www.rusi.org

Occasional Paper

Protecting the Force from Uncrewed Aerial Systems

Jack Watling and Justin Bronk

Occasional Paper

193 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 193 years.

Published in 2024 by the Royal United Services Institute for Defence and Security Studies.

RUSI Occasional Paper, October 2024. ISSN 2397-0286 (Online).

Cover image: A Romania land forces Gepard fires at an illumination mortar at Bemowo Piskie Training Area, Poland, 27 July 2021. Courtesy of Adrian Patoka/Wikimedia

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

The impact of uncrewed aerial systems (UAS) on land operations has been a subject of extensive discussion, from the war in Nagorno-Karabakh in 2020 to Russia's full-scale invasion of Ukraine beginning in 2022. The corollary to the importance of armies fielding UAS is that effective, layered and efficient counter-UAS (C-UAS) capabilities are neither a luxury nor a concept to be explored as part of an abstract 'future force'. They are a basic requirement for a land force to be suitable for operations on the modern battlefield. Without C-UAS capabilities, a force will be seen first, engaged more accurately, and ultimately defeated by an opposing force that successfully fields UAS and C-UAS capabilities at scale. For NATO members, the aiming mark set by the Alliance's senior leadership is to be ready to deter Russia by 2028. Fielding C-UAS capabilities, which are absent in any structured sense from the British Army and from most other NATO land force elements, is therefore an urgent operational requirement.

There is a risk that in attempting to fill this critical gap, NATO members purchase a range of C-UAS capabilities that are overly specialised in dealing with specific threat systems, are not integrated effectively across the force, and cannot keep pace with the threat as UAS continue to rapidly evolve. This paper outlines the core tasks and capabilities required to provide coherent, layered C-UAS protection. The paper then explores how to integrate layered C-UAS protection across land forces without overburdening units and thus preventing them from performing their primary tasks.

The paper concludes that:

- Software solutions are as important as hardware to enable accurate detection, classification and identification of UAS, and the allocation of appropriate effects to efficiently defeat UAS. Software can also reduce the bandwidth requirements for the networking of sensors. In most cases, the necessary data to field robust machine-based filtering is already available in Ukraine, so there should be little difficulty in obtaining libraries of signature data.
- There are multiple active and passive sensor techniques, and a wide range of soft- and hard-kill techniques exist for engaging and either providing a mission kill or physically destroying UAS, but none are a universally applicable solution, and they must be employed together across the force to provide effective and efficient coverage.
- All platoons must have the ability to detect the presence of UAS and have electronic countermeasures to protect themselves from them.

- Across the force, remote weapon stations and other existing platforms should be updated to be able to engage UAS with direct fire.
- At the company level, it is necessary to have dedicated passive sensor arrays capable of detecting, classifying and identifying UAS.
- Battalions should have a dedicated counter-reconnaissance capability with hard-kill C-UAS systems, fielding both self-propelled anti-aircraft artillery and UAS interceptors. An electronic warfare section is also necessary, to update and orchestrate the electronic protection suites at subordinate echelons that provide a soft-kill layer that attacks UAS command links and navigational systems.
- The brigade should have independent C-UAS platoons that can be pushed to support the efforts of company groups, or to close key axes to hostile UAS.
- The brigade should field directed energy systems to efficiently defeat medium-level ISTAR UAS overflying its area of responsibility.
- The brigade should have the responsibility for electromagnetic spectrum command and control (C2) and deconfliction.
- The division should fuse lower-echelon C-UAS capabilities with the common air defence picture and orchestrate a distributed defence in depth of the airspace to avoid local saturation of C-UAS systems at critical sites.
- The point defence role for critical sites such as airbases should see C-UAS capabilities integrated into the wider integrated air and missile defence system at the national, theatre and Alliance levels.
- It is vital that the permissions on training areas allow these capabilities – both soft and hard kill – to be used in combination, alongside the rest of the force's communications and C2 systems. This is to familiarise commanders with the use of C-UAS capabilities and the deconfliction procedures necessary, and to ensure that systems do not commit fratricide. Where it is not possible to train with these capabilities in live exercises, they should be made available in a synthetic training environment.

Introduction

The pervasive threat from uncrewed aerial systems (UAS) on the modern battlefield, as demonstrated in Ukraine since 2022,[1] Nagorno-Karabakh in 2020[2] and Syria since 2015,[3] means that land forces and installations must be protected from the threat from persistent observation and strikes. The counter-UAS (C-UAS) mission, however, poses challenges to systems designed for traditional air and missile defence. One example of this mismatch in capability has been the relatively frequent shooting down of small UAS with multi-million-dollar air defence interceptors, such as when Israel was forced to down a UAS with a Patriot missile in 2017, or the use of Sea Viper/Aster 15 missiles to shoot down Houthi drones in the Red Sea in late 2023.[4]

The number of intermingled friendly and hostile UAS in any given area of operations, and the diversity of their forms and mission sets, means that acquiring C-UAS systems that can engage the full range of threat types and deploying them at all tactical echelons risks being cost prohibitive. However, each echelon of land forces must be protected. As Ukrainian air defence interceptors have become depleted to the point that the Armed Forces of Ukraine (AFU) could no longer afford to routinely use them to engage Russian reconnaissance UAS, the costs of not protecting each echelon have been illustrated by a great increase in Russian reconnaissance-strike activity throughout Ukraine's operational depth.[5] This has enabled extensive Russian targeting with ballistic missile and artillery strikes against critical Ukrainian assets, from aviation to artillery and (ironically) air defence systems, resulting in unsustainable attrition of those assets and materially worsening Ukraine's operational position.[6] The question for Western land forces, which this paper aims to address, is how to extend C-UAS coverage across the relevant tactical echelons within a manageable cost and personnel burden, and in a short period of time. C-UAS defence is a minimum requirement

1. *The Economist*, 'How Cheap Drones are Transforming Warfare in Ukraine', 5 February 2024.
2. Jack Watling, 'The Key to Armenia's Tank Losses: The Sensors, Not the Shooters', *RUSI Defence Systems*, 20 October 2020.
3. Jack Watling and Nick Reynolds, 'Your Tanks Cannot Hide', *RUSI Defence Systems*, 5 March 2020.
4. Chris Baraniuk, 'Small Drone "Shot with a Patriot Missile"', *BBC News*, 15 March 2017; *Navy Lookout*, 'Royal Navy Destroyer HMS Diamond Shoots Down Drone While Escorting Merchant Ships in the Red Sea', 16 December 2023, <https://www.navylookout.com/royal-navy-destroyer-hms-diamond-shoots-down-drone-while-escorting-merchant-ships-in-the-red-sea/>, accessed 16 August 2024.
5. As of 5 August 2023, the authors observed through Ukrainian systems between 1,000 and 1,300 Orlan-10 or Zala reconnaissance UAS overflying Ukrainian positions per day, penetrating as far as Kyiv, Poltava, Dnipro and Zaporizhzhia.
6. For example, see Status-6 (Military & Conflict News), X post, 1 July 2024, <https://x.com/Archer83Able/status/1807855553282298134>, accessed 2 July 2024.

to operate sustainably on the battlefield today; it is a problem that cannot be left to be dealt with as part of an abstract 'future force' concept.

This paper aims to set out an approach for providing a C-UAS capability across a deployed ground force. The need for a force-wide approach is not because destroying any particular UAS is difficult, but because optimising against this task comes at a significant cost in efficiency against other tasks within tactical formations. If a platoon, for example, must field both hard- and soft-kill C-UAS capabilities, it must expand in size, or its core vehicles will become significantly more expensive and complex to operate. This paper outlines the various detection, classification and engagement tools available, and an approach that allows C-UAS tasks to be federated at appropriate echelons so that any capabilities added to the force can be integrated efficiently in the context of operations against a peer adversary.

In developing the C-UAS approach hereafter outlined, this paper draws on the authors' direct observations of the operation of all classes of UAS under exercise conditions, and a considerable proportion of UAS types under operational conditions in Ukraine and elsewhere. The authors have also spent time physically examining UAS and their resilience to electronic warfare (EW) and other C-UAS techniques. It was also necessary to observe the functioning and operation of a range of air defence systems, and to interview air defenders with experience of engaging UAS in a range of conflict zones, from Ukraine to Israel and Iraq. The authors also spoke to teams which had employed novel weapons technologies, such as directed energy weapons, on exercise and operations, to discuss the limitations and challenges of using these tools, and also the opportunities they offer.

This is the second in a series of three papers examining the impact of UAS on modern operations. The first considered how land forces can best employ mass precision strike complexes using UAS.[7] This paper focuses on countering the threat posed by these capabilities. The third will look at the impact of UAS on joint air-ground interactions.

