

HERTZ & MINDS

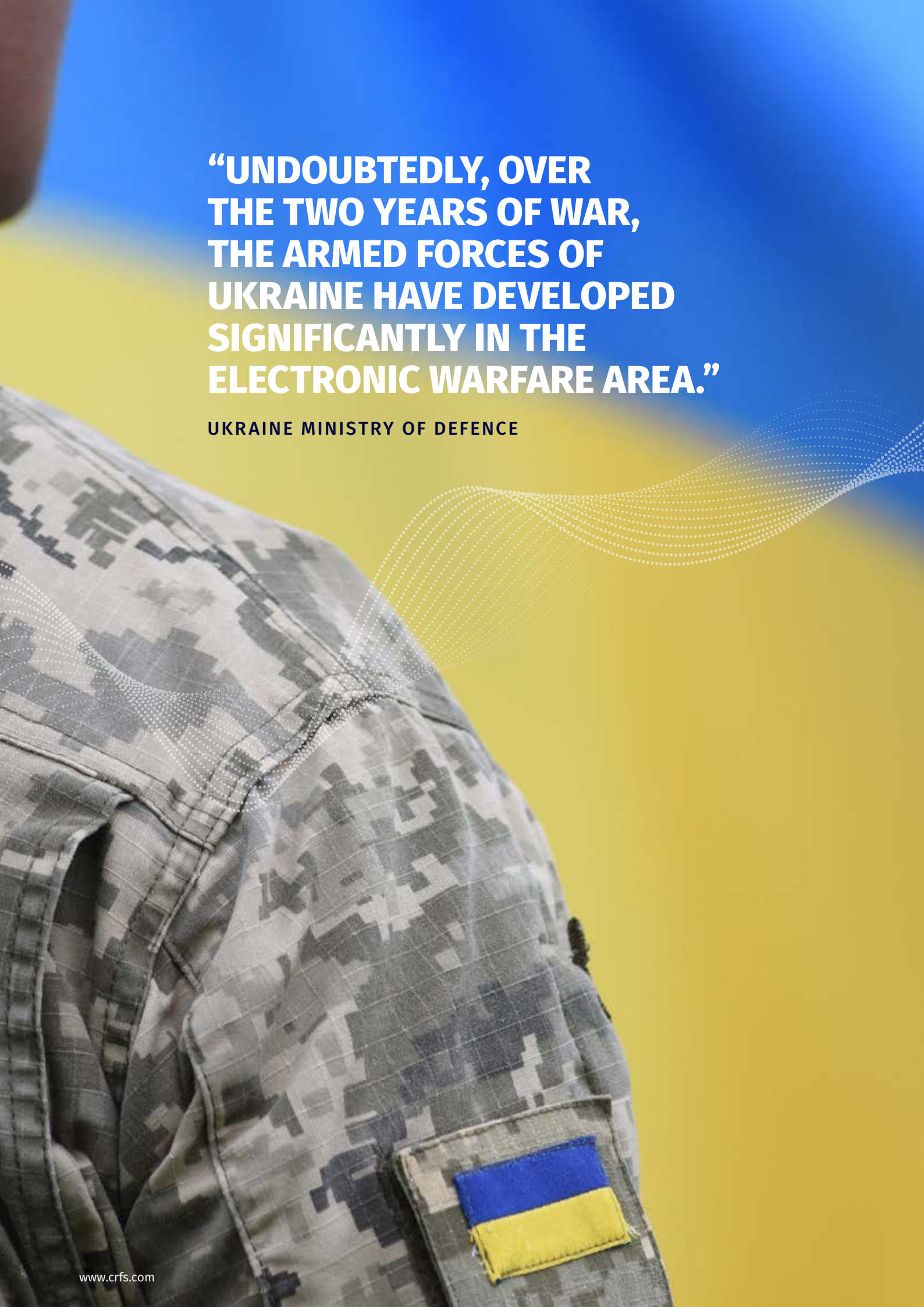
Electronic Warfare
& the tactical land
battle in Ukraine

BY THOMAS WITHINGTON

Sponsored by



Electronic Warfare
by **ARMADA**
INTERNATIONAL



**“UNDOUBTEDLY, OVER
THE TWO YEARS OF WAR,
THE ARMED FORCES OF
UKRAINE HAVE DEVELOPED
SIGNIFICANTLY IN THE
ELECTRONIC WARFARE AREA.”**

UKRAINE MINISTRY OF DEFENCE

HERTZ & MINDS

Russia's invasion of Ukraine is ten years old. Moscow's initial occupation of the country began on 27th February 2014. This invasion resulted in Russia seizing Ukraine's southern Crimea region and parts of her eastern Donbas area. Russia commenced a second invasion on 21st February but failed in her attempt to occupy the rest of Ukraine. Russian military attempt to capture Kyiv and install a puppet government ended in failure. As of August 2024, Russia controls circa 18 percent of Ukraine's territory.¹

