www.rusi.org

Occasional Paper

# Airborne Electromagnetic Warfare in NATO: A Critical European Capability

Justin Bronk


Occasional Paper

**194 years of independent thinking on defence and security**

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 194 years.



RUSI Occasional Paper, March 2025. ISSN 2397-0286 (online)

Cover image: US Navy Boeing EA-18G Growler electronic warfare aircraft; zapper/Adobe Stock

**Royal United Services Institute**
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org
RUSI is a registered charity (No. 210639)

# Contents


**Executive Summary** 1

**Introduction** 3

**I. Electromagnetic Warfare (EW) Basics** 6

Electromagnetic Attack (EA) 6

Electromagnetic Support Measures (ESM) 7

Electromagnetic Countermeasures (ECM) 8

EW is Not the Same as Cyber Warfare 9

**II. Rapidly Evolving Requirements for Effective EW** 11

**III. NATO Reliance on the US for EW in the Air and Space Domains** 17

**Conclusions and Recommendations** 24

**About the Author** 28

# Executive Summary

Airborne electromagnetic warfare (EW) capabilities are critical to Western airpower, but they are also one of the areas in which NATO countries have the greatest dependence on the US military. The scale of this dependence represents a potential risk for the Alliance if Russian aggression occurs when American reinforcements and support capacity are either tied up with a concurrent crisis in another theatre or are otherwise unavailable at scale.

- No single European country has either the existing foundations or sufficient suitably qualified and experienced personnel to rapidly be able to add meaningful capabilities across all aspects of EW. Therefore, creating end-to-end capability within Europe will require genuine multinational partnerships and cooperative specialisation.
- The UK has maintained world-class signals analysis and mission data-programming expertise, especially through the Joint Electronic Warfare Operational Support Centre and the tactical data-focused Typhoon Mission Support Centre. However, maintaining these vital and scarce capabilities in electromagnetic support measures (ESM) and electromagnetic countermeasures (ECM) in an era of rapidly evolving digital threat systems will require increased investment and rapid adoption of AI- and machine learning-enabled toolsets.
- The key to rapidly increasing European NATO's ability to collect electromagnetic intelligence data is to ensure that all the electronic support measures suites being carried by non-traditional ISR platforms – such as modern fighter aircraft and UAVs for other mission sets – are used to their full collection potential.
- A pooled multinational electromagnetic attack squadron procured and run by NATO could allow air forces that are too small to economically field dedicated EW capabilities to meaningfully contribute funding and personnel. There is precedence for this approach in other areas, such as the NATO Airborne Warning and Control System Force (AWACS), the Multinational Multirole Tanker Transport Capability fleet, and the Strategic Airlift Capability fleet.
- European countries should increase funding for the (currently largely experimental) development of stand-in airborne electromagnetic attack (EA) capabilities using relatively cheap uncrewed autonomous systems that can loiter for significant periods over hostile territory, as a means of rapidly expanding EA capabilities.
- The UK has already made significant development progress in novel affordable stand-in EA capability development under the RAF's Autonomous Collaborative Platforms strategy and the work of the Air and Space Warfare Centre. This

represents an obvious route through which increased investment could deliver rapid national and potentially Alliance capability growth.

- Procurement of more expensive but higher performance traditional air-launched stand-in EA capabilities such as ADM-160 MALD-J/X and SPEAR EW should also be pursued as a priority by at least some European countries to enhance the effectiveness of both fourth- and fifth-generation fighter fleets and strike munitions.

# Introduction

Electromagnetic warfare (EW) is a critical and often overlooked facet of modern warfare across all operational domains, particularly as adversaries continue to replace legacy analogue threat systems with digital ones. It is also a particularly acute area of military reliance on the US by other NATO members. EW is perhaps most critical in the air domain, due to the high level of technological sophistication involved, and the degree to which fine performance margins between opposing sensors, effectors and platforms can determine the difference between successful engagements and denial of access to contested airspace.

The air domain is also where Western NATO countries have traditionally maintained the greatest degree of technological and tactical overmatch relative to other potential state adversaries. The manifest battlefield dominance conferred by successfully gaining air superiority in various conflicts has led most Western armed forces to double down on airpower as their key source of lethality and ISR. However, this reliance has led adversary nations such as Russia and China to prioritise the development of ground-based air defences (GBAD) and integrated air defence system (IADS) capabilities, as well as EW capabilities tailored around degrading key facets of Western airpower. NATO reliance on airpower for its conventional deterrence and ultimately warfighting edge also means that if air forces (and equally vital space forces) lose advantage in the electromagnetic spectrum (EMS), this loss represents an even greater risk than it would in other domains.

There are four key reasons why policymakers and defence planners in NATO, and especially in European NATO member countries, need to better understand and bolster the people and resources committed to EW programmes now.

1. Russia is waging an aggressive war in Europe and its military–industrial output and hardened commitment to an adversarial posture towards NATO nations mean that it could rapidly become a direct threat in the coming years. This has led to a major shift in the priorities driving European militaries' force structure planning and funding. However, forces optimised to provide credible defensive capabilities against Russian military threats have very different EW dependencies and vulnerabilities to manage than those optimised for counterinsurgency campaigns against irregular forces.
2. The war against Ukraine has exposed Russia's military to enormous evolutionary pressures, as well as to many Western weapons systems. The result has been a dramatic increase in the pace of Russian EW and sensor development, both in terms of new equipment and the rate at which existing

equipment is updated.[1] This has been driven primarily by the need to improve performance against innovative and rapidly evolving Ukrainian capabilities, but it also has clear implications for the pace at which Western forces would need to be able to adapt in the EMS in any future direct clash with Russian forces.

3. The current degree of dependence by NATO members on the US creates risks for the Alliance as a whole in an increasingly unstable global geopolitical situation where the risk of wider conflict is growing in Europe, the Middle East and the Indo-Pacific simultaneously. Dependence on the US for key military capabilities is hardly a new issue, but few European defence gaps are as stark as for certain key aspects of EW, such as airborne electromagnetic attack (EA). Airborne EA is a crucial requirement for suppression and/or destruction of enemy air defences (SEAD/DEAD) operations and is currently only provided to NATO by periodic detachments from US Navy EA-18G Growler land-based expeditionary squadrons.[2] It is important to understand these dependencies at the policy level. In particular, which areas can be relatively quickly fixed, and which will remain key support areas required from the Pentagon and other US agencies in a NATO context for the foreseeable future? Clarity in this regard is likely to be particularly important in the context of a second Trump administration that has strongly signalled an intent to force other Alliance members to increase their share of burden sharing and defence spending.[3]
4. It is an important moment for policymakers to focus on EW due to the rapid changes in both threat and potential capability opportunities that are being brought about by AI- and machine learning (ML)-enabled technology. On the threat side, these techniques are already helping current and potential future adversaries to greatly increase the rate at which they can evolve their own sensor and EW capabilities. On the other hand, AI and ML tools are particularly well suited to enabling transformative increases in the capacity of medium-sized and even small countries to develop, field and maintain potent EW capabilities, given the correct support and resourcing.

