INTELLIGENCE INFO

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

Integrarea inteligenței artificiale în serviciile de informații

Nicolae Sfetcu

Sfetcu, Nicolae (2023), Integrarea inteligenței artificiale în serviciile de informații, *Intelligence Info*, **3**:1, 68-76, DOI: 10.58679/II25491, https://www.intelligenceinfo.org/integrarea-inteligentei-artificiale-in-serviciile-de-informatii/

Publicat online: 05.12.2023

Integrarea inteligenței artificiale în serviciile de informații

Ing. fiz. Nicolae SFETCU, MPhil[1]
nicolae@sfetcu.com

Integrating artificial intelligence into intelligence agencies

Abstract

Intelligence agencies play a crucial role in national security, and rapid advances in artificial intelligence technologies have provided new tools to enhance their capabilities. This academic essay explores the evolving landscape of intelligence agencies and their increasing reliance on artificial intelligence technologies. It examines the multifaceted use of artificial intelligence within intelligence agencies, exploring its impact on analysis, security, and the ethical implications associated with its implementation.

Keywords: intelligence services, national security, artificial intelligence, AI technologies, intelligence agencies

Rezumat

Serviciile de informații joacă un rol crucial în securitatea națională, iar progresele rapide în tehnologiile inteligenței artificiale au oferit noi instrumente pentru îmbunătățirea capacităților lor. Acest eseu academic explorează peisajul în evoluție al agențiilor de informații și dependența crescândă a acestora de tehnologiile de inteligență artificială (AI). Se analizează utilizarea cu mai multe fațete a inteligenței artificiale în cadrul agențiilor de informații, explorând impactul acesteia asupra analizei, securității și implicațiile etice asociate cu implementarea acesteia.

Cuvinte cheie: servicii de informații, securitatea națională, inteligența artificială, tehnologii IA, agenții de informații

[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. 68-76
ISSN 2821 - 8159, ISSN – L 2821 – 8159, DOI: 10.58679/II25491
URL: https://www.intelligenceinfo.org/integrarea-inteligentei-artificiale-in-serviciile-de-informatii/

Introducere

Pe măsură ce tehnologia avansează, agențiile de informații folosesc IA pentru a-și îmbunătăți capacitățile analitice, a îmbunătăți măsurile de securitate și a aborda amenințările emergente. Cu toate acestea, integrarea AI în cadrul agențiilor de informații ridică considerații etice care merită o examinare atentă.

Serviciile de informații joacă un rol crucial în securitatea națională, iar progresele rapide în tehnologiile IA au oferit noi instrumente pentru îmbunătățirea capacităților lor.

Principalele utilizări potențiale și reale ale IA în serviciile de informații includ automatizarea proceselor administrative și organizaționale, procesele de securitate cibernetic, și analiza informațiilor prin „intelligence augmentat îmbunătățită prin IA”[2]. Conform lui Weinbaum & Shanahan,

> „Viitoarea activitate în domeniul intelligence va depinde de accesarea datelor, de modelarea arhitecturii corporative potrivite în jurul datelor, de dezvoltarea capabilităților bazate pe inteligență artificială pentru a accelera în mod dramatic înțelegerea contextuală a datelor prin echipă om-mașină și mașină-mașină, și de creșterea expertizei analitice capabile să aprofundeze și să navigheze în enorme lacuri de date”[3].

[2] Alexander Babuta, Marion Oswald, și Ardi Janjeva, „Artificial Intelligence and UK National Security: Policy Considerations”, 2 noiembrie 2023, https://rusi.orghttps://rusi.org.

[3] Cortney Weinbaum și John N.T. Shanahan, „Intelligence in a Data-Driven Age”, National Defense University Press, 2018, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1566262/intelligence-in-a-data-driven-age/https%3A%2F%2Fndupress.ndu.edu%2FMedia%2FNews%2FNews-Article-View%2FArticle%2F1566262%2Fintelligence-in-a-data-driven-age%2F.

