DOI: 10.53477/2784-2487-24-02

THE COGNITIVE ELECTRONIC WARFARE IN THE AGE OF ARTIFICIAL INTELLIGENCE

Alida Monica Doriana BARBU; PhD*

Abstract: *Collecting and acting on data has increased the military's dependency on the electromagnetic spectrum (EMS). Electronic Warfare (EW) controls the Electromagnetic Spectrum (EMS) in order to detect, analyze, and track potential threats. EW provides situational awareness for diplomatic insights, defensive measures and offensive options for each country. EW enables Joint Electromagnetic Spectrum Operations (JEMSO). In the EM Operation Environment, the armed forces exploit, protect and attack. More advanced EW can identify, intercept and decode the adversaries' Data. It can also project directed energy to disrupt enemy operations, reducing the impact of conflicts or preventing some armed conflicts before they begin.*

Applying cognitive systems to EW helps the army personnel identify patterns and improve the systems, as well as anticipating the COA. Cognitive Electronic Warfare systems interpret a large amount of data from a range of vast sources to provide hypotheses for action plans. Combining human strategies with computer input ensures the success of Cognitive EW approach. Leaving data collection and probability calculations to computers let humans time to think, to be creative and to use their intuiton in order to find the best solutions.

Keywords: *Electromagnetic spectrum (EMS); Electronic Warfare (EW); Cognitive Electronic Warfare (CEW); AI; Machine Learning; DeepNets; Directed-Energy Weapon (DEW); 2022 Russian-Ukrainian conflict.*

Introduction

Electronic or Electromagnetic warfare (EW) involves the use of electromagnetic spectrum (EM spectrum) or directed energy to impede enemy operations by denying the access to the opponent or attacking him, while ensuring friendly access to the EM spectrum. Land, sea, air or space are the domains where crewed and uncrewed systems can apply Electromagnetic warfare on targets such as communication, radar or other civilian and military assets. (Joint Publication 3-13.1 2012)

In peacetime, Joint Electromagnetic Spectrum Operations (JEMSO) coordinate access to joint users to the Electromagnetic Spectrum (EMS), while in time of armed conflict, tactical, operational and strategic advantages and EMS superiority is the goal through exploit, attack and protect military actions in the Electromagnetic Operational Environment. (Joint Publication 3-85, 2020, v-vi)

From attacks on radar systems, jamming of communications and navigation systems, to electronic masking, probing, reconnaissance and intelligence gathering, EW uses directed energy to block signals between technologies and cut off access to the electromagnetic spectrum. By interfering with computer infrastructure, EW can affect operations in the cyber domain, still, EW should not be confused with cyber warfare and capabilities. Cyber operations use hacking techniques to disrupt a target's computer systems, aiming to degrade the target's capabilities and to obtain Intelligence.

Electronic Warfare (EW) controls the Electromagnetic Spectrum (EM) in order to detect, analyze, and track potential threats. EW provides situational awareness for diplomatic insights, defensive measures and offensive options for each country. EW enables Joint Electromagnetic Spectrum Operations (JEMSO). In the EM Operation Environment, the armed forces exploit, protect and attack. More advanced EW can identify, intercept and decode the adversaries' Data. It can also project directed energy to disrupt enemy operations. "These changes to the battlespace prevent some armed conflicts before they begin and/or reduce the impact and scope of conflicts underway." (www.baesystems.com).When one party controls the Electromagnetic Spectrum in the

* Graduate at the Carol I National University of Defense, Security and Defense Faculty, Master's in Crises Management and Conflict Prevention, Bucharest, Romania; e-mail: alida.barbu7@gmail.com.

area, the use of positioning, accurate navigation, communications are denied to adversaries. The disruption and denial of enemies' use of the EM spectrum is essential to mission success.

Military and Intelligence Forces use in Electronic Warfare (EW) electromagnetic or directed energy and integrated cyber capabilities to pre-empt electronical ennemy threats and attacks. The electromagnetic (EM) spectrum consists of X-rays, Gamma Rays, Radio waves, Ultraviolet, Visible or Infrared light, Millimeter waves, Microwaves. (www.baesystems.com)

Cognitive Electronic Warfare (CEW) is the use of Artificial Intelligence (AI) or Machine Learning – cognitive systems – to enhance development and operation of Electronic Warfare (EW) technologies. Cognitive systems can reason, learn, sense and interact with environments and people, for threat detection, suppression or technologies neutralization. (www.baesystems.com)

1. ELECTRONIC WARFARE

1.1. The Electromagnetic Environment

The Electromagnetic Spectrum or the Electromagnetic Environment (EME), represents a part of the Information Environment. The access to and use of the electromagnetic environment is decisive for military operations. The NATO Electromagnetic Warfare Policy and NATO Electromagnetic Spectrum (EMS) Strategy govern the Alliance's use, development, testing and training of EW capabilities and tactics. (Nord Atlantic Treaty Organization, Electromagnetic warfare, 2023).

