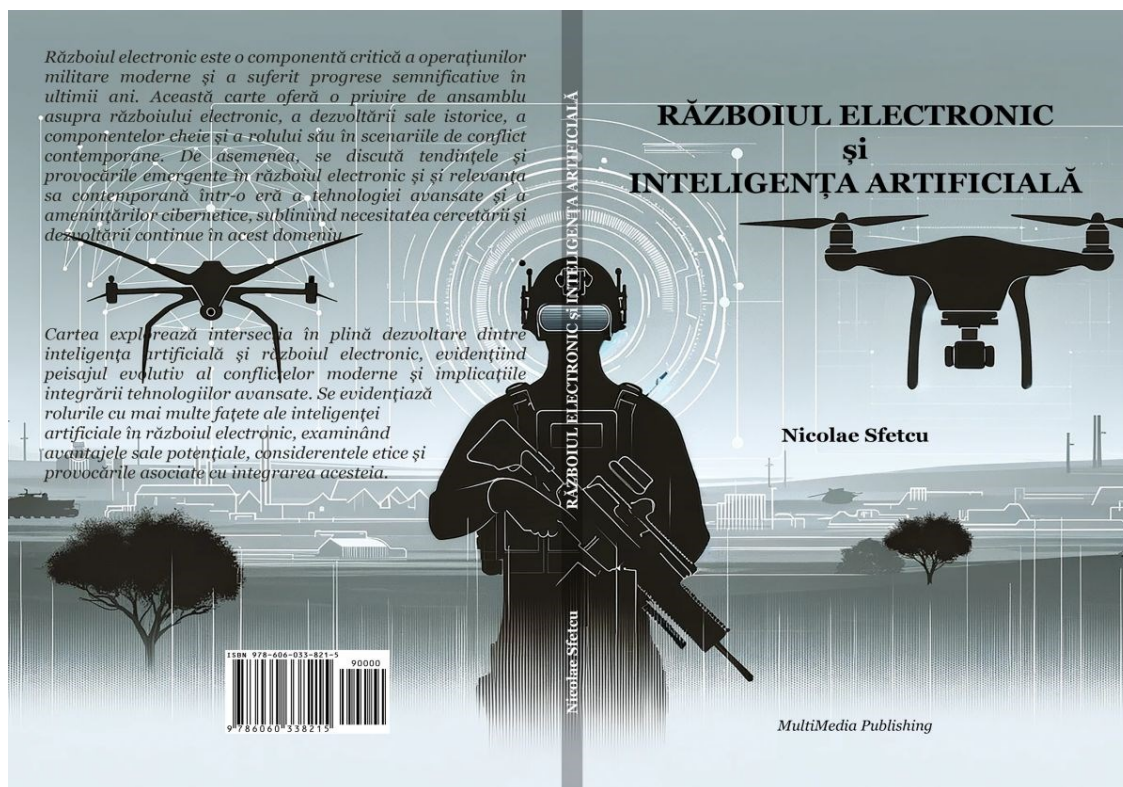
- - Considerații etice

- EW cognitiv

Concluzie

Bibliografie

Cartea



Această carte este ideală pentru profesioniștii în afaceri, strategii militari, și publicul academic.

Redefinirea războiului modern prin tehnologie

- **Titlu Carte:** *Războiul electronic și inteligența artificială*
- **Autor:** Nicolae Sfetcu
- **Editura:** MultiMedia Publishing
- **ISBN:** 978-606-033-821-5
- **DOI:** 10.58679/MM88277

De ce este această carte esențială

- **Relevanță critică:** Explorează intersecția dintre inteligența artificială (IA) și războiul electronic (RE), esențială în conflictele moderne.
- **Perspective actuale:** Abordează amenințările emergente, inclusiv războiul cibernetic, aplicațiile IA pe câmpul de luptă și războiul asimetric.
- **Autor expert:** Nicolae Sfetcu combină cercetarea profundă cu o analiză orientată spre viitor.

Caracteristici principale ale cărții

1. **Acoperire amplă:**
 - Istoria războiului electronic, de la originile sale până în prezent.
 - Analiză detaliată a principalilor actori: SUA, China, Rusia, NATO.
2. **Perspective asupra tehnologiei avansate:**
 - Rolul IA în RE, inclusiv învățarea automată și războiul electronic cognitiv.
 - Integrarea războiului electronic cu cel cibernetic.
3. **Focus strategic:**
 - Aplicații practice pentru apărare și militare.
 - Provocările și implicațiile etice ale IA în război.

Cui se adresează această carte?

- **Profesioniști din domeniul militar:** Obțineți un avantaj în planificarea strategică și operațiunile de RE.
- **Contractori din domeniul apărării:** Înțelegeți nevoile pieței pentru tehnologii emergente.

- **Academicieni și cercetători:** Explorați abordări interdisciplinare în IA și război.
- **Factori de decizie politică:** Formulați strategii naționale pentru mecanisme de apărare bazate pe IA.

Teme abordate

1. **Istoria și evoluția RE**
2. **Componentele de bază ale Războiului Electronic:**
 - Atacul electronic
 - Protecția electronică
 - Suportul electronic
3. **Tehnici IA în RE:**
 - Învățare automată
 - Sisteme fuzzy
 - Algoritmi genetici
4. **Tendențe și actori globali:**
 - Integrarea războiului cibernetic
 - Rolul marilor puteri: SUA, China, Rusia
5. **Provocări etice și operaționale**

Puncte unice de vânzare

- **Conținut de ultimă generație:** Perspective directe asupra celor mai recente progrese tehnologice.
- **Context global:** Explică modul în care RE și IA transformă dinamica puterii internaționale.
- **Perspective aplicabile:** Sfaturi practice pentru profesioniștii din domeniul apărării și tehnologiei.