The war in Ukraine has been fought on land, at sea, in the air, and in the cyber domains. Hostilities have also been vigorously waged in the radio segment of the electromagnetic spectrum.² Both sides have energetically fought for operational and tactical Electromagnetic Superiority and Supremacy (E2S). Broadly speaking, spectrum superiority is a degree of spectrum dominance where one force can use and exploit this resource without prohibitive hostile interference. Electromagnetic supremacy is the condition where the hostile force is incapable of meaningfully challenging their opponent's use and exploitation of the spectrum.³

Why is E2S important? Both Russia and Ukraine depend on the radio spectrum as it is the environment where radio waves do their work. Radio communications, including Satellite Communications (SATCOM), are essential for force Command and Control (C2) and Situational Awareness (SA). Radar, employed for detecting, identifying, and tracking targets as well as gathering SA, also depends on radio transmissions. Global Navigation Satellite Systems (GNSSs) use radio waves to transmit Position, Navigation, and Timing (PNT) signals. Both Russian and Ukrainian Electronic Warfare (EW) capabilities target their opponent's use of radio, radar, and GNSS PNT transmissions. Radio Frequency (RF) dependent systems like radios, radars and GNSS receivers are targeted with jamming. Meanwhile, the collection of Signals Intelligence (SIGINT) by both sides aids situational awareness. For example, the collection of Communications Intelligence (COMINT) can reveal the location of hostile troops. Detect signals from a soldier's handheld radio, and you probably locate the soldier or detect the radio transmissions from a vehicle's transceiver, and you are likely to locate the vehicle. Individual signals can be

'fingerprinted' to help identify what type of device is performing the transmissions. By identifying the transmission type, it is possible to determine the device. For example, determining that a 35 Megahertz/MHz signal comes from an R-187-P1 handheld radio will indicate that the signal is probably coming from a Russian infantry squad commander's radio. It may also be possible to break into hostile encrypted radio traffic and exploit this for intelligence. Once encryption is broken, it also becomes possible to plant misleading or false information into hostile radio traffic to create confusion. GNSS receivers can be fed with false PNT information, potentially causing adversaries to make navigational errors. Jamming the GNSS receivers of satellite-guided precision weapons may cause these weapons to miss their targets. GNSS PNT transmissions include important timing information. Therefore, transmitting fake information into GNSS receivers could cause timing errors for computing or other electronic systems.

Striving to win E2S makes Emissions Control (EMCON) vital. Militaries must do everything possible to keep their radio transmissions to a minimum. It is instructive that the Ukraine theatre has seen the Ukrainian Army use runners and dispatch riders to move messages and written information. Field telephones have also been employed as cabled connections do not emit radio waves.⁴ Nonetheless, it is not always practical to eliminate radio signals altogether. Radio waves travel at the speed of light; 299,274 kilometres-per-second/186,000 miles-per-second). As such, radio is still the technology par excellence for moving voice and traffic within and between forces on a fast-moving battlefield. To this end, militaries adopt a host of EMCON tactics. Tactics can include keeping radio signals as 'quiet' as possible so they can blend

1 'War in Ukraine', 20th May 2024 @<https://www.cfr.org/global-conflict-tracker/conflict/conflict-ukraine> consulted 19th August 2024.

2 The radio segment of the electromagnetic spectrum stretches from frequencies of three kilohertz up to three terahertz.

3 Withington, T, 'A Moving Experience: Evolving Theoretical Frameworks for Electromagnetic Manoeuvre', 18th March 2021 @<https://tdhj.org/blog/post/electromagnetic-manoevre/> consulted 19th August 2024.

4 Confidential discussion with Ukrainian Army signaller.

into the prevailing electromagnetic noise that surrounds us. Quietening signals in this way is one of several Low Probability of Interception/Detection (LPI/D) techniques. Likewise, one side will hunt the Electronic Support Measures (ESMs) of the other. These ESMs are listening to the electromagnetic spectrum to detect, identify, and geolocate radio signals. Destroying these electronic support measures kinetically reduces or eliminates the ESMs one side has available to detect the radio signals of their opponents.

It is essential that EMCON techniques are coupled with hostile ESM attrition and that both are pursued with vigour on today's and tomorrow's battlefields. Continually looking at what is happening in the radio spectrum can reveal a lot. Suppose one side notes that on a day-to-day basis, there is always a general hubbub of radio traffic in their opponent's locale. Suddenly, that hubbub ceases. Does this mean that an attack is about to occur and that the opposing force has adopted EMCON conditions to increase the attack's chance of success? Likewise, does a sudden increase in traffic mean that manoeuvre is imminent or even in progress? As noted above, ESMs can be used to determine the location of hostile troops, units, and formations. Geolocation techniques let ESMs

follow these assets as they manoeuvre, helping commanders plot the position of red forces on the battlefield. Electronic support measures and their antennas do not necessarily need to be monitored continually. Technology allows them to be programmed to react to specific signals, such as those matching the handheld radios used by hostile squad commanders. When these signals are detected, EW cadres are immediately alerted. Several networked ESMs may even be able to give near real-time indications of where these signals are located and whether they are stationary or mobile.

