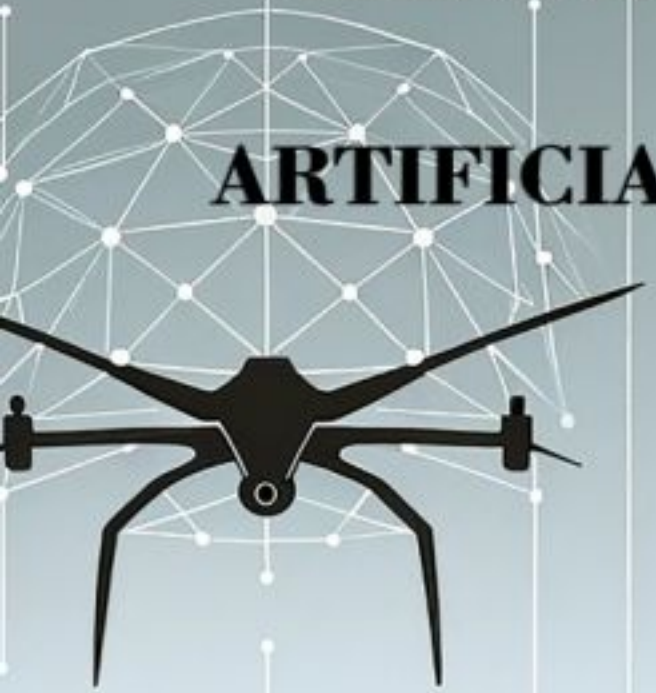
ELECTRONIC WARFARE
and
ARTIFICIAL INTELLIGENCE



Nicolae Sfetcu

MultiMedia Publishing

Electronic Warfare and Artificial Intelligence

BOOK PREVIEW

Nicolae SFETCU[1]

Published by MultiMedia

Sfetcu, Nicolae (2024), *Electronic Warfare and Artificial Intelligence*, MultiMedia Publishing, ISBN 978-606-033-844-4, DOI: 10.58679/MM14430, https://www.telework.ro/ro/e-books/electronic-warfare-and-artificial-intelligence/

Published by MultiMedia Publishing, https://www.telework.ro/en/publishing/

ISBN 978-606-033-844-4
DOI: 10.58679/MM14430
URL: https://www.telework.ro/ro/e-books/electronic-warfare-and-artificial-intelligence/

[1] Researcher - Romanian Academy - Romanian Committee of History and Philosophy of Science and Technology (CRIFST), Division of History of Science (DIS), ORCID: 0000-0002-0162-9973

Contents

Electronic Warfare and Artificial Intelligence

Phys. Eng. Nicolae SFETCU, MPhil

Abstract

Electronic warfare is a critical component of modern military operations and has undergone significant advances in recent years. This book 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

Electronic warfare

Electronic warfare (EW) assists air, ground, naval, and space forces at multiple levels of conflict by limiting the use of the radio frequency (RF) spectrum (Lazarov 2019). A nation's defense system relies on EMS for its command and control (C&C) infrastructure, communications links, weapon systems, and support technologies.

EW enables kinetic warfare, which is simply ineffective in modern warfare without EW (Duke 2023).

Definitions

Electronic warfare (EW) includes “Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy.” (Army 2016).

Electronic warfare includes three major subdivisions: electronic attack (EA), electronic protection (EP), and electronic warfare support (ES) (Army 2000, sec. I–1).

Electronic warfare refers to the use of electronic means in EMS to disrupt, deny, degrade, or deceive an adversary's information or communications systems without causing physical damage (Army 1996).

Information: Facts, data, or instructions in any medium or form. Information also refers to the meaning a human assigns to data through the known conventions used in representing it (Army 2016).

Information Operation (IO): IO is described as the integrated engagement of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC), along with specified support and related capabilities, to influence, disrupt, corrupt, or usurp adversarial and automated human decision-making while protecting us (Army 2020a).

Information Warfare (IW): Information operations conducted during a crisis or conflict to achieve or advance specific objectives on an adversary.

Information superiority: A state of equilibrium in one's favor in the information domain (Army 2020b, 8) or the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same (Army 2016, 257).

Information environment: The aggregate of people, organizations and systems that collect, process, disseminate or act on information (Army 2016, 257).

Electromagnetic environment: The resultant product of the power and time distribution, over various frequency ranges, of the levels of radiated or directed electromagnetic emissions likely to be encountered by a military force, system or platform when performing its assigned mission in its intended operational environment. It is the sum of electromagnetic interference; electromagnetic pulse; electromagnetic radiation hazards to personnel, artillery and volatile materials; and the effects of natural phenomena of lightning and static precipitation (Army 2016, 175).

Operational electromagnetic energy: A combination of the strength, frequency, and duration of electromagnetic emissions that may be encountered by a military force while performing its assigned mission (Army 2000, sec. I–1).

Directed energy: A general term that defines technologies related to the production of a beam of concentrated electromagnetic energy, atomic particles, or subatomic particles. It is used to damage or destroy an adversary's equipment, personnel, and installations (Army 2000, sec. I–4).

Electronic Intelligence (ELINT): The intelligence obtained from non-communicative external EM radiation. Electronic intelligence can be technical, geospatial or both (Kucukozyigit 2006).

Electronic security: The activity aimed at prohibiting unauthorized persons from accessing valuable information, resulting in the protection of friendly systems against activities such as interception or non-communications radiation (Kucukozyigit 2006).

Electronic reprogramming: Represents changes to EW and target-sensitive systems to accommodate changes in equipment, tactics, and the EM environment. These changes can be due to friendly or hostile activities. The desired outcome of electronic reprogramming is to support and increase the effectiveness of sensitive EW and targeting systems and devices used in defensive or offensive weapons and intelligence collection systems (Kucukozyigit 2006).