Ce vor învăța cititorii

- Cum IA revoluționează strategiile de pe câmpul de luptă.
- Tehnici pentru contracararea amenințărilor din războiul asimetric.
- Traectoria viitoare a sistemelor de RE și implicațiile lor globale.
- Cadre etice pentru a echilibra inovația cu responsabilitatea.

Aprecieri pentru carte

- „*Lucrarea lui Nicolae Sfetcu este un studiu de referință care oferă atât profunzime, cât și extensie în domeniul în continuă evoluție al războiului electronic și IA.*” - [David D. Hall]
- „*O lectură obligatorie pentru profesioniștii din domeniul apărării care navighează prin complexitatea conflictelor moderne.*” - [Craig J. Adams]
- Recomandată pe [ResearchGate](https://www.researchgate.net/publication/35488277) și citată de mulți specialiști și academicieni

Descoperă viitorul războiului și comandă acum cartea *Războiul electronic și inteligența artificială!*

MultiMedia Publishing <https://www.telework.ro/ro/e-books/razboiul-electronic-si-inteligenta-artificiala/>

Digital: EPUB (ISBN 978-606-033-822-2), Kindle (ISBN 978-606-033-823-9) PDF (ISBN 978-606-033-824-6)

Tipărit: Format A5, 210 x 148 x 6 mm, 150 g, 112 pagini, ISBN 978-606-033-821-5

[DOI: 10.58679/MM88277](https://doi.org/10.58679/MM88277)

Data publicării: 06.01.2024

Bibliografie

- * * *. „Electronic Warfare Fundamentals”, 2000. <https://falcon.blu3wolf.com/Docs/Electronic-Warfare-Fundamentals.pdf>.
- . *Voennno-morskoi Slovar*. Moscova: Voennoe Izdatelstvo, 1990.
- . *Voennyi Entsiklopedicheskii Slovar*. Moscova: Voennoe Izdatelstvo, 1984.
- Adams, Charlotte. „Cognitive Electronic Warfare: Radio Frequency Spectrum Meets Machine Learning”, 2018. [//interactive.aviationtoday.com/avionicsmagazine/august-september-2018/cognitive-electronic-warfare-radio-frequency-spectrum-meets-machine-learning/](https://interactive.aviationtoday.com/avionicsmagazine/august-september-2018/cognitive-electronic-warfare-radio-frequency-spectrum-meets-machine-learning/).
- Adamy, David. *EW 101: A First Course in Electronic Warfare*. Artech House, 2001.
- AIM. „The AIM Initiative: A Strategy for Augmenting Intelligence Using Machines”, 2019. <https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2019/3286-the-aim-initiative-a-strategy-for-augmenting-intelligence-using-machines>.
- Akhtar, Jabran, și Karl Erik Olsen. „A Neural Network Target Detector with Partial CA-CFAR Supervised Training”. În *2018 International Conference on Radar (RADAR)*, 1–6, 2018. <https://doi.org/10.1109/RADAR.2018.8557276>.
- Allen, Gregory C. *Understanding China’s AI Strategy: Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security*. Center for a New American Security, 2019.
- Allen, John, și Giampiero Massolo. *The Global Race for Technological Superiority. Discover the Security Implication*. Ediție de Fabio Rugge. Milan: Ledizioni, 2020.

- Amuru, SaiDhiraj, Cem Tekin, Mihaela van der Schaar, și R. Michael Buehrer. „A systematic learning method for optimal jamming”. În *2015 IEEE International Conference on Communications (ICC)*, 2822–27, 2015. <https://doi.org/10.1109/ICC.2015.7248754>.
- Army, United States Government US. „Joint Pub 3-58 Joint Doctrine for Military Deception”, 1996.
https://webharvest.gov/peth04/20041021042923/http://www.dtic.mil/doctrine/jel/new_pubs/jp3_58.pdf.
- . „Joint Publication 3-51 Joint Doctrine for Electronic Warfare”, 2000.
https://irp.fas.org/doddir/dod/jp3_51.pdf.
- . „Joint Publication JP 1-02 Department of Defense Dictionary of Military and Associated Terms”, 2016. https://irp.fas.org/doddir/dod/jp1_02.pdf.
- . *Joint Publication JP 3-13 Information Operations Change 1 November 2014*. Independently Published, 2020.
- . „Joint Vision 2020: America’s Military - Preparing for Tomorrow”, 2020.
<https://apps.dtic.mil/sti/citations/ADA526044>.
- Baker, James E. „Artificial intelligence and national security law: A dangerous nonchalance | MIT Center for International Studies”, 2018. <https://cis.mit.edu/publications/starr-forum-report/18-01-report>.
- Barshan, Billur, și Bahaeddin Eravci. „Automatic Radar Antenna Scan Type Recognition in Electronic Warfare”. *IEEE Transactions on Aerospace and Electronic Systems* 48, nr. 4 (octombrie 2012): 2908–31. <https://doi.org/10.1109/TAES.2012.6324669>.
- Bronk, Justin, Nick Reynolds, și Jack Watling. „The Russian Air War and Ukrainian Requirements for Air Defence”, 2022. <https://static.rusi.org/SR-Russian-Air-War-Ukraine-web-final.pdf>.
- Brooks, Risa. „Technology and Future War Will Test U.S. Civil-Military Relations”. War on the Rocks, 26 noiembrie 2018. <https://warontherocks.com/2018/11/technology-and-future-war-will-test-u-s-civil-military-relations/>.
- Browne, J. P. R., și Michael T. Thurbon. *Electronic Warfare*. Brassey’s, 1998.
- Browne, Jack. „Cognitive EW Provides Computer-Powered Protection”. *Microwaves & RF*, 10 mai 2017. <https://www.mwrf.com/markets/defense/article/21848321/cognitive-ew-provides-computerpowered-protection>.
- Brunt, Leroy B. Van. *Applied ECM*. EW Engineering, 1978.
- BSI. „Federal Office for Information Security”. Federal Office for Information Security, 6 noiembrie 2023. https://www.bsi.bund.de/EN/Home/home_node.html.
- Butt, Faran, și Madiha Jalil. *An overview of electronic warfare in radar systems*, 2013. <https://doi.org/10.1109/TAECE.2013.6557273>.
- Cameron, Lori. „Internet of Things Meets the Military and Battlefield: Connecting Gear and Biometric Wearables for an IoMT and IoBT”. *IEEE Computer Society*, 1 martie 2018. <https://www.computer.org/publications/tech-news/research/internet-of-military-battlefield-things-iomt-iobt/>.
- Campen, Alan D. *The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War*. AFCEA International Press, 1992.
- Carlin, John P. „Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats | CSIS Events”, 2016. <https://www.csis.org/events/detect-disrupt-deter-whole-government-approach-national-security-cyber-threats>.