Radio frequency, infrared, electro-optical countermeasures; electronic security; EM compatibility and deception; emission control; spectrum management; EW reprogramming are activities used in EW.

Electronic Warfare (EW) Systems are configuration of EW technologies that are built to execute military missions on ground, air, sea or space platforms. Examples of EW Systems now in use or development include: Anti-Radiation Missiles (ARM), Antennas Arrays, Anti-Jam Electronic Protection Systems, Advanced Threat Infrared Countermeasures (ATIRCM), Common Missile Warning Systems (CMWS), Directional Infrared Countermeasures (DIRCM), Directed Energy Weapons, Electronic Attack and Support Platforms, Infrared Missile Warning System, Geospatial Location and Exploitation Systems, Multi-Spectral Situational Awareness Sensors, Radar Warning Receiver, Storm EW™, etc. (www.baesystems.com)

1.2. The Electronic Warfare Concepts

The modern EW is facing such challenges that it needs other methods than traditional approaches to manage complex problems. The solution was found in incorporating AI techniques (Situation-assessment or SA, decision-making or DM and ML) into EW systems, in order to analyze the system and adapt, since AI, and not only ML, is regarded as the heart of future cognitive EW solutions. Joe Mitola was the one who first used the term in 1999, when cognitive radio was already in use, while cognitive radar term became known since 2006. (Haigh and Andrusenko 2021, 1)

Situation assessment for electronic support (ES) is represented by classification, characterization, causal reasoning, anomaly detection and intent recognition in real-time in-mission learning to recognize new environments and act adequately when facing surprises. DM techniques for electronic attack (EA), electronic protect (EP) and electronic battle management (EBM) assume scheduling and optimization, and most importantly, incorporating ML for better DM and SA. From the AI point of view, radar or communications are treated equally, as well as EP and EA, whose objectives are the only one that make the difference: EA defines objectives with respect to the adversary and EP defines objectives with respect to oneself. The AI techniques apply also to position, navigation, and timing (PNT); cybersecurity; intelligence, reconnaissance, and surveillance (Haigh and Andrusenko 2021, 1-2)

The core concepts of EW (Haigh and Andrusenko 2021, 5-6) are:

1) ES (who is using the electromagnetic spectrum, when, how and where);
2) EP takes countermeasures into consideration and strategies (Antenna directions, frequency agility, waveform design and signal processing) to maintain radar or communications

performance in order to protect the friendly nodes from unwanted effects of noise or jamming.

3) EA denies or degrades the adversary access to its own RF spectrum through directed offensive EM energy, also deceiving the enemy by false information.

EBM is involved in obtaining effective missions, by coordinating effects and changing mission priorities when necessary, also supporting the EW officer. EW BDA assesses the effectiveness of the EA and provides feedback that allows the operator or system to create more effective attacks. EW reprogramming (software, tactics and hardware) modifies the offensive and self-defense systems, as well as intelligence-collection systems, in order to adapt to changes in enemy threat systems and correct system failures.

2. COGNITIVE ELECTRONIC WARFARE

2.1. Features of Cognitive Electronic Warfare

The U.S. Department of Defense invests each year $7B in EW. (Haigh and Andrusenko 2021, xi). The application of AI to make EW systems cognitive ensure the system's adaptability and learning during missions. Cognitive EW will be decisive in future wars. EW systems must respond to previously unknown signals in a digital world of Internet of military things, while feedback must be estimated and known permanently during a mission. Through aggregated sensor understanding, EW systems must be able of adapting on real-time feedback. Through automation, learning can occur faster than humans can reason on data. This adaptation allow the military staff to have success in their missions. Military applications of cognitive technology demand security to protect their functionality, and AI and Machine learning are robust and effective in performing this function. (Haigh and Andrusenko 2021, xii)

Some subfields of AI are Machine Learning, Distributed AI, Robotics, Planning, Human Factors, Machine while Learning comprises Rules, Neural Networks, Support Vector Machines, Decision Trees, Instance-based Learning (Haigh and Andrusenko 2021, 42). DeepNets identify latent features in the data, whereas classical ML approaches rely on traditional feature engineering.