Chapter I of this paper explains the basic types of EW and the dependencies that they have in terms of electronic intelligence (ELINT) collection and mission data updates, and offers a brief outline of the distinction between EW and cyber

1. For example, see Jack Watling and Nick Reynolds, 'Stormbreak: Fighting Through Russian Defences in Ukraine's 2023 Offensive', RUSI, 4 September 2023, pp. 15–19, <https://rusi.org/explore-our-research/publications/special-resources/stormbreak-fighting-through-russian-defences-ukraines-2023-offensive>, accessed 16 January 2025.
2. Richard R Burgess, 'Congress Orders Report on Plan for Future of Navy's Expeditionary EA-18G Squadrons', *Sea Power Magazine*, 4 January 2023, <https://seapowermagazine.org/congress-orders-report-on-plan-for-future-of-navys-expeditionary-ea-18g-squadrons/>, accessed 15 January 2025.
3. Alex Therrien and Frank Gardner, 'Hegseth Sets Out Hard Line on European Defence and Nato', *BBC News*, 12 February 2025.

warfare. Chapter II explores why the EW requirements for maintaining operational effectiveness are changing for Western air forces and militaries more widely and attempts to make them as easy to understand as possible for non-specialists. Chapter III explores specific areas of over-reliance on the US military by other NATO members and explains why these matter for policymakers. One of the reasons why the current gaps in European airborne EW capabilities have been allowed to develop is because the field has traditionally been seen as a niche where a few geeks or 'boffins' work behind the scenes to develop clever gizmos for specialist tasks. In fact, as the paper attempts to explain, bolstering EW centres in multiple countries with skilled personnel and funding to expand and adapt their work to meet the new challenges NATO faces is vital for a host of capability areas across defence. The paper concludes with a summary and recommendations aimed at providing policy advice on how to do so.

For NATO's air and space forces, enhancing European EW capabilities is vital, not only to enhance operational capabilities and reduce dependence on US forces for deterrence purposes, but also to prevent existing systems and weapons from losing their effectiveness against rapidly evolving Russian and potentially Chinese threats.

The paper draws on interviews with EW subject matter experts (SMEs) in several key NATO air forces, including the US Air Force, the RAF, the Swedish air force and the Italian air force, as well as industrial SMEs in both defence primes and smaller specialised defence AI and EW companies. The research phase also involved observation of a major air-led joint SEAD/DEAD exercise at NATO Air Command, and backseat observation of SEAD/DEAD sorties with specialist units of the US and Italian air forces. Due to the highly sensitive nature of many NATO EW capabilities and detailed information on adversary EW, radar and communications systems, much of the research activity cannot be directly quoted or attributed. However, where possible, visits and interviews have been cited. Information is sanitised throughout to avoid disclosure of any classified material, and as such the analysis is aimed at improving understanding of current EW gaps and potential solutions across the defence and the policy community, rather than contributing analysis to advancing the understanding of specialist practitioners already familiar with the topic.

# I. Electromagnetic Warfare (EW) Basics

There are three primary categories of EW used in the air domain: EA, electromagnetic support measures (ESM) and electromagnetic countermeasures (ECM). All are vital components of modern air operations, and as such are important for senior officers and policymakers alike to understand – at least in general terms.

## Electromagnetic Attack (EA)

EA broadly refers to the use of electromagnetic energy to degrade the performance of hostile systems for offensive purposes. This is, in many ways, the simplest form of EW to understand and in non-technical terms would be referred to by many as 'support jamming'. In its most basic form, EA can be conducted through so-called 'noise' jamming, where an emitter is used to flood a given part of the EMS with energy. There are many more complex EA techniques, for example, using digital radio frequency memory (DRFM) jammers to transmit slightly modified variations of hostile radar signals to force them to display inaccurate range or position information. Whether through simple noise jamming or more complex techniques, the goal is to disrupt the ability of enemy radars or communications systems to receive the signals that they rely on to function. This can deny those enemy systems the ability to accurately detect and determine the range to friendly aircraft and incoming weapons, in the case of radars, or to reliably connect, in the case of communications systems.

However, at stand-off ranges, high power output levels are required relative to the signal strength of the target radar to achieve an effective jamming-to-signal ratio, which is a challenge to achieve using compact airborne emitters against large ground-based systems. Radars can 'burn through' noise jamming signals, with their range in any given circumstances dictated by multiple factors, including relative output power and antenna alignment. Modern, frequency-agile digital radars can also rapidly change the frequency and pulse repetition patterns of their own emissions and filter out other signals to greatly reduce the effectiveness of jamming. Most modern radars also have good side-lobe interference detection and rejection capabilities, meaning that they are not particularly susceptible to jamming signals from emitters that cannot draw a direct line of sight to, and

maintain alignment with, the main radar lobe.[4] The consequence, in lay terms, is that conducting effective EA from stand-off assets such as the EA-18G Growler against the latest generation of Russian and Chinese ground-based and maritime radars requires much greater power output and more precisely tailored and agile jamming signals than were needed to provide effective stand-off support EA against previous generation threat radars.

# Electromagnetic Support Measures (ESM)

The second subset of airborne EW is ESM, which encompasses the exploitation of passively collected electromagnetic emissions to identify, track and possibly even target hostile systems. In its broadest sense, ESM refers to the process of using detection and analysis of electromagnetic energy to build an intelligence and situational awareness picture of hostile forces. As such, ESM includes the often-underappreciated but vital role of ISR assets and operators who use a range of (primarily airborne and orbital) platforms to collect and record the signals emitted by hostile systems for subsequent analysis. High-profile examples include the RAF's RC-135W Rivet Joint ELINT/SIGINT (signals intelligence) flights in the Black Sea during the Russian invasion of Ukraine. These sorties probably provided the UK and other NATO nations with invaluable information on the radar signals emitted by a variety of Russian GBAD and combat aircraft systems, at times at considerable risk to the crews.[5] Simply intercepting and recording the signals in question is not enough, however. They must be noticed and isolated within the huge volumes of other signals present in the ever-more crowded EMS and subsequently analysed, tentatively identified and ideally cross-referenced to a geolocated specific enemy threat system to confirm the suspected identity. From that point on, the ELINT intercept can be used to either build a new entry in a national or NATO threat library of enemy radar and communications systems, or update the entry for an existing system that has been recorded emitting previously unseen waveforms.[6] Such databases are crucial for not only detecting and mapping enemy radar and communications systems for operational assessment and planning purposes, but also for programming tactical defensive ESM suites.

4. Warren Boord and John Hoffman, *Air and Missile Defense Systems Engineering* (New York, NY: CRC Press, July 2016), p. 28.
5. Jonathan Beale, 'Rogue Russian Pilot Tried to Shoot Down RAF Aircraft in 2022', *BBC News*, 14 September 2023.
6. Author discussions with ELINT and EW specialists in multiple locations including RAF Waddington, 3 December 2024; RUSI, London, 11 December 2024; Saab Aeronautics, 2 May 2024; SRC, Lincoln, 6 January 2025.

An ESM suite is a vital component of every modern combat aircraft. The traditional active radar in the nose of an aircraft will only detect other airborne, ground-based or maritime assets that are in its cone of regard while it is actively scanning. By contrast, ESM suites enable Western aircraft to detect friendly, unknown and potentially hostile radar emissions of all sorts from multiple directions simultaneously, thereby building situational awareness entirely passively. In the same vein, any active radar emissions from Western aircraft during a state-on-state conflict will likely be rapidly detected by hostile ESM systems, some of which can obtain target-grade ranging and ultimately track information over time if the emissions are constant. In particular, stealth aircraft such as the F-35 must carefully control their own radar emissions to avoid being detected by hostile ESM sensors. This makes their own ability to detect and engage targets passively and using low probability of interception/low probability of detection (LPI/LPD) radar techniques a key determinant of their effectiveness. Therefore, not only are competitive ESM suites vital for warning pilots of threats as a self-protection function, they are also increasingly important as a source of competitive advantage in enabling pilots to operate effectively with minimal need to give away their own position with active radar emissions.