Emission Control (EMCON): The selective and controlled use of EM, acoustic and other emitters to achieve optimal C&C capabilities (Kucukozyigit 2006).

Spectrum management: is the planning, coordination and management of the EM spectrum. The objective is to create an EM environment in which friendly electronic systems can perform their functions without interference or confusion (Army 2000, sec. I-6–7).

Historical development

Electronic warfare has its roots in early radio and radar technologies. They can be traced back to the US Civil War in 1861. With the outbreak of the Civil War in 1861, telegraph wires became one of the most important targets. Military telegraph traffic was diverted to the wrong destinations, false orders were passed to Union commanders, and wires were cut to intercept information to Union forces (Price 1984, 1–2). These can be considered early applications of command, control, communications and intelligence (C3I), early examples of intelligence, jamming and deception (J. P. R. Browne and Thurbon 1998, 3).

The earliest documented use of EW was during the Boer War (1899–1902), when the British Army used a searchlight for Morse code signals from the clouds. The Boers noticed this and used one of their own searchlights in an attempt to jam the British signals (Judd and Surridge 2013).

The first known case of intentional jamming was, surprisingly, not for military purposes, but for civilian purposes, during the 1901 America's Cup yacht races in the United States. That

year, Marconi obtained a contract from the Associated Press. Another company, the Wireless Telegraph Company of America, also won a contract. A third company, the American Wireless Telephone and Telegraph Co., was unable to secure a sponsor, so it decided to jam the others using a more powerful transmitter (Price 1984, 3).

The first intentional use of radio jamming by the military occurred in 1902 during British naval exercises in the Mediterranean, then in 1903 during US naval maneuvers (Price 1984, 4).

During the Russo-Japanese War of 1904–1905, the Japanese located the Russian fleet in the Tsushima Strait and transmitted the information "wirelessly" to the Japanese fleet headquarters. On July 13, 1904, Russian wireless telegraph stations successfully disrupted communication between a group of Japanese battleships. This was also the first example of electronic countermeasures. Later, the captain of the Russian warship Ural requested permission to disrupt Japanese communications with a stronger radio signal, but Russian Admiral Zinovy Rozhestvensky refused, thus allowing the Japanese to win a decisive battle at Tsushima (Rambo 2009).

During World War I and World War II, EW primarily involved radio jamming and radar deception. In 1939, just before the outbreak of World War II, the first ELINT mission was carried out by the German airship Graf Zeppelin along the east coast of Great Britain (Kucukozyigit 2006).

In World War II, the Allies turned to EW in the "Battle of the Beams", using navigational radars to direct bombers, with adversaries attempting to defeat those navigational radars (Rambo 2009). Chaff' was used by the Royal Air Force (code name Window) during World War II to defeat radar tracking systems (McArthur 1990). In the first example of ECCM, the Germans increased the power of their radio transmitter in an attempt to "get through" or overcome British jamming, and this is still one of the main methods of ECCM today.

The Cold War era saw substantial advances in electronic warfare as the superpowers engaged in a technological arms race to overcome each other's surveillance and communications systems. Cold War developments included anti-radiation missiles designed to target enemy radar transmitters (Polmar 1979).

In the first example of ECCM, the Germans increased the power of their radio transmitter in an attempt to "get through" or overcome British jamming, and this is still one of the main methods of ECCM today.

The Cold War era saw substantial advances in electronic warfare as superpowers engaged in a technological arms race to outsmart each other's surveillance and communications systems. Cold War developments included anti-radiation missiles designed to target enemy radar transmitters (Polmar 1979).

During the Korean War (1950–1953) under General Mac Arthur, the US deployed 100 B-29 Superfortress heavy bombers to the theater of war. The North Koreans installed early warning radars and radar-controlled anti-aircraft artillery (AAA), so that aircraft losses became unacceptable (J. P. R. Browne and Thurbon 1998, 26).

Electronic warfare also played a major role during the Vietnam War, where aircraft often relied on EW to survive the battle, although the Vietnamese ECCM operated successfully (Dickson 1987).

In the First Gulf War (Operation DESERT STORM) in 1991, stealth fighters ventured into enemy airspace dropping decoys to trigger enemy radar into action; some carrying anti-radiation missiles that activated instantly as the radars appeared (Campen 1992, XIV).

In 2007, an Israeli strike during Operation Outside the Box (or Operation Orchard) used EW to disrupt Syria's air defenses (Fulghum and Wall 2007) (Katz 2010).

In the early days of the Russian invasion of Ukraine in 2022, Russian EW disrupted enemy radars and communications, disrupting ground-based air defense systems as well as their own communications (Bronk, Reynolds, and Watling 2022). Russian ability to disrupt GPS signals is credited with reducing the success of Ukrainian use of HIMARS and JDAM bombs (Mizokami 2023). According to a report by the Royal United Services Institute on May 19, 2023, Ukraine had lost approximately 10,000 drones per month due to Russian electronic warfare (Jankowicz 2023).

In modern warfare, electronic warfare has become a critical component. With the integration of sophisticated sensors, communication systems and information networks, the electromagnetic spectrum is crowded and contested. EW plays a vital role in gaining the edge in terms of situational awareness and tactical advantage.