This report will discuss the electronic warfare dimensions of the ongoing tactical land battle in Ukraine. It will summarise the use of EW during the various stages of the conflict before discussing aspects of the ongoing tactical battle in the electromagnetic spectrum as part of the wider land war. The report will conclude by drawing some broad observations regarding EW in the tactical land battle in Ukraine to date. Regarding sources, this report has been compiled using trusted open-source material and interviews with key informants. While every endeavour has been made to name sources where possible, the identity of some of the interviewees must remain confidential.





PEACE SHATTERED

Russia commenced her initial invasion of Ukraine on 27th February 2014. The Ukrainian armed forces immediately found themselves fighting a determined foe. Russian aggression was seen in the spectrum as much as in Ukraine's skies, on her lands, in her waters, and in cyberspace. Russia's land forces deployed an array of EW systems during the first invasion.⁵ Systems, like the R-330Zh Zhitel vehicle-mounted electronic attack systems were deployed to attack the Ultra High Frequency (UHF: 300MHz to three gigahertz/GHz) radio links Uninhabited Aerial Vehicles (UAVs), relied on to connect the aircraft to the pilot. Ukrainian Very High Frequency (VHF: 30MHz to 300MHz) military communications were targeted by the RB-301B Borisoglebsk-2B vehicle-mounted jamming system. The RB-301B was joined in this mission by the RB-531B Infauna vehicle-mounted jammer.

Russian EW cadres went to great lengths to attack Ukrainian cellphone use, particularly by Ukrainian troops, correctly identifying this as a tactical centre-of-gravity. The Russian Army's RB-341V Leer-3 system uses Orlan-10 UAVs to form airborne cellphone nodes. Ukrainian cellphones would unwittingly connect with these nodes, which appeared genuine. Leer-3 operators could then determine the location of Ukrainian troops based on their cellphone signals with devastating consequences. Leer-3 could also be used to transmit false or demoralising text messages to Ukrainian troops.⁶ In the land domain at the operational level, Russian electronic warriors worked hard to jam trunk communications linking troops in theatre with Ukraine's politico-military leadership in Kyiv. Systems like the GT-01 Murmansk-BN transportable static jamming system were deployed to attack Ukrainian High Frequency (HF: three megahertz to 30MHz traffic).⁷

⁵ Russia's land forces include her army, airborne forces and naval infantry; the latter two forces which are independent services in their own right.

⁶ Kremenetskyi, B, 'General Staff Armed Forces of Ukraine: Electronic Warfare Lessons Learned from the Anti-Terrorist Operation on the Eastern Ukraine', presentation given to the Association of Old Crows electronic warfare advocacy organisation conference in London, 7th/8th July 2017.

⁷ Ibid.

NEW LOOK

Russia's short war against Georgia in 2008 prompted the launch of what were termed the 'New Look' defence reforms. The end of the Cold War in 1991 triggered a long period of relative decline for the Russian military writ large. The economic dislocation experienced by the country in the years that followed had a downstream impact on the military as budgets faced pressure. Military shortcomings during the war in Georgia led to an increase in funding and the activation of a State Armament Programme.⁸ Running between 2011 and 2020, the programme precipitated a reinvigoration of Russia's EW capabilities across her military. Electronic warfare has always occupied a prominent place in Russian military thinking. Russia claims to have been the first nation to have used EW in combat, notably during the 1904/05 Russo-Japanese War.⁹ An aphorism of Russian military thinking says that if an attacking force attrits one third of their opponent and jams another third, the remaining third will be unable to continue fighting.

The revitalisation of Russian EW assets via New Look initially took the form of an order-of-battle reorganisation. Independent EW brigades were formed to provide operational level electronic warfare capabilities in support of the land battle. Each Russian Army manoeuvre formation, typically a motorised rifle or tank division or brigade, was allotted a single EW company to provide tactical electronic warfare. Individual EW battalions were allocated to each of Russia's Combined Arms Armies (CAAs). CAAs amalgamate Russia's land forces in each of her geographical military districts. The EW battalions act as the bridge between each military district's operational EW brigade and its tactical EW companies. A key role of these EW battalions is assisting military district strategic and operational ground-based air defence. Similarly, EW companies were deployed with Russian airborne forces and naval infantry, with the latter also receiving operational-level EW formations.¹⁰

Beyond the reorganisation of Russia's land forces EW order-of-battle, New Look launched a materiel modernisation of land force electronic warfare capabilities. New EW systems, such as the IRL257E Krasukha-4 vehicle-mounted electronic attack system, began entering service from 2012. Krasukha-4 is deployed with the EW brigades to jam airborne radars transmitting on wavebands of eight gigahertz to 18GHz. Krasukha-4 is paired in these brigades with the IL269 Krasukha-2. The latter targets airborne radars transmitting on frequencies of 2.3GHz to 2.7GHz.¹¹ In 2013, the IL262E Rtut-BM/SPR-2 vehicle-mounted jammer entered service, which targets RF-activated artillery shell fuses. The frequencies the Rtut-BM/SPR-2 attacks do not appear to have been made available in the public domain.

