INFO FLASH
Finabel
European Army Interoperability Centre

Electronic Warfare: Between Recent Military Developments and New Strategic Priorities

WRITTEN BY ANNA CORENTE

Image credits: https://www.flickr.com/photos/cerdec/10444841335/in/photostream/

Introduction

During the last week of March 2022, various sources reported the capture of a Russian advanced electronic warfare system (EWS) by Ukrainian forces. According to Insider and The Time of London, the Ukrainian armed forces identified an abandoned, damaged container covered by tree branches between the town of Makariv and Kyiv. The container was eventually identified as the command post of one of the most advanced Russian EWS, the 1RL257 Krasukha-4.

The Krasukha-4 command module is a broadband jamming system designed to disrupt Low Earth Orbit satellites, ground-based and airborne surveillance radars used by intelligence corps to capture information about the enemy (DCD, 2022). In its complete version, the Krasukha-4 is a two-part structure composed of a command post module and an electronic warfare system. Jammers like this one are specifically designed to track and then interfere with military electronic and communication devices and disrupt unmanned aerial vehicles or deviate enemy's missiles. Among the examples of systems vulnerable to this model of EWS, there are the JSTARS and the AWACS, radars respectively used by the United States and NATO forces.

Starting from 2014, the official debuting year of electronic warfare systems on the battlefield, Russia has been considered a global leader in developing EW technologies. In the same year, the Pentagon noted that "Russia does indeed possess a growing EW capability, and the political and military leadership understand the importance of technical advances in this type of warfare" (U.S. Foreign Military Studies Office, 2014). The possibility of using electromagnetic energy to control the electromagnetic spectrum of the enemy is one of the most essential military capabilities in modern conflict. Therefore, both NATO and EU Member States need to increase their understanding of this type of technology to strengthen their command and control capabilities and realign to the advantage that Russian forces have enjoyed.

Now that Western forces have seized part of the Russian Krasukha-4 unit, it will be further analysed and studied by American experts. On the Russian side, as clearly noted by Kelsey D. Atherton in a Popular Science article, every attempt to rebuild its electronic warfare will have to assume that part of its strategic innovations is now known (2022). Conversely, for NATO and EU Member States, the discovery of the Krasukha-4 opens the door to further technological development of EW capabilities. The finding is also likely to enable NATO and European powers to deploy more advanced detection and destabilisation operations vis-à-vis future opponents.

Electronic Warfare: What is it about?

NATO has described electronic warfare as a "military action that exploits electromagnetic energy, both actively and passively, to provide situational awareness and create offensive and defensive effects" (NATO, 2018). Indeed, EW systems range from indirectly providing support to troops by means of situational awareness, to directly disabling enemy transmissions.

EW capabilities can operate in three broad types of military activities:

1. Electronic Support (ES) that is using informative tools and cyber operations to detect, rapidly intercept and track electromagnetic sources to recognise potential menaces. Providing Electronic Support means to guarantee operations of intelligence, surveillance, and reconnaissance against opponents' military capabilities and communicate with friendly forces.
2. Electronic Protection (EP) is the full package of activities designed to protect friendly signals and devices from any potential attack. It includes neutralising enemy attempts to jam communication networks or destroy electronic facilities.
3. Electronic Attack (EA) is the strategic use of electromagnetic energy to deceive, assault and degrade, temporarily or permanently, enemy electronic sensors. Examples of attacking operations can be both the transmitting of false but credible signals or noise-like signals to others' radars or receivers (EMSOPEDIA).

Modern military forces rely on electromagnetic signals for most of their operations. In fact, drones, satellites, radars, radio devices, autonomous vehicles and other command and control systems communicate and share real-time information by electromagnetic signals.

Nevertheless, the history of Electronic Warfare has a longstanding tradition. Traceable back to the late XIX century, the first development towards the EW was due to the German physician Heinrich Hertz who demonstrated that electronic signals could improve communication, navigation routes and, eventually, military operations (JAPCC, 2018).

