International Journal of Security Studies

Volume 3
Issue 1 *2021*

Article 6

2021

Strategic Invisible Waves: A Review on Electronic Warfare

Nazargi Mahabob
KING FAISAL UNIVERSITY, nazargimahabob@yahoo.com

STRATEGIC INVISIBLE WAVES: A REVIEW ON ELECTRONIC WARFARE

Dr. M. Nazargi Mahabob, Ph.D.

nazargimahabob@yahoo.com

The author is an associate professor in the College of Dentistry in King Faisal University in Al Hasa, Kingdom of Saudi Arabia, where he resides. His country of citizenship is India. He earned bachelor's and master's degrees in dental surgery from the Tamilnadu Government Dental College in India, and a Doctor of Philosophy Degree in dentistry from Vinayaka Mission University in India. He has a special interest in global security and strategic studies.

Strategic Invisible Waves: A Review on Electronic Warfare

Prior to the 20th century, any army that was sufficiently big enough and organized well enough would be able to lay siege to a certain territory; they could defeat the rival army if their size and sheer strength was enough to overwhelm others. This war strategy began changing in the 20th century as many nations, military commanders, and strategists started to realize the importance of fighter planes and missiles as offensive systems in winning the war (Van Niekerk & Maharaj, 2009; Potenziani, 2006). It quickly became evident that in order to win any war, it was essential to have air superiority; this concept became especially important with the start of the Cold War, when air defense became a cold, hard reality. Naturally, as technology progressed, both sides increased their air defense capabilities and many systems were developed as a result. As NATO allies invested significantly more time and money on developing aircrafts, the Soviets gave more importance to their air defense as well.

Some of the defense systems developed are notable, such as the United States' Patriot missile defense system and the Terminal High Altitude Area Defense (THAAD) system. Both are mobile surface-to-air and anti-ballistic missile systems meant to intercept and destroy missiles carrying chemical warheads and cluster bombs. THAAD even has the ability to shoot down ballistic missiles at particular altitudes to minimize damage to the surrounding target area. Similarly, the Soviet Union developed a complete series of surface-to-air and anti-ballistic missile

systems (Adamy, 2001); the most recent of which is the S–500 Triumph. The main advantages of the S–series is that it is a mobile system that can be positioned in different regions and locations. Other countries also developed air defense systems, such as Israel's "Iron Dome" system that was specifically designed to intercept low flying targets.

All of these air defense systems were created primarily to deny opponents air dominance, and all have a similar type of concept that uses radar to identify and destroy the target by launching surface to air missiles (SAM). The types of radars and SAM used varies, but the fundamental concept is the same. Through increased research and inventions, the use of state-of-the-art technologies has increased many fold. Today's battlefield has evolved from simple hand-to-hand fight to a complicated network of communication such as global positioning systems to reach the specified location in all weather conditions either through air, sea, or land (Poisel, 2002).

Even for ground operations, the solder must know the exact location where he has to land and how to coordinate his operation to communicate with colleagues and higher ranks. Imagine what could happen in a situation if suddenly all electronic communication and other electronic devices stop responding? It would be similar to a person suddenly losing all of his communication skills, incapable of speaking, seeing, and hearing; this is electronic warfare. This relatively new form of offensive warfare plays with electromagnetic spectrum/waves (Ryan, 2007).

Although electronic warfare came into use in the early 20th century, many countries have more recently developed an interest in using radiated electromagnetic energy for electronic warfare. This article will analyze the importance of electronic warfare in its existing capacities and in the future battlefield.

Electronic Warfare (EW)

Since the inception of radio communication, electronic communication has dynamically transformed the armed forces. From soldiers identifying their positions and locating targets to navigating aircraft and launching missiles, daily operations depend on electronic waves. Technology has evolved to the point that it is nearly impossible to conduct an operation effectively without these electronic eyes and ears. Both routine and special operational functions are negatively affected by any disturbance to these electronic waves (Shinar & Turetsky, 2002), so research and development continues to more effectively protect these electronic waves, maintain advantage over adversaries, and to enforce the doctrine of area denial. Destroying an army's coordination by disrupting their communication network and—combined with a quick or preemptive response—will result in the failure of their mission (Spezio, 2002). Disrupting an army's telecommunication network during the American civil war meant intercepting telegrams; during World War I telephones were used to communicate with commanders and troops; with the advent of the two-way radio used in World War II, research and development focused on using the electromagnetic spectrum (EMS) for both defensive and

offensive purposes. This new dimension of warfare is called Electronic Warfare (EW).

