TECHNOLOGICAL ADVANCEMENTS IN ELECTRONIC WARFARE AND ITS EFFICACY IN RUSSIA-UKRAINE CONFLICT

Maj Gen AK Srivastava, VSM (Retd)

Abstract

Electronic Warfare (EW) is an important aspect of contemporary military operations and it has rapidly evolved, keeping pace with technological advancements. In modern military operations, full electromagnetic spectrum dominance is imperative for success. Russia-Ukraine war is the latest conflict which the world is witnessing, wherein most sophisticated Electronic Warfare systems have been used. Russia possesses well developed EW systems since long which they have been constantly upgrading. On the other hand, Ukraine did not have matching levels of EW systems. In spite of their superiority, Russian forces were not successful in achieving electromagnetic dominance at least in the initial phases of the conflict. However, they were able to consolidate their EW efforts and increase the effectiveness after the conflict became more static and a war of attrition. Ukraine, with the support from US and NATO (North Atlantic Treaty Organisation) countries, was able to fight back on the EW front. They were able to protect their communication and radars to a great extent and were also able to carry out jamming and disruption of Russian systems.

The article gives a glimpse of the advancements in EW domain over a period of time and carry out a critical analysis of EW operations in Russian-Ukraine conflict. Some useful lessons learnt have been drawn, which will be useful for gearing up our EW systems for electromagnetically dense battlefield environment.

INTRODUCTION

EW is defined as the military actions taken to prevent or reduce enemy's effective use of radiated electromagnetic (EM) energy and actions taken to ensure our own effective use of radiated electromagnetic energy. The information environment in which military operations are conducted is getting extremely complex due to electromagnetic spectrum. There is growing need for the armed forces to have unrestricted access to the electromagnetic environment which provides opportunities and throws challenges for electronic warfare in support of military operations. Within the information operations domain, EW is an element of information warfare.

Electronic Warfare, a sub set of Information Warfare (IW) is the most vital part of IW on the battlefield where it is employed as a weapon. The Electronic Warfare has evolved over a period of time starting from the WWI to the modern day battle environment. As the usage of electromagnetic spectrum has been growing, the Electronic Warfare is also growing to cover new bands of spectrum like Millimetric Wave, Terahertz, Infrared (IR), Optical band and associated technologies. Electromagnetic warfare can be applied from air, sea, land, or space by manned and un-manned systems, and can target communication, radar, infrared or other military and civilian assets. In this article, the developments in the field of EW, its growing importance in the concurrent warfare and an assessment of deployment and effect of Electronic Warfare in Russia-Ukraine war have been reviewed.

THE CONCEPT OF ELECTRONIC WARFARE [1]

The ever increasing proportion of specialisation, complexity and performance of modern weapon systems is directly due to electronics. The basic principle of Electronic Warfare if to exploit adversary's electromagnetic transmissions to gain operational intelligence and apply countermeasures to deny the use of electromagnetic spectrum to the enemy. Simultaneously, take measures to protect one's own unimpeded

use of the same spectrum. The three basic elements of Electronic Warfare are as shown in Figure 1 below.