This paper has three chapters. Chapter I examines the challenges of detecting and classifying UAS and sharing this information as required among various elements. Chapter II explores the strengths and weaknesses of the various available categories of engagement and defeat mechanisms for UAS, to provide an overview of potential approaches. Chapter III examines what is likely to be needed to deploy a C-UAS complex across military echelons, to map at what echelon capabilities might be best integrated. The paper concludes with recommendations for the UK, as a typical NATO armed force, based on the analysis presented.

7. Justin Bronk and Jack Watling, 'Mass Precision Strike: Designing UAV Complexes for Land Forces', *RUSI Occasional Papers* (April 2024).

It is necessary to briefly discuss definitions. UAS are also often referred to as drones, UAVs, remotely piloted air systems (RPAS), first person views (FPVs), one way attacks (OWAs) and various other acronyms and designations that are used to refer to the same or sub-categories of capability. FPV relates to a navigational technique: specifically, one that requires active human control. OWA refers to a mission profile. UAV refers to the aircraft. RPAS and UAS both refer to systems: aircraft and their associated command-and-control (C2) systems and other enabling functions. Of these terms, UAS is the most widely recognised, and so this paper uses this term.

Although this paper concludes that the established categories of UAS 'groups' are operationally unhelpful, the paper is largely concerned with UAS that fall between Group 1 and Group 3, that is from FPVs and small quad-/multi-copters up to lightweight fixed-wing uncrewed aircraft such as the Russian Orlan-10 (see Table 1), or heavier delta-wing Shahed-136 drones.[8] The paper does not deal with larger medium-altitude long-endurance (MALE) Group 4–5 UAS such as the MQ-9 Reaper or the RQ-4 Global Hawk. This is because, by dint of their speed, missions and operating altitude, these are targets for traditional air defence systems, rather than dedicated C-UAS assets. The cost of MALE UAS makes engagement by traditional air defence cost competitive in any case, such that they present a fundamentally different problem from the one explored in this paper.

8. For an overview of the US Department of Defense UAS Group 1–5 classification system, see US Department of Defense, 'Joint Publication 3-30: Joint Air Operations', 25 July 2021, validated 17 September 2021, Figure III-14, p. III-31, <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_30.pdf?ver=2019-09-04-142255-657>, accessed 4 July 2024. For details on the Orlan-10, see James Byrne et al., 'The Orlan Complex: Tracking the Supply Chains of Russia's Most Successful UAV', RUSI, 15 December 2022.

Table 1: UAS Groups

	Characteristics	Examples
Group 1	Less than 20 lbs weight, 1,200 ft above ground level	FPV, DJI-MAVIC III
Group 2	Flight up to 3,500 ft, 21–55 lbs weight	Puma, Desert Hawk II, Lelaka, Zala-421
Group 3	Less than 1,320 lbs maximum weight, altitude ceiling below flight level 180	Orlan-10, Scan Eagle
Group 4	Greater than 1,320 lbs maximum weight, altitude ceiling below flight level 180	MQ-1 Predator, Wing Loon 2, Orion, Mojaher
Group 5	Greater than 1,320 lbs maximum weight, altitude ceiling above flight level 180	Global Hawk, MQ-9 Reaper

Source: US Department of Defense, 'Joint Publication 3-30: Joint Air Operations', 25 July 2021, validated 17 September 2021, Figure III-14, p. III-31, <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_30.pdf?ver=2019-09-04-142255-657>, accessed 4 July 2024.

This paper focuses on land forces and to some extent also on the defence of installations of concern to air forces. Unmanned combat aerial vehicles and other such capabilities designed specifically for air combat are not covered, while uncrewed systems in the context of maritime operations present a substantively different problem, and so are also not covered by this paper.

Finally, the AFU has found that it is useful to draw a clear doctrinal distinction between the defence of forces and the defence of territory, when it comes to C-UAS. Partly as a consequence, the AFU tends to consider countering enemy reconnaissance UAS as an entirely different function from countering long-range one-way-attack UAS. These distinctions make sense in relation to the problems confronting Ukraine. However, for a country like the UK, which must assume that it is operating in an expeditionary capacity, the force must be able to address all of these threats. Furthermore, there are critical pieces of territory to enable an expeditionary force that blur the Ukrainian distinction between protection of forces and territory. Finally, the distinctions between the UAS employed for these missions may converge over time, as is already occurring in the Middle East. For these reasons, this paper considers these issues as one problem set, even though this does not reflect current practice.

I. Detect and Identify

The primary challenge that UAS present to traditional surface-to-air missile (SAM) systems is that as targets they are small, often slow, numerous, relatively cheap, and often operate at low altitude. Moreover, for a traditional target acquisition or fire control radar, opening the doppler gates to be able to see slow-moving UAS with small radar cross sections leads to a very cluttered display with a large number of false positive returns, greatly increasing the workload of the air defence crew.[9] Furthermore, due to the short acquisition ranges possible against many small, low-flying UAS, the number of traditional radar systems needed to provide C-UAS coverage over any significant frontage makes relying on traditional active radar systems cost prohibitive, while proximity to the enemy would likely see these emitters destroyed in unsustainable numbers. Therefore, this chapter focuses on the first set of challenges in defeating UAS: how to affordably identify and classify them, how to discriminate friendly UAS from hostile ones, and how to distribute this information.

Detection

The first requirement for C-UAS capability is to ensure that multiple echelons within land forces, and force protection elements at fixed bases, have the capability to detect and track UAS. There are four primary methods for doing this:

1. Active and passive radar systems that are specifically tailored for C-UAS detection and tracking.
2. Passive acoustic systems that are optimised for detecting the sound signatures of UAS propulsion systems and their flight.
3. Passive radio frequency (RF) analysers that search for radio control signals and analyse them once isolated to provide an identification and location of the UAS and potentially the antennae of the UAS control station.
4. Passive electro-optical (EO)/infra-red (IR) search-and-track systems that scan the sky for the visible shape and contrast signature of UAS.

Each of these detection and tracking approaches has its own advantages and drawbacks, such that forces will need a combination of them to reliably detect UAS. For any of them to be effective it is also necessary to have software able to process the relevant sensor returns.

9. Author observations of air defence systems tracking UAS, UK, April 2021; US, October 2021 and March 2024.

Active radar systems designed for C-UAS detection and tracking often operate in relatively high-frequency parts of the radar spectrum such as the X, Ku or even Ka-bands to ensure high resolution and rapid acquisition of small targets, but in some cases may operate in the somewhat lower frequency S-band to improve range performance for a given power output level.[10] The flipside of detection range performance is the range at which enemy forces will be able to detect and conduct triangulation against the position of a C-UAS radar, with most active-radar systems being detectable by hostile sensors at 50% greater distances than their own functional detection range. A system designed for very short-range coverage that operates in the high-frequency bands will be difficult to detect for enemy systems that are not themselves close to the C-UAS radar in question. However, for longer-range systems, a core limitation of active radar as a primary sensor for C-UAS detection and tracking capability is the inherent requirement to transmit to perform their function. Crucially, this will often be at odds with the requirement to maintain emissions control (EMCON) to avoid giving away a unit's position and inviting strikes cued in by hostile EW direction-finding and -ranging systems. For defending fixed sites such as airbases far from the frontlines, EMCON concerns will be more focused on electromagnetic deconfliction with other systems, rather than avoiding hostile detection and triangulation. Nevertheless, the operational lesson is that for C-UAS operations, active radar are better for fire control than for target acquisition, as the former requires short periods of illumination.