Symbolic AI like Decision Trees manipulate human-readable symbols; non-symbolic approaches, like DeepNets, operate on raw data. Recently, hybrid approaches combine the two. Symbolic knowledge reduces the search space, constructs features, improves search efficiency, explains the models. Hybrid approaches, known as knowledge-based ML or neural-symbolic AI, find solutions more quickly and enable the learner to work even with no training data and work well after real-world training. (Haigh and Andrusenko 2021, 47)

Situation-assessment (SA), decision-making (DM) and ML represent AI techniques for EW. SA techniques for electronic support (ES) include causal reasoning, characterization, classification, intent recognition and anomaly detection. Optimization, scheduling, planning and managing the temporal trade-offs and distributed nature of the problem are DM techniques for electronic protect (EP), electronic attack (EA), and electronic battle management EBM. Using ML improves both SA and DM.

AI incorporates many subfields, covering the broader concepts of Situation Assessment (SA) and Decision Making (DM). AI techniques are planning, optimization, data fusion, while Learning Support Application Areas are Machine vision, NLP, robotics and logistics. ML can predict performance of jamming effectiveness, learning which EA technique is appropriate for which observed emitter behaviors. EW BDA offers performance feedback on these predictions. ML is a concept within AI and DeepNets are techniques within ML, which is more than Deep Learning. Even though DeepNets have the largest visibility, one must not neglect ML or other AI approaches. (Haigh and Andrusenko 2021, 52)

Bengio, Hinton and LeCun won the Turing award for their work about DeepNet architectures in 2018. Common architectures (Haigh and Andrusenko 2021, 45-47) are: a) Convolutional neural networks (CNNs) – convolutional, pooling, and fully connected - neural networks to process data with a known grid-like topology; b) Recurrent neural networks (RNNs)

– neural networks for processing sequential data that have feedback connections (i.e., memory); c) Temporal CNNs deal with time-related, sequence-related and memory-related Deep Learning and could render RNNs obsolete; d) Autoencoders build a model with a bottleneck layer, which is the efficient encoding, and tries to generate a representation of the original input; they eliminate noise and are anomaly detectors; d) Siamese neural nets train on different input data, while they use the same weights on multiple networks; e) Kohonen networks or self-organizing maps (SOMs), visualize an reduce dimensionality; f) A system of two competing neural networks or Generative adversarial networks (GANs) are used to create synthetic data.

Cognitive EW system performs also Data Fusion, which integrates data for situational awareness from various sources (unmanned ground, aerial or underwater systems, radars, space assets, ships, antennas, fighter jets and sensor networks) in order to produce more accurate inferences than those achieved by a single sensor alone Multi-intelligence (multi-INT) data fusion correlates, compares and combines data from different sources of different types to achieve improved accuracy and more specific inferences. (Haigh and Andrusenko 2021, 65)

2.2. AI-based STAP, ARC, BLADE, ICS, WARDEN AND EWPMT – CADETS OF COGNITIVE EW

The Pentagon is investing in the offensive capabilities of AI-based CEW (cognitive electronic warfare). These technologies help more effectively spoof or jam an adversary's radar. DARPA (Defense Advanced Research Projects Agency) is working on projects that apply AI to the EMS and target either wireless or radar communications. **AI-based STAP** (space-time adaptive processing) is meant to overcome adversarial jamming by using Machine Learning algorithms to sense, probe and characterize threats and then generate automatically countermeasures in real-time. (DefenceOne website)

The DARPA Cognitive EW effort began in 2010, providing Adaptive Radar Countermeasures **(ARC)** and Behavioral Learning for Adaptive Electronic Warfare **(BLADE)** for thwarting enemy's radar and its communications.

Jamming capability of the F-35's active electronically scanned array radar (AESA) and Navy's Next Generation Jammer (used on the EA-18G Growler EW aircraft) are examples of Cognitive EW. DARPA's Spectrum Collaboration Challenge in 2016 offered competitors the challenge to develop AI collaborative autonomous spectrum systems to optimize bandwidth in dense communications environments.

DARPA uses Machine Learning algorithms to assess communications emitters and radars in real time and then to produce countermeasures. Threat systems operating across wider bandwidths claim better RF adaptability and processing (Chirico).