Since the introduction of battlefield radios, electronic warfare has been a component of modern conflict, but it has progressed far beyond jamming radios. Electronic warfare systems now sense, exploit, and manipulate the electromagnetic spectrum (EMS). EW is developing as a priority and a focus for development as a relatively affordable and easily implemented means of disrupting the working of an enemy's radar and other systems, as well as defending one's own equivalent systems from interference. With so much modern technology reliant on the electromagnetic spectrum, the battle for electronic overmatch is waged on the airwaves all the time. In modern warfare military personnel heavily rely on the EMS for navigation, positioning, communications, and other capabilities; EW ensures those capabilities for allies and denies them to adversaries (*Vesti* 2017). EW has become an increasingly spoken word in the defense community, though it is not always well understood. Its goal is to prevent an opponent from acquiring control of and an advantage in the electromagnetic (EM) spectrum while allowing friendly and unrestricted access to oneself and allies (Poisel, 2002; Shinar, 2002).

With the expansion of the military and operational capabilities of systems that have EMS, the relevance of electronic warfare systems has increased in order to provide security. This system, which is very effective at using autonomous weapons in general and providing vision, intelligence, and management support to

active elements in the field, is also very reliable and effective at using tactics like information transfer, deception, signal cutting, signal strangling, and target surprise on enemy electromagnetic fields. Infrared, Radio Frequency, Electromagnetic Deception, Radio and GNSS Jamming, Anti-Jamming and Deception, Electronic Masking, Reconnaissance and Intelligence, Eavesdropping, Electronic Reprogramming, Emission Control, and other methods and technologies are used in electronic warfare (Choi et al., 2020).

An Overview of Electronic Warfare

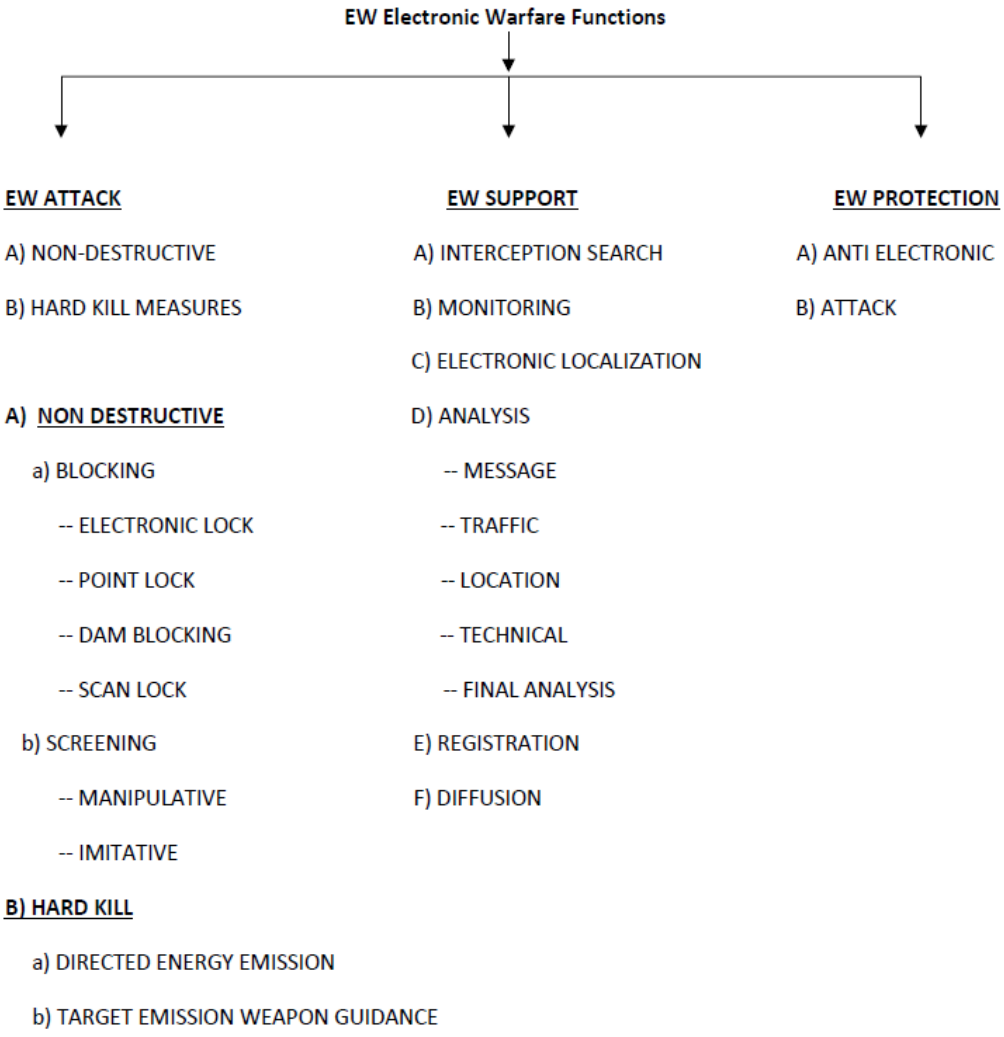
The EW system performs three operational functions on electromagnetic waves/spectrum through command and control: attack, support, and protection (Figure 1).