- Casterline, Kyle A., Nicholas J. Watkins, Jon R. Ward, William Li, și Matthew J. Thommana. „Applications of Machine Learning for Electronic Warfare Emitter Identification and Resource Management”, 2022. <https://secwww.jhuapl.edu/techdigest/content/techdigest/pdf/V36-N02/36-02-Casterline.pdf>.
- Chen, Jian, Shiyong Xu, Jiangwei Zou, și Zengping Chen. „Interrupted-Sampling Repeater Jamming Suppression Based on Stacked Bidirectional Gated Recurrent Unit Network and Infinite Training”. *IEEE Access* 7 (2019): 107428–37. <https://doi.org/10.1109/ACCESS.2019.2932793>.
- Clark, Colin. „Russia Widens EW War, «Disabling» EC-130s OR AC-130s In Syria”. *Breaking Defense* (blog), 24 aprilie 2018. <https://breakingdefense.sites.breakingmedia.com/2018/04/russia-widens-ew-war-disabling-ec-130s-in-syria/>.
- Coats, Daniel. „Intelligence Community Information Environment (IC IE) - Data Strategy”, 2021. https://www.dni.gov/files/documents/CIO/Data-Strategy_2017-2021_Final.pdf.
- Congressional Research Service. „Artificial Intelligence and National Security (R45178)”, 2020. <https://crsreports.congress.gov/product/details?prodcode=R45178>.
- Copp, Tara. „‘It Failed Miserably’: After Wargaming Loss, Joint Chiefs Are Overhauling How the US Military Will Fight”. *Defense One*, 26 iulie 2021. <https://www.defenseone.com/policy/2021/07/it-failed-miserably-after-wargaming-loss-joint-chiefs-are-overhauling-how-us-military-will-fight/184050/>.
- CRA. „Internet of Battlefield Things (IoBT) CRA – DEVCOM Army Research Laboratory”, 2017. <https://arl.devcom.army.mil/cras/iobt-cra/>.
- CRS. „Defense Primer: Electronic Warfare”, 2022. <https://sgp.fas.org/crs/natsec/IF11118.pdf>.
- CS Europe. „Cyber Security Europe | Cyber Security Insight for Boardroom and C-Suite Executives.” Cyber Security Europe, 2023. <https://www.cseurope.info/>.
- Davenport, Thomas, și Ravi Kalakota. „The Potential for Artificial Intelligence in Healthcare”. *Future Healthcare J* 6, nr. 2 (1 iunie 2019): 94–98. <https://doi.org/10.7861/futurehosp.6-2-94>.
- Davis, Zachary. „Artificial Intelligence on the Battlefield: Implications for Deterrence and Surprise”. *PRISM* 8, nr. 2 (2019): 114–31.
- Day, Peter. „Peter Day’s World of Business Podcast”, 2016. http://downloads.bbc.co.uk/podcasts/radio/worldbiz/worldbiz_20150319-0730a.mp3.
- De Spiegeleire, Stephan, Matthijs Maas, și Tim Sweijts. *Artificial Intelligence and the Future of Defense*, 2017.
- Department of Defense. „Summary of the 2018 National Defense Strategy”, 2018. <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.
- Dickson, John R. V. „Electronic Warfare in Vietnam: Did We Learn Our Lessons?.”, 1987. <https://www.semanticscholar.org/paper/Electronic-Warfare-in-Vietnam%3A-Did-We-Learn-Our-Dickson/399e7323fb081cb95db35d3a9d3075154a0de068>.
- DoD. „DoD Announces Release of JADC2 Implementation Plan”. U.S. Department of Defense, 2022. <https://www.defense.gov/News/Releases/Release/Article/2970094/dod-announces-release-of-jadc2-implementation-plan/https%3A%2F%2Fwww.defense.gov%2FNews%2FReleases%2FRelease%2FArticle%2F2970094%2Fdod-announces-release-of-jadc2-implementation-plan%2F>.