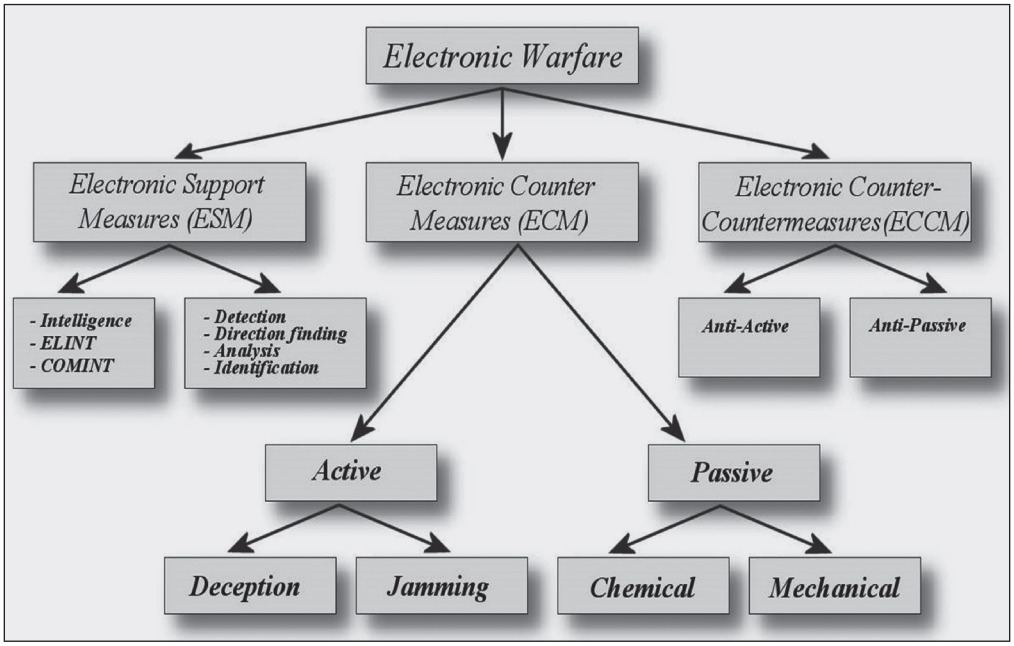

Figure 1 : Elements of Electronic Warfare.[2] **Source:** Christian Wolff, "Types of Electronic Warfare", Radartutorial.edu. https://www.radartutorial.eu/16.eccm/ja05.en.html

Electronic Support Measure (ESM). Part of EW which implies actions taken to search, intercept, locate and identify sources of radiated EM energy for purpose of exploiting it in support of military operations

Electronic Counter Measures (ECM). It involves actions taken to prevent or reduce the enemy's effective use of the EM spectrum. ECM can be either active or passive. Active Measures of ECM includes Jamming and Deception.

Electronic Counter Counter Measure (ECCM). Measures taken to protect one's own electronic systems against enemy ESM & ECM and enhancing the efficacy of own ESM system.

EVOLUTION OF ELECTRONIC WARFARE AS A CRITICAL DOMAIN [3]

Electronic Warfare techniques have evolved over a period of time starting from WWI to exploit the opportunities and vulnerabilities thrown up by the electromagnetic spectrum. During WWI, the electromagnetic spectrum was not very busy. The newly invented radios were used for communications, coordination of operations and for directing fire. Radio receivers were used to monitor enemy's communications and rudimentary direction finding equipment were used to locate the enemy positions. The communications jamming emerged at the same time, but was not widely employed as it was preventing own use of those radio frequencies. Also, the warfare happened slowly and the enemy could evade jamming in various ways.

The use of more sophisticated EW systems started during WWII. Airborne radars and jammers came up and advanced technologies enabled jamming and communicating on different frequencies. The fluid nature of warfare gave definite operational advantage to troops by intercepting, jamming and exploiting enemy's electronic systems. RAF and U.S. bombers made use of metallic chaff which were dispensed to confuse German AD radars. Jamming was also done of German VHF ground to air communications used to guide their fighter aircrafts towards the targets.

During the intense Cold War period in the 1950s and beyond, the competition to develop military arsenals accelerated and so was the case of electronic warfare equipment. Owing to technological advancements, more sophisticated EW systems with higher power, wider frequency ranges, and complex waveforms were developed. The systems were made small to fit into aircrafts and ships. As part of electronic protection measures, stealth aircrafts and ships with drastically reduced RF, IR, acoustic, and visual signatures were developed.

Electronic Warfare is an important aspect of contemporary military operations and it has rapidly evolved, keeping pace with technological advancements. In modern military operations, full EM spectrum dominance is imperative for success. This has led to a competition

amongst the major militaries to lay overwhelming emphasis on the development of next-gen sensors, communications, countermeasures, and counter-countermeasures.

TECHNOLOGICAL IMPERATIVES: KEY TO EW SUCCESS [4]

New technological advancements are constantly augmenting the EW capabilities and ensuring success of EW missions. Some key technologies which are vital for EW equipment include highly sensitive digital receivers, efficient and automated signal analysers and enhanced feature extraction techniques. Spread spectrum techniques and their countermeasures, stealth technologies and addressing dense electromagnetic spectrum are vital for modern EW systems.

Digital beamforming and adaptive technologies have improved the range of the systems and enable interference rejection, super resolution and power management. Antenna technology like Active Electronically Scanned Array (AESA) and compact T/R modules have enabled the development of scalable AESA radars. Multi band and multi-mode RF front ends have helped in the development of software defined radios and configuring of communication & EW functions in a single hardware.