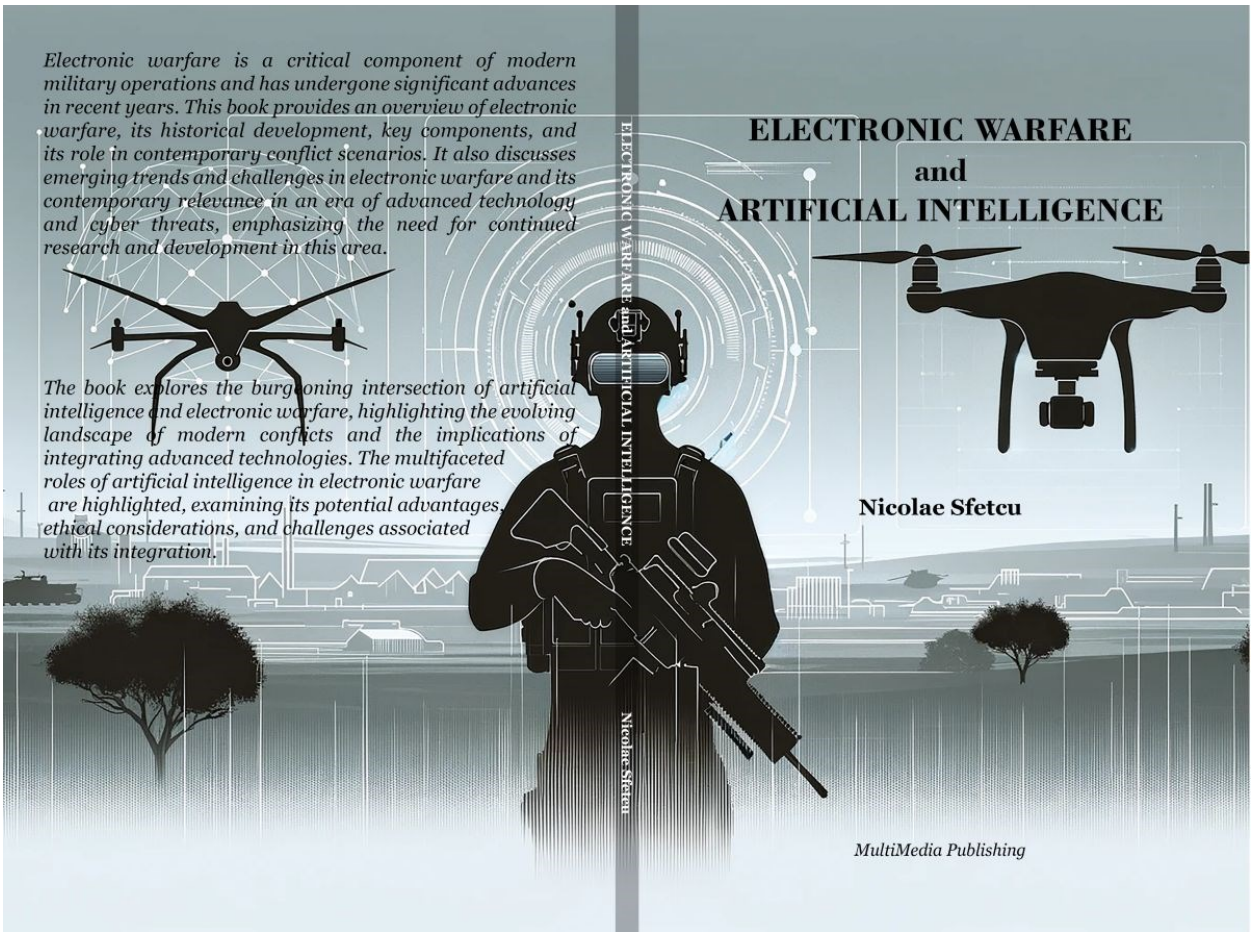
EW in asymmetric warfare: EW is not exclusive to conventional warfare. It has gained importance in asymmetric conflicts, counterinsurgency operations, and counterterrorism efforts. Insurgent groups and non-state actors have also adopted rudimentary electronic warfare techniques.

Cyber-electronic convergence: The convergence of cyber warfare and electronic warfare has seen significant development. Adversaries are increasingly using cyber-attacks to disrupt electronic systems, blurring the lines between the two domains.

Space and electromagnetic spectrum dominance: As space becomes a critical domain for military operations, control of the electromagnetic spectrum in space is paramount. Satellites and space assets are vulnerable to EW attacks.

Contents

Book



Electronic warfare is a critical component of modern military operations and has undergone significant advances in recent years. This book 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.

MultiMedia Publishing https://www.telework.ro/ro/e-books/electronic-warfare-and-artificial-intelligence/ https://www.cartilibrarie.com/carte/electronic-warfare-and-artificial-intelligence/

- Digital: EPUB (ISBN 978-606-033-842-0), Kindle (ISBN 978-606-033-843-7) PDF (ISBN 978-606-033-844-4)

- Print (Blurb)

DOI: 10.58679/MM14430

Publishing date: 20.05.2024

Bibliography

* * *. 1984. *Voennyi Entsiklopedicheskii Slovar*. Moscova: Voennoe Izadatelstvo.

———. 1990. *Voenno-Morskoi Slovar*. Moscova: Voennoe Izadatelstvo.

———. 2000. "Electronic Warfare Fundamentals." https://falcon.blu3wolf.com/Docs/Electronic-Warfare-Fundamentals.pdf.

Adams, Charlotte. 2018. "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/.

Adamy, David. 2001. *EW 101: A First Course in Electronic Warfare*. Artech House.

AIM. 2019. "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, and Karl Erik Olsen. 2018. "A Neural Network Target Detector with Partial CA-CFAR Supervised Training." In *2018 International Conference on Radar (RADAR)*, 1–6. https://doi.org/10.1109/RADAR.2018.8557276.