Russia's 2014 invasion saw a significant deployment of land force EW capabilities. At least one EW company was deployed to support Russian forces in Ukraine and their proxies. This deployment included two Leer-3 systems, at least one Borisoglebsk-2B, two Zhitels, two RP-377LA Lorandit vehicle-mounted HF and V/UHF COMINT and Communications Jamming (COMJAM) systems, and two R-934B V/UHF jamming systems targeting airborne radio communications.¹²

8 Hackett, J, 'If New Looks could kill: Russia's military capability in 2022', 15th February 2022 @ <https://www.iiss.org/en/online-analysis/military-balance/2022/02/if-new-looks-could-kill-russias-military-capability-in-2022/> consulted 19th August 2024.

9 Von Spreckelsen, M, 'Electronic Warfare – The Forgotten Discipline: Why is the Refocus on this Traditional Warfare Area Key for Modern Conflict?', in *The Journal of the Joint Airpower Competence Centre, Journal Edition 17*, (Kalkar: NATO Joint Airpower Competence Centre, December 2018).

10 McDermott, RN, *Russia's Path to the High-Tech Battlespace*, (Washington DC: The Jamestown Foundation, 2022), pages 329, 331.

11 *Ibid*, page 336.

12 It is important to note that, while most Russian land forces EW capabilities are vehicle-mounted, an EW system does not necessarily constitute a single vehicle accommodating a single capability. Some systems, like the Krasukha-2 and Krasukha-4 are indeed housed on a single truck. Others like the Leer-3 are built around a single vehicle and three Orlan-10 UAVs, while systems like the RB-301B Borisoglebsk and GT-01 Murmansk-BN use several trucks. Larger, multi-vehicle systems may be deployed in their entirety or equally may be deployed in a fragmented fashion with individual vehicles deployed to support the tactical and/or operational mission as dictated by the fight. Source - Kremenetskiy, B, 'General Staff Armed Forces of Ukraine: Electronic Warfare Lessons Learned from the Anti-Terrorist Operation on the Eastern Ukraine'.

INVASION REDUX

The February 2022 invasion saw an altogether larger deployment of Russian land forces EW assets compared to what was witnessed in 2014 and the aftermath. The large deployment was not surprising as the goal of the Russian government was the occupation of Ukraine proper and its eventual absorption into Russia. The author's own analysis suggests that the 2022 invasion was supported by all six of the Russian land forces' EW brigades. These brigades were supported by at least two EW battalions and possibly 28 of the army's 32 EW companies.¹³

Despite this large deployment, the performance of Russian land forces EW appeared lacklustre. Targets for Russian EW cadres included GNSS PNT signals, military/civilian HF and V/UHF traffic, Ukrainian cellular networks, civilian and military SATCOM, UAV radio links, and airborne and ground-based radar. During and immediately after the 2022 invasion, Russia's efforts against PNT signals and cellphone networks appeared to be localised at best. Russian radar jamming was unable to holistically jam Ukrainian ground-based air surveillance and fire control/ground-controlled interception radars. Efforts to kinetically attrit Ukrainian ground-based radar using anti-radiation missile have also been left wanting. As such, Ukraine's integrated air defence system has continued to operate. Russian forces attempted to shut down Ukraine's access to the Starlink and Viasat SATCOM networks during and immediately after the invasion using a cyberattack. These attacks were quickly remedied. "Russia did not prepare her EW forces very thoroughly," remarks Iaroslav Kalinin, chief executive officer of Infozahyst, a Ukrainian EW

company.¹⁴ Russian forces lacked capabilities like Counter-Uninhabited Aerial Vehicle (CUAV) systems, he added.¹⁵ Russian EW cadres did enjoy some success against Ukrainian unencrypted V/UHF tactical radio. However, Russian COMJAM struggled against secure systems like Single Channel Ground and Airborne Radio System (SINGARS) transceivers gifted by the United States.¹⁶ Despite the force weight of EW assets deployed by Russia at the tactical and operational level, Russian land forces have failed to win neither electromagnetic superiority nor supremacy. That said, winning E2S has also eluded Ukraine so far.

It could be argued that Russia's failure to dominate the spectrum was a factor in the failure of the February 2022 invasion. Kyiv remained in Ukrainian control, its government intact. To exacerbate matters, Ukrainian forces were subsequently able to expel Russian forces from some of the land they had occupied. By early April 2022, Russia had been evicted from areas she controlled in northern and northeastern Ukraine. This precipitated the war's transformation into a largely attritional battle. As of early May 2022, Russian forces remained in control of large tracts of eastern, southeastern, and southern Ukraine, including Crimea. Ukraine's vaunted summer offensive of early June 2023 provided some modest gains. Ukraine was reported to have liberated some 370 square kilometres (143 square miles) of her territory from Russian control. This must be set against the 518 square kilometres (200 square miles) of Ukrainian territory Russia succeeded in capturing in 2023.¹⁷ Some of this territory was gained during a Russian attempt to capture the eastern Ukrainian city of Kharkiv, which began on 10th May.