According to the JAPCC Journal, one of the first recorded examples of EW occurred already in 1904, during the Russo-Japanese War, when the Russian forces successfully jammed Japanese naval communications. However, it was only during World War II, that both the Allies and the Axis forces started making extensive use of EW capabilities. Such capabilities, furtherly ameliorated and strengthened, were also deployed during Vietnam and the Gulf War of 1991.

After their first employment, EMS were immediately recognised for making military operations more efficient and being crucial for long-distance military activities. Nevertheless, the general western attraction to these technologies seemed to fade rapidly. On the contrary, in view of EW technological and strategic possibilities, countries such as Russia and China have significantly and steadily invested in EMS capabilities all along the last decades. More in detail, as also recognised by NATO commanders, especially Russia, has demonstrated considerable proficiency and has made quick advances across this domain (McCrory, 2021).

However, recent warfare developments and the emergence of new cyber and information threats have reignited the NATO and EU interest in the field of EW.

NATO and EU Strategic Development

In recent years, because of rapid technological advancements, NATO and EU Members have had to adapt to new forms of hybrid and technological challenges. NATO Members, who highly rely on electronic data and electromagnetic signals for their military operations, have recently found themselves in a position of vulnerability.

In one of its public documents, the NATO Supreme Allied Commander Transformation underlined the criticalities and the gaps that the Alliance had to face in terms of EW and EWS (NATO, n.d.). Among such critical aspects, the Commander stressed the difficulty in closing the NATO EW/EWS warfighting capabilities gap if compared to other international Powers. Indeed, NATO operational commanders lacked the "ability to understand the Electromagnetic Environment (EME) and orchestrate EW activities and actions across the levels of warfare and land, maritime, air, space, and cyberspace forces for integrated and unified action in joint operations at operationally relevant speed and scale" (NATO, n.d.). Therefore, to increase its deterrence capacities, NATO has recently revitalised its Electronic Warfare Advisory Committee (NEWAC), responsible for overseeing the development of NATO's EW doctrine, policy and command and control techniques. Moreover, the Alliance has shifted from isolated EW operations in the EMS to joint Electromagnetic Operations (EMO) in the so-called Electromagnetic Environment (EME), to face the rapidity through which the EMS ecosystem changes.

For what concerns the European Union, the European Commission has recently awarded contracts for EW-related projects under its European Defence and Industrial Development Programme (JED, 2021). Several projects have also been deployed by the Permanent Structured Cooperation (PESCO). Among the examples, there is the "Electronic Warfare Capability and Interoperability Programme For Future Joint Intelligence, Surveillance And Reconnaissance (Jisr)" with the objective of producing a comprehensive feasibility study of the existing EU electronic warfare capabilities and recognise defensive gaps to be filled within the Union Members.

However, some challenges in adapting to EW developments remain for both organisations. Indeed, issues of interoperability and standardisation are now at the core of the EU and Alliance discussion. For example, the PESCO initiative "Airborne Electronic Attack" is intended exactly to go in the direction of reinforcing the readiness for EW conflicts but also increasing the dialogue and the share of best practices between military partners. In this context, Spain, France, and Sweden are cooperating to strengthen interoperability between European and NATO air forces, with the aim of developing a platform for Airborne Electronic Attack (AEA) missions that could adapt to the latest in electronic warfare requirements (PESCO).

Future Developments

Nowadays, all military factions are struggling to maintain or obtain a substantial EW capability advantage that will play - and already plays - a fundamental role in modern military operations.

However, as clarified by Gavin O'Connell, Business Development and Sales Director at Chemring Technology Solutions, the new EWS must be able to operate in an increasingly complex, multi-domain, hybrid, and cross-organisation/national environment. In this context, if it is true that Russia has demonstrated to have an effective sophistication advantage in its electromagnetic systems so far, the Ukrainian conflict has changed part of the traditional EW dynamics. EWS has now entered urban scenarios where their synchronisation operations change radically. Hence, it becomes more challenging for operators to execute EW missions in this kind of warfare (Military Times, 2022). What is evident is that future electronic warfare will require more resilient and highly adaptable systems, increased collaboration, and the alignment of both traditional strategies and modern techniques.

