 Jet: © CC, Alex Belyukov; Background: © RDVector – stock.adobe.com

Ukrainian Forces have recovered Russian Electronic Warfare (EW) equipment for technical intelligence purposes. This includes the Khibiny EW complex, which is integrated on several Russian combat aircraft, including the Sukhoi Su-34.

Electronic Warfare in Ukraine

Preliminary Lessons for NATO Air Power Capability Development

By Mr Duncan McCrory CEng FRAeS, Freeman Air and Space Institute, King's College London

Introduction

The Russian Federation has invested heavily in Cyber and Electronic Warfare (EW) since the 2008 military reforms as an asymmetric response to NATO military capabilities that depend on sophisticated electronic systems.¹ However, Russia has not fully capitalized on this investment during the current invasion of Ukraine. This paper highlights some key issues and offers recommendations for EW capability development to improve the survivability and effectiveness of NATO air operations in highly contested environments. This paper is based on a presentation delivered by the author

at the NATO Integrated Air & Missile Defence conference hosted at the Italian Air & Space Operations Command in Poggio Renatico on 23 March 2023.

Electronic Warfare During the Initial Invasion

During the initial invasion, the VKS (Vozdushno-Kosmicheskiye Sily; Russia's Aerospace Forces) conducted intensive attacks on Ukraine's Ground-Based Air Defences (GBAD), using a combination of cruise and ballistic missile strikes and anti-radiation weapons.

Russia's invasion force also included its largest combat deployment of EW capabilities to date.² Russian electronic attack systems and aerial decoys jammed and confused Ukraine's air defence radars, many of which had to be taken offline and relocated.

Despite these combined kinetic and non-kinetic attacks on Ukraine's GBAD network, the Ukrainian Air Force (UAF) managed to prevent the VKS from gaining air superiority. This is a remarkable achievement, since the UAF pilots were significantly outnumbered by the VKS, who operate far superior combat aircraft equipped with better weapons, sensors, and EW systems, and were supported by airborne early warning platforms and space-based capabilities. Ukrainian air crew also faced the persistent threat of Russia's strategic Surface-to-Air Missile (SAM) systems, including SA-21s deployed in Belarus and Crimea.³

Whilst these threats imposed significant tactical constraints, the UAF quickly adapted their tactics to survive and remain effective in this high-threat environment. By flying at very low altitudes, below 100 ft in some cases, the UAF pilots were able to hide below the radar horizon of Russian SAMs, using ground clutter and terrain masking to avoid detection, before popping up to engage VKS fighter aircraft.⁴

Russia's Command and Control Issues

Significant weaknesses in command and control compounded Russia's inability to gain control of the air. A lack of planning and preparedness, coupled with procurement and encryption key distribution issues, forced many units to use civilian handheld radios and mobile phones, instead of secure, jam-resistant tactical radios.⁵

Ukrainian EW forces exploited these weaknesses by eavesdropping on Russia's unencrypted transmissions, jamming their communications, and performing targeting for long-range weapons using direction-finding techniques.⁶ Ukrainian EW forces also used electronic attack capabilities to degrade the performance of VKS's airborne early warning platforms, and one of these aircraft was sabotaged in Belarus with an Unmanned Air System (UAS) attack.⁷

Russia's command and control issues hindered their ability to conduct joint air and land operations, and to make real-time tactical decisions in the battlespace. Additionally, the failure to de-conflict EW activities with the rest of their operations led to unintentional jamming of their own forces. The resultant confusion and disruption caused by this electronic fratricide led Russia to scale back its electronic attack efforts, thus enabling Ukrainian GBAD to become more effective.⁸


VKS's Vulnerability to GBAD

Once Ukraine's GBAD network recovered, much of the VKS's aircraft were also forced to fly at low altitude to avoid being shot down by Ukrainian medium and high-altitude SAM systems. Consequently, VKS aircraft came directly within the engagement envelopes of large concentrations of Ukrainian short-range air defence (SHORAD) systems. Ukrainian forces inflicted heavy losses on low-flying Russian fixed-wing aircraft and helicopters, primarily using Man-Portable Air Defence Systems (MANPADS), including the US Stinger, the Russian Igla-series, and the more sophisticated laser-guided UK Starstreak, which cannot be defeated by conventional countermeasures.