# Electromagnetic Countermeasures (ECM)

ECM involves the use of electromagnetic energy by a platform to defend itself from enemy attacks, generally by degrading the signals received by enemy fire control radars, datalink connections or missile seekers. These techniques are also sometimes known as self-protection jamming or self-screening jamming. Whereas EA or support jamming is traditionally conducted from stand-off ranges to improve the survivability of other friendly aircraft and weapons, ECM is conducted by the platform under attack itself. As such, ECM techniques can generally assume that they will be able to achieve alignment with the main lobe of an enemy radar, since said radar will need to have the aircraft or weapon it is trying to engage within its main lobe to achieve a guidance-grade target track. ECM is also traditionally likely to be conducted from shorter distances away from the threat radar in question, compared with stand-off EA techniques. This main lobe alignment and potentially shorter range to the threat means that ECM systems can be effective in degrading a given radar threat using a significantly smaller antenna array with lower peak power output potential than an EA jammer would require, albeit probably only for a short period of time. Most modern combat aircraft carry a sophisticated ECM suite that either relies on externally carried pods or antenna arrays integrated into the airframe, as well

as use of the main attack radar antenna itself to emit tailored jamming signals in some cases.

Once an on-board ESM suite detects and classifies radar emissions as a threat to the aircraft, the ECM suite can then be used to conduct focused jamming, using either older 'noise'-based techniques or more sophisticated techniques such as spoofing using DRFM technology, to try to deny the attacking radar accurate ranging information for a short period. The aim is to break the kill chain on any missile that might be being guided towards the aircraft, and thus provide a window for the aircraft to either escape the missile engagement zone, or to destroy or disable the threat in question with its own weapons. ECM techniques can greatly increase the self-defence capabilities of modern combat aircraft when they are engaged, especially alongside other defensive countermeasures systems such as towed radar decoys, evasive manoeuvres and dispensing radar-reflective clouds of chaff. However, ECM suites rely on up-to-date mission data loads for their effectiveness. This is because aperture size and onboard power and cooling constraints mean that most fighter-mounted ECM suites have a relatively low peak power output capacity compared with large Russian or Chinese ground-based or maritime air defence radars. Therefore, a purely noise-based jamming approach is unlikely to be effective against these systems using onboard ECM systems. Furthermore, the closer an aircraft flies to a radar threat, the greater power it must use to prevent that radar from achieving burn-through against its EA or ECM jamming and achieving a lock regardless.[7] This means that even with a highly capable ECM suite and other countermeasures, there are limits to how far any aircraft can penetrate into Russian or Chinese IADS coverage, especially if they lack high-end radar cross-section reduction features.

# EW is Not the Same as Cyber Warfare

In very simple terms, EW can be thought of as techniques to create effects or gain intelligence on hostile systems through the medium of pulses of electromagnetic energy, whereas cyber warfare can be thought of as techniques to create effects or gain intelligence on hostile systems through the medium of digital code.[8] However, in practice, the boundaries between the two are increasingly blurred, and since both take place in the EMS, they are often

7. Yu-Hai Mao, 'Rejection of Active Interference', in Gaspare Galati (ed.), *Advanced Radar Techniques and Systems* (London: Institution of Engineering and Technology, 1993).
8. NATO, 'Electromagnetic Warfare', last updated 22 March 2023, <https://www.nato.int/cps/in/natohq/topics_80906.htm>, accessed 13 January 2025.

discussed together.[9] For example, some more advanced EW techniques can use tailored signals to create subtle spoofing effects in enemy systems with a low probability of being detected compared with traditional 'jamming'. However, crafting such signals successfully relies on a deep understanding of the code on which the enemy system is running, and how it interprets incoming signals and displays them to operators as information. One way of accessing the required data to gain the required level of knowledge of enemy systems would be through cyberattacks on the units that operate them.

For example, if a cyberattack had been successfully conducted against an adversary state's air defence system, it could enable the attacker to then produce a tailored EA signal that could be emitted by aircraft equipped with suitable EA or ECM systems in flight. The subsequent EW effects delivered by that airborne asset during an airstrike might cause the adversary air defence system to fail to display contacts correctly or display false contacts that would sow confusion among operators. The effects would appear similar to those that might be caused by a cyberattack but would technically be an EA/ECM effect achieved with a signal tailored using data obtained through a prior cyber penetration.

9. See, for example, Stuart Peach, 'NATO Electronic Warfare and Cyberspace Resilience', in Joint Air Power Competence Centre, 'Delivering NATO Air & Space Power at the Speed of Relevance: Read Ahead', May 2021, pp. 151–58, <https://www.japcc.org/essays/nato-electronic-warfare-and-cyberspace-resilience/>, accessed 13 January 2025.

# II. Rapidly Evolving Requirements for Effective EW

As a rule, building and maintaining effective EW capabilities requires access to up-to-date and detailed databases containing information about enemy radar, communications and EA systems. For an ECM or EA signal to be effective at disrupting or suppressing enemy radars or seeker heads, it must be tailored to the way that the threat systems themselves emit. Likewise, for an ESM system to be able to reliably detect and identify threat radars, let alone perform more advanced functions, the ESM library must include accurate data on the signal patterns emitted by the threat system in question. For much of the 20th century, such databases might only need to contain the frequency bands, pulse repetition patterns and power levels associated with a given adversary radar system, for example. Collecting these could be very challenging until a system was encountered in actual combat and its emissions recorded, identified and catalogued. However, once a given analogue radar was in the threat database of a nation, any EA or ECM signal developed to counter it could remain effective for some time. Unfortunately, this is no longer true, due to the rapid digitisation of Russian and Chinese radar (and communications) systems.

Today, a majority of the most notable ground-based and maritime – and some airborne – radar systems fielded by Russian and Chinese forces can be, and are, regularly reprogrammed using a simple USB connection to change the signal patterns they emit.[10] This means that to maintain accurate threat libraries of hostile systems, NATO must update them in orders of magnitude faster than in previous decades. Collection can be done through either intercepting and identifying novel signals from emitting radars using assets with good ELINT collection capabilities, or obtaining the information through covert means. In some ways, this part of the EW problem set is becoming easier, because many modern combat and ISR aircraft have potent potential ELINT detection and collection capabilities, thanks to sophisticated ESM suites. The F-35 is an obvious example, but most modern fighters, such as the Eurofighter Typhoon, Rafale, Gripen and latest standards of the F-16, F-15 and F/A-18E/F family, also have

10. Author discussions with Ukrainian military technical experts, Ukraine, July 2023; author discussions with US Air Force SEAD specialists, Ramstein Air Base, Germany, 25 October 2024.

sophisticated ESM and ECM suites that under the right circumstances will detect and can record novel radar signatures. What this means is that a huge amount of potentially useful ELINT data is gathered routinely by assets that are not performing dedicated ISR taskings, but rather are automatically recording radar signals detected by their ESM suites during more traditional combat air missions. In some ways, such data can be even more useful than that collected using dedicated ELINT assets, since enemy radar and EW system operators are likely to be more careful with emission control around known ELINT collection assets, compared with when monitoring potentially hostile fighters. Orbital surveillance and monitoring of the EMS is also becoming an increasingly important part not only of strategic ISR but even of day-to-day operational planning and targeting activities, in Ukraine and elsewhere.[11] The problem, however, is that the resulting quantities of potentially significant ELINT data being gathered by a wide variety of dedicated and non-dedicated ELINT assets in the air and in orbit are far too great to analyse and exploit in a timely fashion using traditional methods, which rely heavily on manual analysis by intelligence analysts. It is no use having an asset that has detected and recorded a new signal pattern unless that novel signature can be spotted within the terabytes of ELINT data being gathered every day, analysed, correctly identified as coming from a specific threat system, and then exploited to produce updated mission data for friendly EA, ESM and ECM systems.