Passive radar systems rely on detecting the energy reflected off targets from background sources of electromagnetic emissions such as television, WiFi or third-party active radar. To be effective they rely on accurate electromagnetic spectrum (EMS) surveys of the operating environment, although space-based EMS surveying renders this less of a challenge than has historically been the case.[11] Modern techniques such as passive coherent location allow relatively high-resolution ranging and track information to be gathered, while remaining entirely passive and thus covert.[12] Indeed, in an electromagnetically contested environment, passive systems have often been found to provide more reliable returns than active systems.[13] These systems are likely to have limited capability

10. For an overview of radar frequency bands and uses, see Radar Tutorial.eu, 'Waves and Frequency Ranges', <https://www.radartutorial.eu/07.waves/Waves%20and%20Frequency%20Ranges.en.html>, accessed 2 July 2024.
11. See, for example, comments on EMS scrape frequency for Ukraine by T J Holland at the Association of the United States Army Land Pacific Symposium and Exposition, Waikiki, Hawaii, 16 May 2023. See 'Panel Discussion: Observations from the Russo-Ukrainian War', 16 May 2023, <https://www.dvidshub.net/video/883558/lanpac-day-1-part-4>, accessed 19 August 2024.
12. NATO Science and Technology Organisation, 'Passive Coherent Locator History and Fundamentals', Lecture SET-243, <https://www.sto.nato.int/publications/STO%20Educational%20Notes/STO-EN-SET-243/EN-SET-243-01.pdf>, accessed 2 July 2024.
13. Author observation of comparisons between active and passive radar tracks of aerial targets operating in Kursk Oblast, September 2024.

in environments where there is comparatively little background 'noise' in terms of emissions, such as in the Arctic, where population density is very low. However, in most scenarios, as demonstrated on exercise and operations, there is more than enough background emissions activity to ensure that passive radar systems can form a valuable part of C-UAS detection and tracking suites.[14]

Passive acoustic sensors rely on identifying the distinctive sound signature created by a UAS's propulsion system and the interaction between its surfaces and the air. Although useable data can be obtained using cheap microphones, using this data requires the capacity to filter out false-positive detections and other background noise. Modern sound software makes the processing straightforward, but having a library of acoustic signatures and an algorithm that can distinguish between them is valuable intellectual property that is harder to generate and obtain.[15] Major improvements in machine learning-enabled post-processing capabilities in recent years have driven a corresponding improvement in passive acoustic detection and limited tracking capabilities.[16] The main limitations of acoustic sensors are the lack of ranging capability, since a single microphone can only provide bearing to a target; and that they have comparatively short range compared with radar and RF detection, or against targets with significant signature reduction features. As with RF capabilities, ranging can be achieved through multi-static triangulation. Acoustic sensors generally provide 2D tracking with too great a latency to guide fire control, but are incredibly cost efficient and reliable for target acquisition. The primary advantages of acoustic sensors are that they are completely passive and thus covert, requiring comparatively little electrical power and cooling capacity to operate, and that they can also provide additional capabilities such as shot detection and bearing for ground units.

Passive RF analysers are highly effective at detecting the presence of most reconnaissance and tactical UAS, because most classes of UAS receive or transmit data in one direction to perform their functions. For example, automatic navigation and target-recognition algorithms might enable a UAS to conduct ISTAR flights without the need for a real-time command-and-control signal from operators, but the UAS must still transmit to pass its ISTAR data back to ground stations, otherwise it cannot provide a real-time or close to real-time ISTAR function. With modern machine learning-enabled signal processing and analysis techniques, there are many RF analysis sensor solutions that can provide forces

14. Author observation of test and operational data from a range of high and low electromagnetic activity environments in the US, Norway, Finland, Ukraine and Russia, 2022–24.
15. Author tests of microphone detection of UAS, Norway, February 2021; US, October 2023; and Ukraine, 2024.
16. Author interview with designer of Ukrainian acoustic UAS detection and tracking architecture, Ukraine, 6 July 2023.

with a reliable means of at least detecting the presence of, and possibly also identifying or even locating, UAS within a tactical area.

EO/IR scan and track systems rely on cameras searching the sky for points of contrast created by small UAS. Like acoustic sensors, they generally rely on powerful post-processing techniques to filter out false positives, both from lighting artefacts and from other flying objects, such as birds. They also rely on direct line of sight, although the same can be said of most of the other techniques here. The primary drawback of optical scan and track sensors is their comparatively short range and their vulnerability to rapid degradation in adverse weather conditions, such as fog, rain or dust, although UAS also perform poorly under these conditions. The benefits are that they are passive, consume limited power and cooling capacity, and can also incorporate ranging capabilities with an inbuilt laser that can be slewed on once a target has been detected. They can also support a weapons system to be slewed to engage a target and offer passive fire control.

Classification

Detecting that a UAV is present is a prerequisite for taking countermeasures, but it is insufficient for ensuring that the countermeasures adopted are appropriate. The appropriate response to the detection of a quadcopter that is conducting observation is different from the response required when a short-range loitering munition-type UAV, such as a Lancet-3M, is detected. Nor is the appropriate response to detecting the overflight of a long-range reconnaissance UAV, such as an Orlan-10, the same as detecting the overflight of a long-range OWA UAV, such as a Shahed-136. Classifying the activity being conducted and thus the threat posed is a vital step in any C-UAS capability.

For hostile aircraft, the traditional primary air defence approach involves first determining the type of aircraft, to infer the threat posed. An Su-35 Flanker, an Su-34 Fullback or an Il-22 Coot can be relatively safely assumed to be conducting certain mission sets based on their inherent capabilities, limitations and role within enemy doctrinal structures. Second, analysis of the aircraft's detected heading, altitude and routing are also likely to provide a good indication of its current task. An Su-35 Flanker-M pair flying a racetrack pattern at high altitude inside their own airspace, for example, are likely to be conducting a defensive counter air patrol.

By contrast, this type- and flight pattern-based approach is not nearly as reliable when seeking to classify the threat posed by UAS, and is likely to become less reliable as their employment proliferates. This is because the task performed by many types of UAS is variable, depending on the modules they carry, while their external form factors often are both relatively generic and also change

frequently.[17] Current approaches to classification within militaries tend to focus on the size, speed and altitude of the UAS, but this is problematic because these variables alone do not necessarily distinguish their mission or, therefore, the threat they pose. It is, in some cases, easy to associate airframe with task, but for many classes of UAS it is not a safe assumption. Classification needs, therefore, to be determined by comparing a wider range of characteristics, including a UAS's electronic emissions, flight profile and silhouette. One of the most important classification criteria is to identify a UAS's method for determining its location, or 'self-localisation'. This is a particularly useful characteristic to assess because it provides not only insight into the likely mission of the UAS, but also data on how that mission can be disrupted.

Emissions include the receipt of signals from a ground control station, the sending of signals to a ground control station or offboarding of data to a command post, or the emissions of sensors including radar, laser, light detection and ranging (LIDAR), and other sensor types. In most cases emissions can be monitored with a spectrum analyser. In combination with a flight profile, such emissions can confirm what a particular UAS is doing. For example, a UAS that is emitting consistently and is flying either at medium altitude or hovering in place for a sustained period is probably conducting ISR. A UAS that is emitting constantly but is flying on a determined course at low altitude is probably an FPV flying towards an identified target. A UAS that is not consistently emitting and is flying quickly at low or medium altitude with a consistent course is probably a OWA UAS flying to a pre-designated position. Some categories, such as autonomously guided OWA munitions, may not emit in this way, but in these cases they will generally fly in straight lines, turning at programmed waypoints – thus distinguishing them from a short-range reconnaissance UAV – and they may emit from the sensors necessary for their autonomous functioning. Flight profile can be determined by optical observation or acoustic or radar tracking to build up a picture of altitude, bearing and speed over time. Machine-learning algorithms can be used to build a library of recognised profiles and accelerate precise classification.

Silhouette is best determined with EO/IR observation. In many cases the exact silhouette of a UAS can be compared against a database of previously observed UAS to determine its type. Where the exact type of UAS cannot be determined, the shape of the body and wing can often reveal its task. Designs such as the Russian Lancet 3 or the Iranian Missile 358, for example, have cylindrical fuselages like a missile, with multiple control surfaces that also provide lift in place of standard wings. This means that they can (and indeed, must) cruise at relatively high speeds and are very agile, but the configuration produces considerable drag, which limits their range and endurance for a given size.

17. Bronk and Watling, 'Mass Precision Strike'.

These designs are, therefore, typically associated with short-range strike tasks with some loiter time, rather than missions that require endurance, such as ISR. By contrast, long, high aspect ratio wings are much more appropriate for ISR, due to high cruising efficiency at slower speeds. A delta wing format is in some ways a middle ground that produces enough lift to enable more fuel and heavier warheads to be carried for a given airframe size, but at the cost of higher drag during cruise. This makes it the configuration of choice for many OWA UAVs, such as the Shahed 136. Quad- and multicopter designs are slightly more ambiguous in terms of the mission they are likely performing, although the silhouette of their payload is usually clear as it is carried externally, and so the threat they pose may be deducible by observation.

Sound signatures are also a means of classifying specific UAS. The combination of the power unit, the propulsion system and the interaction of a UAS's airframe with the air it displaces, all produce distinct sounds that when combined can produce a sufficiently unique pattern to allow accurate classification of a UAS. While automation of classification requires an extensive library and effective algorithm, human operators can often distinguish specific UAS types with limited training. Classification by sound has proven highly reliable. Where a new class or variation in build of UAS is detected, these features can also provide clear signals as to its task and thus the threat presented.

The methods UAS use for self-localising include Radio Frequency Line of Sight, paired Global Positioning and Inertial (GNSS/Inertial), and Beyond Visual Line of Sight radio and optical navigation, including simultaneous localisation and mapping, optical flow or visual odometry. Each of these navigational methods is optimised for different ranges and functions and is compatible with different tasks, aiding classification, but is also a critical dependency for the UAS in executing the task, meaning that if the navigational logic can be confirmed, an effective defeat mechanism can be paired with the target.