¹³ Withington, T, 'Rah, Rah, Rash Putin?', 2nd March 2022 @ <https://www.armadainternational.com/2022/03/russia-ukraine-invasion-electronic-warfare/> consulted 19th August 2024 and Withington, T, 'The Underwhelming Performance of Russian Land Forces Electronic Warfare; Watt Happened?', 18th August 2022 @ <https://tdhj.org/blog/post/watt-happened/> consulted 19th August 2024.

¹⁴ Interview with Iaroslav Kalinin, chief executive officer, Infozahyst, 24th July 2024.

¹⁵ *Ibid.*

¹⁶ Withington, T, 'The Underwhelming Performance of Russian Land Forces Electronic Warfare; Watt Happened?'

¹⁷ Holder, J, 'Who's Gaining Ground in Ukraine? This year, No-One', 20th March 2024 @ <https://www.nytimes.com/interactive/2023/09/28/world/europe/russia-ukraine-war-map-front-line.html> consulted 19th August 2024.



“EW SYSTEMS DEPLOYED AT THE TACTICAL LEVEL MUST BE EASY TO REPLACE, HENCE MASS PRODUCED, AND CAPABLE OF SEVERAL MISSIONS: TACTICAL JAMMERS USED BY MOUNTED OR DISMOUNTED TROOPS MUST ATTACK UAVS AND GNSS-GUIDED WEAPONS, BUT ALSO ATTACK HOSTILE RADIOS IN THE LOCALE.”

LONDON: ROYAL UNITED SERVICES INSTITUTE

THE UAV THREAT

A key lesson from Ukraine's summer offensive was the need to ensure that small tactical units have electronic protection, particularly against UAVs. Electronic warfare assets must also be widely distributed across the land manoeuvre force. As well as jamming UAVs, tactical EW assets must engage GNSS-guided weapons like air-launched ordnance and artillery. EW systems deployed at the tactical level must be easy to replace, hence mass produced, and capable of several missions: Tactical jammers used by mounted or dismounted troops must attack UAVs and GNSS-guided weapons, but also attack hostile radios in the locale.¹⁸

However, the need to hit these targets raises questions about electromagnetic fratricide. UAVs use UHF links. It is paramount that attacking these links does not come at the expense of inadvertently hitting friendly tactical communications. Russian forces were reportedly adept at regularly resetting or changing their UAV radio frequencies, although they have experienced electromagnetic fratricide problems in other areas. Ukrainian EW cadres would need to discover Russian UAV frequencies anew before they could be attacked. Russian ground forces have been observed to be increasingly good at tightly coordinating EW use with manoeuvre.¹⁹ This was a tactic that they suffered difficulties with following the second invasion.

One aspect of the tactical EW land battle is that when Russian units reduce or stop jamming, Ukrainian units will choose to deluge targets with UAVs carrying kinetic weapons, often with devastating consequences.²⁰ It is not possible for Russian units to simply maintain a continuous wall of jamming in their locale. This can make it impossible for troops to perform inter- or intra-unit radio communications. EW equipment is unlikely to be designed for continuous use, which risks inflicting excessive wear and tear on components. Generators, which produce noise and heat, would need to run continuously to provide electricity, which demands fuel. Choosing moments when Russian electronic protection is weak or non-existent to strike makes sense and reveals a potentially interesting fact. That Russian manoeuvre forces reduce jamming at certain times indicates that Russian radio communications may not be electronically compatible with jamming signals. Are Russian jamming tactics causing significant electromagnetic fratricide?

¹⁸ Watling, J, Danyluk, OV, Reynolds, N, *Preliminary Lessons from Ukraine's Offensive Operations, 2022-23*, (London: Royal United Services Institute, July 2024), page 37.

¹⁹ *Ibid*, page 38.

²⁰ Watling, J, Reynolds, N, *Stormbreak: Fighting Through Russian Defences in Ukraine's 2023 Offensive*, (London: Royal United Services Institute, September 2023), page PDF 11

TACTICAL INGENUITY

Excepting Ukraine's drive into Russia's Kursk Oblast in the west of the latter country from 6th August, the war has largely now assumed a slow-moving attritional nature. This has given both sides the chance to dig in. Russian forces now reportedly deploy one EW system for every one to two kilometres (0.6 miles to 1.2 miles) of front. Circa 90 percent of the electronic warfare waged by either side at the tactical level is focused on the Counter-UAV (CUAV) fight. Ukrainian UAV experts have developed tactics to avoid Russian jamming: Ukrainian UAVs may use the same frequencies as Russian uninhabited aircraft; thus, the Russians cannot jam Ukrainian UAVs without hitting their own assets.²¹ Other, more avantgarde tactics are being employed, such as the use of artificial intelligence algorithms. These algorithms are being developed to ensure a UAV performs its mission independent of radio signals linking the aircraft to its pilot or a GNSS PNT signal.²² Rapidly changing UAV control frequencies across a wide waveband outside of that covered by Russian CUAV jammers is also proving effective.²³