Utilizări și aplicații

Iată câteva utilizări comune ale AI de către agențiile de informații:

- **Colectarea și procesarea datelor:** Sistemele IA pot colecta, curăța și procesa automat cantități mari de date structurate și nestructurate (”big data”) din diverse surse, inclusiv informații open-source, social media și documente clasificate. Această capacitate permite analiștilor să acceseze o gamă mai largă de informații rapid și eficient. Algoritmii AI pot analiza cantități mari de date din diverse surse, cum ar fi imagini din satelit, rețele sociale, interceptări de comunicare și multe altele, pentru a identifica modele și tendințe care ar putea să nu fie evidente pentru analiștii umani. Acest lucru poate ajuta la detectarea amenințărilor potențiale sau a activităților suspecte.
    - Web Scraping: AI poate automatiza colectarea de date dintr-o varietate de surse de pe internet, inclusiv social media, articole de știri și baze de date publice.
    - Analiza textului: procesarea limbajului natural (NLP) bazată pe inteligență artificială poate extrage informații valoroase din cantități mari de date text nestructurate, permițând analiștilor să identifice rapid tendințele, sentimentele și informațiile cheie.
    - Algoritmii AI pot fi utilizați pentru a procesa și analiza cantități mari de date, inclusiv informații open-source, imagini din satelit și conținut din rețelele sociale.
    - Tehnicile de învățare automată pot identifica modele, anomalii și potențiale amenințări din surse de date nestructurate. Algoritmii IA pot identifica modele și anomalii în cadrul datelor, permițând detectarea comportamentului neobișnuit sau a potențialelor amenințări. Acest lucru este deosebit de valoros în identificarea tendințelor emergente și a amenințărilor neconvenționale.
- **Procesarea limbajului natural (NLP):** Tehnologia NLP permite agențiilor să proceseze și să înțeleagă automat volume mari de date textuale, inclusiv rapoarte scrise, postări pe rețelele sociale, e-mailuri și multe altele. Analiza sentimentelor poate ajuta la măsurarea opiniei publice și a sentimentelor legate de diferite subiecte de interes.
    - NLP permite agențiilor să proceseze și să înțeleagă cantități mari de date textuale, inclusiv comunicații multilingve și criptate.
    - Analiza sentimentelor poate ajuta la înțelegerea opiniilor publice și la identificarea riscurilor potențiale. A poate fi folosită pentru a evalua sentimentul publicului pe platformele de social media și posturile de știri, oferind informații despre opinia publică, potențialele tulburări sau sprijinul public pentru anumite probleme sau actori.
    - Analiza comportamentală: prin monitorizarea comportamentului utilizatorului și a sistemului, analiza datelor poate identifica activitățile suspecte, ajutând la prevenirea amenințărilor interne.
- **Recunoașterea imaginilor, fețelor și video:** Algoritmii avansati de viziune computerizată permit analiza imaginilor și videoclipurilor pentru identificarea

obiectelor, locațiilor și indivizilor. Acest lucru este crucial pentru urmărirea și identificarea țintelor de interes. AI poate fi folosită pentru a analiza imagini și videoclipuri de la camere de supraveghere, drone sau alte surse pentru a identifica obiecte, persoane sau anomalii de interes. Tehnologiile de recunoaștere facială și de detectare a obiectelor sunt deosebit de relevante pentru eforturile de securitate și de combatere a terorismului.

- Viziunea computerizată bazată pe inteligență artificială poate analiza imagini și videoclipuri pentru a identifica obiecte, oameni și locații, ceea ce este valoros pentru urmărire și monitorizare.
- Instrumentele de analiză a imaginilor bazate pe inteligență artificială pot identifica obiecte, locații și chiar persoane în fotografii și videoclipuri.
- Tehnologia de recunoaștere facială ajută la identificarea potențialelor amenințări sau a persoanelor de interes.
- Serviciile de informații folosesc sisteme bazate pe inteligență artificială pentru a monitoriza și urmări activitățile indivizilor și grupurilor de interese.