The future technologies like nanoelectronics, with Carbon Nanotube (CNT) will make the EW systems compact and scalable. A single CNT can carry out all functions of components required in a receiver. The nano receivers under development are heading towards universal RF processor which will configure different radio bands from a vast grid of nano cells, each earmarked for a single frequency slot. It will be possible to reconfigure the system to achieve the functionality of a different radio. Many more such technologies are under development.

ELECTRONIC WARFARE IN RUSSIA-UKRAINE CONFLICT

Russia-Ukraine war is the latest conflict which the world is witnessing, wherein most sophisticated Electronic Warfare systems have been used. Russia possesses well developed EW systems since long which they have been constantly upgrading. Since Ukraine was a part of

USSR earlier, they also possess some old Russian EW knowledge and systems. However, as the war progressed, they received considerable support from the US and NATO countries and gave a stiff fight in the EW domain.

Commenting on EW in this conflict, the commander of the USSF's Space Delta 3 Col Nicole Petrucci said during an event, "What we have seen in the Ukraine-Russia conflict is more EW than we have ever seen before".[5]

Russia and Ukraine have been jamming each other's electronic systems. Ukraine has employed electronic warfare to strengthen its air defence against Russian missiles and drones. Russia, on the other hand has been carrying out jamming and interference of signals to disrupt global positioning system satellites that are being employed by Ukraine for guided aerial and artillery munitions.

Russia is known to have a total of five EW brigades, out of which, three brigades are deployed against Ukraine. Ukraine is using many radios and electronic equipment supplied by NATO. Russian EW operators already have experience in dealing with these radios based on their operations in Syria. Therefore, they are able to jam radio sets being operated by Ukraine.

The most powerful and actionable tool in EW is ECM which includes jamming. For example, the Russian R-330Zh Zhitel can jam satellite communications, GPS and cellular networks. Russian forces also resorted to deception as part of ECM in that they used RB-341V Leer-3 system to break into cellular network of eastern Ukraine and passing fake orders to troops during the insurgency period of 2014 to 2022. The range of Leer-3 for jamming VHF and UHF frequencies is extended by using repeaters mounted on Orlan-10 drones.

ESM, is used for detection, monitoring, direction finding and analysis of enemy's transmissions. The process identifies the vulnerabilities in the targeted transmissions from radios, radars and other electronic devices for exploitation. Using their ESM capabilities, most ECM systems using Direction Finding equipment can find the coordinates of enemy radio

and cellphone transmissions which can be used to direct fire and destroy these targets.

Russian exclusive ESM system Moskva-1 is a precision HF/VHF receiver that can detect the reflections of commercial TV and radio signals from targets like ships and aircrafts and find their coordinates. Thus, this passive receiver can track targets and pass on the data to suitable weapon systems for carrying out neutralisation.[6]

RUSSIAN EW CAPABILITIES

Russia has well-organised and equipped EW units and formations since long, which are well trained and battle hardened. Their five EW brigades are deployed with five Russian military districts, which were West, South, North, Central and East districts. These EW brigades support regional EW operations that include jamming of enemy surveillance radars and satellite communications over long ranges. These brigades are equipped with heavier EW equipment like Krasukha-2, Krasukha-4, Leer-3, Moskva-1, and Murmansk-BN systems. Besides, each Russian Army Maneuver Brigade has one EW Company on its orbat which have lighter equipment like R-330Zh Zhitel and carry out EW support within about 50 km range.

Table 1 below gives out the details of major EW equipment held with Russian Army.

S. No.	EW SYSTEM	PURPOSE	YR FIELDED	DESCRIPTION
1	1RL257 Krasukha-4	Targets X-band and KU-band radars, on aircraft, drones, missiles, and low-orbit satellites	2014	Based on two KamAZ-6350 trucks, one a command post and the other fitted with sensors
2	1L269 Krasukha-2	Targets S-band radars, particularly on airborne platforms. Often used paired with the Krasukha-4	2011	Also based on two KamAZ-6350 trucks
3	RB-341V Leer-3	Disrupts VHF and UHF communications, including cellular communications and military radios, over hundreds of kilometres	2015	Consists of a truck-based command post that works with Orlan-10 drones to extend its range