Allen, Gregory C. 2019. *Understanding China's AI Strategy: Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security*. Center for a New American Security.

Allen, John, and Giampiero Massolo. 2020. *The Global Race for Technological Superiority. Discover the Security Implication*. Edited by Fabio Rugge. Milan: Ledizioni.

Amuru, SaiDhiraj, Cem Tekin, Mihaela van der Schaar, and R. Michael Buehrer. 2015. "A Systematic Learning Method for Optimal Jamming." In *2015 IEEE International Conference on Communications (ICC)*, 2822–27. https://doi.org/10.1109/ICC.2015.7248754.

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 Publication JP 3-13 Information Operations Change 1 November 2014*. Independently Published.

———. 2020b. "Joint Vision 2020: America's Military - Preparing for Tomorrow." https://apps.dtic.mil/sti/citations/ADA526044.

Baker, James E. 2018. "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, and Bahaeddin Eravci. 2012. "Automatic Radar Antenna Scan Type Recognition in Electronic Warfare." *IEEE Transactions on Aerospace and Electronic Systems* 48 (4): 2908–31. https://doi.org/10.1109/TAES.2012.6324669.

Bronk, Justin, Nick Reynolds, and 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.

Brooks, Risa. 2018. "Technology and Future War Will Test U.S. Civil-Military Relations." War on the Rocks. November 26, 2018. https://warontherocks.com/2018/11/technology-and-future-war-will-test-u-s-civil-military-relations/.

Browne, J. P. R., and Michael T. Thurbon. 1998. *Electronic Warfare*. Brassey's.

Browne, Jack. 2017. "Cognitive EW Provides Computer-Powered Protection." Microwaves & RF. May 10, 2017. https://www.mwrf.com/markets/defense/article/21848321/cognitive-ew-provides-computerpowered-protection.

Brunt, Leroy B. Van. 1978. *Applied ECM*. EW Engineering.

BSI. 2023. "Federal Office for Information Security." Federal Office for Information Security. November 6, 2023. https://www.bsi.bund.de/EN/Home/home_node.html.

Butt, Faran, and Madiha Jalil. 2013. *An Overview of Electronic Warfare in Radar Systems*. https://doi.org/10.1109/TAEECE.2013.6557273.

Cameron, Lori. 2018. "Internet of Things Meets the Military and Battlefield: Connecting Gear and Biometric Wearables for an IoMT and IoBT." IEEE Computer Society. March 1, 2018. https://www.computer.org/publications/tech-news/research/internet-of-military-battlefield-things-iomt-iobt/.

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

Carlin, John P. 2016. "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, and Matthew J. Thommana. 2022. "Applications of Machine Learning for Electronic Warfare Emitter Identification and Resource Management." https://secwww.jhuapl.edu/techdigest/content/techdigest/pdf/V36-N02/36-02-Casterline.pdf.

Chen, Jian, Shiyou Xu, Jiangwei Zou, and Zengping Chen. 2019. "Interrupted-Sampling Repeater Jamming Suppression Based on Stacked Bidirectional Gated Recurrent Unit Network and Infinite Training." *IEEE Access* 7:107428–37. https://doi.org/10.1109/ACCESS.2019.2932793.

Clark, Colin. 2018. "Russia Widens EW War, 'Disabling' EC-130s OR AC-130s In Syria." *Breaking Defense* (blog). April 24, 2018.

https://breakingdefense.sites.breakingmedia.com/2018/04/russia-widens-ew-war-disabling-ec-130s-in-syria/.

Coats, Daniel. 2021. "Intelligence Community Information Environment (IC IE) - Data Strategy." https://www.dni.gov/files/documents/CIO/Data-Strategy_2017-2021_Final.pdf.

Congressional Research Service. 2020. "Artificial Intelligence and National Security (R45178)." 2020. https://crsreports.congress.gov/product/details?prodcode=R45178.

Copp, Tara. 2021. "'It Failed Miserably': After Wargaming Loss, Joint Chiefs Are Overhauling How the US Military Will Fight." Defense One. July 26, 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. 2017. "Internet of Battlefield Things (IoBT) CRA – DEVCOM Army Research Laboratory." 2017. https://arl.devcom.army.mil/cras/iobt-cra/.

CRS. 2022. "Defense Primer: Electronic Warfare." https://sgp.fas.org/crs/natsec/IF11118.pdf.

CS Europe. 2023. "Cyber Security Europe | Cyber Security Insight for Boardroom and C-Suite Executives." Cyber Security Europe. 2023. https://www.cseurope.info/.

Davenport, Thomas, and Ravi Kalakota. 2019. "The Potential for Artificial Intelligence in Healthcare." *Future Healthc J* 6 (2): 94–98. https://doi.org/10.7861/futurehosp.6-2-94.

Davis, Zachary. 2019. "Artificial Intelligence on the Battlefield: Implications for Deterrence and Surprise." *PRISM* 8 (2): 114–31.

Day, Peter. 2016. "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, and Tim Sweijs. 2017. *Artificial Intelligence and the Future of Defense*.

Department of Defense. 2018. "Summary of the 2018 National Defense Strategy." https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

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

DOD. 2020. "DoD Data Strategy." https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF.

DoD. 2022. "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.

Doskalov, Mikhail. 2013. "Perspektivy Razvitiia Sistemy Radioelektronnoi Borby Rossiiskoj Federatsii Na Period Do 2020 Goda." In *Oboronnyi Kompleks RF: Sostoianie i Razvitie*. http://federalbook.ru/files/OPK/Soderjanie/OPK-9/III/Doskalov.pdf.