- DOD. „DoD Data Strategy”, 2020. <https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF>.
- Doskalov, Mikhail. „Perspektivy razvitiia sistemy radioelektronnoi borby Rossiiskoj Federatsii na period do 2020 goda”. În *Oboronnyi kompleks RF: Sostoianie i razvitie*, 2013. <http://federalbook.ru/files/OPK/Soderjanie/OPK-9/III/Doskalov.pdf>.
- Dudczyk, Janusz, și A. Kawalec. „Specific emitter Identification based on graphical representation of the distribution of radar signal parameters”. *Jokull* 63 (11 noiembrie 2013): 408–16.
- Duke, Audrey. „Harnessing Chaos: Unleashing Electromagnetic Warfare for Enhanced Joint Operations”, 2023. <https://apps.dtic.mil/sti/citations/AD1206172>.
- Dunn Cavelty, Myriam. „Cyber-Allies: Strengths and Weaknesses of NATO’s Cyberdefense Posture”. SSRN Scholarly Paper. Rochester, NY, 1 februarie 2012. <https://papers.ssrn.com/abstract=1997153>.
- EASA. „Concepts of Design Assurance for Neural Networks (CoDANN)”, 2020. <https://www.easa.europa.eu/sites/default/files/dfu/EASA-DDLN-Concepts-of-Design-Assurance-for-Neural-Networks-CoDANN.pdf>.
- Elbir, Ahmet M., Kumar Vijay Mishra, și Yonina C. Eldar. „Cognitive Radar Antenna Selection via Deep Learning”. arXiv, 4 februarie 2019. <https://doi.org/10.48550/arXiv.1802.09736>.
- EMK, SU. „ECHO Network”, 2023. <https://echonetwork.eu/>.
- European Defence Agency. „Enhancing EU Military Capabilities Beyond 2040”, 2023. <https://eda.europa.eu/docs/default-source/eda-publications/enhancing-eu-military-capabilities-beyond-2040.pdf>.
- Freedberg Jr, Sydney J. „US Has Lost «Dominance In Electromagnetic Spectrum»: Shaffer”. *Breaking Defense* (blog), 3 septembrie 2014. <https://breakingdefense.com/2014/09/us-has-lost-dominance-in-electromagnetic-spectrum-shaffer/>.
- Freedberg, Sydney J. „Electronic Warfare «Growing»; Joint Airborne EW Study Underway”. *Breaking Defense* (blog), 23 iunie 2017. <https://breakingdefense.sites.breakingmedia.com/2017/06/electronic-warfare-growing-joint-airborne-ew-study-underway/>.
- Friedrich, Nancy. „AI and Machine Learning Redefine the EW Landscape | 2020-12-08 | Microwave Journal”, 2020. <https://www.microwavejournal.com/articles/35107-ai-and-machine-learning-define-the-ew-landscape>.
- Fulghum, David A., și Robert Wall. „Israel Shows Electronic Prowess | Aviation Week Network”, 2007. <https://aviationweek.com/israel-shows-electronic-prowess>.
- Gambrell, Dorothy, și Charissa Isidro. „A Visual Guide to the World’s Military Budgets”. *Bloomberg.Com*, 11 martie 2022. <https://www.bloomberg.com/news/features/2022-03-11/the-largest-militaries-visualized>.
- Gannon, Brian P. „Implement AI in Electromagnetic Spectrum Operations”. U.S. Naval Institute, 1 august 2023. <https://www.usni.org/magazines/proceedings/2023/august/implement-ai-electromagnetic-spectrum-operations>.
- Gao, Jingpeng, Yi Lu, Junwei Qi, și Liangxi Shen. „A Radar Signal Recognition System Based on Non-Negative Matrix Factorization Network and Improved Artificial Bee Colony Algorithm”. *IEEE Access* 7 (2019): 117612–26. <https://doi.org/10.1109/ACCESS.2019.2936669>.
- Gecgel Cetin, Selen, Caner Goztepe, și Gunes Karabulut Kurt. *Jammer Detection based on Artificial Neural Networks: A Measurement Study*, 2019. <https://doi.org/10.1145/3324921.3328788>.