Electronic Attack (EA)

This part of the system functions in offensive mode by either nondestructive (soft kill) or destructive (hard kill). It tries to control the enemy's electromagnetic spectrum by launching attacks on the opponent and disrupting, denying, destroying, or deceiving their electronics infrastructure. It can be carried out by jamming, spoofing, or sending powerful Electromagnetic Pulses (EMP) on the opponent's electronic communication systems. Electromagnetic Pulses (EMP) are sudden bursts of very high-power electromagnetic impulses. This kind of sudden burst has the capacity to damage electronic components in its vicinity and can also inflict damage to physical objects and humans.

Figure 1

Mind Map for Electronic Warfare



Electronic Protection (EP)

Electronic protection basically consists of counter measures to protect military facilities, personnel, and communication channels from any form of electronic attacks. It's similar to electronic defense or shield or insulation from electronic attack. If facilities are not properly protected, electronic attacks can have

devastating effects on the functioning of the military. Spread spectrum technologies are a widely used method of Electronic Defense. Other examples of Electronic Defense are the use of restricted frequency, stealth technology, and emission control. EP methods are intended to eradicate, decrease, or lessen the effects of unintended/unwanted EM signals. These characteristics and processes work together to keep friendly capabilities operational. The Modular Electromagnetic Spectrum Deception Suite (MEDS) would be capable of simulating the emissions produced by army units of various sizes. This means that an adversary would spend time researching it or avoid the area altogether; it would also make noise to hide valid messages (Frater & Ryan, 2001).

Electronic Warfare Support (ES)

ES supports tasks such as surveillance and reconnaissance of the electronic spectrum. ES is the side of warfare that gathers information (geolocation, frequency, modulation type, copy of communication signals, device type, etc.) about an enemy by intercepting radiated energy. For rapid response, stand-alone systems are mainly used. By installing data link equipment for electronic information transmission, a standalone radar warning receiver (RWR) system that performs simple self-defense and threat alert can be extended to detect and identify remote dangers (Kjellén, 2018).

Modern fighter planes and surveillance ships, such as the Aegis class, employ an integrated system that pool resources from all EW and electronic

systems. Unfriendly emitters are detected continuously from all directions using radiofrequency and electro-optical receivers installed around the perimeter of the airframe. All sensors are combined by a central computer and shown on the pilot's helmet visor. The system also combines data from off-board sensors to create a complete picture of the electrical environment in the area (Wade, 2019).

The military uses electronic warfare to take advantage of an adversary's electromagnetic emissions; they can block or jam communication or spectrum, causing communications and navigation to be disrupted (GPS). They can also intercept and decode messages to learn about an adversary's plans. Electronic warfare is typically silent and undetectable, yet it has the potential to cause significant harm to the adversary. Any military can wreak havoc by causing a loss or disruption in communication, with the most serious consequence being an inability to communicate with other parts of the force. Because every piece of equipment and machine includes electronics and communicates through EM waves, electronic warfare can take place on land, sea, and in the air

Obtaining EW supremacy is critical to attaining key objectives such as air superiority, area denial, and dominance in the war. Without it, an enemy might disrupt and degrade navigation systems on precision guided munitions (PGMs), causing missiles to deviate from their intended route and suppressing a country's air defense systems (Poisel, 2002; Frater & Ryan, 2001).