A popular perception of Russian land forces doctrine is that the manoeuvre force is tightly bound to doctrine, rarely exhibiting tactical flexibility and ingenuity. This is disputed by some Ukrainian EW experts who note that their Russian counterparts can be flexible and innovative regarding how they employ electronic warfare. Although this level of ingenuity can vary from unit to unit, Russian EW cadres and Russian land manoeuvre forces writ large have been good at learning lessons and tactical adaptation.²⁴ One example of this trend was the realisation that large, vehicle-

mounted EW systems deployed at tactical/operational levels are vulnerable to attack by Ukrainian artillery and UAVs. Instead, these systems are now routinely deployed some distance from the front or sometimes moved back into Russia. Large EW systems have been replaced at the tactical edge with small, highly mobile, backpack or vehicle-mounted multifunction EW systems. These multifunction systems can jam local communications, hit GNSS signals, and engage UAVs. Relatively low-cost, they are easy to replace. However, these lessons have not been lost on Ukrainian forces, which have adopted a similar approach.²⁵

Networking of EW assets has been important to both sides by maximising the sum of deployed EW systems.²⁶ Placing large numbers of distributed Electronic Support Measures (ESMs) across the battlefield allows the collection of SIGINT across a large area, improving situational awareness. At the same time, this tactic helps identify potentially large numbers of communications systems and networks as targets. The distributed approach is invaluable for detecting and tracking UAVs via their radio transmissions. Large, distributed EW networks have good geolocation attributes: The more ESMs are deployed and networked, the better techniques such as Angle of Arrival or Time Difference of Arrival for target location become. Networking these ESMs via radio links can increase vulnerability to jamming. Using wired links makes sense on a relatively static battlefield, reducing the danger of electronic attack. Networked ESMs also have graceful degradation. One unserviceable or destroyed electronic support measure does not stop the wider collection of SIGINT.

21 Withington, T, 'The Electromagnetic Battle for Ukraine' in the *Journal of Electromagnetic Dominance*, (Washington DC: Association of Old Crows, March 2024).

22 Confidential discussion with Ukrainian UAV expert.

23 *Ibid.*

24 *Ibid.*

25 *Ibid.*

26 Written statement provided to the author by the Ukrainian Ministry of Defence.



Ukraine's land forces have been learning too. As well as countering UAVs, Ukrainian EW cadres have focused on detecting and jamming Russian VHF tactical communications. This exploitation has been aided by the attrition of experienced Russian troops and inexperience of replacements: "As newer, younger and inexperienced Russian forces continue to form a greater percentage of those on the front lines, their lack of good communications security practices will continue to be exploited by NATO forces supporting Ukraine, and of course by Ukraine herself," says Jim Kilgallen, chief executive officer of COMINT Consulting.²⁷ Ensuring that tactical EW use is deconflicted and that manoeuvre forces understand the potential of electronic warfare has been similarly important: "Considerable attention has been paid to the interaction between (the) electronic warfare units of all (the Ukrainian) defence forces (with) echeloning by directions, frequencies, and timings," the Ukrainian MOD articulated in a written statement.²⁸ This concentration on jamming is reciprocated by Russia's manoeuvre force, which works hard to detect and jam Ukrainian tactical communications. However, the advantages and disadvantages for both sides in the COMJAM aspect of the tactical battle is not fixed: "It should be noted that radio jamming effectiveness constantly decreases due to the creation of new interference-resistant radio communications, the use of new radio technologies and the kinetic engagement of enemy electronic warfare equipment."²⁹

An example of the speed that innovation achieves in wartime is Ukraine's Himera Tech Himera-G1 handheld radio. Unveiled in October 2023, this system has been developed as a secure squad radio.³⁰ Secure squad radios have been a key capability that both Russian and Ukrainian troops have been short of. The use of civilian standard 'walkie-talkie' radios, which are an easy target for electronic warfare, by Russian dismounted troops has been well-documented.³¹ The Himera-G1 transmits 25 times less power than the civilian standard Baofeng and Motorola radios used by both sides for intra-squad communications.³² As a result, the Himera-G1 is harder to detect, making it more discreet. Ukraine's defence industry is also developing systems to jam Russian digital communications, impeding Russian tactical and operational C2. Doctrinally, the Ukrainian military has eagerly embraced the E2S mindset: "Ensuring superiority in the radio frequency spectrum is one of EW's main tasks ... EW effects are intended to limit the enemy's use of the radio frequency spectrum for its own benefits."³³ Nonetheless, the embrace of technology brings its own challenges: "Some of the technologies are truly unique (and) certain equipment, due to its technical characteristics, cannot be used by the armed forces of Ukraine."³⁴ This process of evaluation, while unavoidable, absorbs time and resources.