Dudczyk, Janusz, and A. Kawalec. 2013. "Specific Emitter Identification Based on Graphical Representation of the Distribution of Radar Signal Parameters." *Jokull* 63 (November):408–16.

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

Dunn Cavelty, Myriam. 2012. "Cyber-Allies: Strengths and Weaknesses of NATO's Cyberdefense Posture." SSRN Scholarly Paper. Rochester, NY. https://papers.ssrn.com/abstract=1997153.

EASA. 2020. "Concepts of Design Assurance for Neural Networks (CoDANN)." 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, and Yonina C. Eldar. 2019. "Cognitive Radar Antenna Selection via Deep Learning." arXiv. https://doi.org/10.48550/arXiv.1802.09736.

EMK, SU. 2023. "ECHO Network." 2023. https://echonetwork.eu/.

European Defence Agency. 2023. "Enhancing EU Military Capabilities Beyond 2040." https://eda.europa.eu/docs/default-source/eda-publications/enhancing-eu-military-capabilities-beyond-2040.pdf.

Freedberg, Sydney J. 2014. "US Has Lost 'Dominance In Electromagnetic Spectrum': Shaffer." *Breaking Defense* (blog). September 3, 2014. https://breakingdefense.com/2014/09/us-has-lost-dominance-in-electromagnetic-spectrum-shaffer/.

———. 2017. "Electronic Warfare 'Growing'; Joint Airborne EW Study Underway." *Breaking Defense* (blog). June 23, 2017. https://breakingdefense.sites.breakingmedia.com/2017/06/electronic-warfare-growing-joint-airborne-ew-study-underway/.

Friedrich, Nancy. 2020. "AI and Machine Learning Redefine the EW Landscape | 2020-12-08 | Microwave Journal." 2020. https://www.microwavejournal.com/articles/35107-ai-and-machine-learning-redefine-the-ew-landscape.

Fulghum, David A., and Robert Wall. 2007. "Israel Shows Electronic Prowess | Aviation Week Network." 2007. https://aviationweek.com/israel-shows-electronic-prowess.

Gambrell, Dorothy, and Charissa Isidro. 2022. "A Visual Guide to the World's Military Budgets." *Bloomberg.Com*, March 11, 2022. https://www.bloomberg.com/news/features/2022-03-11/the-largest-militaries-visualized.

Gannon, Brian P. 2023. "Implement AI in Electromagnetic Spectrum Operations." U.S. Naval Institute. August 1, 2023. https://www.usni.org/magazines/proceedings/2023/august/implement-ai-electromagnetic-spectrum-operations.

Gao, Jingpeng, Yi Lu, Junwei Qi, and Liangxi Shen. 2019. "A Radar Signal Recognition System Based on Non-Negative Matrix Factorization Network and Improved Artificial Bee Colony Algorithm." *IEEE Access* 7:117612–26. https://doi.org/10.1109/ACCESS.2019.2936669.

Gecgel Cetin, Selen, Caner Goztepe, and Gunes Karabulut Kurt. 2019. *Jammer Detection Based on Artificial Neural Networks: A Measurement Study*. https://doi.org/10.1145/3324921.3328788.

Gigova, Radina. 2017. "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, and Aaron Courville. 2016. *Deep Learning: Adaptive Computation and Machine Learning Series*. MIT Press.

Grant, P. M., and J. H. Collins. 1982. "Introduction to Electronic Warfare." *IEE Proceedings F (Communications, Radar and Signal Processing)* 129 (3): 113–32. https://doi.org/10.1049/ip-f-1.1982.0020.

Gulhane, Tejaswi Singh and Amit. 2018. "8 Key Military Applications for Artificial Intelligence." 2018. https://blog.marketresearch.com/8-key-military-applications-for-artificial-intelligence-in-2018.

Guzenko, V. F., and A. L. Moraresku. 2017. *Radioelektronnaia Borba. Sovremennoe Soderzhanie*. Moscova: Informatsionnyi Most.

Haigh, Karen Zita, and Julia Andrusenko. 2021. *Cognitive Electronic Warfare: An Artificial Intelligence Approach*. Artech House.

Hamilton, Serena, A.J. Jakeman, and John Norton. 2008. "Artificial Intelligence Techniques: An Introduction to Their Use for Modelling Environmental Systems." *Mathematics and Computers in Simulation* 78 (July):379–400. https://doi.org/10.1016/j.matcom.2008.01.028.

Haney, Brian. 2019. "Applied Artificial Intelligence in Modern Warfare and National Security Policy." SSRN Scholarly Paper. Rochester, NY. https://doi.org/10.2139/ssrn.3454204.

Henney, Megan. 2019. "Big Tech Has Spent $582M Lobbying Congress. Here's Where That Money Went." Text.Article. FOXBusiness. Fox Business. May 8, 2019. https://www.foxbusiness.com/technology/amazon-apple-facebook-google-microsoft-lobbying-congress.

Hoehn, John. 2021. "Defense Primer: What Is Command and Control?" https://apps.dtic.mil/sti/citations/AD1169627.

Insinna, Valerie. 2022. "China Could Obtain 1,500 Nuclear Warheads by 2035, Pentagon Estimates." *Breaking Defense* (blog). November 29, 2022. https://breakingdefense.sites.breakingmedia.com/2022/11/china-to-obtain-1500-nuclear-warheads-by-2035-pentagon-estimates/.

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, and Keith Surridge. 2013. *The Boer War: A History*. Bloomsbury Academic.