- **Analiza vorbirii și audio:**
  - AI poate transcrie și analiza limbajul vorbit, făcându-l util pentru monitorizarea comunicărilor și conversațiilor în diferite limbi.
  - Tehnologia de recunoaștere a vorbirii poate transcrie și analiza înregistrări audio, ajutând agențiile de informații să monitorizeze și să urmărească conversațiile și să identifice vorbitori sau dialecte specifici.
- **Analiza geospațială**: AI poate procesa date geospațiale, cum ar fi imagini din satelit și date GPS, pentru a monitoriza mișcarea forțelor militare, dezvoltarea infrastructurii și alte aspecte geografice de interes.
- **Monitorizarea rețelelor sociale:**
  - AI poate cerceta cantități mari de date din rețelele sociale pentru a identifica amenințările emergente, pentru a urmări activitățile indivizilor sau a grupurilor și pentru a monitoriza sentimentele.
- **Vulnerabilități IoT**: Pe măsură ce Internetul Lucrurilor (IoT) crește, la fel crește și vulnerabilitățile acestor dispozitive, creând oportunități pentru atacatori de a compromite rețelele. Eterogeneitatea dispozitivelor IoT vin în diferite forme și dimensiuni, cu sisteme de operare, firmware și protocoale de comunicare diferite. Această diversitate creează un peisaj de securitate complex, ceea ce face dificilă implementarea măsurilor de securitate uniforme pe toate dispozitivele.
  Internetul obiectelor (IoT) include dispozitive cu senzori, capacitate de procesare, software și alte tehnologii care conectează și schimbă date cu alte dispozitive și sisteme prin Internet sau alte rețele de comunicații[4]. Există o serie de preocupări cu privire la confidențialitate și securitate datorate creșterii tehnologiilor și produselor IoT, care necesită abordări specifice din partea guvernelor pentru dezvoltarea de standarde internaționale și locale, orientări și cadre de reglementare[5]. În acest sens Internetul obiectelor militare (IoMT) este o clasă de Internet al obiectelor pentru

[4] Muhammad Shafiq et al., „The Rise of "Internet of Things": Review and Open Research Issues Related to Detection and Prevention of IoT-Based Security Attacks", Wireless Communications and Mobile Computing 2022 (3 august 2022): e8669348, https://doi.org/10.1155/2022/8669348.

[5] NYC, „NYC Office of Technology and Innovation - OTI", 2021, https://www.nyc.gov/content/oti/pages/.

operațiuni de luptă și război. O rețea complexă de entități interconectate care comunică continuu între ele pentru a coordona, învăța și interacționa cu mediul fizic, pentru a realiza o gamă largă de activități într-un mod mai eficient și mai informat[6]. Viitoarele bătălii militare vor fi dominate de inteligența mașinilor și războiul cibernetic[7]. În IoMT există posibilitatea de a încorpora în sistem obiecte neînsuflețite și inofensive, cum ar fi plante și roci, prin dotarea acestora cu senzori care le vor transforma în puncte de colectare a informațiilor[8]. În IoMT există posibilitatea de a încorpora în sistem obiecte neînsuflețite și inofensive, cum ar fi plante și roci, prin dotarea acestora cu senzori care le vor transforma în puncte de colectare a informațiilor[9]. În IoMT sunt esențiale comunicarea între entitățile implicate[10], și colaborarea reciprocă dintre agenții umani și entitățile electronice din rețea[11].

- **Identificarea amenințărilor:**
    - AI poate scana seturi vaste de date pentru a identifica indivizi sau entități de interes și pentru a urmări activitățile și asociațiile acestora de-a lungul timpului.
- **Evaluarea amenințărilor**: sistemele AI pot ajuta la evaluarea credibilității și severității amenințărilor și la prezicerea potențialelor activități teroriste prin analiza diferitelor surse de date, inclusiv comunicațiile online.
    - AI poate ajuta la evaluarea credibilității și gravității amenințărilor prin analizarea unei game largi de surse de date și identificarea indicatorilor comuni ai potențialelor amenințări.
    - Algoritmii AI pot identifica modele și anomalii în date, facilitând detectarea potențialelor amenințări sau tendințe care ar putea fi trecute cu vederea de către analiștii umani.
- **Analiza augmentată**: {004} 2 Ce este analiza cu inteligență augmentată? Analiza de inteligență sporită a fost diferit definită; dar în linii mari, este utilizarea AI pentru ca „...să îmbunătățească inteligența umană, mai degrabă decât să o opereze independent sau să o înlocuiască. Este conceput pentru a face acest lucru prin îmbunătățirea procesului decizional uman și, prin extensie, a acțiunilor întreprinse ca răspuns la deciziile îmbunătățite" (IEEE, 2019). Analiza augmentată a

[6] Lori Cameron, „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/.