S. No.	EW SYSTEM	PURPOSE	YR FIELDED	DESCRIPTION
4	RH-330Zh Zhitel	Jammer; can shut down GPS and satellite communications over a radius of tens of kilometers	2011	Consists of a truck command post and four telescopic-mast phased-array antennas
5	Murmansk-BN	Long-range detection and jamming of HF military radios	2020	Russian sources claim it can jam communications thousands of kilometers away
6	R-934B	VHF/UHF jammer that targets wireless and wired communications	1996	Consists of either a truck or a tracked vehicle and a towed 16-kilowatt generator
7	SPN-2, 3, 4	X- or K u-band jammers that target airborne radars and air-to-surface guidance-control radars	(not available)	Consists of a combat-control vehicle and an antenna vehicle
8	Repellent-1	Antidrone system	2016	Weighs more than 20 tonnes
9	Moéskva-1	Precision HF/VHF receiver for passive coherent location of enemy ships and planes	2015	Published sources cite a range of up to 400 kilometers

Table 1: Major Russian EW Equipment [7,8]

ECCM is meant to protect electronic systems from ESM and ECM. With highly sophisticated sensors and jammers having been developed, ECCM has become extremely important aspect of EW for survivability on the battlefield. ECCM encompasses technologies and methods to shield electromagnetic systems from being detected or jammed. Some of the ECCM techniques include frequency hopping and spread spectrum techniques that are resistant to jamming. One example during the Russia- Ukraine war is use of US supplied SINCGARS radios by Ukraine which have anti jamming measures.

INITIAL LACK OF IMPACT OF RUSSIAN EW

Russia is known to have well equipped EW units and formations with highly skilled and experienced personnel. Therefore, it was expected that Russian forces, with their overwhelming proportion of EW resources, would dominate the electromagnetic spectrum right from the beginning.

Russia had earlier invaded the Crimean Peninsula in Feb 2014, a part of Ukraine and captured it. Since then, Russians have been using EW as a vital part of their operations in no war-no peace situation, also called 'Grey Zone' warfare in the Donbas region. Russians used Leer-3 EW vehicles along with Orlan-10 drones to jam Ukrainian communications. They were also breaking into the local mobile-phone networks and sending publicity material. Ukrainian radios were detected, geo located and targeted.

However, in the major escalation, when the Russian invasion commenced in February 2022, it was observed that the Russian EW was not effective. Ukrainian forces were not facing the levels of jamming which they had experienced in Donbas. The effect of drones and ground based EW operations was also not visible. Russian forces did carry out physical destruction of some radio stations and TV towers, however, Ukrainian leadership remained in communication with other counties.

REASONS FOR THE FAILURE OF RUSSIAN EW[9]

There were some inherent differences in the operational conditions prevailing during the Russian invasion of Ukraine as compared to Donbas region. The key factors are summarised in the seceding paragraphs.

- **Slow Progress of Russian Offensive due to Lack of Air Superiority.** The Stinger shoulder-fired missiles provided by NATO to Ukraine inflicted heavy attrition on Russian helicopters and jets. So when Russian troops crossed the border, the desired levels of air superiority was not available, making their progress slow and thereby they faced constraints in use of drone based EW equipment. On 03 Mar 2022, the UK's Ministry of Defence said the Russian advance on Kyiv has been delayed by "staunch Ukrainian resistance, mechanical breakdown and congestion".[10]

- **Lack of Manoeuvre Space.** There were difficulties in moving forward due to lack of manoeuvre space and Ukrainian resistance. Also, there were problems in deploying ground based EW equipment due to lack of deployment areas for jammers in predominantly urban environment.

- **Inability to Effectively Employ Russian Drones.** Russian forces could not send their drones at far distances due to limited range and vulnerability of control signals in Ka and Ku bands. Russians resorted to advance along multiple axes with Ukrainian forces interspersed between Russian columns and jamming by Ukrainians was effective due to close ranges.

- **Dense Electromagnetic Environment**. Dense population in the areas of operations led to dense electromagnetic environment. With civilian cellphone networks transmissions and military communications getting mixed up, it was difficult for Russian systems to identify military transmitters.

- **Use of NATO Single-Channel Ground and Airborne Radio System, or SINCGARS by Ukraine Forces**. Ukrainian Forces had some Single Channel Ground and Airborne Radio System (SINCGARS) radios and were trained in its operation, but the numbers were very limited. However, after the invasion by Russian forces, large number of these radios were provided by NATO to Ukraine. Their earlier radios were made in Russia and they had some vulnerabilities which were known to Russians, and hence could be exploited. SINCGARS have in-built high grade encryption and frequency hopping features which make them jam resistant.