CADET creates coalition battle plans, integrating HTN planning. CADET is a knowledge-based tool that delivers realistic and detailed battle plans, integrated for the U.S. Army and DARPA with several battle management systems. The goals for a tactical course of action (COA) are presented by the human personnel, CADET comes with a detailed schedule of the operation, resource consumption or routing, coordinates team efforts, even supports autonomous action, but always with man-in-the-loop. (Haigh and Andrusenko 2021, 118).

The use of mixed reality (virtual and real worlds in real time) systems is a new vulnerability, which enemies could exploit through targeting cognition: distracting personnel by injecting virtual data; cluttering displays by planting real-world objects; motion sickness induced by Information flooding; confusing the user with real-world objects false alarms.

The applied cognitive engineering principles during system development do not ensure the safety of systems. Adversary interfering by cognitive effects in virtual settings could consist in reducing trust in equipment. inducing cybersickness, manipulating emotion, causing confusion or anxiety.

The DARPA Intrinsic Cognitive Security program **(ICS)** explores formal methods (mathematical approaches), using MR system designs to mitigate potential cognitive attacks. Cognitive engineering provides Formal methods meant to protect the MR user, based on models applicable to MR system. Modeling user behavior in the immersive systems will also help the

understanding of people's behaviour in the MR domain. Also, users will perform different MR-related tasks with commercial technologies. Phase 1 of the 36-month ICS effort focuses on developing guarantees to desirable properties of mixed reality systems and supporting cognitive models to enable proofs of the guarantees. Phase 2 will proof the usefulness of the guarantees in MR systems. The developed prototypes will demonstrate how using commercially available software and hardware will lessen vulnerabilities. (Wilding, DARPA)

The Waveform Agile Radio-frequency Directed Energy **(WARDEN)** program wants to develop theory, hardware and computational models to extend for backdoor attacks the range of high-power microwave (HPM) systems. HPM systems are a category of directed energy weapons (DEWs) that use electromagnetic (EM) radiation to disable, disrupt or damage electronic circuits and components.

Raytheon's **EWPMT** software assists since 2014 the U.S. army commander's ability to coordinate, plan and synchronize spectrum management, EW and Cyber operations. EW targeting, EW mission planning and simulation capabilities of EWPMT support COA development. The display of the electromagnetic operational environment, the electromagnetic order of battle and communications assets, as well as analytics are provided by EWPMT who takes in data from sensors in real time and identifies and geolocates new threats. Sensors being turned off on a specific frequency when they're detected by the sensing system is an automated action that helps the human component of the AI-human team. (Haigh and Andrusenko 2021, 131).

3. THE MODERN ELECTRONIC WARFARE IN THE 21ST CENTURY

3.1. EW in the Russian - Ukrainian conflict since 2022 till present times

The US Space Forces believe that the electronic war in Ukraine could exceed in scope a possible conflict between China and the US, a conflict in which China would try to interfere, including kinetically, with the satellites of the US military used for navigation and timing and disrupt the ability to effectively use C4ISR (command, control, communications, computers, intelligence, surveillance and reconnaissance) through electronic warfare. Ukraine and Russia have jammed each other's systems, with Russia interfering with signals to disrupt global positioning system satellites that help Ukraine use US-supplied air and guided artillery munitions, and Ukraine countering enemy missiles and drones with electronic means. (Gordon 2024)

In December 2010, the Russian Army system known as Borisoglebsk 2, was the first land-based multifunctional electronic warfare of Russian Army with jamming stations for electronic reconnaissance, satellite-based navigation signals and mobile satellite communications suppression. (deagel.com)

Russian aircraft had important losses in Ukraine in March 2022 (Bronck 2022), but by late April 2022, the extensive Russian jamming infrastructure deployed in Donbas electronically suppressed radio signals and GPS of Ukrainian UAVs.

In October 2023 Russian jammers and video feedback were impairing small battlefield Ukrainian UAV activity (The Economist 2023), yet three Russian Palantin EW system were destroyed by Ukraine who also suppressed the satellite radio navigation.