[7] Alexander Kott, 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.

[8] Shalini Saxena, „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/.

[9] Friedemann Mattern și Christian Flörkemeier, „Vom Internet der Computer zum Internet der Dinge", *Informatik-Spektrum* 33, nr. 2 (1 aprilie 2010): 107–21, https://doi.org/10.1007/s00287-010-0417-7.

[10] Kim Gudeman, „Next-Generation Internet of Battle Things (IoBT) Aims to Help Keep Troops and Civilians Safe", 2017, https://ece.illinois.edu/newsroom/news/3875.

[11] William Lawless et al., „Connect the Dots on State-Sponsored Cyber Incidents - Compromise of the Czech Foreign Minister's Computer", Council on Foreign Relations, 2019, https://www.cfr.org/index.php/cyber-operations/compromise-czech-foreign-ministers-computer.

inteligenței a fost posibilă de noile dezvoltări ale tehnologiei AI, în special de dezvoltarea învățării automate și a învățării profunde. ; Brewster, 2021; Cornille, 2021; Marcum et al., 2017; Biroul Secretarului Apărării, 2017, 19; Pellerin, 2017; US Navy, 2019; [Taddeo et al., 2021]), contraterorism (Campedelli et al. al., 2021; Doyle et al., 2014; McKendrick, 2019; Rassler, 2021), poliție și combaterea criminalității (Dixon & Birks, 2021; Eggers și colab., 2019; GCHQ, 2021; Ni și colab., 2020; Serious Fraud Office, 2020; Vegt et al., 2022), monitorizarea drepturilor omului și utilizări umanitare (Freeman, 2021; Marin & Kalaitzis, 2020; Pizzi și colab., 2021; Ryan & Van Antwerp, 2019) și colectarea de informații supraveghere (Vieth & Wetzling, 2019).{004}

- **Fuziunea datelor:**
    - AI poate integra date din mai multe surse, inclusiv inteligența umană (HUMINT), inteligența semnalelor (SIGINT) și inteligența cu sursă deschisă (OSINT), pentru a oferi o imagine cuprinzătoare a unei situații.
- **Securitate cibernetică:** Securitatea cibernetică a devenit o componentă critică a lumii noastre digitale moderne. Odată cu integrarea tot mai mare a tehnologiei în fiecare aspect al vieții noastre, securitatea infrastructurii noastre digitale este de o importanță capitală. Acest eseu va aprofunda în analiza securității cibernetice, examinând principiile sale fundamentale, peisajul amenințărilor în evoluție, rolul analizei datelor în securitatea cibernetică și tendințele viitoare în acest domeniu. AI este utilizată pentru a detecta și a răspunde la amenințările cibernetice, inclusiv monitorizarea traficului de rețea pentru activități suspecte, identificarea vulnerabilităților și previziunea potențialelor atacuri cibernetice. Poate fi folosit și în operațiuni cibernetice ofensive.
    - Agențiile de informații folosesc AI pentru a îmbunătăți securitatea cibernetică prin detectarea și atenuarea amenințărilor cibernetice.
    - Sistemele de detectare a intruziunilor bazate pe inteligență artificială pot identifica activități și vulnerabilități neobișnuite ale rețelei.
    - Spionajul cibernetic este o amenințare omniprezentă și în evoluție, care ridică provocări semnificative pentru securitatea națională, interesele corporative și confidențialitatea individuală. Acest eseu academic oferă o analiză cuprinzătoare a spionajului cibernetic, explorând diferitele sale aspecte, de la motive și metode până la implicațiile pentru guverne, organizații și indivizi. În plus, examinează contramăsurile și strategiile folosite pentru a atenua riscurile asociate cu această formă din ce în ce mai sofisticată de criminalitate cibernetică.
    - Amenințările persistente avansate (APT) sunt o clasă de amenințări cibernetice care reprezintă o provocare semnificativă pentru organizații și națiuni din întreaga lume. APT-urile sunt cunoscute pentru tacticile, tehnicile și procedurile lor avansate, precum și pentru capacitatea lor de a se infiltra și de a opera în mod persistent în sistemele țintă pentru perioade îndelungate. Acest eseu își propune să ofere o analiză cuprinzătoare a APT-urilor, inclusiv caracteristicile, originile, metodele, consecințele și strategiile de apărare ale acestora. Amenințări persistente avansate (APT) reprezintă una dintre cele mai insidioase și provocatoare forme de