- Gigova, Radina. „Who Putin thinks will rule the world | CNN”, 2017. <https://edition.cnn.com/2017/09/01/world/putin-artificial-intelligence-will-rule-world/index.html>.
- Goodfellow, Ian, Yoshua Bengio, și Aaron Courville. *Deep Learning: Adaptive Computation and Machine Learning Series*. MIT Press, 2016.
- Grant, P. M., și J. H. Collins. „Introduction to Electronic Warfare”. *IEE Proceedings F (Communications, Radar and Signal Processing)* 129, nr. 3 (1 iunie 1982): 113–32. <https://doi.org/10.1049/ip-f-1.1982.0020>.
- Gulhane, Tejaswi Singh and Amit. „8 Key Military Applications for Artificial Intelligence”. Data accesării 23 decembrie 2023. <https://blog.marketresearch.com/8-key-military-applications-for-artificial-intelligence-in-2018>.
- Guzenko, V. F., și A. L. Moraresku. *Radioelektronnaia borba. Sovremennoe sodержanie*. Moscova: Informatsionnyi Most, 2017.
- Haigh, Karen Zita, și Julia Andrusenko. *Cognitive Electronic Warfare: An Artificial Intelligence Approach*. Artech House, 2021.
- Hamilton, Serena, A.J. Jakeman, și John Norton. „Artificial Intelligence techniques: An introduction to their use for modelling environmental systems”. *Mathematics and Computers in Simulation* 78 (1 iulie 2008): 379–400. <https://doi.org/10.1016/j.matcom.2008.01.028>.
- Haney, Brian. „Applied Artificial Intelligence in Modern Warfare and National Security Policy”. SSRN Scholarly Paper. Rochester, NY, 15 septembrie 2019. <https://doi.org/10.2139/ssrn.3454204>.
- Henney, Megan. „Big Tech Has Spent \$582M Lobbying Congress. Here’s Where That Money Went”. Text.Article. FOXBusiness. Fox Business, 8 mai 2019. <https://www.foxbusiness.com/technology/amazon-apple-facebook-google-microsoft-lobbying-congress>.
- Hoehn, John. „Defense Primer: What Is Command and Control?”, 2021. <https://apps.dtic.mil/sti/citations/AD1169627>.
- Insinna, Valerie. „China Could Obtain 1,500 Nuclear Warheads by 2035, Pentagon Estimates”. *Breaking Defense* (blog), 29 noiembrie 2022. <https://breakingdefense.sites.breakingmedia.com/2022/11/china-to-obtain-1500-nuclear-warheads-by-2035-pentagon-estimates/>.
- Jankowicz, Mia. „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. *The Boer War: A History*. Bloomsbury Academic, 2013.
- Junfei, Yu, Li Jingwen, Sun Bing, și Jiang Yuming. „Barrage Jamming Detection and Classification Based on Convolutional Neural Network for Synthetic Aperture Radar”. În *IGARSS 2018 - 2018 IEEE International Geoscience and Remote Sensing Symposium*, 4583–86, 2018. <https://doi.org/10.1109/IGARSS.2018.8519373>.
- Kadlecová, Lucie, Nadia Meyer, Rafaël Cos, și Pauline Ravinet. „Mapping the Role of Science Diplomacy in the Cyber Field”, 2020.
- Kang, Li, Jiu Bo, Liu Hongwei, și Liang Siyuan. „Reinforcement Learning based Anti-jamming Frequency Hopping Strategies Design for Cognitive Radar”. În *2018 IEEE International*

- Conference on Signal Processing, Communications and Computing (ICSPCC)*, 1–5, 2018. <https://doi.org/10.1109/ICSPCC.2018.8567751>.
- Katz, Yaakov. „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>.
- Kjellén, Jonas. „Russian Electronic Warfare - The role of Electronic Warfare in the Russian Armed Forces”, 2018. <https://web.archive.org/web/20181010174505/https://www.foi.se/report-search/pdf?fileName=D%3A%5CReportSearch%5CFiles%5C4c547bec-bdfa-4bdb-a1c9-018097aaf615.pdf>.
- Kolesov, N. A., și I. G. Nasenkov. *Radioelektronnaia Borba. Ot eksperimentov proshlogo do reshayushchego fronta budushchego*. Moscova: Centre for Analysis of Strategies and Technologies (CAST), 2015.
- Kolhatkar, Sheelah. „How Elizabeth Warren Came Up with a Plan to Break Up Big Tech”. *The New Yorker*, 20 august 2019. <https://www.newyorker.com/business/currency/how-elizabeth-warren-came-up-with-a-plan-to-break-up-big-tech>.
- Kott, Alexander. „Challenges and Characteristics of Intelligent Autonomy for Internet of Battle Things in Highly Adversarial Environments”, 20 martie 2018.
- Kott, Alexander, David S. Alberts, și Cliff Wang. „Will Cybersecurity Dictate the Outcome of Future Wars?” *Computer* 48, nr. 12 (decembrie 2015): 98–101. <https://doi.org/10.1109/MC.2015.359>.
- Krylov, G. O., S. L. Larionova, și Nikitina. *Bazovye poniatiia informatsionnoi bezopasnosti*. Moscova: OOO RUSAJNS, 2017.
- Kube, Courtney. „Russia Is Jamming American Drones in Syria, Officials Say”. *NBC News*, 10 aprilie 2018. <https://www.nbcnews.com/news/military/russia-has-figured-out-how-jam-u-s-drones-syria-n863931>.
- Kucukozyigit, Ali. „Electronic Warfare (EW) Historical Perspectives and Its Relationship to Information Operations (IO) - Considerations for Turkey”, 2006.
- Lakhin, Andrei, și Andrei Korobeinikov. *Sostoianie i perspektivy razvitiia voisk radioelektronnoi borby Vooruzhennykh Sil Rossiiskoi Federatsii*. Moscova: Informatsionnyi Most, 2016.
- Lazarov, Lazar. „Perspectives and Trends for the Development of Electronic Warfare Systems”. *2019 International Conference on Creative Business for Smart and Sustainable Growth (CREBUS)*, martie 2019, 1–3. <https://doi.org/10.1109/CREBUS.2019.8840074>.
- Lee, Gyeong-Hoon, Jeil Jo, și Cheong Hee Park. „Jamming Prediction for Radar Signals Using Machine Learning Methods”. *Security and Communication Networks* 2020 (24 ianuarie 2020): e2151570. <https://doi.org/10.1155/2020/2151570>.
- Li, Huiqin, Yanling Li, Chuan He, Jianwei Zhan, și Hui Zhang. „Cognitive Electronic Jamming Decision-Making Method Based on Improved Q -Learning Algorithm”. *International Journal of Aerospace Engineering* 2021 (22 decembrie 2021): 1–12. <https://doi.org/10.1155/2021/8647386>.
- Li, Xueqiong, Zhitao Huang, Fenghua Wang, Xiang Wang, și Tianrui Liu. „Toward Convolutional Neural Networks on Pulse Repetition Interval Modulation Recognition”. *IEEE Communications Letters* PP (16 august 2018): 1–1. <https://doi.org/10.1109/LCOMM.2018.2864725>.
- Li, Yangyang, Ximing Wang, Dianxiong Liu, Qiuju Guo, Xin Liu, Jie Zhang, și Yitao Xu. „On the Performance of Deep Reinforcement Learning-Based Anti-Jamming Method