A real-world example of the potential risks that are posed to air forces and other parts of the Joint Force when the ELINT collection, subsequent processing, exploitation and dissemination (PED) and mission data update cycle does not keep pace with changing threats was seen during the initial NATO response to Russia's full-scale invasion of Ukraine in February 2022. US Air Force F-35s from the 388th Fighter Wing deployed to Europe to take part in the enhanced deterrence and reassurance patrols that were mounted along NATO's eastern border in the weeks following the start of the invasion. During that period, Russian air defence systems were operating using 'war modes' that had previously not been observed or collected by NATO ELINT systems. As a result, despite having the most capable ESM suite on any NATO fighter on the Eastern border, the 388th Fighter Wing's F-35s did not always recognise and correctly identify Russian GBAD systems. In the words of the Wing's commanding officer, Colonel Craig Andrle: 'We're looking at an SA-20 [NATO's name for the S-300 surface-to-air missile system]. I know it's an SA-20. Intel says there's an SA-20 there, but now my jet doesn't ID

11. Command sergeant major, US Army XVIII Corps, referencing supplying Ukrainian teams with more than 30 'cuts' of the EMS per day from orbital assets, panel discussion, US Army 2023 LANPAC Symposium & Exposition, Honolulu, Hawaii, 17 May 2023.

it as such, because that SA-20 is operating, potentially, in a war reserve mode that we haven't seen before'.[12]

In this case, as Andrle made clear, the pilots and wider NATO Air Command mission planning structure had other sources of intelligence to draw on which meant that the SA-20 battery in question was already geolocated and positively identified, so there was no direct risk to the F-35s or their crews. In fact, in this case, the result was positive because the ability of the F-35's ESM suite to detect and record the signals at a high level of fidelity, and geolocate their source, enabled that new 'war mode' signal to be matched to a known SA-20 site. It is reasonable to assume that subsequently that new signal was added to Allied threat library entries for the SA-20 system and incorporated into the ESM mission data loads, not only for US Air Force F-35s but also for a wide range of other NATO aircraft. EA and ECM countermeasures could be developed and optimised against the new 'war mode', leveraging the ELINT collection capabilities of the F-35. However, in a direct clash with Russian forces, NATO forces would be likely to face similar challenges with previously unseen and rapidly changing 'war mode' signal patterns from GBAD and airborne threat systems that had not been previously geolocated or positively identified. Pilots are at significantly increased risk if their aircraft cannot rapidly and accurately identify ground-based and aerial sources of radar emissions, and are therefore unable to identify what sort of threats they are facing and at what ranges they need to take mitigating action.

In other words, the pace of change that adversary threat systems are now capable of requires changes to the way that the ELINT collection, PED and mission data update cycle is conducted by air forces, and at the Joint Force level across NATO. Fortunately, there are several promising opportunities offered for militaries looking to reform the PED cycle, and even the execution phase of EW operations. AI and ML processes are, in many ways, ideally suited to providing genuinely revolutionary improvements in PED capacity, as well as holding out the promise of novel tactics and techniques for EA and ECM. Broadly speaking, one way to think of the strengths and weaknesses of AI in its currently practical guises is that it is an increasingly powerful way to provide accurate and rapid answers to relatively simple questions that are asked across vast and complex datasets. However, AI and ML tend to be far less useful when the questions, tasks or instruction sets are complex or contain subjective elements. Speeding up and enhancing PED on ELINT data is, therefore, an application to which AI is well suited, since the instructions can be simple – for example, asking the program

12. Remarks in Rachel Cohen, 'The US Air Force Sent F-35s to Defend NATO. Here's What it Learned', *Air Force Times*, 31 March 2023, <https://www.airforcetimes.com/news/your-air-force/2023/03/31/the-us-air-force-sent-f-35s-to-defend-nato-heres-what-it-learned/>, accessed 18 January 2025.

to strip out known signals and/or flag unknown signals, or subtly changed signals within a vast quantity of ELINT intercept data.[13]

Relatively simple AI processes can, in this way, be used to strip out the vast majority of data that is not of interest to human analysts, highlighting the few signals that are unknown or likely to be new variations on already known systems that have changed their signal behaviour. This allows scarce skilled human intelligence analysts to focus their analytical skills and time on these few unknown or altered signals, and on cross-referencing them with other sources of surveillance and geo-intelligence to generate a high-confidence attribution of each new signal detected to a specific hostile system. As a result, procuring and incorporating AI- and ML-enabled tools, either in-house or as a service from trusted industry partners, can dramatically increase the speed at which air forces (and other parts of the Joint Force) can produce updates to threat libraries and mission data files. The RAF recently found an increase of over 21,000% in the speed at which large datasets collected by one of its frontline platforms could be analysed, through the use of relatively simple AI-enabled tools from industrial partners.[14] However, incorporating such tools into national and Alliance PED cycles requires the procurement flexibility and funding to contract with industry or recruit the necessary specialists at scale, and an approach to security and data management that enables such partners to work in the often highly classified spaces within which EW work traditionally sits.[15]

Once a hostile radar, communications or EW signal has been collected, isolated within other data, analysed, and positively identified, there is still more work to do before frontline EA, ESM and ECM capabilities can benefit. When a new signal is entered into either a national or Alliance threat library database, it must then be used to update the mission data on frontline weapons systems and platforms. For example, in the UK, most ELINT signals analysis, exploitation and threat library update work is conducted by the Joint Electronic Warfare Operational Support Centre (JEWOSC) at RAF Waddington, while the processing of 'tactical data' from each sortie, and update work on platform-specific mission data loads, are conducted elsewhere. Examples include the Australian, Canadian and UK Reprogramming Laboratory (ACURL) for the F-35, or the Mission Support Centre at RAF Coningsby for Typhoon.[16] Therefore, if analytical and exploitation

13. Author discussions with AI experts working on military EW-related programmes, Helsing, London, 28 October 2024 and SRC, Lincoln, 6 January 2025.
14. Howie Edwards, speaking at the International Fighter Conference, Berlin, 6 November 2024; author discussions with RAF specialists, RAF Waddington, 3 December 2024.
15. Author discussions with AI experts working on military EW-related programmes, Helsing, London, 28 October 2024 and SRC, Lincoln, 6 January 2025.
16. RAF, 'Multi-Million Dollar Lightning Data Centre Ready for Action', 25 February 2020, <https://www.raf.mod.uk/news/articles/multi-million-dollar-lightning-data-centre-ready-for-action/>, accessed 18 January 2025; Inzpire, 'Inzpire Limited to Provide Requirements Managers and Data Experts to Typhoon Mission

work is greatly streamlined and improved by the use of new tools such as AI- and ML-enabled technologies, corresponding investment will still be needed to enable similar improvements in the pace at which mission data support centres can get the updated threat signals flying on frontline aircraft. If not, the risk is that platforms and weapons systems will not be able to have their mission data updated fast enough to benefit fully from a more rapid strategic and operational level collection and PED cycle, even if that is achieved.

There have already been impressive demonstrations that point the way forward in mission data updates, relying on a mix of technological improvements and regulatory/certification process changes. One example is the rate at which Ukrainian forces and their international partners have been able to broadly keep pace with the rapid and accelerating pace of Russian EW and UAV control signal evolution, through attached specialists at relatively low tactical echelons conducting regular reprogramming of Ukrainian UAVs and EW equipment.[17] Countries that have maintained close support links to the Ukrainian Armed Forces have benefited from significant learning opportunities inherent in exposure to the rapid pace of enforced mission data and control frequency adaptation in that theatre. An example more directly related to traditional air force business was the successful demonstration by the US Air Force of passing ECM and ESM system library updates to an F-16 Block 50 in flight in 2021, albeit in a flight test context, rather than a frontline unit.[18]

The holy grail of EW that many militaries are hoping AI will unlock is what is usually known as 'cognitive electromagnetic warfare'.[19] Cognitive EW aims to create systems that upon encountering previously unseen signals automatically analyse them and provide a likely identification, then configure and emit a tailored ECM or EA signal in real time, or at least close to real time.[20] These techniques would reduce the degree of reliance on pre-programmed mission data files that contain accurate and up-to-date threat libraries. The US Air Force's 350th Spectrum Warfare Wing has reportedly already been making progress on implementing at least some cognitive EW techniques for several years in a

Support Centre', 16 June 2020, <https://www.inzpire.com/news/inzpire-limited-to-provide-requirements-managers-and-data-experts-to-typhoon-mission-support-centre>, accessed 18 January 2025.