The sensors necessary to determine these considerations are generally the same as those required to detect the presence of a UAS. However, unlike detection, classification often requires the comparison of the returns from two or three sensors and the application of either judgement by the operator or, if automated, a logic engine attuned to prioritise threats to the force from objects according to their task once classified. This information is necessary to enable an appropriate defeat mechanism to be applied to each threat, and for threats to be engaged at both the appropriate echelon and in the right order. Where insufficient defeat mechanisms may be available, classification also provides the information to assess which threats from enemy UAS can be mitigated by passive measures, and which enemy UAS must be defeated, given that the threat they pose cannot be mitigated.

Discrimination

One of the most prevalent challenges in C-UAS operations is the risk of fratricide. This can be fratricide of friendly communications and other capabilities. For example, during one exercise observed by the authors, a C-UAS system classified all personal radios worn by friendly troops in its area of regard as UAS and promptly collapsed all squadron communications.[18] C-UAS capabilities are also very liable to destroy friendly UAS. During an operation observed by the authors, electronic protection from UAS similarly collapsed blue-force tracking across a divisional frontage, driving troops to have to revert to map-based navigation for a protracted period.[19] In Israel, one of the authors observed how Israel Defense Forces had taken to shooting down both friendly and enemy UAS that flew over their units.[20] Ukrainian and Russian air defences, meanwhile, have each accounted for a large proportion of their own larger UAS losses.[21] Conversely, the Islamic Revolutionary Guard Corps used the flight path of American UAS returning to a base in Jordan to fly a strike UAS to attack the base, with US air defenders presuming it to be friendly.[22] The same method – following a known international flight path – enabled a UAS strike by the Houthis on Tel Aviv.[23] The underlying problem is discrimination. The problems with discrimination of UAS arise from three causes:

1. There are too many UAS launched by too many separate units to enable precise blue-force tracking of them. This makes centralised deconfliction impracticable.
2. UAS are sufficiently varied in shape and function, and simultaneously similar enough in silhouette and flight profile, to be difficult to differentiate in terms of who launched them.
3. The threat UAS may pose to those beneath them, either via direct strikes or observation leading to precision artillery strikes, leaves little time to discriminate.

18. Author observation of large-scale field exercise, US, March 2024.
19. Operation observed by one of the authors, March 2024.
20. Author observations, Northern Israel, March 2024. It is worth noting that this has also been a challenge for Ukrainian pilots flying fixed-wing assets, and as a phenomenon has a long history dating back to the First World War.
21. Author interviews with Ukrainian air defenders and air battlespace managers, Ukraine, August 2022, October 2022, and April, May and July 2023. There are many reported examples. For Ukrainian friendly fire, see Joseph Trevithick, 'Ukrainian TB2 Shot Down over Kyiv by Friendly Forces', *The Warzone*, 4 May 2023, <https://www.twz.com/ukrainian-tb2-shot-down-over-kyiv-by-friendly-forces>, accessed 6 July 2024.
22. Phil Stewart, Steve Holland and Idrees Ali, 'Three US Troops Killed in Jordan Drone Strike Linked to Iran', *Reuters*, 29 January 2024.
23. Rami Amichay, 'Tel Aviv Hit by Drone Attack Claimed by Iranian-backed Houthis', *Reuters*, 19 July 2024.

The solution to this problem should be federated by altitude, and by the type of UAS under discussion. For fixed-wing ISR UAS intended to operate at medium altitude, the fact that they fly above the range of most lower-echelon organic C-UAS effectors means that they do not need to be discriminated by those echelons. At the same time, these UAS are large enough and have enough power to be able to carry an encrypted transponder, which emits a pre-programmed signal when it receives a pre-programmed interrogative message.[24] In this way, a system optimised for defeating these targets should be able to carry a capability to interrogate the target and, on receiving the appropriate electronic handshake, desist from targeting the system. Once a UAS has been shot down over enemy territory, there is a significant risk that the transponder will be captured. For this reason, the IFF (identification, friend or foe) signature would need to be updated to prevent hostile UAS from replicating it to avoid being intercepted, probably on a 24-hour basis. This approach is consistent with what is typically done with crewed aircraft.

Such a solution is not viable for quadcopters and tactical UAS because most lack the payload and/or power storage to be fitted with an IFF transponder, and most of the capabilities that would passively detect and target them would not have an ability to interrogate a transponder. Here tactics, techniques and procedures (TTPs) must be used to avoid fratricide. For the company group, organically attached UAS can likely be protected by being controlled through the company mobile ad hoc network (MANET) that bears its tactical communications.[25] Thus, UAS generated from within the company group would appear on blue-force tracking. Since these UAS would fly from and return to the company's area of responsibility, this would present little problem. The challenge emerges when a battalion or UAS attached at battalion, or to support arms, flies UAS over company battlespace, since these capabilities will not be part of the company MANET and would saturate the capacity of the network if their integration was attempted.[26]

For OWA capabilities, the indication to friendly forces on their route of advance as to their time and course should allow for C-UAS teams to accurately discriminate. For ISR UAS, the problem with such an approach is that they must also overfly friendly positions en route back from a mission, and if subjected to jamming, may endeavour to autonomously return to the base station on an unplanned route. For these capabilities, it may make sense for the flight plan to include a

24. Sagetech Avionics, 'MX12B Mode 5 IFF Transponder', <https://sagetech.com/transponders/mx12b/>, accessed 6 July 2024.
25. Jack Watling, 'Supporting Command and Control for Land Forces on a Data-Rich Battlefield', *RUSI Occasional Papers* (July 2023).
26. This is a problem that the authors have observed on exercise and operations on several occasions, discussed earlier.

point at which it traverses the Forward Line of Own Troops (FLOT)/Forward Line of Enemy Troops. On the outbound portion, deconfliction can be by warning to the unit occupying the battlespace. For the return portion, it may make sense for the UAS to emit a signal once it has crossed the FLOT – with the appropriate signal being determined by the sensors available to C-UAS systems – to indicate that it is friendly. As these emissions would likely be detectable by the enemy, they would need to be updated regularly, likely with a predistributed schedule of emissions given once per day, with a new signal per hour. Since the UAS would not have the schedule but would have the signal relevant to when they are flying, if the enemy captured one or monitored the signal, they could not then use it on their own UAS within the period of that signal being relevant. This would not be an entirely reliable system, but it would reduce friendly shoot-downs.

Distribution and Cueing

Once a UAS has been detected and identified as hostile, the next stages required for any C-UAS effect are to communicate that information to other assets within and potentially beyond the unit in the affected area of operations. This is primarily important for cueing C-UAS effectors and/or additional sensors onto the detected threat if that is required to obtain a weapons-grade track. It is also important to pass the information to the rest of the unit(s) in the vicinity to allow them to adjust activity according to the category of UAS threat detected. This is a critical requirement to minimise risk to the force and buy time for C-UAS effectors to be brought to bear.

The communication of information to effectors for cueing can be simple or complex depending on the way that the C-UAS capability has been integrated into the force. If the sensors and effectors are concentrated on dedicated vehicles, hand-off between initial detection, track and discrimination sensors and systems to effectors can potentially take place on the same vehicle or at least within a small subset of those within a given unit. On the other hand, if detection relies on a distributed array of sensors such as multi-static passive radar arrays or acoustic sensor arrays mounted on multiple vehicles throughout a unit, then the communications links between them and any effector will need to be complex, resilient and low latency.

For passive sensors that cannot produce high-resolution track data, which includes acoustic, some passive radar and most RF analysers, producing a track suitable for weapon guidance will require cueing on a secondary sensor that can generate the required track resolution. For most relatively short-range C-UAS tasks, the simplest solution is to use the azimuth data provided by passive sensors to cue on a sensor ball with a high-resolution EO/IR camera and integral laser

rangefinder. Non-dedicated C-UAS optics, such as those found in sensor balls on remote weapon stations (RWS) or turret-mounted optical suites, should be able to relatively easily acquire UAS within several kilometres once provided with an accurate bearing to search, and ideally a rough range and speed of travel.

Alternatively, active fire control radar systems such as those that provide ranging, speed and bearing data for self-propelled anti-aircraft guns (SPAAGs) or for missile cueing and guidance for SAM systems can be cued onto targets detected by wide area systems. The information that needs to be passed for cueing such systems does not need to be track-quality high-resolution data, but merely enough to enable those SPAAG and SAM systems to engage with minimal radar illumination times by only having to search a limited scan volume to acquire the target.