- Confronting Intelligent Jammer”. *Applied Sciences* 9, nr. 7 (ianuarie 2019): 1361. <https://doi.org/10.3390/app9071361>.
- Liao, Xiaofeng, Bo Li, și Bo Yang. „A Novel Classification and Identification Scheme of Emitter Signals Based on Ward’s Clustering and Probabilistic Neural Networks with Correlation Analysis”. *Computational Intelligence and Neuroscience* 2018 (5 noiembrie 2018): e1458962. <https://doi.org/10.1155/2018/1458962>.
- Liu, Yemin, Shiqi Xing, Y. Li, Dong Hou, și Wang Xuesong. „Jamming recognition method based on the polarization scattering characteristics of chaff clouds”. *IET Radar, Sonar & Navigation* 11 (8 august 2017). <https://doi.org/10.1049/iet-rsn.2017.0121>.
- Liubin, Mikhail Dmitriyevich. „K voprosu ob istorii razvitiia i perspektivakh radioelektronnoi borby”. *Voennaia mysl*, nr. 3 (2009): 64–75.
- Magrassi, Paolo. *A World of Smart Objects: The Role of Auto-Identification Technologies*, 2002. ———. *Why a Universal RFID Infrastructure Would Be a Good Thing*, 2002.
- MarketsAndMarkets. „Artificial Intelligence (AI) in Military Market Size Growth Opportunities Industry Trends and Analysis 2030”. MarketsandMarkets, 2023. <https://www.marketsandmarkets.com/Market-Reports/artificial-intelligence-military-market-41793495.html>.
- Martino, Andrea De. *Introduction to Modern EW Systems*. Artech House, 2012.
- McArthur, Charles W. *Operations Analysis in the United States Army Eighth Air Force in World War II*. American Mathematical Soc., 1990.
- McDermott, Roger N. „Russia’s Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum”. ICDS, 17 septembrie 2017. <https://icds.ee/en/russias-electronic-warfare-capabilities-to-2025-challenging-nato-in-the-electromagnetic-spectrum/>.
- MeriTalk. „DARPA Floats a Proposal for the Ocean of Things”, 2018. <https://www.meritalk.com/articles/darpa-floats-a-proposal-for-the-ocean-of-things/>.
- Microwaves, Microwaves & RF. „BAE Bets on Use of Artificial Intelligence in Electronic Warfare”. Microwaves & RF, 15 iulie 2019. <https://www.mwrf.com/markets/defense/article/21849838/bae-systems-bae-bets-on-use-of-artificial-intelligence-in-electronic-warfare>.
- Ministry of Defence. „Data Strategy for Defence”. GOV.UK, 2021. <https://www.gov.uk/government/publications/data-strategy-for-defence>.
- . „Defence Artificial Intelligence Strategy”. GOV.UK, 2022. <https://www.gov.uk/government/publications/defence-artificial-intelligence-strategy/defence-artificial-intelligence-strategy>.
- . „Digital Strategy for Defence”. GOV.UK, 2021. <https://www.gov.uk/government/publications/digital-strategy-for-defence-delivering-the-digital-backbone-and-unleashing-the-power-of-defences-data>.
- Mizokami, Kyle. „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/>.
- NATO. „Electromagnetic Warfare”. NATO, 2023. https://www.nato.int/cps/en/natohq/topics_80906.htm.
- . „The 107th NATO Electronic Warfare Advisory Committee (NEWAC) Convenes in Brussels”. NATO, 2019. https://www.nato.int/cps/en/natohq/news_171280.htm.