amenințări cibernetice, caracterizate prin sofisticarea, persistența și natura lor vizată.

- **Contraterorismul**: AI poate ajuta la identificarea persoanelor cu legături cu grupuri extremiste sau la detectarea difuzării online a conținutului extremist.
- **Simulări și modelare:**
    - AI poate fi folosit pentru a crea modele predictive și simulări pentru a înțelege mai bine situațiile geopolitice complexe, conflictele potențiale sau impactul schimbărilor de politică.
- **Analiza predictivă:** Modelele de învățare automată pot prognoza potențialele amenințări de securitate și evoluții geopolitice pe baza datelor istorice, evenimente curente și diferiți indicatori. Analiza predictivă ajută agențiile de informații să se pregătească în mod proactiv pentru potențialele amenințări. Învățarea automată poate ajuta la prezicerea evenimentelor sau amenințărilor viitoare pe baza datelor și tendințelor istorice, ajutând agențiile de informații să aloce resurse și să planifice în consecință.
    - AI poate ajuta la analiza predictivă prin evaluarea datelor istorice pentru a prognoza potențialele amenințări și tendințe de securitate.
    - Modelele de învățare automată pot ajuta la identificarea amenințărilor și vulnerabilităților emergente.
    - Modelele de învățare automată pot prezice evenimente sau tendințe viitoare pe baza datelor istorice, ajutând agențiile de informații să anticipeze potențiale riscuri de securitate.

Se așteaptă ca IA să fie deosebit de utilă în domeniul inteligenței, datorită seturilor mari de date disponibile pentru analiză[12]. Proiectul Maven încorporează viziunea computerizată și algoritmi IA în celulele de colectare a informațiilor pentru identificarea activităților ostile[13]. Agenția Centrală de Informații (CIA) are cca. 140 de proiecte în dezvoltare care folosesc IA[14]. IARPA lucrează la proiecte pentru dezvoltarea de algoritmi pentru recunoașterea și traducerea vorbirii multilingve în medii cu zgomot, localizarea geografică a imaginilor fără metadatele asociate, fuzionarea imaginilor 2D pentru a crea modele 3D și construirea de instrumente pentru deducerea funcției unei clădiri pe baza

[12] Congressional Research Service, „Artificial Intelligence and National Security (R45178)".

[13] Jack Corrigan, „Indian Strategic Studies: Three-Star General Wants AI in Every New Weapon System", 2017, https://www.strategicstudyindia.com/2017/11/three-star-general-wants-ai-in-every.html.

[14] Patrick Tucker, „What the CIA's Tech Director Wants from AI", Defense One, 6 septembrie 2017, https://www.defenseone.com/technology/2017/09/cia-technology-director-artificial-intelligence/140801/.

modelului de analiza vietii[15], și în domeniul logisticii militare pentru întreținerea predictivă a aeronavelor[16].

Pentru a combate tehnologiile false profunde (deep fake), DARPA a lansat proiectul Media Forensics (MediFor), care urmărește să „detecteze automat manipulările, să ofere informații detaliate despre modul în care au fost efectuate aceste manipulări și să argumenteze despre integritatea generală a media vizuale”[17], și SemaFor, care încearcă să dezvolte algoritmi care va detecta, atribui și caracteriza automat diferite tipuri de falsuri profunde[18].