  There were certain videos released showing Russian armoured convoys stuck along the roads near indicating that there were problems of logistics back up delaying the move. The effect was felt on the move of other elements also including EW equipment. Also, the Russian forces remained on the move, due to which they could not set up heavy systems like the Krasukha-4.

CONSOLIDATION OF RUSSIAN EW EFFORTS[11]

Russian forces slowly consolidated their EW efforts and started becoming more effective. Excalibur artillery shells, which were received by Ukraine from the US in March 2022 had GPS navigation system which were

Figure 2 : Russian Jammer Krasukha 4. **Source :** https://spectrum.ieee.org/the-fall-and-rise-of-russian-electronic-warfare

highly accurate. By March 2023, they suddenly started missing their targets due to jamming of GPS signals. Similarly, Joint Direct Attack Munitions (JDAM) guided aerial bombs and Guided Multiple Launch Rocket System GMLRS long-range missiles, which are used with U.S-made High Mobility Artillery Rocket Systems (HIMARS) started missing the targets. Jamming was also being carried out of the control signals of Ukrainian drones, making them crash.

The operational situation in Ukraine has considerably changed and Russia forces are at an advantage now. Russia has consolidated its positions in Ukraine's South and East. Ukraine has suffered heavy attrition in men and weapons. With consolidation of positions, the front lines are better defined and the Russian logistics support has also improved considerably. Russian forces are now using their EW systems for directing indirect weapons. The Russian aim of capturing Kyiv in a quick operation did not materialize and the conflict has changed to a

war of attrition, which provides opportunities to Russian forces to use EW advantageously. Russian forces are no longer spread over multiple lines in built up areas and they are able to find Ukrainian positions and direct fire at them.

Russia has overwhelming superiority in EW resources as compared to Ukraine with three EW brigades deployed in this conflict. The Russian EW operators have gained enough experience with SINCGARS radios and are able to detect the emissions with Leer-3 and Orlan-10 drones. Though due to high grade encryption and frequency hopping, it may be difficult to intercept and exploit, it is possible to detect the transmissions and carry out its geolocation. The well-defined front lines enable Russian EW units to target Ukrainian military units based on the detected transmissions.

Russians had found it difficult to use their powerful EW system, Krasukha-4 during advance towards Kyiv. Now in the Donbas region, EW brigades are effectively using the Krasukha-4 to jam the radars and communication links on Ukrainian drones, thus degrading their surveillance.

Russian forces have also carried out re-organisation of their forces to suit the present conflict. The manoeuvre brigades with an strength of two thousand have been reorganised into battalion tactical groups (BTGs) with each having one section of maneuver brigade's EW company for close support. The GTGs are using short range jammers like the R-330Zh Zhitel to jam the control signals of Ukrainian drones ranging from Bayraktar TB2s to DJI Mavics. R-934B VHF and SPR-2 VHF/UHF jammers are being used to degrade communications. Russian EW is fully exploiting the loopholes when Ukrainian units use older radios and cellphones.

UKRAINE'S FIGHT BACK[12]

Ukraine has also augmented its EW resources to counter the Russian electronic attacks. They have successfully employed US supplied counter-drone systems and have downed large number of Russian

Figure 3 : Russian Leer-3 EW System with Orlan-10 Drone for Range Extension. **Source :** https://spectrum.ieee.org/the-fall-and-rise-of-russian-electronic-warfare

drones by jamming of GPS and control signals. They have also been reported to have used high power microwave to damage electronic components in drones and disable them.

They are also using the EW systems provided by the US to jam the communication systems of the Russians with considerable success. The Russian forces do not have very advanced radios like SINCGARS in all their units and often use mobile phones and unencrypted radios for communications which are susceptible to jamming and DF. Russia's latest radio, the 'Azart' sixth-generation SDR, developed by Russia's NPO Angstrem are being introduced in service, but, so far, their numbers are small.

Well defined front lines are also helping Ukrainian EW as it is more convinient to carry out location fixing without ambiguity. Ukraine's EW

have worked on the vulnerabilities of Russian high power systems as it is easy to detect their transmissions. Ukrainian EW is now detecting transmissions from Leer-3 and Krasukha-4 and making them targets.

Ukraine is in the process of developing indigenous EW System. One Ukrainian company, Infozahyst is engaged in developing such equipment. In a modest beginning, two of their equipment have already been introduced in service. These are 'Plastun-RP3000' man-portable direction finder, and truck-mounted version, the Khortytsia-M. Many more equipment are under development.