17. Author discussions with Ukrainian military technical experts, Ukraine, July 2023.
18. US Air Force, 'F-16 Receives In-flight Software Update During Recent Flight Test', 31 July 2021, <https://www.af.mil/News/Article-Display/Article/2715206/f-16-receives-in-flight-software-update-during-recent-flight-test/>, accessed 18 January 2025.
19. See, for example, Australian Government, Department of Defence Science and Technology, 'Cognitive Electronic Warfare', 5 March 2020, <https://www.dst.defence.gov.au/sites/default/files/publications/documents/DSC%202035%20CogEW%20Fact%20Sheet%20PRO.pdf>, accessed 18 January 2025.
20. For an in-depth discussion of cognitive EW theory, see Karen Haigh and Julia Andrusenko, *Cognitive Electronic Warfare: An Artificial Intelligence Approach* (Boston, MA: Artech House, 2021).

practical context.[21] However, as with so many things where AI is seen as key to unlocking radical progress, fielding reliable and certifiable cognitive EW systems on frontline aircraft and weapons at scale requires overcoming major challenges at both the technical and organisational levels.[22] For example, maintaining up-to-date 'blue force' signal libraries is an important requirement for ESM techniques, because if there is high confidence that all radar and EW signals from national and Allied assets are known and programmed into ESM suites, then anything unknown across various signal categories can be theoretically presumed hostile. However, if cognitive EW techniques are used to develop novel ECM or EA signals 'on the fly', tailored in response to novel threats, then those AI- or ML-generated ECM/EA signals would also be being received by the ESM suites of Allied assets, and would be registered as unknown, and possibly hostile. Even if actual friendly fire can be prevented through various IFF (identification friend or foe) deconfliction mechanisms, the use of cognitive EW techniques for ECM/EA signal generation would still need to be carefully managed to avoid interference with blue-force sensors and the risk of compromising the capacity of national and Allied assets to distinguish between novel adversary signals and novel friendly ones. In other words, fratricide in the EM spectrum is a major risk that cognitive EA/ECM systems will need to overcome before they can be fielded at any scale in practical combat situations.

21. Josh Koslov, commander of the US Air Force's 350th Spectrum Warfare Wing, quoted in Joseph Trevithick, 'F-35 Patrols Near Russia Highlight Case For Cognitive Electronic Warfare', *The War Zone*, 28 April 2023, <https://www.twz.com/f-35-patrols-near-russia-highlight-case-for-cognitive-electronic-warfare>, accessed 18 January 2025.
22. Larry Fenner Jr, commander of the US Air Force's 350th Spectrum Warfare Wing, quoted in Shaun Waterman, 'Air Force Electronic Warfare Chief Sees Limits to AI', *Air & Space Forces Magazine*, 14 November 2024, <https://www.airandspaceforces.com/air-force-electronic-warfare-chief-sees-limits-to-ai/>, accessed 18 January 2025.

# III. NATO Reliance on the US for EW in the Air and Space Domains

There are many areas of heavy reliance on the US within NATO, but two of the most glaring and potentially serious are in the EW domain. The first is ELINT collection, distribution and analytical capacity, and resulting threat library data. While details are classified, and for good reason, in outline terms the US provides the vast majority of the current capacity in NATO. The US military operates by far the largest and most diverse fleet of both airborne and orbital ISR assets in the Alliance, and some of the most capable non-traditional ELINT-gathering platforms. The US also runs the Distributed Common Ground System (DCGS), a global network architecture into which data from ISR platforms can be uploaded, transmitted to the appropriate military entities and intelligence agencies across the US government and the US Department of Defense for analysis and exploitation, and subsequently redistributed as intelligence products to frontline user groups.[23] The US also maintains the most complete and up-to-date threat libraries in NATO, which many Allies rely on, either through direct access where security agreements allow, or through US-supplied mission data updates for American-supplied weapons systems such as the F-35 and the F-16. However, it is important to clarify that European reliance on the US is not total, and there are other states within the Alliance that have capabilities in the collection, PED and mission data generation fields.

For example, France and Sweden both produce highly capable ECM suites for the Rafale and Gripen fighter aircraft respectively, and both have a national capability to produce mission data updates for those systems.[24] They also both have national ELINT collection capabilities. For Sweden, these include the ESM suites on the ASC 890 Erieye AWACS and its upcoming replacement the S 106 GlobalEye. French collection capabilities are fairly extensive, including the E-3F Sentry AWACS, the 'CERES' ELINT satellites and the 'ASTAC' pods for the Mirage

23. US Air Force, 'Air Force Distributed Common Ground System', <https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104525/air-force-distributed-common-ground-system/>, accessed 20 January 2025.
24. Author discussions with Armée de l'Air pilots and observation of Rafale EW capabilities during a sortie, Saint-Dizier, 15 March 2024; author discussions with Swedish air force pilots, Ronneby, 16 October 2024; author discussions with Saab EW experts, Linköping, 2 May 2024.

2000D that allow it to perform ELINT collection tasks.[25] Germany and Italy both maintain small but highly skilled ESM- and ECM-focused analysis and mission data-programming teams to support their respective Tornado ECR squadrons and upcoming Eurofighter EK and EA-37B programmes.[26]

The UK has purchased three RC-135W Rivet Joint aircraft that it operates in close cooperation with the larger US Air Force RC-135W fleet – to the point that crews from each country routinely fly on both UK and US airframes.[27] The arrangement is highly beneficial for the UK, since operating the RC-135W within a joint enterprise grants unique access into the US Air Force's own highly secretive Rivet Joint 'ecosystem'. However, it has also provided the US with major benefits beyond the additional three British airframes and crew capacity. During the war in Ukraine, British risk tolerance has been significantly higher than that of the US for crewed intelligence-collection flights, meaning that RAF RC-135W crews have flown tense missions in the Black Sea throughout the war, where US Air Force crews have not had political permission to operate.[28] Consequently, through the RAF RC-135W fleet, the US system has probably gained access to ELINT data on Russian surface-to-air missile (SAM) radars, EW equipment and other systems operating in war reserve modes that it might not have been able to collect itself. The UK has also maintained genuinely world-class signals analysis and mission data programming expertise through the JEWOSC, as well as at the tactical data-focused Typhoon Mission Support Centre and the F-35 ACURL. However, the scale remains distinctly modest, and much of the work of these organisations is conducted in close coordination and with significant enablement from the US intelligence system – which is both a significant force multiplier and a source of dependency.