USA and other allies helped Ukraine with their spoofing and jamming methods against Russian electronic systems and gave Ukraine armored vehicles, long-range missiles and secure communication devices. Detection and a better access to critical sources of situational awareness are the high priority of the American army, but also how to deal with the situations when digital harassment makes impossible the use of GPS. (Demarest 2024)

Some U.S. precision-guided weapons, such as Excalibur, Joint Direct Attack Munition (JDAM) and GLSDB, the Boeing-Saab product, showed vulnerability in front of Russian jamming. Even though they assured good results at the beginning of the ostilities, once the Russian army adapted and learnt how to act against them, they became useless. (Gall 2024)

Ukrainian drones were able to repel Russian forces, damaging tanks and armored vehicles. Stupor is the advanced electromagnetic weapon used by Russian forces against Ukrainian

unmanned aerial vehicles and can disrupt Glonass and GPS satellite navigation signals (Frahan 2022). The drone is neutralized by Stupor's blocking the operator's signal to the drone and lands at a desired location. (Dangwal 2022).

Each war represents an opportunity to produce sophisticated weaponry and learn about the opponent's previously secret technology. The performance of the weapons used is monitored by all parties to guide future conflicts. The US Department of Defense is aware of possible armed conflicts with China in the Indo-Pacific or with Russia in Europe, so is investing in sophisticated electronic warfare equipment as well as jam-resistant navigation equipment. BAE Systems was awarded $318 million for M-code GPS cards. The $402 million second-generation battlefield transportable and dismountable positioning, navigation and timing system was produced by TRX Systems. (Demarest 2024)

3.2. Directed-energy weapons (DEW)

In the United States, DARPA, the Pentagon, the Air Force Research Laboratory and the Naval Research Laboratory aim to counter hypersonic cruise missiles, ballistic missiles and hypersonic glide vehicles with **directed-energy weapons (DEW)**, which damage the target (missiles, personnel, optical devices and vehicles).

Non-lethal weapons like microwave, electromagnetic, acoustic, particle beams, laser weapons can paralyse the adversary until conventional forces enter the scene. They disable communications, disrupt sensor systems, penetrate electrical systems, affecting military and civilian infrastructures as well. The United States, but also Russia, China, Germany, France, United Kingdom, Israel, Pakistan and India are developing this technology. (Herbert 1991, 90). Turkey (DailySabah 2019) and Iran (Tehran Times 2019) pretend to have military-grade directed-energy weapons in active service,

High power microwaves from the Electromagnetic weapons spectrum were used to destroy Iraqi electronic systems by the U.S. military during Persian Gulf War. (https://premium. globalsecurity.org) Turkey claims to have used for the first time in battle between military forces a directed-energy weapon (ALKA) in Libya, August 2019. (Ahval News 2019).

The operational advantages of Directed energy weapons over conventional weaponry are their almost perfect flat trajectory due to the lack of affect from the wind, gravity and Coriolis force; the extended to line-of-sight and precise aim; its discretion, since radiation is invisible and doesnțt generate sound (Defence iQ' 2012); the travel at light-speed and long range of lasers, which can also reduce logistical problems (ammunition supply); cheaper than conventional weapons; the difficulty of attribution to a certain actor the high-powered microwave weapons use to degrade electronics such as drones (Grand-Clément 2022).

The Vigilant Eagle, a ground based system which employs High Power Microwaves (HPM), was produced by **Raytheon** in 2005. The Vigilant Eagle is successful in defeating MANPADS missiles. (Vollin 2006)

The BAE Systems high-powered microwave weapon **Bofors HPM Blackout**, purportedly non-lethal, has a microwave sourse, a pulsed power unit and a horn antenna. It evaluates the threats from electromagnetic effects. (Karlsson, 2009, 499-501)

EL/M-2080 Green Pine Long Range Anti-Ballistic Missile Radar tracks and detects Tactical Ballistic Missiles (TBMs) (https://www.iai.co.il/p/elm-20802080s-green-pine).

The Northrop Grumman's **AESA Radars,** positioned on fighter aircraft, are using the Sabr, APG-81, Vader and Starlite Systems and providing surveillance and intel to armed forces. (www.northropgrumman.com)

Thor is a system that uses high-power microwaves to protect against drones as a counter electronic effect, with less engagement time than nets, guns and laser systems and an extended effect. (https://afresearchlab.com/technology/thor)

Radio Frequency Directed Energy Weapon (RFDEW) uses beams radio waves to disrupt the adversaries' electronics and take down drone swarms. The UK Military uses RFDEW as a cheaper alternative to air defence missile-based systems. (https://des.mod.uk/, 16th of May 2024)

A laser weapon is a weapon with directed-energy based on lasers. **Dragon Fire,** created in the **United Kingdom**. It can engage any target at a classified range within line-of-sight, being used against drones. (https://ukdefencejournal.org.uk/)

Genasys (formerly LRAD Corporation) developed an acoustic hailing device to send warning tones and messages over longer distances. LRAD is a non-lethal directed-acoustic-energy weapon non-projectile crowd control. (https://genasys.com/)

During Operation Orchard or Operation Outside the Box in 2007, Israeli jets attacked with electronic warfare systems a Syrian nuclear site near the Euphrates River and succeeded to deactivate the Syrian air defenses. (Katz 2010).