27 Interview with Jim Kilgallen, chief executive officer of COMINT Consulting.

28 Written statement provided to the author by the Ukrainian Ministry of Defence.

29 Ibid.

30 Ibid.

31 'Ukraine conflict: Ukraine develops jam-resistant radio', 18th October 2023 @ <https://www.janes.com/osint-insights/defence-news/defence/ukraine-conflict-ukraine-develops-jam-resistant-radio> consulted 20th August 2024.

32 Source - <https://x.com/RALee85/status/1523192344522207232?lang=en> consulted 20th August 2024.

33 'Ukraine conflict: Ukraine develops jam-resistant radio'.

34 Written statement provided to the author by the Ukrainian Ministry of Defence.



**“BOTH SIDES ARE TRYING
THEIR BEST TO DEVELOP
AND FIELD EW SYSTEMS
AS QUICKLY AS POSSIBLE.”**

IAROSLAV KALININ

THE INDUSTRIAL FACTOR

Whichever side prevails in the spectrum will likely be the one that can identify tactical electromagnetic lessons learned, develop and industrialise a solution and get this to the troops as quickly as possible. “Both sides are trying their best to develop and field EW systems as quickly as possible,” says Mr. Kalinin. “Right now, Ukraine has the upper hand from a development perspective, but not regarding speed of production.”³⁵ Ukraine has shown acumen in rapidly identifying militarily useful technologies from both the civilian and military sectors and rapidly deploying these on the battlefield. Brave1 is the leading Ukrainian organisation that acts as a bridge between the Ukrainian MOD and armed forces. The organisation identifies military requirements and matches these needs with promising technologies.³⁶ “Electronic warfare (EW) is one of the key priorities for Brave1... (For example) effective EW allows us to neutralise both reconnaissance and strike drones without using scarce air defence missiles.”³⁷ Brave1 says that the organisation currently has 180 registered developmental projects, 20 of which “have been codified according to NATO (North Atlantic Treaty Organisation) standards.” Around 110 companies are supporting these development initiatives. Brave1 works hard to encourage electronic warfare companies to find potential solutions to challenges. The organisation also works to streamline and reduce as much as possible the bureaucratic processes associated with getting new EW systems into the hands of the soldier. As of mid-2024, a particular focus of Brave1 is on close quarter EW systems “that directly protect military personnel, their positions, and

equipment. Soldiers on the front lines are already using such tools, and the state is actively procuring them.”³⁸

Despite Ukraine appearing to have the advantage concerning the research, development, manufacturing, and deployment of tactical EW systems, this should not be taken for granted. “We currently have problems regarding mass production,” says Mr. Kalinin. “Russia has more territory than Ukraine and more capacity for mass production of equipment in much safer conditions. In Ukraine, we must dodge rocket and missile attacks daily. We cannot strike every Russian manufacturer and every factory.”³⁹

Nonetheless, Russia should probably not take such safety for granted. Since 25th February 2022, the Ukrainian military has been attacking politico-military and industrial targets within the country. A significant part of the KRET industrial concern, which specialises in EW, is based in the west and south of Russia. Facilities owned and operated by KRET will be high-priority targets for Ukrainian UAV and missile attacks. KRET itself may also be a stumbling block vis-à-vis the need to equip Russian frontlines with tactical EW systems. Russian EW engineers “do not always have the flexibility to implement decisions quickly because of the politico-bureaucratic situation in Russia, says Mr. Kalinin. “Their decision-making behind closed doors can work against getting new developments into the field quickly. They have one big problem in that one big company has all the EW budget.”⁴⁰

³⁵ Interview with Iaroslav Kalinin.

³⁶ Written statement provided to the author by the Ukrainian Ministry of Defence.

³⁷ Written statement provided to the author by Brave1.

³⁸ Written statement provided to the author by Brave1.

³⁹ Interview with Iaroslav Kalinin.

⁴⁰ Ibid.

CONCLUSIONS

That Ukraine is still fighting has remained unconquerable to Russia is testament to how the former has manoeuvred in the spectrum: “Ukraine’s EW success, in particular in the continuous and clever adaptations of tactical drones, rapid assimilation of western technologies and in the deep exploitation of target Russian communications in occupied Ukraine and beyond their borders well into the Caucasus have been key,” says Mr. Kilgallen: “Ukraine has held an invading force that is exponentially superior in every materiel and personnel category completely at bay.”⁴¹

The ongoing war in Ukraine is a prelude to how near-peer adversaries will fight in the spectrum in the wars of tomorrow. Lessons drawn from this conflict relate not only to the application of EW in support of the land battle at the tactical level, but to spectrum operations in other domains at all levels of war. The spectrum battle in Ukraine is performed, to a greater or lesser extent, alongside everyday spectrum use. Civilians go about their daily business throughout the country using their cellphones like everyone else. Harrowing footage of battles fought is gathered on these devices and shared around the world. Shutting off the spectrum to civilians in a warzone solely for military use is not an option. The likelihood of operations being performed in areas where there is no civilian spectrum use in the future is almost zero. According to the International Telecommunications Union (ITU) as of 2023, 90 percent of the world’s population has access to cellular communications.⁴² The ITU is the United Nations organisation tasked with governing global use of the radio segment of the electromagnetic spectrum. Initiatives like SpaceX’s Starlink global SATCOM constellation are extending broadband internet coverage globally. North America and much of Latin America have Starlink coverage, as does most of Europe, parts of Western and Eastern Africa, Australasia, Japan, and much of Southeast Asia. Greenland, Africa, the Middle East, and South Asia will follow in the coming years.⁴³