Outside the areas of capability mentioned, most European NATO members lack dedicated ELINT collection capabilities and significant EW-focused analytical and mission data reprogramming capacity. This is largely a function of the fact

25. Craig Hoyle, 'Sweden to Gift its Saab 340 Airborne Early Warning Aircraft to Ukraine', Flight Global, 31 May 2024, <https://www.flightglobal.com/defence/sweden-to-gift-its-saab-340-airborne-early-warning-aircraft-to-ukraine/158568.article>, accessed 20 January 2025; Scramble: Dutch Aviation Society, 'Interim Electronic Intelligence Aircraft for the French Air and Space Force', 13 May 2024, <https://www.scramble.nl/military-news/interim-electronic-intelligence-aircraft-for-the-french-air-and-space-force>, accessed 20 January 2025.
26. Author discussions with Italian air force EW and capability development specialists, Rome, 11 November 2024; author discussions with German air force Tornado ECR aircrew and former commanders, Ramstein, 23–24 October 2024.
27. Khalem Chapman, 'USAF, RAF Crews Conduct Joint RC-135 Training at Red Flag 23-1', *Key Aero*, 6 March 2023, <https://www.key.aero/article/usaf-raf-crews-conduct-joint-rc-135-training-red-flag-23-1>, accessed 21 February 2025; *Air & Space Forces Magazine,* 'RC-135V/W Rivet Joint', <https://www.airandspaceforces.com/weapons-platforms/rc-135v-w/>, accessed 20 January 2025.
28. George Allison, 'Typhoons Escort British Surveillance Aircraft over Black Sea', *UK Defence Journal*, 18 October 2022, <https://ukdefencejournal.org.uk/typhoons-escort-british-surveillance-aircraft-over-black-sea/>, accessed 20 January 2025; Beale, 'Rogue Russian Pilot Tried to Shoot Down RAF Aircraft in 2022'.

that these comparatively specialised areas are difficult to grow and maintain in medium- to small-sized military forces that lack the economies of scale and career management flexibility that come from larger force structures. For many smaller countries, 'covering the basics', such as fielding a mechanised brigade, a squadron or two of fighter aircraft and a few naval vessels, is a major task within the personnel and funding available. It is, therefore, unsurprising that few countries have managed to generate or sustain significant modern ELINT collection and EW support centres. This means that the gaps that do exist in the capacity of larger non-US NATO member states such as the UK, France, Germany and Italy are more impactful in the EW domain than the overall size of the Alliance would suggest. It is an area where most NATO member states are simply too small to add significant capacity to the Alliance unless they choose to make it a specific area of national specialisation or cooperate in multinational programmes.[29]

Differences in security standards and classification criteria between NATO member states also complicate the sharing and pooling of EW support capacity in many cases, especially outside the Five Eyes countries. The result is that in many cases countries rely on either the US or other European manufacturers of their various weapons systems to provide prompt mission data updates. This represents a level of sovereign dependency, and thus potentially risk, but for most smaller European states is likely to represent a better 'product' in terms of access to relatively up-to-date mission data for their platforms than they would be able to achieve by trying to build EW collection, PED and mission data programming capacity at a national level.

The second area of heavy NATO dependency on the US is in airborne EA, or support jamming, where almost all the Alliance's capability resides in the EA-18G Growler squadrons of the US Navy, and to some degree (with a focus on disrupting hostile communications rather than radars) in the US Air Force's EC-130H Compass Call and new EA-37B Compass Call aircraft.[30] There are no comparable capabilities elsewhere in NATO air forces – although the Italian air force has ordered two EA-37B aircraft that should be in service by the late 2020s.[31] The US F-16CMs at Spangdahlem, Italian Tornado ECRs at Ghedi and German Tornado ECRs at Schleswig are all SEAD aircraft with impressive ESM and some ECM capabilities. However, these types lack the capacity to perform the airborne EA

29. For a detailed examination of the arguments for national mission specialisation among European NATO air forces, see Justin Bronk, 'The Case for Greater Mission Specialisation by NATO's European Air Forces', *RUSI Occasional Papers* (February 2025), <https://rusi.org/explore-our-research/publications/occasional-papers/case-greater-mission-specialisation-natos-european-air-forces>, accessed 4 March 2025.
30. See Abraham Mahshie, 'On NATO's Eastern Flank, Navy Growlers Highlight Air Force's Electronic Warfare Gap', *Air & Space Forces Magazine*, 13 May 2022, <https://www.airandspaceforces.com/on-natos-eastern-flank-navy-growlers-highlight-air-forces-electronic-warfare-gap/>, accessed 20 January 2025.
31. Author discussions with Italian air force planning officers and commanders, Rome, 11 November 2024.

to provide escort jamming to other platforms as a Growler would.[32] 'Step 1' of the German Eurofighter EK programme to replace the Tornado ECR in Luftwaffe service by 2030 will bring enhanced stand-off SEAD capabilities, but the ambition to add a 'Step 2' with airborne EA support jamming capability is still in the planning phase, and will not be operational until at least the early 2030s.[33] What makes the Growler unique is that in addition to its highly capable ESM suite for detecting and classifying enemy radar emissions, it carries three AN/ALQ-99 or new AN/ALQ-249 Next Generation Jammer pods to generate the power and provide the array aperture sizes needed for effective stand-off EA against ground-based radars.[34] The Growler's two-seat design also means that there is an additional crew member who can fully focus on monitoring the behaviour of enemy radars and adjusting the EA effects required accordingly. Having been derived from the F/A-18E/F Super Hornet airframe, the Growler also has fighter-class performance that helps it to reach the altitudes and speeds required to maintain alignment with the aircraft or weapons it is protecting, and the threat radar in question.

The only existing European-made pod designed to increase fighter ECM capabilities towards the power levels and bandwidth coverage of the AN/ALQ-99 is made by Saab. Their EA pod was developed and tested on the Gripen C/D and uses the same 'Aeraxis' EW architecture as their Gripen E/F fighter and the upcoming Eurofighter EK, but with additional power output and bandwidth coverage potential.[35] However, the Aeraxis pod has not yet been purchased by the Swedish air force or the Luftwaffe, who remain focused on optimising ESM and ECM for platform self-protection over dedicated support EA. The UK is in a similar position with its plans to retrofit advanced ECM capabilities onto its 40 Tranche 3 Typhoons as part of the ECRS Mk2 radar programme.[36]

The lack of any European equivalent to replace the support EA role that is currently fulfilled by US Navy EA-18Gs is a serious risk for NATO's defensive

32. Author discussions with US Air Force F-16CM aircrew and backseat sortie observation at Spangdahlem Air Base, 25 June 2024; author discussions with Italian air force Tornado ECR aircrew and backseat sortie observation at Ghedi Air Base, 22 January 2025.
33. Gareth Jennings, 'Luftwaffe Confirms Intent to Expand Scope of Eurofighter EK Capability', *Janes*, 15 October 2024, <https://www.janes.com/osint-insights/defence-news/defence/luftwaffe-confirms-intent-to-expand-scope-of-eurofighter-ek-capability>, accessed 20 January 2025.
34. Joseph Trevithick, 'EA-18G Growlers with New Jamming Pods Onboard Carrier Heading to Middle East', *The War Zone*, 6 August 2024, <https://www.twz.com/air/ea-18g-growlers-with-new-jamming-pods-onboard-carrier-heading-to-middle-east>, accessed 20 January 2025.
35. Author discussions with Saab EW experts, Linköping, 26 March 2024 and 2 May 2024; Saab, 'Saab Receives Order for Arexis Sensor Suite for German Eurofighters', 26 March 2024, <https://www.saab.com/newsroom/press-releases/2024/saab-receives-order-for-arexis-sensor-suite-for-german-eurofighters>, accessed 20 January 2025.
36. BAE Systems, 'New Electronic Warfare Radar Takes to the Skies for the First Time', 27 September 2024, <https://www.baesystems.com/en-uk/article/new-electronic-warfare-radar-takes-to-the-skies-for-the-first-time->, accessed 20 January 2025.

capabilities against any future Russian aggression. This is because airborne EA is a vital component of the composite air operations (COMAO) packages that NATO would need to employ to successfully degrade the Russian IADS in the first weeks of any direct conflict. Airborne EA is critical for enhancing the capability of traditional non-stealth combat aircraft such as the Typhoon, Rafale, Gripen and F-16 to operate on the outer edges of SAM engagement zones to provide stand-off weapons and other supporting effects, and also for degrading Russia's ability to shoot down incoming precision-guided munitions. The US Navy has previously tried to withdraw funding for the expeditionary Growler squadrons, although at the time these plans were blocked by Congress.[37] However, as the Growler is a critical component of all US Navy carrier air wings and demand for the type consistently outstrips the number available in all theatres, these are among the most likely US military assets to be unavailable for operations in Europe in the event of a concurrent crisis in the Indo-Pacific or US withdrawal from European defence deployments. The increasing numbers of F-35s present in Europe will reduce, but not remove, the degree of risk that this airborne EA dependency represents.