Witnessing Russia's heavy losses serves as a stark reminder of the threat posed by GBAD and the proliferation of MANPADS in particular. Platform EW protection capabilities, including Radio Frequency (RF) and Infrared (IR) countermeasures, will remain vital to safeguard NATO aircraft. The proliferation of MANPADS is set to continue, with nations such as China now actively competing with Russia for global exports. China has learned through reverse-engineering foreign weapons and has continuously upgraded and improved the performance of its indigenous systems. For instance, the FN-6 is a reverse-engineered copy of the European Mistral missile system.⁹ However, the FN-6 is equipped with an upgraded digital infrared seeker for improved targeting and resistance to countermeasures, such as flare rejection.¹⁰

There is also evidence of a significant rise in the proliferation of advanced Chinese MANPADS in the hands of violent extremists and other non-state actors. For



 Krashuka-2: © CC, Vitaly V. Kuzmin; Grid: © ihor – stock.adobe.com

Russian EW forces have attempted to disrupt NATO ISR operations with Electronic Attack capabilities. The KRET Krasukha-2 is designed to jam Airborne Early Warning and Control (AWACS) radar.

instance, in 2014, ISIL/Daesh operatives in Syria and Iraq were equipped with the FN-6, in addition to various Russian-origin MANPADS.¹¹ This highlights an unquestionable need to develop and procure advanced laser-based Directed Infrared Countermeasures to safeguard NATO air operations against the growing MANPADS threat.

Air Superiority Cannot Be Assumed

Although Ukraine has successfully blunted VKS low-altitude operations, Russian Su-35 and Mig-31 interceptors operating at high altitude have shot down

significant numbers of Ukrainian ground attack aircraft using long-range radar-guided missiles. This threat, compounded by the presence of Russia's strategic SAMs, has led to a state of mutually denied air superiority.

Russia has improved the effectiveness of its EW operations since the initial invasion, with considerable success in countering Ukrainian UAS. Russian EW forces have also attempted to jam NATO ISR aircraft operating on the periphery of Ukraine's border.¹² Of greater concern are the aforementioned strategic SAMs deployed by Russia in Belarus and Crimea, which are holding NATO ISR aircraft at significant risk, in addition to harassment from Russian combat aircraft. Russian aircrew

have already committed several unprofessional and dangerous acts against NATO ISR platforms; the risk of further aggression and miscalculation ending in tragedy must not be underestimated.¹³

In addition to procuring weapons from Iran and North Korea, Russia is receiving non-lethal military aid and satellite imagery from China.¹⁴ With President Putin having openly declared a 'no limits' relationship between the two nations, it is entirely possible that Russia could seek support from China to re-arm its military forces.

Ultimately, the crisis in Ukraine has demonstrated that, unlike the past two decades of counter-insurgency operations in the Middle East, control of the air cannot be assumed. Instead, we are seeing a return to conditions similar to those faced in Kosovo during Operation Allied Force, where NATO aircraft had to conduct operations in highly contested airspace.

NATO EW Capability Development Priorities

If a direct conflict were to emerge with Russia, NATO would need to fight hard to gain access, survive, and achieve air superiority. EW will be a key enabler, and NATO needs to develop a full spectrum of Suppression and Destruction of Enemy Air Defence (SEAD/DEAD) capabilities.