721 physical and cyberattacks were launched over the **U.S. electrical infrastructure** in the past decade. **NNEMP weapons** can be easily made, and are available for purchaising online, without any license required. (Owen 2023)

The Havana medical symptoms **(Havana syndrome)** were reported in Havana, Cuba, etc. by US personnel who assumed microwave energy was causing those symptoms (Myre 2021). Seven US intelligence agencies concluded no foreign rival was involved (Myre 2023). The *60 Minutes* investigative report from March 2024 made the Russian GRU Unit 29155 responsable to these attacks (Pelley 2024) (FitzGerald, 2024). The prohibited blinding laser weapons used by Russia in Donbas war zone (2018) inflicted severe eye injury to an Ukrainian Border Guards serviceman. (Ponomarenko 2018)

In 1997, The TECOM Technology Symposium concluded that determining the target effects of non-lethal weapons on personnel is very challenging because the potential lethal injury of human testing. (Herbert Dennis, https://apps.dtic.mil/) Directed-energy weapons may cause neurophysiological disorders and target the central nervous system. Vertigo, nausea, disorientation, pain, epileptic seizures because of repetitive visual signals or difficulty breathing (potentially lethal) could indicate the use of of non-lethal electromagnetic weapons.

CONCLUSIONS

Brian Holden Reid wrote in his book “The Science of War: Back to the First Principles” (Holden-Reid 2014), that surprise is still a decisive element of military operations. The new technologies made it challenging to obtain surprise on the transparent battlefield, yet, they could be the key of innovative battlefield doctrines and the surprise itself by inflicting indecision, technological overconfidence, cognitive dissonance, confirmation bias, a failure to process, misconceptions about enemy capabilities.

Classical ML has been present in EW systems for years, enriching results, due to the developments of Deep Learning, such as Natural Language and Image Processing. Three factors have an important contribution: labeled data, bigger computers and insights on how to connect the networks.

As more wireless devices – both defense and commercial – are added, the competition for the finite spectrum becomes more fierceful: the erosion of the access to the electromagnetic spectrum by disrupting the military’s ability to receive and send infrared, radio and radar signals. along with the prevalence of advanced digital signal processing in adversary systems and software-defined architectures.

The Q-values of all possible actions of each MDP state are estimated by DeepNet from Deep Q-Networks (DQNs), reducing the number of samples required and the computational burden of conventional Q-learning. RF tasks like coexistence, signal classification, jamming and anti-jamming have been given to DQNs.

In interaction with the real environment, it is critical to learn from only one sample. Real environment imposes constant oversight for planning and enables ML to improve empirical models and performance. Execution monitoring ties the DM to the SA, the actions to the observations, and the EP/EA/EBM to the ES, the heart of every EW system. The quality of the ES influences EP and EA performance. ES analyzes the environment and helps DM.

The challenges of interrelationship between humans and machines are: behavior, performance and physiological factors of Human state sensing and assessment; information-sharing and communication between human and machine; establishing DM balance and workload by function allocation; mutual training and adaptive learning between human and machine; human and machine data fusion and integration in order to generate a shared world model.

As the EW community explores cognitive EW technology development and cognitive systems concepts, it becomes clear that cognitive technology is the future of EW, but also of all areas of defence electronics and operations within the EM Spectrum (EMS).

BIBLIOGRAPHY

BOOKS

1. Haigh, K. Z. and Andrusenko, J., 2021. *Cognitive Electronic Warfare*. An Artificial Intelligence Approach. Boston: London, Artech House.
2. Holden-Reid, B., 2014. *The Science of War. Back to First Principles*. London and New York. Routledge Taylor and Francis Group.