Junfei, Yu, Li Jingwen, Sun Bing, and Jiang Yuming. 2018. "Barrage Jamming Detection and Classification Based on Convolutional Neural Network for Synthetic Aperture Radar." In *IGARSS 2018 - 2018 IEEE International Geoscience and Remote Sensing Symposium*, 4583–86. https://doi.org/10.1109/IGARSS.2018.8519373.

Kadlecová, Lucie, Nadia Meyer, Rafaël Cos, and Pauline Ravinet. 2020. "Mapping the Role of Science Diplomacy in the Cyber Field."

Kang, Li, Jiu Bo, Liu Hongwei, and Liang Siyuan. 2018. "Reinforcement Learning Based Anti-Jamming Frequency Hopping Strategies Design for Cognitive Radar." In *2018 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC)*, 1–5. https://doi.org/10.1109/ICSPCC.2018.8567751.

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

Kjellén, Jonas. 2018. "Russian Electronic Warfare - The Role of Electronic Warfare in the Russian Armed Forces." 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., and I. G. Nasenkov. 2015. *Radioelektronnaia Borba. Ot Eksperimentov Proshlogo Do Reshayushchego Fronta Budushchego*. Moscova: Centre for Analysis of Strategies and Technologies (CAST).

Kolhatkar, Sheelah. 2019. "How Elizabeth Warren Came Up with a Plan to Break Up Big Tech." *The New Yorker*, August 20, 2019. https://www.newyorker.com/business/currency/how-elizabeth-warren-came-up-with-a-plan-to-break-up-big-tech.

Kott, Alexander. 2018. "Challenges and Characteristics of Intelligent Autonomy for Internet of Battle Things in Highly Adversarial Environments," March.

Kott, Alexander, David S. Alberts, and Cliff Wang. 2015. "Will Cybersecurity Dictate the Outcome of Future Wars?" *Computer* 48 (12): 98–101. https://doi.org/10.1109/MC.2015.359.

Krylov, G. O., S. L. Larionova, and Nikitina. 2017. *Bazovye Poniatiia Informatsionnoi Bezopasnosti*. Moscova: OOO RUSAJNS.

Kube, Courtney. 2018. "Russia Is Jamming American Drones in Syria, Officials Say." NBC News. April 10, 2018. https://www.nbcnews.com/news/military/russia-has-figured-out-how-jam-u-s-drones-syria-n863931.

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

Lakhin, Andrei, and Andrei Korobeinikov. 2016. *Sostoianie i Perspektivy Razvitiia Voisk Radioelektronnoi Borby Vooruzhennykh Sil Rossiiskoi Federatsii*. Moscova: Informatsionnyi Most.

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)*, March, 1–3. https://doi.org/10.1109/CREBUS.2019.8840074.

Lee, Gyeong-Hoon, Jeil Jo, and Cheong Hee Park. 2020. "Jamming Prediction for Radar Signals Using Machine Learning Methods." *Security and Communication Networks* 2020 (January):e2151570. https://doi.org/10.1155/2020/2151570.

Li, Huiqin, Yanling Li, Chuan He, Jianwei Zhan, and Hui Zhang. 2021. "Cognitive Electronic Jamming Decision-Making Method Based on Improved Q -Learning Algorithm." *International Journal of Aerospace Engineering* 2021 (December):1–12. https://doi.org/10.1155/2021/8647386.

Li, Xueqiong, Zhitao Huang, Fenghua Wang, Xiang Wanga, and Tianrui Liu. 2018. "Toward Convolutional Neural Networks on Pulse Repetition Interval Modulation Recognition." *IEEE Communications Letters* PP (August):1–1. https://doi.org/10.1109/LCOMM.2018.2864725.

Li, Yangyang, Ximing Wang, Dianxiong Liu, Qiuju Guo, Xin Liu, Jie Zhang, and Yitao Xu. 2019. "On the Performance of Deep Reinforcement Learning-Based Anti-Jamming Method Confronting Intelligent Jammer." *Applied Sciences* 9 (7): 1361. https://doi.org/10.3390/app9071361.

Liao, Xiaofeng, Bo Li, and Bo Yang. 2018. "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 (November):e1458962. https://doi.org/10.1155/2018/1458962.

Liu, Yemin, Shiqi Xing, Y. Li, Dong Hou, and Wang Xuesong. 2017. "Jamming Recognition Method Based on the Polarization Scattering Characteristics of Chaff Clouds." *IET Radar, Sonar & Navigation* 11 (August). https://doi.org/10.1049/iet-rsn.2017.0121.

Liubin, Mikhail Dmitriyevich. 2009. “K Voprosu Ob Istorii Razvitiia i Perspektivakh Radioelektronnoi Borby.” *Voennaia Mysl*, no. 3, 64–75.

Magrassi, Paolo. 2002a. *A World of Smart Objects: The Role of Auto-Identification Technologies*.

———. 2002b. *Why a Universal RFID Infrastructure Would Be a Good Thing*.

MarketsAndMarkets. 2023. “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. 2012. *Introduction to Modern EW Systems*. Artech House.

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

McDermott, Roger N. 2017. “Russia’s Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum.” ICDS. September 17, 2017. https://icds.ee/en/russias-electronic-warfare-capabilities-to-2025-challenging-nato-in-the-electromagnetic-spectrum/.

MeriTalk. 2018. “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. 2019. “BAE Bets on Use of Artificial Intelligence in Electronic Warfare.” Microwaves & RF. July 15, 2019. https://www.mwrf.com/markets/defense/article/21849838/bae-systems-bae-bets-on-use-of-artificial-intelligence-in-electronic-warfare.

Ministry of Defence. 2021a. “Data Strategy for Defence.” GOV.UK. 2021. https://www.gov.uk/government/publications/data-strategy-for-defence.