UKRAINE'S KURSK OFFENSIVE SUPPORTED BY ELECTRONIC WARFARE AND DRONES[13]

Ukraine launched a surprise offensive on 06 Aug 2024 advancing into Russian territory and threatening the city of Kursk. During this offensive, Ukrainian forces planned and executed EW operation very meticulously and effectively. According to Russian military Telegram channel Troika (Three), the Ukrainians forces disabled Russian reconnaissance drones, denying intelligence to the enemy using new interceptor FPVs. Thereafter, avoiding enemy observation, short-range jammers were moved forward to advance positions which were already fed with data from ESM activities carried out in preparation to this offensive.

STARLINK EFFECT[14]

In February 2022, American company SpaceX activated their Starlink satellite internet service in Ukraine to replace internet and communication networks destroyed by Russians during the conflict. Since then, Starlink is being used by Ukrainian government, military and civilians. The Starlink internet has provided a significant benefit to Ukraine's military units, enabling them to share real-time drone inputs, and provide communications where cellphone services have been disrupted. The network has been very useful in guiding Ukraine's drone attacks on Russian targets, thus providing considerable boost to Ukraine's operational efficiency.

Starlink operates a large constellation of thousands of low-earth orbit satellites. It uses narrow beams of the Ku and Ka bands, and the antennas are very small due to higher frequencies which are steered to reject unwanted signals. Thus, they are difficult to jam. The data over the network is encrypted making it highly secure.[15]

RECOMMENDATIONS

- The analysis of EW operations in Russia Ukraine conflict brings out that EW has to be planned as part of overall operational plans and not in isolation. Movement and deployment of EW resources and logistics support have to be facilitated by commanders to harness its full potential. Russian forces found it difficult to extend the ranges of jammers through drones due to lack of air superiority in the intended areas of operations.
- Conventional EW equipment, especially the jammers are high power equipment which are bulky and often carried on heavy mobile vehicles. Taking them close to the enemy lines in the battlefield is fret with the risk of being a target. Hence, there is a need to lay proper emphasis on light weight equipment operating from alternate platforms to work in echelons.
- EW is a weapon of war and EW planning must be fully dovetailed and synchronised with the overall operational plan. It should not be employed in isolation.
- Jamming of enemy's electronic devices is extremely resource heavy. Also, all the systems cannot be jammed all the time. There should be proper prioritisation of targets as per the operational conditions.
- Anti-jamming measures like frequency hopping and spread spectrum techniques are a must for the radios for operational deployment.

- Incorporation of encryption in devices is highly essential as it provides protection against monitoring by ESM devices and also denies information regarding the type of network. Thus it makes it difficult for the enemy to prioritise the targets.
- The vulnerability of GPS signals from the enemy jammers puts a big question mark on GPS based navigation and guidance systems. This calls for having option of working in GPS denied environment. There should be alternative systems like inertial navigation, and advancements like quantum technology based inertial navigation require due consideration.
- Open-source intelligence is critical, including social media posts. Russian soldiers are being targeted when they violate rules and use their cell phones.
- Ukrainian political leaders used social media to communicate directly with their people.
- There should always be provision for alternate means of communications available during the operations. For example, Starlink proved to be a great enabler for Ukraine during a crisis situation.
- Perhaps the biggest lesson from Ukraine for EW is that winning the airwaves does not equal winning the war.

CONCLUSION

Although Russia possesses well developed EW systems since long time which they have been constantly upgrading. But Russian forces were not successful in achieving electromagnetic dominance in the battlefield at least in the initial phases of the conflict. This happened due to various reasons like lack of air superiority, slow progress of battle which led not difficulties in movement and deployment of heavy EW equipment. However, they were able to consolidate their EW efforts and increase the effectiveness after the conflict became more static and a war of attrition.

Ukraine, with the support from US and NATO countries, was able to fight back on the EW front. They were able to protect their communication and radars to a great extent and were also able to carry out jamming and disruption of Russian systems.

The employment of EW in this conflict has thrown up many important lessons which have been closely watched by the leading militaries of the world. It is hoped that the lessons learnt will guide the nations including India to be better prepared for an intense battle in the electromagnetic spectrum.

★★★

Maj Gen Ashok Kumar Srivastava, VSM (Retd) has commanded a Signal Regiment in the sensitive Akhnur Sector of J&K, along the Line of Control. After retirement from service, the General Officer has worked with the corporate sector, wherein he headed technological ventures related to Communications, Surveillance Devices, Command & Control solutions and GISArmy and Spectrum Management for the three services.