II. Engagement and Defeat

Once a UAS has been detected, classified and identified, the force must apply the appropriate countermeasure to defeat it. Understanding the options and their various advantages and dependencies allows a force to field an appropriate array of options for protecting itself from UAS. This chapter therefore explores how UAS can be defeated in their mission through the targeting of their sensors, communications and navigation, and their enablers, or by physically destroying them.

Sensor Defeat

With the exception of GNSS-guided OWA systems, almost all UAS require functional sensors to pose a threat to forces or installations. Thus, one of the core approaches that can be taken as part of C-UAS defence is to temporarily or permanently degrade the sensors used by UAS that are operating in the vicinity of friendly assets.

Success is heavily contingent on being able to accurately determine the activity that a given UAS is conducting, and thus on what sensors it is likely to rely. As discussed in Chapter I, there are multiple potential methods that can be used, but the critical thing for the success of any sensor defeat effector is that the effector in question receives the data as quickly as possible.

Since a substantial proportion of hostile UAS activity will be either ISTAR-type missions or FPV attack missions, the capability to blind optical sensor suites is critical for C-UAS approaches that rely on sensor defeat. Retroreflector technology using lasers to detect the reflected returns from lenses has seen extensive use in recent conflicts, including in Ukraine, and offers the potential to rapidly pinpoint and then dazzle or even permanently damage hostile optics.[27] While this has until recently primarily been used to counter snipers and anti-tank guided missile teams and to degrade vehicle optics on the ground, if cued by an appropriate detection system, such technology can be used in the C-UAS role. Furthermore, the power requirements for a laser capable of dazzling sensitive optics are far lower than for more ambitious laser C-UAS systems, which aim to shoot down UAVs. This means that systems with retroreflector and laser dazzle

27. Arjan L Mieremet, Ric M A Schleijpen and P N Pouchelle, 'Modeling the Detection of Optical Sights Using Retro-Reflection', Proceedings of SPIE Conference (Vol. 6950, 13 May 2008); Trevor Seets, Alec Epstein and Andreas Velten, 'Watching the Watchers: Camera Identification and Characterization Using Retro-Reflections', *Opt Express* (Vol. 32, No. 8, 2024), pp. 13836–50.

capacity can be much smaller and relatively cheap, and have a much greater magazine depth for a given space, weight and power installation. This in turn means that optical sensor defeat capabilities are more feasible than many other C-UAS effector solutions for use by forward forces at low echelons close to the frontlines. This approach has a proven track record on defensive counter-aid suites for crewed platforms. However, if a system does not have sufficient power to permanently damage the optics of a hostile UAS, its sensor-defeat capacity will only last for as long as the operator can maintain direct line of sight to the target. Thus, for lower-powered systems, it would be necessary to have numerous effectors across the frontage held by a unit to ensure effective coverage, whereas for more powerful systems, a smaller number might be sufficiently effective. Another issue with relying on this capability in isolation is that cameras can be protected from retroreflective detection.

Passive defeat approaches are also important to consider. For example, against FPV-type direct attack UAS or loitering munitions, such as Lancet-3M, which use either EO or IR sensors for terminal guidance, using smoke as an obscurant can be highly effective if the unit being targeted can be warned promptly about the presence and likely category of incoming threat. Even for future systems that are likely to use AI and/or machine learning, and enabled automatic target selection and terminal guidance to avoid the need for a vulnerable connection to a human operator, the use of obscurants should remain highly effective if triggered in time. 'Hot smoke' compounds that give a sufficient thermal signature and can effectively blind IR sensors as well as EO ones are an obvious choice given the versatility they offer against multiple types of hostile UAS/munitions. Smoke launchers are already a core component of the defensive systems on most main battle tanks, and given the increasing prevalence of UAS and loitering munition threats, could and probably should be mounted on a wider range of vehicles throughout most formations. The critical determinant of whether such systems can form a reliable part of sensor-defeat C-UAS approaches will be the communications architecture to enable the detect, track and classify functions of the sensor and processing layers to pass real-time and accurate warnings to the forward elements under attack with a sufficiently low false-positive rate. Finally, UAS can have their effectiveness reduced using multispectral camouflage and overhead protection on fighting positions, such that it requires much longer times on target to locate units and distinguish targets.

Soft Kill

For ISR UAS there is a requirement to offboard sensor data for them to achieve their mission, whether they are remotely piloted or autonomous systems. There is also usually a requirement for them to receive intermittent commands to fly to or orientate their sensors towards and orbit points of interest. There can be significant levels of automation in flight, but periodic receipt of data is generally necessary. The prevention of an ISR UAS from receiving such instructions can in many cases drastically limit its utility. If the data it is gathering cannot be offboarded, this is even more problematic, as the latency introduced if the data can only be recovered upon landing means that its value is greatly diminished.[28] The easiest method for preventing an ISR UAS from achieving its mission therefore is simply to apply jamming against the receiver to sever its ability to receive instructions. In many cases this will cause the UAS to return to its base station and therefore end its mission. A similar approach can be effective against short-range FPVs. Jammers, however, are vulnerable to direction finding and strike, such that jammers cannot be used continuously unless the effect is passed between several that have been distributed.

Autonomously navigating UAS, either because they have lost contact with a control station or because they are strike systems following a pre-programmed route, must still have a method for accurately tracking their own position during flight. The same is true for future UAS systems with much greater levels of autonomy leveraging AI. This can be done through GNSS, sensors such as LIDAR or optical terrain contour-matching, inertial navigation, simultaneous localisation and mapping, optical flow or visual odometry. Usually, it will be a combination. Localised jamming or spoofing of GNSS signals can often achieve a soft kill against simpler systems, as can damage or interference with the onboard sensors of UAS through electronic attack. For example, if the navigation system of a UAS can be spoofed to indicate that it is flying above its actual altitude, it can be induced to execute a controlled flight into terrain. If a UAS is forced by the denial of GNSS to rely on inertial navigation for a sustained period, it can be brought significantly off target over time through drift. Even a relatively limited positional error induced in hostile ISTAR UAS, in particular, can lead to them passing inaccurate target coordinates to long-range strike systems, protecting the observed formation and wasting enemy precision munitions.

There are more specialised forms of soft kill. If encryption keys for a UAS have been identified, either from captured UAS or from poor drills for key distribution by the enemy, or if a UAS receives data via certain channels, it becomes possible to conduct either a protocol-based electronic attack or cyber attack against the

28. Author observations of ISR UAS missions flying over Russian positions in Ukraine, June 2022.

system. This can, for example, alter what is shown on a video feed to push false information back to the base station.[29] Alternatively, it could hijack the UAS and force it to land somewhere harmless, enabling recovery and exploitation. These capabilities are more specialised than routine jamming and require dedicated operators with access to intelligence. These techniques are also opportunistically available, rather than persistently dependable.

None of the forms of soft kill outlined above are guaranteed methods for defeating a UAS. One way to make jamming data transfer difficult, for example, is for a UAS to communicate on two non-adjacent frequencies, which hop, and to compare the message received on each. If one differs from the other, a third frequency is used and compared to the existing frequences to determine which is genuine, and then the false one is closed off.[30] If the frequencies can be hopped quickly, it requires a very capable jammer to reliably track and defeat the signal. Similarly, a UAS that has an eight-element antenna for GNSS can receive signals on multiple navigational frequencies and compare them, and can compare the alignment of received signals, such that effectively denying GNSS requires specialised equipment and operators.[31] While such specialised capabilities can be fielded, they cannot be available across all echelons and so where such bespoke jamming is held must be carefully prioritised.

That soft kill can be overcome across much of the front does not mean that it lacks utility. What the proliferation of soft kill capabilities achieves is that it significantly raises the sophistication and quality requirements for hostile UAS to enable them to successfully prosecute missions. This reduces the frequency and volume of the threat and requires the enemy to be more careful to avoid losing their UAS. UAS that have been designed with more costly and capable features to make them resistant to soft kill techniques are not necessarily any more survivable against hard kill approaches. By reducing the number that must be intercepted, soft kill capabilities make it more economical to conduct hard kill defence and reduce the risk of hard kill systems being saturated. Soft kill defences can also be more easily made persistent and can have a wide-area effect. Historically, the need for dedicated EW systems to deliver soft kill made it difficult to have such capabilities available across all echelons. However, today, the emergence of software-defined systems means that with the right programming and the right antenna, most tactical communications systems can be repurposed to deliver EW effects. Thus, it can be characterised as an opportunity, rather than an opportunity cost, to equip the force with useful soft kill C-UAS capabilities.