- Neri, F. „Introduction to electronic defense systems”, 1991. <https://www.semanticscholar.org/paper/Introduction-to-electronic-defense-systems-Neri/8d8aed6d92ecf7af850f09a2ee740380c2d4b366>.
- Noh, Sanguk, și Unseob Jeong. „Intelligent Command and Control Agent in Electronic Warfare Settings”. *International Journal of Intelligent Systems* 25, nr. 6 (2010): 514–28. <https://doi.org/10.1002/int.20413>.
- Northrop. „Electronic Warfare and Sensors”, 2022. https://info.breakingdefense.com/hubfs/E-Book_EW_&_Sensors_Northrop_Grumman_Breaking_Defense.pdf.
- ODIN. „Borisoglebsk-2 (RB-301B) Russian Amphibious Multipurpose Jamming Complex”, 2023. [https://odin.tradoc.army.mil/WEG/Asset/Borisoglebsk-2_\(RB-301B\)_Russian_Amphibious_Multipurpose_Jamming_Complex](https://odin.tradoc.army.mil/WEG/Asset/Borisoglebsk-2_(RB-301B)_Russian_Amphibious_Multipurpose_Jamming_Complex).
- Parker, Paul. „The Internet of Battlefield Things Is Coming. Are IT Pros Ready?” C4ISRNet, 3 octombrie 2018. <https://www.c4isrnet.com/opinion/2018/10/03/the-internet-of-battlefield-things-is-coming-are-it-pros-ready/>.
- Petrov, Nedyalko, Ivan Jordanov, și Jon Roe. „Radar Emitter Signals Recognition and Classification with Feedforward Networks”. *Procedia Computer Science*, 17th International Conference in Knowledge Based and Intelligent Information and Engineering Systems - KES2013, 22 (1 ianuarie 2013): 1192–1200. <https://doi.org/10.1016/j.procs.2013.09.206>.
- Poisel, Richard. *Introduction to Communication Electronic Warfare Systems*. Artech House, 2008.
- Polit, Kate. „Army Takes on Wicked Problems With the Internet of Battlefield Things”, 2018. <https://www.meritalk.com/articles/army-takes-on-wicked-problems-with-the-internet-of-battlefield-things/>.
- Polmar, Norman. „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. *The History of US Electronic Warfare*. Association of Old Crows, 1984.
- Qiang, Xing, Zhu Wei-gang, și Bo Yuan. „Jamming Style Selection for Small Sample Radar Jamming Rule Base”. *2018 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC)*, septembrie 2018, 1–5. <https://doi.org/10.1109/ICSPCC.2018.8567613>.
- Qu, Zhiyu, Wenyang Wang, Changbo Hou, și Chenfan Hou. „Radar Signal Intra-Pulse Modulation Recognition Based on Convolutional Denoising Autoencoder and Deep Convolutional Neural Network”. *IEEE Access* 7 (2019): 112339–47. <https://doi.org/10.1109/ACCESS.2019.2935247>.
- Rahman, H. *Introduction to Electronic Defense Systems*. Boca Raton, FL, USA: CRC Press, 2019.
- Rambo. „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>.
- Rogosa, Alexander. „Shifting Spaces: The Success of the SpaceX Lawsuit and the Danger of Single-Source Contracts in America’s Space Program”. *Federal Circuit Bar Journal* 25 (2016 2015): 101.
- Rowlands, Greg. „The Internet of Military Things & Machine Intelligence: A Winning Edge or Security Nightmare? | Australian Army Research Centre (AARC)”, 2017. <https://researchcentre.army.gov.au/library/land-power-forum/internet-military-things-machine-intelligence-winning-edge-or-security-nightmare>.

- Russell, Stephen, și Tarek Abdelzaker. „The Internet of Battlefield Things: The Next Generation of Command, Control, Communications and Intelligence (C3I) Decision-Making”. În *MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM)*, 737–42, 2018. <https://doi.org/10.1109/MILCOM.2018.8599853>.
- Saxena, Shalini. „Researchers Create Electronic Rose Complete with Wires and Supercapacitors”. *Ars Technica*, 1 martie 2017. <https://arstechnica.com/science/2017/03/researchers-grow-electronic-rose-complete-with-wires-and-supercapacitors/>.
- Sfetcu, Nicolae. „Evoluția inteligenței artificiale în domeniul securității naționale”. *Intelligence Info*, 10 noiembrie 2023. <https://www.intelligenceinfo.org/evolutia-inteligentei-artificiale-in-domeniul-securitatii-nationale/>.
- . „Rolul serviciilor de informații în război”. *Intelligence Info*, 3 august 2023. <https://www.intelligenceinfo.org/rolul-serviciilor-de-informatii-in-razboi/>.
- Shankar, M., și B. Mohan. „Recent Advances in Electronic Warfare-ESM Systems”, 2013. <https://www.semanticscholar.org/paper/RECENT-ADVANCES-IN-ELECTRONIC-WARFARE-ESM-SYSTEMS-Shankar-Mohan/bf6e4c372514695dd167eebf6f9dfb78ca120f6a>.
- Shao, Guangqing, Yushi Chen, și Yinsheng Wei. „Convolutional Neural Network-Based Radar Jamming Signal Classification With Sufficient and Limited Samples”. *IEEE Access* 8 (2020): 80588–98. <https://doi.org/10.1109/ACCESS.2020.2990629>.
- Sharma, Purabi, Kandarpa Kumar Sarma, și Nikos E. Mastorakis. „Artificial Intelligence Aided Electronic Warfare Systems- Recent Trends and Evolving Applications”. *IEEE Access* 8 (2020): 224761–80. <https://doi.org/10.1109/ACCESS.2020.3044453>.
- Silicon Labs. „The Evolution of Wireless Sensor Networks”, 2013. <https://www.silabs.com/documents/public/white-papers/evolution-of-wireless-sensor-networks.pdf>.
- Simonite, Tom. „Artificial Intelligence Fuels New Global Arms Race”. *Wired*, 2017. <https://www.wired.com/story/for-superpowers-artificial-intelligence-fuels-new-global-arms-race/>.
- Singer, Peter W., și Allan Friedman. *Cybersecurity: What Everyone Needs to Know*. OUP USA, 2014.
- Singh, Mohinder. „Electronic Warfare”, 1988. <https://www.drdo.gov.in/sites/default/files/publications-document/Electronic%20Warfare.pdf>.
- Skolnik, Merrill I. *Radar Handbook, Third Edition*. McGraw-Hill Education, 2008.
- Smith, Craig. „Eye On AI”. *Eye On AI*, 28 august 2019. <https://www.eye-on.ai>.
- Smith, Patrick. *Russian Electronic Warfare: A Growing Threat to U.S. Battlefield Supremacy*. American Security Project, 2022.
- Smith, Ron, și Scott Knight. „Applying Electronic Warfare Solutions to Network Security - Canadian Military Journal”, 2005. <http://www.journal.forces.gc.ca/vo6/no3/electron-eng.asp>.
- SPARTA. „SPARTA Consortium”, 2023. <https://www.cybersecurityintelligence.com/sparta-consortium-5594.html>.
- Stackpole, Beth. „Keeping the Connected Soldier Connected with Simulation”. *Digital Engineering*, 1 septembrie 2016. <https://www.digitalengineering247.com/article/keeping-the-connected-soldier-connected-with-simulation>.