NOTES

1 *Nimish Gupta, "A Perspective on Electronic Warfare (EW)", USI Publication, available at https://www.usiofindia.org/publication-journal/a-perspective-on-electronic-warfare-ew.html*

2 *Christian Wolff, "Types of Electronic Warfare", Radartutorial.edu. https://www.radartutorial.eu/16.eccm/ja05.en.html*

3 *Mario LaMarche, "The History of Electronic Warfare: An Overview of Electronic Warfare Part 1", Mercury Systems Inc, Blog, 04 Sep 2018 available at https://www.mrcy.com/company/blogs/history-electronic-warfare-overview-electronic-warfare-part-1*

4 *Rajesh Uppal, "Mastering the Electromagnetic Battlefield: Electronic Warfare technology Trends and Market Dynamics", IDST, 30 March 2024. https://idstch.com/technology/electronics/mastering-the-electromagnetic-battlefield-electronic-warfare-technology-trends-and-market-dynamics/*

5 *Chris Gordon, "'More EW Than We Have Ever Seen Before' in Ukraine, Space Force Official Says", Air & Space Forces Magazine, 24 April 2024. https://www.airandspaceforces.com/ew-ukraine-space-force-training-electronic-warfare-leader-says/*

[6] *Bryan Clark, "The Fall and Rise of Russian Electronic Warfare", IEEE Spectrum, 30 Jul 2022. https://spectrum.ieee.org/the-fall-and-rise-of-russian-electronic-warfare*

[7] *Jonas Kjellén, "Russian Electronic Warfare: The role of Electronic Warfare in the Russian Armed Forces", FOI September 2018. https://dl.icdst.org/pdfs/files3/906f2544ddd693eb1118881a5baff0a3.pdf*

[8] *Richard Scott, "From the JED Archives: Tuning In, Turning On: Russia Brings Radio Electronic Combat to the Fore", Journal of Electronic Dominance, December 2020. https://www.jedonline.com/2022/03/22/from-the-jed-archives-tuning-in-turning-on-russia-brings-radio-electronic-combat-to-the-fore/#:~:text=In%20the%20Swedish%20Defence%20Research,to%20that%20of%20other%20combat*

[9] *Mark Cazalet, "Silent Struggle: Accounts from the Frontlines of Ukraine's Electronic War", European Security & Defence Article, 21 Sep 2023. https://euro-sd.com/2023/09/articles/33980/silent-struggle-accounts-from-the-frontlines-of-ukraines-electronic-war/#:~:text=At%20the%20start%20of%20the,fragging%20their%20own%20side's%20communications*

[10] *Nigel Walker, "Conflict in Ukraine: A timeline", Research Briefing, House of Commons, 16 Sep 2024. https://researchbriefings.files.parliament.uk/documents/CBP-9847/CBP-9847.pdf*

[11] *Oleksandr Tartachnyi, "The Invisible War: Inside the electronic warfare arms race that could shape course of war in Ukraine", The Kyiv Independent, 12 Mar 2024. https://kyivindependent.com/the-invisible-war-inside-the-electronic-warfare-arms-race-that-could-shape-course-of-the-war/*

[12] *Mark Cazalet, "Silent Struggle: Accounts from the Frontlines of Ukraine's Electronic War", European Security & Defence Article, 21 Sep 2023. https://euro-sd.com/2023/09/articles/33980/silent-struggle-accounts-from-the-frontlines-of-ukraines-electronic-war/*

[13] *David Hambling, "Ukraine's Kursk Offensive Blitzed Russia With Electronic Warfare And Drones", Forbes, 09 Aug 2024. https://www.forbes.com/sites/davidhambling/2024/08/09/ukraines-kursk-offensive-blitzed-russia-with-electronic-warfare-and-drones/*

[14] *Nick Paton Walsh, "Ukraine relies on Starlink for its drone war", CNN, 26 Mar 2024. https://edition.cnn.com/2024/03/25/europe/ukraine-starlink-drones-russia-intl-cmd/index.html*

[15] *News Article, "How is Starlink Ukraine's strategic tool in the face of Russian invasion ", The Economic Times, 15 Feb 2024. https://economictimes.indiatimes.com/news/defence/how-is-starlink-ukraines-strategic-tool-in-the-face-of-russian-invasion/articleshow/107710900.cms*