Air and Space-based ISR will remain vital to gaining intelligence on adversary air defences and informing the development of countermeasures. Mission planning, mission data, on-board defensive aids, and expendable active and passive countermeasures will be crucial to breaking the adversary's kill chain and maximizing the survivability and lethality of NATO aircraft in future hostile environments. Finally, a plethora of offensive systems, including electronic attack and anti-radiation weapons, will be necessary to disrupt, deceive, and destroy hostile air defence networks.



Ukrainian Forces have inflicted significant losses on Russian aircraft using Man-Portable Air Defence Systems (MANPADS), such as the UK Starstreak (pictured above), which cannot be defeated by conventional EW countermeasures.

Accelerating EW Capability Development

Time is of the essence and funding is often limited to flagship programmes. Therefore, NATO should seek to learn from and more fully exploit existing EW capabilities and new developments within allied nations. For example, Ukraine has captured several high-value Russian EW assets during the conflict, and is reported to have handed these over to allied nations for technical intelligence purposes.¹⁵ NATO should aim to make best use of the intelligence gained from these efforts to develop and update electronic countermeasures.

Additionally, the Royal Air Force (RAF) Rapid Capabilities Office is reported to be experimenting with low-cost autonomous air systems, designed to operate in swarms and use compact EW payloads to disrupt and confuse air defence systems.¹⁶ Furthermore, the RAF is integrating a Modular Air Platform Protection System

onto crewed ISR platforms, which is compliant with the NATO Defensive Aids System (NDAS) standard and capable of integrating advanced RF and IR countermeasure systems to provide protection against a variety of threats.¹⁷

Doctrine and training are equally important to technology development and equipment acquisition. Cyber and Electromagnetic activities cannot be an afterthought; they must be tightly woven into joint force manoeuvre plans. Additionally, regular training in electronically representative environments will help allied forces to survive and remain effective in the presence of EW threats, such as those deployed by Russia in Ukraine. Further investment and strengthening of the NATO Joint Electronic Warfare Core Staff (JEWCS) is recommended to enhance their capacity to deliver this training across the Alliance. Specialist training will also be necessary to ensure that NATO aircrew develop proficiency in the tactics, techniques,



The NATO Joint Electronic Warfare Core Staff supports all NATO Headquarters and Commands in the development of EW policy, concepts, doctrine, and experimentations, in addition to providing expertise and training for operations in electronically-contested environments.

and procedures required to work together and deliver complex kinetic and non-kinetic effects, such as those employed on SEAD/DEAD operations. However, given the proliferation of space-based SIGINT capabilities, NATO will need to consider novel means to conduct EW training in the live environment, coupled with greater use of secure synthetic facilities to prevent adversary intercepts.

Ultimately, whether it is safeguarding our aircrew or disrupting, degrading, and denying adversary situational awareness, communications, and targeting, Electronic Warfare will be the fundamental enabler to more survivable and effective NATO air operations in hostile environments in the future. ●

1. McCrory, D., 'Russian Electronic Warfare, Cyber and Information Operations in Ukraine: Implications for NATO and Security in the Baltic States', *RUSI Journal* 165, no. 7, 2020, pp. 34–44.
2. Withington, T., 'The Underwhelming Performance of Russian Land Forces Electronic Warfare – Watt Happened', *The Defence Horizon Journal*, 18 August 2022. <https://www.thedefencehorizon.org/post/watt-happened> (accessed 4 May 2023).
3. Bronk, J. and Watling, J., 'The Russian Air War and Ukrainian Requirements for Air Defence', *RUSI*, p. 12. <https://static.rusi.org/SR-Russian-Air-War-Ukraine-web-final.pdf> (accessed 9 May 2023).
4. *Ibid.*, pp. 10–12.
5. Cranny-Evans, S. and Withington, T., 'Russian Comms in Ukraine: A World of Hertz', editorial, *RUSI*, 9 March 2022. <https://rusi.org/explore-our-research/publications/commentary/russian-comms-ukraine-world-hertz> (accessed 4 May 2023).