The F-35 was designed to operate against Russian GBAD systems, and it combines reduced radar cross-section for passive stealth with its own stand-in ECM/EA capabilities. The details of these capabilities are classified, which prevents a detailed explanation of their strengths and limitations here. The author has observed these F-35 stand-in ECM/EA capabilities being used to significant effect in multiple NATO exercise and during multinational live training sorties to protect themselves and nearby aircraft from active threats. They are a key and often underappreciated part of the aircraft's capability to operate in contested airspace. However, it is notable that the US Air Force still heavily draws on the US Navy's five expeditionary land-based EA-18G squadrons for force protection in high-threat areas even where F-35 and F-22 are in use.[38] Stealth aircraft also inherently benefit greatly from airborne EA support, since it further enhances the effectiveness of their signature-reduction features by degrading enemy radar performance that is already likely to be relying on minimal signal returns. It is also notable that, as with any EA/ECM capability set, the F-35 itself will rely on having up-to-date mission data files informed by accurate threat libraries to remain effective against rapidly changing enemy radar systems in any future conflict. For most Alliance members, these mission data updates will have to come from the US, although the UK and to a lesser extent Norway, Italy and the Netherlands have some national mission data reprogramming capabilities.[39]

37. Burgess, 'Congress Orders Report on Plan for Future of Navy's Expeditionary EA-18G Squadrons'.
38. See *ibid.*; Mahshie, 'On NATO's Eastern Flank, Navy Growlers Highlight Air Force's Electronic Warfare Gap'.
39. RAF, 'Multi-Million Dollar Lightning Data Centre Ready for Action'; 350th Spectrum Warfare Wing, 'F-35 Partner Support Complex', <https://www.350sww.af.mil/Units/350th-Spectrum-Warfare-Group/F-35-PSC/>, accessed 21 February 2025.

One area of EW development where multiple NATO member states, including the US, are currently investing, and which might help mitigate the current reliance on US Navy Growlers, is stand-in EA systems. As side-lobe interference detection and rejection capabilities continue to improve on Russian and Chinese radar systems, the advantages of stand-in jamming as opposed to traditional stand-off airborne EA will continue to increase, since stand-in ECM and EA emitters have a much better chance of being able to maintain alignment with the main lobe of a given threat radar. Expendable stand-in jammers are already an established part of the NATO arsenal, in the shape of the ADM-160 Miniature Air-Launched Decoy-Jammer (MALD-J) and the upgraded MALD-X, albeit again provided by the US.[40] The UK has a long-running stand-in jammer prototype in the SPEAR EW offshoot from the SPEAR 3 (Selective Precision Effects At Range 3) programme, with a compact EA payload in place of the explosive warhead in the primary SPEAR missile.[41] However, while the SPEAR EW programme has continued to be funded at a limited scale, the UK has not yet committed to purchasing the system as a frontline capability.[42]

Less traditional approaches are also being actively explored, informed in part by lessons and operational data and experimentation in Ukraine, on ways to use uncrewed systems or even balloon-mounted EA emitters to provide loitering stand-in EA effects against air defences and other key Russian targets.[43] As multiple states explore the potential of cheaper uncrewed autonomous systems to augment traditional combat air platforms, such as the US Collaborative Combat Aircraft or the UK's Autonomous Collaborative Platform programmes, one of the most alluring potential early use cases is likely to be for stand-in EA.[44] The latter could provide meaningful increases in Joint Force capabilities to penetrate and degrade a Russian or Chinese IADS, and allow novel autonomous platforms to be experimentally introduced into service without necessarily triggering the

40. *Air & Space Forces Magazine*, 'ADM-160 MALD', <https://www.airandspaceforces.com/weapons-platforms/adm-160-mald/>, accessed 20 January 2025.
41. Thomas Newdick, 'UK's New SPEAR 3 Mini Cruise Missile Succeeds in First End-to-End Test', *The War Zone*, 18 November 2024, <https://www.twz.com/air/uks-new-spear-3-mini-cruise-missile-succeeds-in-first-end-to-end-test>, accessed 20 January 2025; Tyler Rogoway, 'SPEAR Mini-Cruise Missile Getting an Electronic Warfare Variant to Swarm with is a Huge Deal', *The War Zone*, 1 December 2019, <https://www.twz.com/29789/spear-mini-cruise-missile-getting-an-electronic-warfare-variant-to-swarm-with-is-a-huge-deal>, accessed 20 January 2025.
42. George Allison, 'UK Boosts Funding for SPEAR-EW Jammer Development – DSEI23', *UK Defence Journal*, 12 September 2023, <https://ukdefencejournal.org.uk/uk-boosts-funding-for-spear-ew-jammer-development-dsei23/>, accessed 20 January 2025.
43. Author discussions with Ukrainian military technical experts, Ukraine, July 2023; author discussions with US Air Force EW and SEAD experts, Ramstein, 25 October 2024; author discussions with RAF specialists at the Air and Space Warfare Centre, RAF Waddington, 3 December 2024.
44. *Airforce Technology*, 'Collaborative Combat Aircraft (CCA), USA', 21 June 2024, <https://www.airforce-technology.com/projects/collaborative-combat-aircraft-cca-usa/>, accessed 20 January 2025; RAF, 'Autonomous Collaborative Platform Strategy', 27 March 2024, <https://assets.publishing.service.gov.uk/media/66019fa8f1d3a0666832acfc/RAF_Autonomous_Collaborative_Platform_Strategy.pdf>, accessed 20 January 2025.

legal, regulatory and ethical challenges that arming such autonomous systems is likely to generate.

Of course, for novel uncrewed systems or decoys to successfully plug the current gaps in non-US airborne EA capability, they will need to be procured in reasonable numbers and distributed to the units that in wartime or during exercises would prepare and launch them. Even if autonomous stand-in EA assets can be made individually cheap enough to use repeatedly at scale, doing so will still require a logistics, command and control, mission planning and deployment architecture within the Joint Force to deploy them when and where they are needed in coordination with the COMAO. This will require people, funding and planning to be allocated to the problem at a scale significantly beyond that currently being devoted to innovative R&D and experimentation work.

# Conclusions and Recommendations

Russian (and Chinese) threat systems are now evolving at a sufficiently rapid pace that ensuring a constant flow of accurate updates to EW mission data loads for weapons systems and platforms will be critical for ensuring combat effectiveness in any NATO Article 5 situation. This is particularly true in the air domain, due to the reliance by aircrew on ESM suites for situational awareness in many situations, and the need for effective ECM and EA options to keep platforms safe when engaged and to allow stand-off weapons to penetrate defences. In many cases, it may not be cost effective to replicate EW enablement provided by larger partner states at a national level. However, it is important for defence planners and senior leaders across NATO to be aware of which national EW dependencies are in this category, and which current risks are being held by their forces that could be mitigated with targeted investment. In some countries and armed services where such matters have traditionally been viewed as 'niche', senior leaders and planners may well be unclear about exactly what level of risk they are holding in the EW domain. This is especially likely given the rapid and ongoing evolution of both the threat and the technologies available to potentially help meet it. In such cases, senior leaders should be making it a priority to be thoroughly briefed both by national EW specialists (where available) and/or by experts from allies and partners, to allow centralised planning and budget allocation to be adjusted accordingly.