29. Joseph Trevithick, 'Green Berets Hijacked WiFi to Control Home Security System Then Vanish in Mock Raid', *The Warzone*, 29 August 2024.
30. This is how the Lancet-3M functions. Author tested in laboratory, Ukraine, May 2024.
31. Such as with the Kometa-M antenna used on a range of Russian systems. Inspected and tested by the author on multiple occasions, most recently in Ukraine, May 2024.

Hard Kill

Physical destruction of UAS can be achieved via various means, each of which has implications in terms of efficiency, cost and enablement. The three broad means of destruction are gunfire, manoeuvring interceptors and directed energy.

Gunfire

For most military forces, adapted existing small- and medium-calibre cannon mounted on vehicles represent the most obvious potentially available distributed C-UAS effectors. While it is a near-universal response of troops who observe UAS to shoot at them with whatever weapons are available, the fact is that UAS represent a difficult target set. Most are small and can move erratically in three dimensions, and accurately estimating their range from a shooter is difficult to do visually. Effectiveness even with standard rifles can be improved by providing some soldiers with specialist C-UAS sights that help calculate distance and speed and provide an aiming cue for the shooter.[32] Shotguns have also had limited success as a last-ditch defence against Lancet series loitering munitions and FPV attacks in Ukraine. However, relying on soldiers as a significant layer in C-UAS defence is a terrible strategy because of the inherently low probability of kill, and the fact that soldiers have other important tasks to carry out.

As a rule, the base requirement for more reliable gunfire-based C-UAS effects is a system with either optics containing a laser rangefinder or a fire control radar system that can provide an accurate slant range and speed estimate for a precise firing solution. RWS can and should be used for this task. Dedicated anti-aircraft systems, such as the highly effective German-made Gepard SPAAG, also feature the capability to programme each shell to detonate as it reaches the target vicinity. This enables specialist anti-aircraft cannon ammunition to provide a blast-fragmentation effect to greatly increase the likelihood of critical damage to UAS and even cruise missiles with only short bursts of fire. The effectiveness of .50 BMG and 12.7-mm or 14.5-mm systems could also be improved with specialist ammunition, though even with standard ball, appropriately modified RWS can achieve kills against UAS with single shots.[33] The major downside of dedicated SPAAGs as C-UAS effectors is that they are relatively expensive and specialised vehicles that represent a significant opportunity cost to acquire, and an additional logistical burden on units to which they are assigned.

32. For example, see description of SMASH-series of C-UAS sights in Joseph Trevithick, 'British Army Paratroopers Get Computerized Rifle Sights to Shoot Down Drones', *The Warzone*, 5 March 2024, <https://www.twz.com/land/british-army-paratroopers-get-computerized-rifle-sights-to-shoot-down-drones>, accessed 3 July 2024.
33. Author observations of engagements under test conditions, July 2024.

However, the upside is that not only can they be equipped with heavier calibre cannon with a greater rate of fire than other medium-armoured vehicles, but they also generally come equipped with their own dedicated detect/classify/discrimination sensor suite to cue on their weapons. They can also provide devastating firepower against dismounted enemy infantry and lightly armoured vehicles in a ground-support role, and are much more capable against hostile aircraft, missiles and attack aviation than many other dedicated C-UAS effectors.

Most modern general purpose armoured fighting vehicle (AFV) designs also include the option for a gyrostabilised 25–40 mm rapid firing cannon armament, mounted either in a turret or in an RWS, with EO/IR optics, laser range finding and programmable ammunition. Thus, if provided with suitable air burst ammunition, and specified with the requisite elevation for the gun, there is clear potential to adapt regular AFVs relatively easily to provide a significant degree of C-UAS effector capacity for land formations in a package that otherwise retains its full utility as a regular AFV. Without specialised sensor suites for detecting and classifying UAS themselves, regular AFVs with suitably specified turret/RWS armament would still need to have their optics cued onto a rough target bearing by offboard detection systems.

Two significant drawbacks of cannon-based C-UAS effectors are ammunition consumption and limited range. Both are linked to the calibre of the system chosen. Higher calibre guns will be able to engage UAS out to longer ranges and at higher altitudes, but will also be able to carry fewer ready rounds within each vehicle, and rounds will be more expensive and bulky to transport from a sustainment point of view. Even relatively large calibre rapid-fire cannon such as the British Army's 40-mm Cased Telescope Armament System would still be unable to reliably engage ISR UAVs, such as the Russian Orlan-10, at maximum cruising altitudes of 16,000 ft.[34] In other words, while cannon-based effectors can provide a significant volume of effective close-range C-UAS capability if provided with the correct cueing, specialist ammunition and sensors, the requirement to also have a missile, directed-energy or interceptor-UAS system to cover the medium-altitude ISTAR part of the UAV threat spectrum would not be removed.

Interceptors

The most common currently fielded form of manoeuvrable interceptors for C-UAS tasks are shoulder-fired man-portable air defence systems (MANPADS) such as the FIM-92 Stinger, which employ an IR/UV (heat-seeking) passive head

34. Estimates of maximum effective air-defence range and altitude for various cannon calibres from industry subject matter expert interviewed online by authors, 2 July 2024; 30x113 mm – 1,500 m and 750 m; 35x228 mm – 3,500 m and 3,000 m; 40x255 CTAS – 4,000 m and 3,500 m.

to acquire and guide the weapon in on the hotter engine components of larger UAS. There are three core drawbacks to such systems for C-UAS defence. First, they have limited effective range, which prevents them from engaging medium-altitude ISTAR UAVs, such as Orlan-10. Second, they are much more expensive than small UAS or even than many medium-sized UAS, and so are not necessarily a sustainable answer to massed threats. Third, they are not suitable for engaging small UAS and FPV attack drones, as these electrically powered systems are too small and do not produce a viable heat signature to gain a lock.

Traditional SAM systems designed for anti-aircraft or missile defence tasks are also not well suited for C-UAS work, primarily because they are generally too large, expensive and overstretched relative to air and missile defence requirements to be sustainably used to engage even medium-sized UAVs. Second, radar-guided SAM systems use Doppler gates to filter out returns from static or slow-moving objects to reduce clutter, which also means that many systems struggle to reliably detect and track UAS that are hovering or moving at slow speeds. However, the upside of SAM systems compared with cannon or EW-based effectors is range, and therefore defensive coverage potential. If cued in by connected sensors, a launcher can also potentially engage UAVs that are beyond line of sight, further increasing the area that can be protected by a given number of launch systems.

Due to the far lower travel speed of UAVs compared with the aircraft and missiles that SAM systems are typically designed to engage, the ideal size of a C-UAS SAM is significantly smaller and can thus be cheaper and carried in larger numbers for a given volume. One promising option for SAM systems that are better suited to engaging ISTAR UAVs is the adaptation for ground launch of existing missiles designed for within-visual-range combat for air forces. One example is the British AIM-132 Advanced Short Range Air-to-Air Missile (ASRAAM), designed for use on RAF Typhoon fighters, which has successfully been adapted for cueing and launch by ground vehicles in the C-UAS role in Ukraine.[35] While the range achievable will be significantly shorter than when launched from a fighter aircraft, when intercepting slow flying UAVs at medium altitudes, it is still significant. Existing short-range air-to-air missiles also offer the prospect of reduced cost per munition due to commonality across services, and the potential to use weapons in a ground role that have run out of airframe carriage hours but are otherwise still fully functional.

One emerging subtype of interceptor for C-UAS work are systems such as the Iranian–Houthi 358 Saqr [Missile] or the growing range of interceptor UAS fielded by Ukrainian and Russian forces. The 358 Saqr is a two-stage SAM which uses

35. Thomas Newdick and Tyler Rogoway, 'Air-To-Air Missiles from UK Now Being Used by Ukraine as SAMs', *The Warzone*, 4 August 2023, <https://www.twz.com/asraam-air-to-air-missiles-from-uk-being-used-by-ukraine-as-sams>, accessed 4 July 2024.

an initial rocket booster to launch the main turbojet-powered section to high altitude and high subsonic speed, where it can then loiter for some time and intercept even high-end UAVs such as MQ-9 Reapers.[36] Anduril has proposed the Roadrunner: a single-stage canister-launched system powered by dual micro turbojets that can launch and, if unsuccessful, land itself vertically, and is designed to intercept hostile UAS by direct impact and destroy them with an integral warhead.[37] Roadrunner is not yet an effective capability, but Ukrainian units have achieved significant results with experimental versions of the concept, albeit using propeller-driven solutions. The critical element in making this capability cost effective is to have an offboard sensor provide guidance, preferably electro-optical or a laser which can be seen by a sensor in the nose of the UAS.[38] Alternatively an interceptor can be guided by a radar. Such systems offer significant potential area coverage against ISTAR UAVs if cued in by an appropriate sensor layer. With utility against helicopters and potentially against ground targets, this class of system is likely to proliferate.