Today, once western forces have intercepted one of the Russian most advanced EW modules and potentially gained new operational awareness, the race to further technological development continues.

Bibliography

Atherton, K. D. (2022). The US could get a peek into Russia's electronic warfare secrets thanks to Ukraine. Popular Science. Available at: https://www.popsci.com/technology/russian-electronic warfare-equipment ukraine/#:~:text=Ever%20since%20Russia%20first%20debuted,system%20failure%20for%20necessary%20equipment.

BAE Systems, Electronic Warfare, Website. Available at: https://www.baesystems.com/en-us/productfamily/electronic-warfare

U.S. Foreign Military Studies Office (2014). Russia EW or IW?. OE Watch Commentary. Available at: https://web.achive.org/web/20151025092534/http://fmso.leavenworth.army.mil/OEWatch/201412/Russia_08.html

McCrory, D. (2021). Russian Electronic Warfare, Cyber and Information Operations in Ukraine. The RUSI Journal, 165:7, 34-44. Available at: https://www.tandfonline.com/doi/full/10.1080/03071847.2021.1888654

Military Times (2022). Russia's electronic warfare capability. C4ISRNET Conference Highlight. Available at: https://www.youtube.com/watch?v=slrnrae855E&t=62s

Moss, S. (2022). Ukrainian troops seize Russian electronic warfare system, hand to US. Data Centre Dynamics (DOC). Available at: https://www.datacenterdynamics.com/en/news/ukrainian-troops-seize-russian-electronic-warfare-system-hand-to-us/

NATO MC 64/11, 4 Jul. 2018
NATO Supreme Allied Commander Transformation, NATO C2 of EW Overview and Q & A. Available at: https://www.act.nato.int/application/files/2716/1465/8746/rfi021008_overview.pdf

O' Connell, G. The Future Of Electronic Warfare In Europe. Global Defence Technology. Available at: https://defence.nridigital.com/global_defence_technology_special/the_future_of_electronic_warfare_in_europe

Parker, C. (2022). Dumped unit may hold military secrets. The Times of London. Available at: https://www.thetimes.co.uk/article/dumped-unit-may-hold-military-secrets-9ttjl3zxg

Bibliography

Peach, S. (2021). NATO Electronic Warfare and Cyberspace Resilience. JAPCC Joint Air and Space Power Conference 2021. Available at: https://www.japcc.org/wp-content/uploads/JAPCC-Conf-Read-Ahead-2021-16.pdf

PESCO, Airborne Electronic Attack (Aea). Available at: https://www.pesco.europa.eu/project/airborne-electronic-attack-aea/#:~:text=This%20capability%20will%20allow%20European,and%20in%20cross%2Ddomain%20operations.

PESCO, Electronic Warfare Capability And Interoperability Programme For Future Joint Intelligence, Surveillance And Reconnaissance (Jisr). Available at: https://www.pesco.europa.eu/project/electronic-warfare-capability-and-interoperability-programme-for-future-joint-intelligence-surveillance-and-reconnaissance-jisr-cooperation/

Sgamba, G. Electro Magnetic Spectrum Operation (EMSO). EMSOPEDIA. Available at: https://www.emsopedia.org/entries/electro-magnetic-spectrum-operation-emso/

Shoaib, A. (2022). Ukraine captures one of Russia's most advanced electronic warfare systems, which could reveal military secrets, reports say. INSIDER. Available at: https://www.businessinsider.com/russian-hi-tech-warfare-system-seized-ukraine-hold-military-secrets-2022-3?r=US&IR=T

JED News (2021). European Commission Announces EW-Related Capability Projects. Available at: https://www.jedonline.com/2021/09/20/european-commission-announces-ew-related-capability-projects/

von Spreckelsen Malte (2018). Electronic Warfare – The Forgotten Discipline. Why is the Refocus on this Traditional Warfare Area Key for Modern Conflict? In APCC Journal Issue 27. Available at: https://www.japcc.org/electronic-warfare-the-forgotten-discipline/