———. 2021b. “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.

———. 2022. “Defence Artificial Intelligence Strategy.” GOV.UK. 2022. https://www.gov.uk/government/publications/defence-artificial-intelligence-strategy/defence-artificial-intelligence-strategy.

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

NATO. 2019. “The 107th NATO Electronic Warfare Advisory Committee (NEWAC) Convenes in Brussels.” NATO. 2019. https://www.nato.int/cps/en/natohq/news_171280.htm.

———. 2023. “Electromagnetic Warfare.” NATO. 2023. https://www.nato.int/cps/en/natohq/topics_80906.htm.

Neri, F. 1991. “Introduction to Electronic Defense Systems.” In . https://www.semanticscholar.org/paper/Introduction-to-electronic-defense-systems-Neri/8d8aed6d92ecf7af850f09a2ee740380c2d4b366.

Noh, Sanguk, and Unseob Jeong. 2010. “Intelligent Command and Control Agent in Electronic Warfare Settings.” *International Journal of Intelligent Systems* 25 (6): 514–28. https://doi.org/10.1002/int.20413.

Northrop. 2022. “Electronic Warfare and Sensors.” https://info.breakingdefense.com/hubfs/E-Book_EW_&_Sensors_Northrop_Grumman_Breaking_Defense.pdf.

ODIN. 2023. "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.

Parker, Paul. 2018. "The Internet of Battlefield Things Is Coming. Are IT Pros Ready?" C4ISRNet. October 3, 2018. https://www.c4isrnet.com/opinion/2018/10/03/the-internet-of-battlefield-things-is-coming-are-it-pros-ready/.

Petrov, Nedyalko, Ivan Jordanov, and Jon Roe. 2013. "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 (January):1192–1200. https://doi.org/10.1016/j.procs.2013.09.206.

Poisel, Richard. 2008. *Introduction to Communication Electronic Warfare Systems*. Artech House.

Polit, Kate. 2018. "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. 1979. "The U. S. Navy: Electronic Warfare (Part 2)." U.S. Naval Institute. November 1, 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.

Qiang, Xing, Zhu Wei-gang, and Bo Yuan. 2018. "Jamming Style Selection for Small Sample Radar Jamming Rule Base." *2018 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC)*, September, 1–5. https://doi.org/10.1109/ICSPCC.2018.8567613.

Qu, Zhiyu, Wenyang Wang, Changbo Hou, and Chenfan Hou. 2019. "Radar Signal Intra-Pulse Modulation Recognition Based on Convolutional Denoising Autoencoder and Deep Convolutional Neural Network." *IEEE Access* 7:112339–47. https://doi.org/10.1109/ACCESS.2019.2935247.

Rahman, H. 2019. *Introduction to Electronic Defense Systems*. Boca Raton, FL, USA: CRC Press.

Rambo. 2009. "Information Warfare: History of Electronic Warfare." *INFORMATION WARFARE* (blog). December 7, 2009. https://ew30.blogspot.com/2009/12/such-is-reliance-on-electromagnetic-em.html.

Rogosa, Alexander. 2015. "Shifting Spaces: The Success of the SpaceX Lawsuit and the Danger of Single-Source Contracts in America's Space Program." *Federal Circuit Bar Journal* 25:101.

Rowlands, Greg. 2017. "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, and Tarek Abdelzaher. 2018. "The Internet of Battlefield Things: The Next Generation of Command, Control, Communications and Intelligence (C3I) Decision-Making." In *MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM)*, 737–42. https://doi.org/10.1109/MILCOM.2018.8599853.

Saxena, Shalini. 2017. "Researchers Create Electronic Rose Complete with Wires and Supercapacitors." Ars Technica. March 1, 2017. https://arstechnica.com/science/2017/03/researchers-grow-electronic-rose-complete-with-wires-and-supercapacitors/.

Sfetcu, Nicolae. 2023a. "Evoluția inteligenței artificiale în domeniul securității naționale." Intelligence Info. November 10, 2023. https://www.intelligenceinfo.org/evolutia-inteligentei-artificiale-in-domeniul-securitatii-nationale/.

———. 2023b. "Rolul serviciilor de informații în război." Intelligence Info. August 3, 2023. https://www.intelligenceinfo.org/rolul-serviciilor-de-informatii-in-razboi/.

———. 2024. "Războiul electronic și inteligența artificială." MultiMedia. January 8, 2024. https://www.telework.ro/ro/e-books/razboiul-electronic-si-inteligenta-artificiala/.

Shankar, M., and B. Mohan. 2013. "Recent Advances in Electronic Warfare-ESM Systems." In . https://www.semanticscholar.org/paper/RECENT-ADVANCES-IN-ELECTRONIC-WARFARE-ESM-SYSTEMS-Shankar-Mohan/bf6e4c372514695dd167eebf6f9dfb78ca120f6a.

Shao, Guangqing, Yushi Chen, and Yinsheng Wei. 2020. "Convolutional Neural Network-Based Radar Jamming Signal Classification With Sufficient and Limited Samples." *IEEE Access* 8:80588–98. https://doi.org/10.1109/ACCESS.2020.2990629.

Sharma, Purabi, Kandarpa Kumar Sarma, and Nikos E. Mastorakis. 2020. "Artificial Intelligence Aided Electronic Warfare Systems- Recent Trends and Evolving Applications." *IEEE Access* 8:224761–80. https://doi.org/10.1109/ACCESS.2020.3044453.

Silicon Labs. 2013. "The Evolution of Wireless Sensor Networks." https://www.silabs.com/documents/public/white-papers/evolution-of-wireless-sensor-networks.pdf.