As Dr. Jack Watling and others note in their superb analysis of Ukraine’s 2023 summer offensive, military operations, particularly employing timely, precision fires, depend on unimpeded access to the spectrum.⁴⁴ Land force targets are detected through visual or SIGINT reconnaissance. Details of the target’s coordinates are shared with a headquarters. A request for fires is made, and this is communicated to the artillery or close-air support aircraft, which execute the mission. It is highly likely that the voice and data traffic integral to this process is carried across radio links, which are, in turn, dependent on access to the spectrum. “The number of systems communicating is increasing. The volume of data being passed is increasing,” notes Dr. Watling and his colleagues.⁴⁵

A second key trend likely to be witnessed is the continual deployment of passive, networked, unattended ESMS across the battlefield. Commanders will be afforded a continual near-real time picture of what is happening in the radio spectrum at any moment. The availability of what may be a constant stream of signals intelligence could help shorten sensor-to-shooter times: Passive sensors detect a Signal of Interest (SOI). Artificial Intelligence (AI) and Machine Learning (ML) techniques embedded in the ESMS determine this SOI as hostile. These techniques continually study the red force’s use of the radio spectrum and draw conclusions. Commanders will verify that the SOI is likely using other techniques, such as matching the SOI with overhead UAV imagery of the target. The target is then engaged kinetically, electronically through jamming, or perhaps with both vectors. AI and ML techniques may show promise in being able to overcome LPI/D techniques in the future. These techniques could trawl through the terabytes of data that networked, passive ESMS continually gather, stripping away extraneous noise and finding the SOI. What is more, AI and ML techniques can perform such work in seconds: a process that could take humans hours, if not days, to perform.

Balances will need to be struck between the need to attack hostile spectrum use while preserving one’s own access, placing a premium on efficient spectrum management. Adequate training can help address these necessities. All troops need to be ‘spectrum minded’ even if electronic warfare or signals it is not their core discipline. The manoeuvre force makes efforts to protect itself from air, artillery and opposing manoeuvre threats. It must likewise take precautions when facing threats in the spectrum.

If there is one clear message from the Ukrainian war applicable to spectrum operations writ large, it is that NATO and allied forces can no longer take their ownership of E2S for granted.⁴⁶ This is not only because of the threat posed by the EW capabilities of near-peer forces. Military spectrum users will be forced to share that space with other actors, such as civilians and media organisations, no matter how intense the battle. Nations must assume that they will have to fight and hold every hertz of spectrum they can, depriving it to the enemy and thus preserving one’s own ability to electromagnetically manoeuvre in this space. Shutting down the spectrum in a locale is likely to be simply impossible. It may risk alienating local civilians who are perhaps sympathetic to friendly forces. The need to win the battle for E2S to enable electromagnetic manoeuvre will be matched against the battle for ‘hertz and minds’. Both are fights that will have to be won.

41 Interview with Jim Kilgallen, chief executive officer of COMINT Consulting.

42 International Telecommunications Union, ‘Almost 40 per cent of the world’s population now covered by 5G’ @<https://www.itu.int/itu-d/reports/statistics/2023/10/10/ff23-mobile-network-coverage/> consulted 20th August 2025.

43 ‘Coverage Map’ @<https://www.starlink.com/map> consulted 20th August 2024.

44 Dr. Jack Watling is senior research fellow for land warfare at the Royal United Services Institute.

45 Watling, J, et al, *Preliminary Lessons from Ukraine’s Offensive Operations, 2022-23*, page 37.

46 Lorillo, P, ‘EMSO in Modern Conflicts: Looking at the Russo-Ukrainian War’ in *Journal of Electromagnetic Dominance*, (Washington DC: Association of Old Crows: September 2023).



ABOUT THE AUTHOR

Thomas Withington is an award-winning analyst and writer specialising in electronic warfare, radar and military communications and a Research Associate at the Royal United Services Institute. He has written widely on these subjects for a range of specialist and general publications, and he edits Armada International's electronic warfare and military communications webpages and monthly newsletters. He also works as a consultant and adviser in these areas for several leading government and private sector clients and provides regular commentary on security and defence aspects of electromagnetic spectrum use for major media organisations around the world.



Electronic warfare & RF:
A tactical approach to
dominating the spectrum

 **CRFS**

EXTRAORDINARY
RF TECHNOLOGY

CRFS is an RF technology specialist for the defense industry, national security agencies, system integrators, and technology platform partners. We provide advanced capabilities for real-time spectrum monitoring, situational awareness, and electric warfare support to help our customers understand and exploit the electromagnetic environment in congested and contested environments.