ARTICLES

1. Joint Publication 3-13.1. 08 February 2012. *Electronic Warfare. Chairman of the Joint Chiefs of Staff (CJCS) – Armed Forces of the United States of America*. pp. i, v–x
2. Joint Publication 3-85, 22 May 2020, *Joint Electromagnetic Spectrum Operations*, https://www. jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_85.pdf
3. Nord Atlantic Treaty Organization, 22 Mar. 2023 09:56, *Electromagnetic warfare*, https://www.nato.int/cps/en/natohq/topics_80906.htm
4. Graham, J. D., Gale, D., Sommars, W. and Scott, M., "Shiva Star – Marauder Compact Torus System", Eighth IEEE International Conference on Pulsed Power, San Diego, CA, USA, 1991, pp. 990-993, doi: 10.1109/PPC.1991.733452.
5. Karlsson, M. U., Olsson, F., Åberg, D. and Jansson, M., "Bofors HPM blackout – a versatile and mobile L-band high power microwave system". 2009 IEEE Pulsed Power Conference, Washington, DC, USA, 2009, pp. 499-501, doi: 10.1109/PPC.2009.5386327.
6. Owen, J. E., February 2023. An EMP or Solar Incident Could Result in Blackout Warfare, U.S. Marine Corps, Proceedings Vol. 149/2/1, 440. https://www.usni.org/magazines/proceedings/2023/february/emp-or-solar-incident-could-result-blackout-warfare
7. Herbert, D. B., 1 March 1991. "Non-Lethal Weaponry: From Tactical to Strategic Applications" (PDF). Joint Force Quarterly (21). National Strategic Studies | National Defense University: 87–91. https://ndupress.ndu.edu/portals/68/Documents/jfq/jfq-21.pdf

WEBSITE CONTENT

1. Airborne Aesa Systems, Northrop Grumman, https://www.northropgrumman.com/what-we-do/air/active-electronically-scanned-array-aesa-radars
2. Chirico, F., *Cognitive EW, Emsopedia*, https://www.emsopedia.org/entries/cognitive-ew/
3. Ministry of Defence, *Defence Science and Technology Laboratory and James Cartlidge*. 16 May 2024.
4. Tactical High Power Operational Responder (THOR), *The Air Force Research Laboratory*, https://afresearchlab.com/technology/thor
5. Vollin, J., "Vigilant Eagle: ground-based countermeasure system against MANPADS", Proc. SPIE 6203, Optics and Photonics in Global Homeland Security II, 62030F (9 May 2006); https://doi.org/10.1117/12.673686
6. Wilding, M., *Intrinsic Cognitive Security (ICS)*, DARPA, https://www.darpa.mil/program/intrinsic-cognitive-security

7. Grand-Clément, S., 12 May 2022. "Directed energy weapons: a new look at an 'old' technology". United Nations Institute for Disarmament Research, https://unidir.org/directed-energy-weapons-a-new-look-at-an-old-technology/
8. LRAD by Genasis, Long Range Acoustic Devices, https://genasys.com/lrad-products/
9. Ministry of Defence, DES Comms, May 16th, 2024, Cutting-edge drone killer radio wave weapon developing at pace, https://des.mod.uk/cutting-edge-drone-killer-radio-wave-weapon-developing-at-pace/
10. BAE Systems, Electronic Warfare, https://www.baesystems.com/en-us/productfamily/electronic-warfare