Inteligența artificială poate fi utilizată și pentru a crea „modele digitale de viață”, în care „amprenta” digitală a unui individ este „combinată și corelată cu istoricul achizițiilor, rapoartele de credit, CV-urile profesionale și abonamentele” pentru a crea un profil comportamental cuprinzător[19].

DoD a dezvoltat un concept de Comandă comună a tuturor domeniilor și Control (JADC2)[20], pentru a crea o singură sursă de informații, cunoscută și sub denumirea de „imagine comună de funcționare”, pentru factorii de decizie[21].Serviciile de informații au dezvoltat proiecte înrudite, precum Proiectul Convergență al armatei și Sistemul avansat de management al luptei al Forțelor Aeriene[22], iar programul Mosaic Warfare al DARPA urmărește să folosească AI[23].

---

[15] IARPA, „Research Programs”, 2023, https://www.iarpa.gov/index.php/research-programs.

[16] Marcus Weisgerber, „Defense Firms to Air Force: Want Your Planes' Data? Pay Up”, Defense One, 19 septembrie 2017, https://www.defenseone.com/technology/2017/09/military-planes-predictive-maintenance-technology/141133/.

[17] William Corvey, „Media Forensics”, 2017, https://www.darpa.mil/program/media-forensics.

[18] Congressional Research Service, „Artificial Intelligence and National Security (R45178)”.

[19] Clint Watts, „Artificial Intelligence Is Transforming Social Media. Can American Democracy Survive?”, *Washington Post*, 28 octombrie 2021, https://www.washingtonpost.com/news/democracy-post/wp/2018/09/05/artificial-intelligence-is-transforming-social-media-can-american-democracy-survive/.

[20] Hoehn, „Defense Capabilities : Joint All Domain Command and Control / John R. Hoehn, Nishawn S. Smagh. - Vanderbilt University”, 2020, https://catalog.library.vanderbilt.edu/discovery/fulldisplay/alma991043717816903276/01VAN_INST:vanui.

[21] Colin Clark, „«Rolling The Marble:» BG Saltzman On Air Force's Multi-Domain C2 System”, *Breaking Defense* (blog), 8 august 2017, https://breakingdefense.sites.breakingmedia.com/2017/08/rolling-the-marble-bg-saltzman-on-air-forces-multi-domain-c2-system/.

[22] Jay Koester, „JADC2 'Experiment 2' Provides Looking Glass into Future Experimentation”, www.army.mil, 2020, https://www.army.mil/article/234900/jadc2_experiment_2_provides_looking_glass_into_future_experimentation.

[23] DARPA, „Strategic Technology Office Outlines Vision for “Mosaic Warfare””, 2017, https://www.darpa.mil/news-events/2017-08-04.

DOD testează alte capabilități ale IA pentru a permite comportamentul cooperant sau roitul (acțiunea simultană ”în roi” a unui număr mare de unități mici de atac)[24].

Concluzie

Pe măsură ce serviciile de informații integrează din ce în ce mai mult AI în operațiunile lor, beneficiile analizei îmbunătățite și măsurilor de securitate trebuie să fie cântărite în raport cu considerentele etice implicate. Găsirea unui echilibru între progresul tehnologic și protejarea drepturilor individuale este esențială pentru utilizarea responsabilă și etică a inteligenței artificiale în cadrul agențiilor de informații. Cercetarea continuă și dialogul sunt esențiale pentru a naviga în aceste probleme complexe și pentru a se asigura că IA servește drept forță pentru bine în domeniul securității naționale.

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.

[24] Mary-Ann Russon, „Google Robot Army and Military Drone Swarms: UAVs May Replace People in the Theatre of War”, International Business Times UK, 16 aprilie 2015, https://www.ibtimes.co.uk/google-robot-army-military-drone-swarms-uavs-may-replace-people-theatre-war-1496615.

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.

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.