Countries and Electronic Warfare

The United States is the largest user of electronic warfare systems and paid more attention to this subject through having large EW operational based systems, using electronic warfare systems from the sea, air, unmanned aerial vehicles, and land. Unmanned aerial vehicles were used initially for the purpose of observation and surveillance and has since demonstrated UAVs capabilities in EW. High altitude and long endurance surveillance help gather large volumes of data and keeps eyes and ears on the adversaries. The CREW Duke EW system has been used for a long time to jam remotely operated roadside IEDs. Now it has upgraded AN/MLQ-44A PROPHET SGINT Vetronics EW vehicles to AN/MLQ-44Ba vehicle that could provide electronic surveillance as well as locate and suppress enemy communications and networks. It also provides near real time digital information to the army (Lee et al., 2020).

A huge network of EW and counter EW Suites are being used in aircrafts such as the F-35, F-22, F-16, F-18 and in some other dedicated aircrafts including theEC-37 and EC-128. The Boeing EA-18G Growler is a modified version of F/-18F Super Hornet and operates from aircraft carriers. This aircraft is designed for EW attack and counter measures. The United States also uses high altitude and long endurance drones like RQ-4 Global Hawk to collect real time data.

The AN/ALQ-218,ALQ-99,AN/ASQ-239, and NGJ electronic warfare and countermeasure systems are used in the EA-18G Growler, the F-22, and the F-35.

The AN/ALQ-250 Eagle passive active warning survivability system (EPAWSS) provides radar warning and situational awareness; this helps combat the air defense systems, allowing the fighter to achieve deeper penetration into an enemy's territory. The AN/ASQ-239 system produced by BAE is one of the most advanced, fully integrated electronic warfare and 360-degree situational awareness as well as quick response capabilities. LAN/ALQ- 254(V)1 Viper Shield EW system will provide a virtual electronic shield to the aircraft(F-16). Its AGEIS class combat system in ships provides electronic surveillance and counter measures in the sea. The AN/SLQ-32 is currently functioning as a primary electronic warfare system in use by U.S. Navy ships. A newly developed system, the AN/SLQ-32(V)7 SEWIP Block III, is more dynamic than existing one and will provide cutting-edge electronic attack capability. It will allow groups of ships to better work together to defeat threats electronically. While the United States' early contributions to and interest in the development of EW systems waned after the cold war era, this past decade has seen a resurge of interest, and the USA returned to research and development in EW (Potenziani, 2006; Ryan, 2007; Frater, 2001).

Even though Russia was successful in disrupting Japanese radio communications during the Russian-Japan war, it failed to suppress Georgia's air defense systems during the 2008 Russian-Georgian War. Several Russian planes were lost as a result of this situation. Learning the value of EW, Russia has invested in EW and has made significant advancements in its EW capabilities over its

competitors. Since 2009 Russia has continually engaged in EW modernization, with upgraded EW systems entering service at the strategic, operational, and tactical levels to supplement the capabilities of all branches and arms of the military. In recent years, Moscow has made significant progress in purchasing and developing EW capacity across its Armed Forces branches and service arms. Objectives for the Il-22PP Porubshchik EW aircraft include its ability to silence any radio transmissions, air defense radars, early warning aircraft, air command posts, and ground communication centers. It disrupts the radio traffic of tactical and strategic aircraft, as well as unmanned aerial vehicles (UAVs) and reconnaissance (Spezio, 2002; McDermott, 2017).

The Krasukha-4 EW ground complex blocks GPS transmissions within a300-kilometer radius. The communication channels used to transfer information have no barriers to jamming. Not only will the technology on this future platform have to efficiently jam AWACS aircraft, manned and unmanned aircraft, air defense systems, ground equipment, and signals from the enemy's satellite grouping, it will also have to jam signals from the enemy's satellite grouping.