NEWS OR MAGAZINE ARTICLES

1. Frahan, A. H., 6 July 2022. "Defense News – Russian army confirms use of Stupor anti-drone rifle in Ukraine". TASS via armyrecognition.com. https://www.armyrecog nition.com/news/army-news/2022/russian-army-confirms-use-of-stupor-anti-drone-rifle-in-ukraine
2. Air Force Flight Test Center, December 21, 2006. *YAL-1A Airborne Laser Returned to the Center After Modification*, Air Force Test Center, Dec. 21, 2020, https://www.aftc.af.mil/News/On-This-Day-in-Test-History/Article-Display-Test-History/Article/2422739/december-21-2006-yal-1a-airborne-laser-returned-to-the-center-after-modification/
3. Myre, G., October 21, 2021. 5:04 AM. "Long before Havana Syndrome, the U.S. reported microwaves beamed at an embassy". NPR.org. https://www.npr.org/2021/10/21/1047342593/long-before-havana-syndrome-u-s-reported-microwaves-beamed-at-an-embassy
4. Dangwal, A., From FIFA World Cup to Ukraine – Russia Uses Electromagnetic Stupor Anti-Drone Weapon To Counter Ukrainian UAVs. July 7, 2022. Eurasian Times, https://www.eurasiantimes.com/from-fifa-world-cup-to-ukraine-russia-uses-electromagnetic-stupor-anti-drone-weapon-to-counter-ukrainian-uavs/
5. Pelley, S., 2024-03-31. "Havana Syndrome mystery continues as a lead military investigator says bar for proof was set impossibly high – CBS News". www.cbsnews.com. https://www. cbsnews.com/news/havana-syndrome-culprit-investigation-new-evidence-60-minutes-transcript/
6. FitzGerald, J., 1 April 2024. "Havana syndrome: Report links mystery illness to Russian intelligence unit". www.bbc.com. BBC News, https://www.bbc.com/news/world-us-canada-68706317
7. Kononenko, B., 06 June 1996. pp 48-51. "Silent Space Is Being Monitored". Moscow ARMEYSKIY SBORNIK..http://www.fas.org/news/russia/1996/druma189_s96005.htm
8. AI-Enabled Electronic Warfare, *DefenceOne*, https://www.defenseone.com/insights/cards/how-ai-changing-way-warfighters-make-decisions-and-fight-battlefield/3/?oref=d1-cards-cardstack-toc
9. *Thaad-ER in Search of a Mission*, Aviation Week Network, January 20, 2015, https://aviationweek.com/defense-space/thaad-er-search-mission
10. *ELM-2080 Green Pine Long Range Anti-Ballistic Missile Radar*, Iai, https://www.iai.co.il/p/elm-20802080s-green-pine
11. Hengst, G., Sept. 26, 2008. "Test results show Active Denial System as nonlethal weapon". *Air Force*. https://www.af.mil/News/Article-Display/Article/122302/test-results-show-active-denial-system-as-nonlethal-weapon/
12. Homaeefar, M., March 3, 2019 – 17:11. "IRGC Navy develops anti-laser weapon", *Tehran Times*. https://www.tehrantimes.com/news/433633/IRGC-Navy-develops-anti-laser-weapon
13. Ergocun, G., 30 September 2019. "Turkey's laser weapon ARMOL passes acceptance tests". *DailySabah*. https://www.aa.com.tr/en/economy/turkeys-laser-gun-passes-acceptance-tests/1597850
14. "Is Turkey the first country to shoot down a drone with a laser?". 3 September 2019. Ahval. https://ahvalnews.com/libya-turkey/turkey-first-country-shoot-down-drone-laser
15. Gall, C. and Vladyslav G., "Some U.S. Weapons Stymied by Russian Jamming in Ukraine". May 25, 2024. *The New York Times*, https://www.nytimes.com/2024/05/25/world/ europe/us-weapons-russia-jamming-ukraine.html

16. "Defence IQ talks to Dr Palíšek about Directed Energy Weapon systems", Nov. 20, 2012, Defence iQ', https://www.defenceiq.com/army-land-forces/articles/we-talk-to-dr-pali-ek-about-directed-energy-system
17. Demarest, C., *Electronic warfare in Ukraine has lessons for US weapons, navigation*. C4ISRNET. Monday, May 6, 2024. https://www.c4isrnet.com/electronic-warfare/2024/05/06/electronic-warfare-in-ukraine-has-lessons-for-us-weapons-navigation/
18. Katz, Y., September 29, 2010. "And They Struck Them with Blindness". *The Jerusalem Post*. https://www.jpost.com/Magazine/Features/And-they-struck-them-with-blindness
19. *Borisoglebsk-2*.deagel.com, https://web.archive.org/web/20151104021259/https://www.deagel.com/Aircraft-Protection-Systems/Borisoglebsk-2_a003063001.aspx
20. Bronk, J., Reynolds, N. and Watling, J., 7 November 2022. *The Russian Air War and Ukrainian Requirements for Air Defence*. Royal United Services Institute for Defence and Security Studies, https://static.rusi.org/SR-Russian-Air-War-Ukraine-web-final.pdf
21. "Trenches and tech on Ukraine's southern front". 29 October 2023. *The Economist*. https://www.economist.com/europe/2023/10/29/trenches-and-tech-on-ukraines-southern-front
22. Ponomarenko, I., 2 October 2018. "Another blinding laser attack on Ukrainian soldier reported in Donbas war zone". *KyivPost*. https://www.kyivpost.com/post/7891
23. Gordon, C., "More EW Than We Have Ever Seen Before in Ukraine", *Space Force Official Says, Air and Space Forces Magazine*, April 24, 2024 https://www.airand spaceforces.com/ew-ukraine-space-force-training-electronic-warfare-leader-says/