Simonite, Tom. 2017. "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., and Allan Friedman. 2014. *Cybersecurity: What Everyone Needs to Know*. OUP USA.

Singh, Mohinder. 1988. "Electronic Warfare." https://www.drdo.gov.in/sites/default/files/publcations-document/Electronic%20Warfare.pdf.

Skolnik, Merrill I. 2008. *Radar Handbook, Third Edition*. McGraw-Hill Education.

Smith, Craig. 2019. "Eye On AI." Eye On AI. August 28, 2019. https://www.eye-on.ai.

Smith, Patrick. 2022. *Russian Electronic Warfare: A Growing Threat to U.S. Battlefield Supremacy*. American Security Project.

Smith, Ron, and Scott Knight. 2005. "Applying Electronic Warfare Solutions to Network Security - Canadian Military Journal." 2005. http://www.journal.forces.gc.ca/vo6/no3/electron-eng.asp.

SPARTA. 2023. "SPARTA Consortium." 2023. https://www.cybersecurityintelligence.com/sparta-consortium-5594.html.

Stackpole, Beth. 2016. "Keeping the Connected Soldier Connected with Simulation." Digital Engineering. September 1, 2016. https://www.digitalengineering247.com/article/keeping-the-connected-soldier-connected-with-simulation.

State Council. 2017. "A Next Generation Artificial Intelligence Development Plan." *China Copyright and Media* (blog). July 20, 2017. https://chinacopyrightandmedia.wordpress.com/2017/07/20/a-next-generation-artificial-intelligence-development-plan/.

Sydney J. Freedberg Jr. 2020. "Project Rainmaker: Army Weaves 'Data Fabric' To Link Joint Networks." *Breaking Defense* (blog). November 17, 2020.

https://breakingdefense.sites.breakingmedia.com/2020/11/project-rainmaker-army-weaves-data-fabric-to-link-joint-networks/.

Taddeo, Mariarosaria. 2012. "An Analysis for a Just Cyber Warfare." In *2012 4th International Conference on Cyber Conflict (CYCON 2012)*, 1–10. https://ieeexplore.ieee.org/document/6243976.

Tang, Author: Hazel. 2020. "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). April 9, 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. 2022. "The Vulnerability of AI Systems May Explain Why Russia Isn't Using Them Extensively in Ukraine." Forbes. 2022. https://www.forbes.com/sites/erictegler/2022/03/16/the-vulnerability-of-artificial-intelligence-systems-may-explain-why-they-havent-been-used-extensively-in-ukraine/.

Tegmark, Max. 2018. "Life 3.0: Being Human in the Age of Artificial Intelligence | Mitpressbookstore." July 31, 2018. https://mitpressbookstore.mit.edu/book/9781101970317.

Tsui, Chi-Hao Cheng, James. 2022. *An Introduction to Electronic Warfare; from the First Jamming to Machine Learning Techniques*. New York: River Publishers. https://doi.org/10.1201/9781003337171.

Tucker, Patrick. 2022. "AI Is Already Learning from Russia's War in Ukraine, DOD Says." Defense One. April 21, 2022. https://www.defenseone.com/technology/2022/04/ai-already-learning-russias-war-ukraine-dod-says/365978/.

US Marine Corps. 2016. "Electronic Warfare." https://www.marines.mil/Portals/1/Publications/MCRP%203-32D.1%20(Formerly%20MCWP%203-40.5).pdf.

Vincent, James. 2017. "Elon Musk and AI Leaders Call for a Ban on Killer Robots." The Verge. August 21, 2017. https://www.theverge.com/2017/8/21/16177828/killer-robots-ban-elon-musk-un-petition.

Waghray, Namrita, and P. M. Menghal. 2011. "Simulation of Radar Topology Networks to Evolve the Electronic Warfare Survivability Metrics." *2011 3rd International Conference on Electronics Computer Technology*, April, 355–59. https://doi.org/10.1109/ICECTECH.2011.5941622.

Wan, Tao, Xinying Fu, Kaili Jiang, Yuan Zhao, and Bin Tang. 2019. "Radar Antenna Scan Pattern Intelligent Recognition Using Visibility Graph." *IEEE Access* 7:175628–41. https://doi.org/10.1109/ACCESS.2019.2957769.

Wang, Feng, Shanshan Huang, Hao Wang, and Chenlu Yang. 2018. "Automatic Modulation Classification Exploiting Hybrid Machine Learning Network." *Mathematical Problems in Engineering* 2018 (December):e6152010. https://doi.org/10.1155/2018/6152010.

Wei, Dongxu, Shuning Zhang, Si Chen, Huichang Zhao, and Linzhi Zhu. 2019. "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 (5): 1550147719847444. https://doi.org/10.1177/1550147719847444.

Weisgerber, Marcus. 2017. "The Pentagon's New Algorithmic Warfare Cell Gets Its First Mission: Hunt ISIS." Defense One. May 14, 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, and Yucel Topcu. 2012. "Operational Advantages of Using Cyber Electronic Warfare (CEW) in the Battlefield." In *Cyber Sensing 2012*, 8408:151–59. SPIE. https://doi.org/10.1117/12.919454.

You, Shixun, Ming Diao, and Lipeng Gao. 2019. "Deep Reinforcement Learning for Target Searching in Cognitive Electronic Warfare." *IEEE Access* 7:37432–47. https://doi.org/10.1109/ACCESS.2019.2905649.

Zhang, Ming, Ming Diao, Lipeng Gao, and Lutao Liu. 2017. "Neural Networks for Radar Waveform Recognition." *Symmetry* 9 (5): 75. https://doi.org/10.3390/sym9050075.