Directed Energy

There are two primary classes of directed-energy effectors for C-UAS: high-powered microwave (HPM) systems and high-energy laser (HEL) systems. HPM systems emit energy in a narrow cone-shaped beam, and so can potentially provide effects against multiple UAS at once if they are operating close to one another. On the other hand, it is much harder to control for potential electronic fratricide and collateral damage due to the wider area of effect of the weapon compared to HEL systems. HELs are precise due to the inherent nature of a focused laser beam, but as a result can only engage a single UAS at once and may require a significant dwell time on each target to achieve destructive effect. The energy also potentially goes a long way beyond the target and may also refract unpredictably in certain atmospheric conditions, making clearing arcs of fire potentially more complex than for cannon or missile-based systems. The higher the power output of a HEL system, the lower the dwell time required on a given target, and the greater effective range it can have, especially in inclement weather conditions. However, higher power outputs also require more power generation capacity, larger banks of capacitors to store charge for 'shots', and greater cooling capacity, so mobile installations become less practical, and costs increase significantly.

36. Defense Intelligence Agency, 'Iran: Enabling Houthi Attacks Across the Middle East', February 2024, p. 20, <https://www.dia.mil/Portals/110/Documents/News/Military_Power_Publications/Iran_Houthi_Final.pdf>, accessed 4 July 2024; *Global Defense News* Army Recognition Group, 'Yemen's Houthis Have Now Destroyed More Than $150 Million of American Drones After Burning a Fifth MQ-9 Reaper', 29 May 2024, <https://armyrecognition.com/news/aerospace-news/2024/yemens-houthis-have-now-destroyed-more-than-150-million-of-american-drones-after-burning-a-fifth-mq-9-reaper>, accessed 4 July 2024.
37. Anduril, 'Roadrunner', <https://www.anduril.com/roadrunner/>, accessed 4 July 2024.
38. Author observation of intercepts by experimental systems in Ukraine, August 2024.

One of the issues that has hampered the development and fielding of practical HEL systems for wider short-ranged air defence (SHORAD) tasks is that most systems have been required to potentially deal with a wide variety of threats, including incoming mortar rounds and missiles, to enable them to replace traditional cannon systems such as Phalanx. Successfully engaging incoming munitions, many of which travel at high subsonic or supersonic speeds and so present a short engagement window, demands high power levels. However, if HEL systems were to be procured specifically for C-UAS functions, they could be functional with far more modest power outputs, as UAS tend to be relatively slow and relatively lightly built.

HPM and HEL systems also tend to be rather more expensive to procure than comparable missile or cannon systems, but far cheaper per engagement and with a greater potential magazine depth. The effectiveness of HEL systems also tends to drop substantially in heavy rain, fog or very dusty environmental conditions due to increased atmospheric refractive disruption and attenuation. However, many UAS are also not particularly effective in such conditions due to airframe or sensor limitations.

Offensive C-UAS

The measures discussed above involve hard- or soft-kill effectors that aim to defeat enemy UAS in flight. However, C-UAS effects can also be achieved by targeting ground control stations and other enabling assets embedded within hostile ground forces. Even future strike UAS that may operate with a significant degree of autonomy will still need to be launched and monitored by a unit on the ground, while ISTAR UAS must transmit data back to ground control stations, and in many cases receive instructions or mission updates while in flight from teams of ground-based operators. These ground teams and control stations are an important potential attack surface against which C-UAS detection and effector capabilities can and should be optimised. In Chapter I, widespread distribution of RF analysers was discussed as one of the key approaches for detection of hostile UAS. These analysers will not only detect UAS, but as they would be spread out across a unit's frontage, could also be used to triangulate emissions from hostile UAS ground control stations.

Exploiting this information can be done in several ways. If the triangulation or raw data is shared to the battalion or brigade headquarters, various methods could be used to decrease the effectiveness of ongoing hostile UAS operations. In the first instance, a brigade might allocate electronic attack capabilities to jam frequencies over the control station, thus achieving a similar effect to a soft kill directly against each UAS. Against a system with a dual-frequency

communications link, as described in previous sections, simultaneous jamming of the base station and the UAS can be particularly effective. While the range necessary to jam a ground control station behind the enemy frontlines will require significant power and thus a dedicated EW system, limiting the duration such an effect can be applied, targeted use of such capabilities could be sufficient to disrupt, for example, a large-scale loitering munition strike wave.

The ground control station can be subjected to physical fires. Optimally, this results in the death or wounding of the UAS operators, and thus not only the defeat of the UAS they are controlling at the time, but also a diminution of specialist adversary expertise. However, even if strikes fail to hit the operators, they may damage the antennae being used to send signals and thus sever the ability to regain control of the UAS. The value is that, unlike soft-kill methods, kinetic damage against either operators or control equipment not only achieves defeat of the UAS in its mission, but also creates persistent, rather than time-bound, degradation.

Alongside direction-finding location of hostile ground control sites, the other function of spectrum analysers being distributed across the front is an ability to collect large volumes of signals traffic. Decryption of such signals and/or sustained collection for pattern-of-life analysis may allow the identification of launch points, indicators of when the enemy is moving to them, and mapping of the support structure for enemy UAS complexes. These can then be pre-emptively targeted, to try to strike UAS and their crews on the ground while they are preparing to launch.

III. Deploying a C-UAS Complex

Having explored the means available for detecting, classifying, identifying and tracking a UAS, and how it can be defeated, this chapter considers how the force can integrate these capabilities to provide the relevant density of protection to enable it to operate. The chapter is in three parts. The first considers how C-UAS capabilities should be distributed across a force for its own protection. The second examines the protection of critical targets. The third discusses the C2 required to coordinate these capabilities.

Defining Requirements at Echelon

As described in Chapter I, the foundational C-UAS capability is situational awareness through the ability to detect UAS. This capability is required at all echelons because without it, no countermeasures can be initiated. The simplest means for detecting UAS at the FLOT is a spectrum analyser. The addition of acoustic sensors, which today can be vehicle mounted[39] or man-packable,[40] is also exceedingly useful for passive sensing of UAS and other threats.[41] Acoustic sensors on vehicles also allow UAS to be tracked over time as they overfly units.

In terms of self-defence against UAS organic to platoon, it is possible for a software-defined radio with an appropriate antenna to be mounted on a vehicle and programmed for electronic attack. Having such a jammer within a platoon of vehicles would not allow complex jamming to be carried out by the vehicle crew, who would likely lack the expertise to programme bespoke attacks. However, as EW specialists build bespoke attacks for specific classes of UAS, it could become possible for this library to be pushed to these radios, so that if an emissions pattern has been classified it can be effectively engaged. This platoon EW could also be used to deny GNSS over its position to protect it from precision strike, although this would require the antenna, a generator and the software-defined radio to be offset from the vehicles when static, and so dismountable,

39. As integrated on Ajax. See Ministry of Defence (MoD) and Defence Equipment & Support, 'Innovative Threat Detection System for Ajax', 15 March 2018, <https://des.mod.uk/ajax-threat-detection-system-acusonic-sensor-army/>, accessed 7 July 2024.
40. Author observation of man-packable acoustic array, US, October 2022.
41. Data shared with author on reliability of detection and classification of UAS using acoustic sensors in testing, February 2021, and observation of Ukrainian acoustic sensors, Ukraine, April 2023.

to avoid drawing fire. The use of directional jamming could also be used to reduce the signature of the platoon emissions. While not able to craft attacks, the platoon would need to be conversant with when and how to employ the capability, analogous to how platoons manage electronic countermeasures to protect themselves from IEDs. Furthermore, with the advent of non-cooperative swarming in Ukraine, and cooperative swarming around the corner, increasing investment in the 'detect/identify/track' phases of the C-UAS cycle is critical.[42] Increasing capability and distributing sensors ensures expensive and bespoke C-UAS capabilities are not overwhelmed and attrited.

The ability of platoons to self-defend will be constrained by the fact that they lack enough platforms to be able to dedicate any to C-UAS functions. However, it may be possible to modify some capabilities to have a C-UAS capability. Laser rangefinders on vehicles, for example, if they can pivot upwards, could be programmed to dazzle UAS, as discussed in Chapter II. RWS can also be programmed to track UAS electro-optically and to engage them to defeat OWA UAS and low-level reconnaissance UAS with significant efficiency.[43]

A company group would lack the capacity to support significantly increased numbers of vehicles dedicated to C-UAS tasks within its organic order of battle. Nevertheless, it would make sense for a pair of vehicles to have dedicated search and classification capabilities. This could be achieved with a light vehicle carrying a mast with passive sensors cueing an electro-optical sensor. In combination with the ability to distribute the sensors at platoon level, this would allow a company commander to have a detailed detection and classification ability over their assigned battlespace.[44] As most tactical actions are ultimately actions by company groups, it follows that it would be necessary for a more dedicated C-UAS capability to support a company operation. Holding these organically within the company would likely overburden it, but having them attached to the company group from higher echelon would be viable.