The Russian Krasukha-2 system can analyze signal kinds and then jam an adversary's radar. The capacity of Russia to spoof signals is a unique characteristic of Krasukha-2. When an actor imitates, or "spoofs," authentic Global Navigation Satellite System (GNSS) signals in order to alter positioning, navigation, and timing (PNT) data, this is referred to as spoofing. Spoofing is generally done by

providing fake positional information to an attacker. Russia intentionally emits the identical signals on GNSS frequencies to prevent receivers from locking on to the genuine GNSS signals (Kjellén, 2018).

Borisoglebsk-2 is best known for its participation in eastern Ukraine, where it is said to have hampered the use of Ukrainian drones by blocking incoming GPS signals. The nerve center for Russia's air defense and other electronic countermeasure systems is Moskva-1. This system continuously monitors electronic emissions over a 400-kilometer radius on all frequency ranges, acquiring electronic intelligence and performing jamming and electronic suppression as needed. The Baikal-1ME automated system is interoperable with EW unit systems, which are highly mobile and difficult to track down. The psychological and cyber operations capabilities used against Ukrainian government forces, which includes gaining access to soldiers' communication systems, tries to demoralize and weaken troops' morale (McDermott, 2021).

Despite the fact that the United States continues to have a military edge in conventional weaponry, Moscow today has a crucial asymmetrical advantage that attempts to close the gap. There have been several reports of Russian EW assaults in Syria that have either interfered with communications or falsified GPS signals from other providers in the area. According to a statement made by U.S. Special Operations Commander General Raymond Thomas in August 2018, Russia, which used electronic warfare systems primarily through signal cutters in the Syrian field,

has frequently disrupted communication between troops in operations carried out using U.S. warplanes and unmanned aerial vehicles. According to a statement made by U.S. Special Operations Commander General Raymond Thomas in August 2018, Russia used electronic warfare systems in Syria, primarily signal cutters, to frequently disrupt communication between troops in operations carried out using U.S. warplanes and unmanned aerial vehicles (Vardhan & Garg, 2014). In addition to the United States and Russia, Israel, China, the United Kingdom, France, Italy, and India have also considerably developed their expertise in EW techniques.

The Growing Importance of Electronic Warfare

To execute military operations, modern militaries rely on communications equipment that employs a wide range of frequencies. As a result, contemporary forces use electronic warfare to try to control the spectrum. The higher the role of electronic warfare in conflict, the more advanced a military foe is considered. For the past few decades, interest in EW technology has been limited to a few practical applications. Because of the reliance of worldwide armies on electromagnetic spectrums, it has now emerged as one of the most promising areas for defense research and development. This domain has developed as a critical one for having the ability to have superiority and advantage over the enemies. The increased use of low-cost drones and loitering munitions by both state and non-state actors has prompted countries to conduct active studies in this area. In the long term, utilizing EW against these low-cost drones and loitering munitions will be less expensive

than using a high-cost air defense system. Because current air defense systems do not provide a foolproof shield, EW can be used in conjunction with them (air defense systems) to close the gaps. Without firing a single shot, EW allows users to engage in "non-contact operations" that jam, blind, disrupt, and demoralize an enemy (Frater & Ryan, 2001).

EW is a source of concern for Russia and the United States since critical objectives such as attaining air superiority rely heavily on achieving EW supremacy. Without it, an adversary can disrupt and degrade the navigation systems on precision guided munitions (PGMs), causing missiles to deviate from their intended route, as well as jam a country's air defense systems.

Target Saturation Concept

Using newly emerged drone swarm technology and simultaneously launching huge quantity of missiles/shells toward targets will ultimately create fatigue in any type of air defense system currently under use and leads to fail. In several previous incidents, it has been noted that the advanced air defense systems were unable to engage and neutralize the incoming hostile projectiles with100% effectively. In recent conflicts, low-cost drones have effectively evaded these highly technical and complicated air defense systems. Even with high tech radars, multiple target engaging, and quick responding systems there is a limitation in maximum targets engagement, reloading time, and cost effectiveness. In addition, using smaller, multiple, and low flying drones make modern air defense systems

less effective in defending their assets. This disadvantage of target saturation can be overcome by using the combinations of projectile/kinetic energy-based air defense systems and Electronic Warfare systems. Russia successfully handled these types of threats in Syria using a combination of Pantsir mobile air defense and the EW system to neutralize a majority of drone attacks on their Khmeimim air base. Since most of the drones are guided by GPS and all of them contain electronic circuits, they can be either jammed or spoofed through EW. A combination of conventional air defense with EW will work more effectively.