Across NATO, the overall level of dependence on the US is very high for most EW capabilities, especially in terms of dedicated airborne and orbital collection assets, exploitation capacity for ELINT data once collected, and airborne EA to provide support jamming to Allied aircraft and weapons against high-end threat systems. **This represents a potential risk for the Alliance in the event of Russian aggression when American reinforcements and support capacity are tied up with a concurrent crisis in another theatre or are otherwise unavailable at scale**. In attempting to redress the balance and reduce this risk, European states should try to reinforce areas of comparative strength, rather than trying to replicate the full spectrum of American EW capabilities at a tiny scale in every country.

There are pre-existing areas of expertise that could be significantly enhanced with targeted increases in personnel allocation and funding, as well as contracted support from specialist defence industrial partners. Examples include:

- High-end hardware manufacturing capability for arrays in Italy, Sweden and France.
- Expertise and capacity in ELINT analysis and mission data update production in the UK.
- Expertise in Russian threat radar and tactics in the SEAD squadrons in the German and Italian air forces, and in elements of the UK armed forces that have worked most closely with Ukrainian partners since February 2022.
- ECM programming and fighter integration experience and capacity in France and Sweden.

This is by no means an exhaustive list, nor does it imply that states not mentioned in relation to a given facet have no capability in that area. Rather, it is intended to demonstrate that there are solid foundations that could be built upon in multiple non-US member states.

For the UK government, it is worth focusing on the fact that the UK has successfully maintained world-class signals analysis and mission data programming expertise, especially through the JEWOSC, as well as at the tactical data-focused Typhoon Mission Support Centre. However, maintaining these vital and scarce capabilities in ESM and ECM in an era of rapidly evolving digital threat systems will require increased investment and rapid adoption of AI- and ML-enabled toolsets.

However, it should also be clear that, even with increased investment, such comparatively small and specialised centres of talent and experience could only significantly reduce overall NATO reliance on the US military in the EW realm through greatly increased multinational cooperation and data sharing. **No single European country has either the existing foundations or sufficient suitably qualified and experienced personnel to rapidly be able to add meaningful capabilities across all aspects of EW. Therefore, to create end-to-end capability within Europe will require genuinely multinational partnerships**.

It is also unlikely that European NATO air forces will be able to replicate most of the dedicated airborne and orbital ELINT collection capabilities that the US contributes to the Alliance, given the huge costs and timeframes that such an effort would entail. For orbital capabilities, leveraging commercial SIGINT/ELINT constellations such as HawkEye 360 would seem sensible, but these would almost certainly be unable to fully replicate US capabilities such as Advanced

Orion.[45] Many NATO countries do operate significant numbers of fighter aircraft and other maritime and land-based systems that offer ELINT collection capabilities, at least in theory. The F-35, Typhoon, Rafale, Gripen and specialist SEAD aircraft such as the Tornado ECR all have sensitive ESM suites, and some can be fitted with specialised ELINT-gathering pods, as can long-endurance UAVs such as the MQ-9 Reaper.[46] **The key to rapidly increasing European NATO's ability to collect ELINT data, therefore, is to ensure that all the ESM suites being carried by non-traditional ISR platforms for other mission sets are used to their full collection potential**. This means an increased emphasis on getting tactical data off non-traditional ISR platforms and fed into either national, NATO or US systems such as DCGS for analysis and exploitation. It also means investing in technologies such as AI- and ML-enabled analytical tool sets that can enable relatively small teams of human analysts to find new and unknown signals or changes in known patterns within the vast ELINT datasets that modern combat aircraft collect.

For airborne EA capabilities to augment, and if necessary replace, the vital contribution of the US Navy's EA-18G Growlers, options are limited in the immediate term. The European nation that is closest to having an existing fighter-mounted solution is Sweden, with the combination of Gripen C/D or the new Gripen E with the existing Aeraxis EA pod. Even a relatively small number of pods acquired and integrated into the existing Gripen fleet could allow the Swedish air force to make a uniquely valuable contribution to European SEAD/DEAD capabilities through specialising in airborne EA. Another option that should be seriously considered is the establishment of a multinational NATO airborne EA squadron, along similar lines to the existing NATO AWACS, Multinational Multirole Tanker Transport squadron and Strategic Airlift Capability C-17 squadron.[47] **A pooled multinational EA squadron could allow air forces that are too small to economically field dedicated EW capabilities to contribute funding and personnel meaningfully**. It might also provide a vehicle to marginally ease classification and bilateral disclosure challenges for countries outside Five Eyes, by enabling the US to provide 'black boxed' mission data updates and assign US nationals to the NATO unit to operate any particularly sensitive systems.

45. HawkEye360.com, 'Advanced Space-based RF GEOINT & ELINT', <https://www.he360.com/>, accessed 13 February 2025; *Gunter's Space Page,* 'Orion 5, 6, 7, 8, 9, 10, 11, 12', <https://space.skyrocket.de/doc_sdat/orion-5_nro.htm>, accessed 13 February 2025.
46. Nick Zazulia, 'New MQ-9 Sensor Option Undergoes Successful Testing', *Avionics International,* 12 February 2019, <https://www.aviationtoday.com/2019/02/12/new-mq-9-sensor-option-undergoes-testing/>, accessed 20 January 2025.
47. NATO, 'Airborne Early Warning and Control Force', <https://awacs.nato.int/>, accessed 20 January 2025; NATO, 'Strategic Airlift', last updated 7 March 2024, <https://www.nato.int/cps/en/natohq/topics_50107.htm>, accessed 20 January 2025.

Another recommendation is to **increase funding for the (currently largely experimental) development of stand-in EA capabilities using relatively cheap uncrewed autonomous systems that can loiter for significant periods over hostile territory**. Such relatively cheap platforms tend to be propellor powered and cruise at slow airspeeds to enable them to attain the required ranges and endurance with compact airframes. Therefore, these systems will also require novel and likely cross-domain and cross-service solutions for fielding, supporting and deploying them alongside traditional combat aircraft in any conflict with Russia (or China for the US).

A final recommendation is that to reduce technical risks and increase the problem set that NATO can pose to adversaries, **procurement of more expensive traditional air-launched stand-in EA capabilities such as ADM-160 MALD-J/X and SPEAR EW should also be pursued as a priority by at least some countries in Europe**. In the long term, the ever-increasing side-lobe interference rejection capabilities of digital radar systems are likely to mean that stand-in EA has a longer developmental road to run than stand-off EA aircraft like the Growler. Therefore, investment in autonomous or at least automatic stand-in EA capabilities appears a wise choice for European states seeking to close the EW gaps in NATO's European order of battle.

# About the Author

**Justin Bronk** is the Senior Research Fellow for Airpower and Technology in RUSI's Military Sciences research team, and Editor of *RUSI Defence Systems*. He has particular expertise on the modern combat air environment, Russian and Chinese ground-based air defences and fast jet capabilities, the air war during the Russian invasion of Ukraine, uncrewed combat aerial vehicles and novel weapons technology. Justin also holds a visiting Professor II position at the Royal Norwegian Air Force Academy. His PhD from the Defence Studies Department of King's College London examined Balancing Imagination and Design in British Combat Aircraft Development.

Justin is also a private pilot with more than 300 flying hours in light aircraft and gliders. In addition, he has more than 25 hours' backseat flying experience with nine different air forces on fast jet types including Eurofighter Typhoon, Rafale, Gripen, F-16, CF-18, Tornado, T-38 and Hawk.