6. Detsch, J. and MacKinnon, A., 'The Ukrainians Are Listening: Russia's Military Radios Are Getting Owned', 22 March 2022, *Foreign Policy*. <https://foreignpolicy.com/2022/03/22/ukraine-russia-military-radio/> (accessed 19 February 2023).
7. Jennings, G., 'Ukraine Conflict: Russian A-50 AEW&C Aircraft Sabotaged in Belarus', *Janes*, 28 February 2023. <https://www.janes.com/defence-news/news-detail/ukraine-conflict-russian-a-50-awec-aircraft-sabotaged-in-belarus> (accessed 12 March 2023).
8. *Ibid.* 3, p. 13.
9. US Army, 'ATP 7-100.3 Chinese Tactics', p. C-3, 2001. https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN34236-ATP_7-100.3-001-WEB-3.pdf (accessed 4 March 2023).
10. 'Chinese Man-Portable Air Defense Systems', *Vermilion China*, 15 December 2022. <https://www.vermilionchina.com/p/18-chinese-man-portable-air-defense> (accessed 4 March 2023).
11. UK Ministry of Defence, 'Evidence on UK military operations in Syria and Iraq. Memorandum submitted by UK Ministry of Defence', House of Commons Defence Select Committee, 1 December 2015. <https://committee.parliament.uk/writtenevidence/62938/html/> (accessed 6 May 2023).
12. Bertrand, N., 'Intelligence: Russia Has Taken to Trying to Jam NATO Plane's Radar', *CNN*, 11 March 2022. <https://edition.cnn.com/2022/03/10/politics/nato-surveillance-flight-russia-belarus/index.html> (accessed 13 March 2023).
13. Gibbons-Neff, T. and Schmitt, E., 'Miscommunication Nearly Led to Russian Jet Shooting Down British Spy Plane, US Officials Say', *The New York Times*, 12 April 2023. <https://www.nytimes.com/2023/04/12/world/europe/russian-jet-british-spy-plane.html> (accessed 15 April 2023).
14. Jones, A., 'US Sanctions Chinese Satellite Firm for Allegedly Supplying SAR Imagery to Russia's Wagner Group', *Space News*, 27 January 2023. <https://spacenews.com/u-s-sanctions-chinese-satellite-firm-for-allegedly-supplying-sar-imagery-to-russias-wagner-group/> (accessed 8 March 2023).
15. Dangwal, A., 'Russia's "Most Advanced" Electronic Warfare (EW) Jamming Pod Mounted on Su-30 Fighter Seized By Ukraine', *The EurAsian Times*, 13 September 2022. <https://eurasianimes.com/russias-electronic-warfare-ew-jamming-pod-ukraine/> (accessed 6 May 2023).
16. Trevithick, J., 'RAF Tests Swarm Loaded With BriteCloud Electronic Warfare Decoys To Overwhelm Air Defenses', *The Drive*, 8 October 2020. <https://www.thedrive.com/the-war-zone/36950/raf-tests-swarm-loaded-with-britecloud-electronic-warfare-decoys-to-overwhelm-air-defenses> (accessed 5 March 2023).
17. UK Ministry of Defence, 'New National Enterprise Approach for Air Platform Protection', 18 July 2022. <https://www.gov.uk/government/news/new-national-enterprise-approach-for-air-platform-protection> (accessed 5 March 2023).

ABOUT THE AUTHOR

Mr Duncan McCrory

Freeman Air and Space Institute,
King's College London



Mr Duncan McCrory is an Aerospace Systems Engineer with twenty years of experience in mission systems for ISR and Combat Air platforms, including Chief Engineer and Capability Management roles.

Duncan is currently pursuing a PhD at the Freeman Air & Space Institute, King's College London. Duncan's PhD

research is focussed on the challenges posed by Anti-Access/Area-Denial environments to Air and Space-based ISR operations.

Duncan is a Chartered Engineer and was elected a Fellow of the Royal Aeronautical Society in 2017 for his contribution to aviation.