- State Council. „A Next Generation Artificial Intelligence Development Plan”. *China Copyright and Media* (blog), 20 iulie 2017. <https://chinacopyrightandmedia.wordpress.com/2017/07/20/a-next-generation-artificial-intelligence-development-plan/>.
- Sydney J. Freedberg Jr. „Project Rainmaker: Army Weaves ‘Data Fabric’ To Link Joint Networks”. *Breaking Defense* (blog), 17 noiembrie 2020. <https://breakingdefense.sites.breakingmedia.com/2020/11/project-rainmaker-army-weaves-data-fabric-to-link-joint-networks/>.
- Taddeo, Mariarosaria. „An analysis for a just cyber warfare”. În *2012 4th International Conference on Cyber Conflict (CYCON 2012)*, 1–10, 2012. <https://ieeexplore.ieee.org/document/6243976>.
- Tang, Author: Hazel. „Preparing for the Future of Artificial Intelligence. Executive Office of the President: National Science and Technology Council and Committee on Technology. October, 2016.” *AIMed* (blog), 9 aprilie 2020. <https://ai-med.io/executive/preparing-for-the-future-of-artificial-intelligence-executive-office-of-the-president-national-science-and-technology-council-and-committee-on-technology-october-2016/>.
- Tegler, Eric. „The Vulnerability of AI Systems May Explain Why Russia Isn’t Using Them Extensively in Ukraine”. *Forbes*, 2022. <https://www.forbes.com/sites/ericteglert/2022/03/16/the-vulnerability-of-artificial-intelligence-systems-may-explain-why-they-havent-been-used-extensively-in-ukraine/>.
- Tegmark, Max. „Life 3.0: Being Human in the Age of Artificial Intelligence | Mitpressbookstore”, 31 iulie 2018. <https://mitpressbookstore.mit.edu/book/9781101970317>.
- Tsui, Chi-Hao Cheng, James. *An Introduction to Electronic Warfare; from the First Jamming to Machine Learning Techniques*. New York: River Publishers, 2022. <https://doi.org/10.1201/9781003337171>.
- Tucker, Patrick. „AI Is Already Learning from Russia’s War in Ukraine, DOD Says”. *Defense One*, 21 aprilie 2022. <https://www.defenseone.com/technology/2022/04/ai-already-learning-russias-war-ukraine-dod-says/365978/>.
- US Marine Corps. „Electronic Warfare”, 2016. [https://www.marines.mil/Portals/1/Publications/MCRP%203-32D.1%20\(Formerly%20MCWP%203-40.5\).pdf](https://www.marines.mil/Portals/1/Publications/MCRP%203-32D.1%20(Formerly%20MCWP%203-40.5).pdf).
- Vincent, James. „Elon Musk and AI Leaders Call for a Ban on Killer Robots”. *The Verge*, 21 august 2017. <https://www.theverge.com/2017/8/21/16177828/killer-robots-ban-elon-musk-un-petition>.
- Waghray, Namrita, și P. M. Menghal. „Simulation of radar topology networks to evolve the electronic warfare survivability metrics”. *2011 3rd International Conference on Electronics Computer Technology*, aprilie 2011, 355–59. <https://doi.org/10.1109/ICECTECH.2011.5941622>.
- Wan, Tao, Xinying Fu, Kaili Jiang, Yuan Zhao, și Bin Tang. „Radar Antenna Scan Pattern Intelligent Recognition Using Visibility Graph”. *IEEE Access* 7 (2019): 175628–41. <https://doi.org/10.1109/ACCESS.2019.2957769>.
- Wang, Feng, Shanshan Huang, Hao Wang, și Chenlu Yang. „Automatic Modulation Classification Exploiting Hybrid Machine Learning Network”. *Mathematical Problems in Engineering* 2018 (4 decembrie 2018): e6152010. <https://doi.org/10.1155/2018/6152010>.
- Wei, Dongxu, Shuning Zhang, Si Chen, Huichang Zhao, și Linzhi Zhu. „Research on Deception Jamming of Chaotic Composite Short-Range Detection System Based on Bispectral

- Analysis and Genetic Algorithm–Back Propagation”. *International Journal of Distributed Sensor Networks* 15, nr. 5 (1 mai 2019): 1550147719847444. <https://doi.org/10.1177/1550147719847444>.
- Weisgerber, Marcus. „The Pentagon’s New Algorithmic Warfare Cell Gets Its First Mission: Hunt ISIS”. *Defense One*, 14 mai 2017. <https://www.defenseone.com/technology/2017/05/pentagons-new-algorithmic-warfare-cell-gets-its-first-mission-hunt-isis/137833/>.
- Yasar, Nurgul, Fatih Mustafa Yasar, și Yucel Topcu. „Operational advantages of using Cyber Electronic Warfare (CEW) in the battlefield”. În *Cyber Sensing 2012*, 8408:151–59. SPIE, 2012. <https://doi.org/10.1117/12.919454>.
- You, Shixun, Ming Diao, și Lipeng Gao. „Deep Reinforcement Learning for Target Searching in Cognitive Electronic Warfare”. *IEEE Access* 7 (2019): 37432–47. <https://doi.org/10.1109/ACCESS.2019.2905649>.
- Zhang, Ming, Ming Diao, Lipeng Gao, și Lutao Liu. „Neural Networks for Radar Waveform Recognition”. *Symmetry* 9, nr. 5 (mai 2017): 75. <https://doi.org/10.3390/sym9050075>.