Global Market

In the last decade, more and more countries have recognized the importance of EW and have begun to engage in research and development. As per the report published by Allied Market Research, the global electronic warfare market generated $15.81 billion in 2020, and is estimated to reach $23.56 billion by 2028, growing at a CAGR of 5.6% from 2021 to 2028 (GLOBE NEWSWIRE). Significant technological improvements and the integration of electronics into military equipment are leading to a trend toward multilayered defense systems, which is projected to drive the electronic warfare market over the next several years. The increased use of UAV systems, as well as the necessity for ground surveillance and communication jamming, all serve as potential for the electronic warfare sector.

Conclusion

Based on history, we can deduce that the army with superior weaponry and tactics has always had the upper hand in battle. Since the introduction of electronic technology into the battlefield, its use has increased manifold, and it has become an indispensable part of army operations. Even under the current scenario, we can say that conducting operations without these electronics is impossible. To avert an unfavorable scenario and to maintain their competitive advantage over adversaries, countries started working on—and continually improve—electronic warfare.

References

Adamy, D. (2001). *EW 101: A first course in electronic warfare* (Vol. 1). Artech House.

Choi, S., Kwon, O-J., Oh, H., & Shin, D. (2020). Method for effectiveness assessment of electronic warfare systems in cyberspace. *Symmetry 12*(12). https://doi.org/10.3390/sym12122107

Electronic warfare: How to neutralize the enemy without a single shot. (2017). *Vesti*. https://www.vesti.ru/article/1519602

Frater, M., & Ryan, M. (2001). *Electronic warfare for the digitized battlefield*. Artech House.

Kjellén, J. (2018). *Russian electronic warfare: The role of electronic warfare in the Russian armed forces*. Swedish Defence Research Agency.

Lee, J., Jung, K. H., Jung, K. H., Choi, Y., Chung, Y-S., & Chung, H-K. (2020). Improved active interference canceling algorithms for real-time protection of 2nd/3rd level facilities in electronic warfare environment. *Appl. Sci. 10*(7). https://doi.org/10.3390/app10072405

McDermott, R. N. (2017). *Russia's electronic warfare capabilities to 2025: Challenging NATO in the electromagnetic spectrum*. International Centre for Defence and Security. https://euagenda.eu/upload/publications/untitled-135826-ea.pdf

McDermott, R. (2021). Russian military considers new electronic warfare aircraft. *Eurasia Daily Monitor 18*(92), 3-5.

Poisel, R. A. (2018). *Introduction to communication electronic warfare systems*. Artech House.

Potenziani, E., II. (2006). Current and future trends in military electronic warfare systems and the role of thin films and related materials. *Ferroelectrics 342*(1), 151-161. https://doi.org/10.1080/00150190600946302

Ryan, M. (2007). Joint publication 3-13.1 electronic warfare [Book Review]. J. Battlef. Technol.

Shinar, J., & Turetsky, V. (2002). Interceptor missile guidance: A mature science or a new challenge? *IFAC Proceedings 35*(1), 91-96. https://doi.org/10.3182/20020721-6-ES-1901.01240

Spezio, A. E. (2002). Electronic warfare systems. *IEEE transactions on microwave theory and techniques 50*(3).633-644. 10.1109/22.989948

Van Niekerk, B., & Maharaj, M. (2009). The future roles of electronic warfare in the information warfare spectrum. *Journal of Information Warfare 8*(3).1–13.

Vardhan, S., & Garg, A. (2014). Information jamming in electronic warfare: Operational requirements and techniques. *International Conference on Electronics, Communication and Computational Engineering*.49-54.

Wade, N. M. (2019). *Cyber1 Smartbook: Cyberspace Operations & Electronic Warfare*. Lightning Press.

Electronic Warfare Market to Generate $23.56 Billion by 2028: GLOBE NEWSWIRE. May 26, 2021.