The battalion is likely the lowest echelon with a sufficient logistics and sustainment capability to support dedicated C-UAS platforms, which would need to be assigned to support subordinate companies. Critically, at this echelon, C-UAS should not simply be thought of as a defensive activity, but rather as a counter-reconnaissance mission: to offensively degrade the enemy's sensor picture by hunting and destroying their UAS. Counter-reconnaissance has a defensive benefit, but in

42. 'Non-cooperative swarming' refers to the use of significant numbers of UAS in the same area or against the same target simultaneously, but where the UAS in question are not exchanging positional data or other mission data to coordinate their flight behaviour. 'Cooperative swarming' involves the use of four or more UAS which are exchanging positional and situational awareness data to coordinate in-flight behaviour automatically.
43. Author observation of 50.cal RWS achieving UAS defeat within five single shots, Ukraine, July 2024.
44. Author observations of attached C-UAS capabilities in various configurations, attached to a squadron group, US, March 2024.

assigning missions to the battalion assets, the mindset of these troops should be offensive.

There are two obvious requirements at battalion: an EW section and a C-UAS platoon. The EW section could run its own baselines, but as software-defined radios become pervasive, the expertise of these personnel might better be employed to first gather, monitor and interpret data recovered from the distributed antennae across the battalion's companies. Second, this section can use software updates, pushed to the dedicated software-defined radios across the battalion, to deliver more specialised EW effects, and to update effects so that they keep pace with adversary adaptation. Third, these personnel provide the picture of the EMS within the battalion's area of responsibility necessary to inform electromagnetic battlespace management and thus reduce fratricide.

The C-UAS platoon would be an augmentation to the battalion support company. The most immediately relevant capability for this platoon is a SPAAG system, cued by the subordinate sensors, but with its own ability to interrogate targets. This capability could be distributed to support company lines of effort so that there is interlocking coverage across the battalion's frontage while on the defensive. Additional SPAAG platoons could then be added to support the battalion if committed to offensive operations, held at brigade. It is also eminently feasible for the turrets of SPAAGs to hold launch canisters.[45] In the first instance, these can hold MANPADS, allowing engagement of helicopters, cruise missiles and some classes of UAS. However, canisters could also hold interceptor UAS, guided by the electro-optical sensor of the SPAAG. These capabilities can engage aviation but are optimised for economically striking UAS at medium altitude. If a SPAAG has four canisters on its turret, there is no technical reason why it cannot have both MANPADS and interceptor UAS ready to fire. For light forces, interceptor UAS can be mounted in canisters on a light vehicle and guided either electro-optically or with a radar mounted on the vehicle.

The brigade is the echelon at which there is the ability to have standalone C-UAS capabilities. As the echelon at which EW deconfliction and management is likely best placed, the brigade should have the ability to conduct bespoke and dedicated electronic attack, using an EW company with large and specialised antennae. With regard to hard kill, the brigade can hold independent SPAAG units of action to protect key sites and distribute to reinforce battalion lines of effort. But the brigade is also the echelon with the requirement to be able to provide area defence for a sustained period against medium-altitude ISR UAS, and it has the opportunity for sufficient access to the common air picture to control such capabilities. The most efficient systems in this role are likely truck-mounted

45. This is done on the US Army's Maneuver Air Range Short Defense (M-SHORAD), on Pantsir, and on a range of other short tactical air-defence systems.

directed-energy weapons, but given the limitations of these systems in various weather conditions, it also makes sense for the brigade to have access to a missile or interceptor UAS able to engage targets at medium altitude. This should be employed as a secondary capability.

Just as the brigade should hold independent SPAAG platoons to allocate to its subordinate battalions, so too should the division have independent C-UAS batteries that it can use to defend critical sites, or else field in support of brigades. The considerations for these divisional units of action, however, intended to protect sites from loitering munitions and OWA munitions, should be optimised against a slightly different target set than those intended to knock down ISR UAVs. Ultimately, divisional C-UAS units must be able to defeat salvos, and this is therefore considered next.

C-UAS Defence of Critical Targets

The requirements for C-UAS defences around fixed points such as logistics hubs, airbases and ports differ in several important ways from the requirements to defend land forces on the battlefield. First, unless they are near the frontlines, the primary threat to such bases and installations is likely to come from cruise and ballistic missile attacks, but augmented by salvos of OWA UAS. This means that the C-UAS task is to protect not only the installations in question, but also the SAM systems, such as Sky Sabre or Patriot, which provide the primary means of defence against attack from above. Any attempt to provide C-UAS defences at every location that might be attacked throughout a given country, let alone across NATO, would be cost and personnel prohibitive. However, given the limited range and slow transit speeds of most classes of UAS, C-UAS coverage for point defence tasks can be prioritised around installations closer to likely conflict zones, such as RAF Akrotiri in the Eastern Mediterranean or Tallinn Airport as an airhead location in Estonia.

Here, adversary OWA systems such as Shahed-136 could cause major problems at relatively short notice, especially if equipped with anti-radiation seeker heads to threaten traditional air-defence radars that are emitting to defend against simultaneous cruise and/or ballistic missile strikes. Even though systems such as Sky Sabre, NASAMS (National Advanced Surface-to-Air Missile System) or Patriot can engage the size of UAS that can travel hundreds of kilometres, this would risk rapidly and unsustainably depleting their ammunition. In other words, C-UAS defence capabilities are likely to become increasingly critical to ensuring that higher-end integrated air and missile defence systems can sustainably operate at locations within range of hostile UAS attacks.

The best way to avoid saturation of point defences at a site is to defeat a salvo over a significant distance, using dispersed capabilities. The efficacy of this approach may be seen in Israel's defeat of a large complex strike from Iran, in which most of the UAS and cruise missiles were defeated by aircraft before they reached Israel.[46] This is also the approach adopted by Ukraine's mobile defence groups. A point defence system cannot have command over a dispersed set of effectors, but it should be emphasised that if the land force has the range and depth of effectors described in the previous section of this chapter, a major salvo should be significantly attrited before it reaches key targets, as reserves and land force elements in the rear can manoeuvre their C-UAS capabilities to provide a distributed defence in depth. In Ukraine, this defence in depth approach relies on around 50,000 personnel, operating in mobile groups with SHORAD weaponry to achieve a high rate of intercept.[47] At the same time, this dispersed defence, while reducing the risk of saturation of a point defence, does not obviate the need for point defences or for protection of critical SAM systems responsible for protecting sites from ballistic missiles that cannot be defeated in depth.

Compared to the C-UAS detection, classification and engagement systems that might be suitable for integrating into mobile land forces for defensive or offensive tasks at various echelons, systems explicitly designed for point defence can be significantly larger and heavier and consume more power. C-UAS operators will need to be able to be part of the recognised air picture being used to coordinate IAMD activities, and this could help with cueing fire control systems and effectors onto incoming threats in addition to dedicated organic C-UAS sensor layers. In some ways, the point defence task could be considered ideal for HEL- or HPM-type directed-energy-based effectors, since higher power outputs and sufficient capacitors and cooling for a deep magazine are easier than in mobile installations. However, depending on the location of the base or installation in question and the equipment being used on and around it, guarding against collateral damage may still be a complex task, especially for HPM effectors. For cannon- or missile-based defence systems, there is likely to be a greater emphasis on effectiveness against salvo attacks than on the ability to deal with sustained attack by many small systems, the significant distance from the frontlines meaning that most very small and cheap hostile systems will lack the range to reach them unless inserted covertly for single salvos.

That said, the use of any kind of kinetic or EW effector around an airbase, for example, is likely to require careful coordination and deconfliction with both military and civilian traffic. For that reason, any missile-, cannon- or EW-based

46. Thomas Newdick, 'Intel from Saudi Arabia, UAE Helped Defend Israel Against Iranian Attack: Report', *The Warzone*, 15 April 2024, <https://www.twz.com/news-features/intel-from-saudi-arabia-uae-helped-defend-israel-against-iranian-attack-report>, accessed 19 August 2024.
47. Author interviews in Ukraine, most recently July 2024.

effector designed for point defence at installations and bases will require robust communications links and coordination TTPs between them, military and civil air traffic control and any IAMD recognised air picture. However, given the relatively specialised nature of many of the C-UAS detection and threat classification sensors discussed in the first section of this chapter, it may be worth deploying and operating such sensors alongside those designed to feed into larger IAMD systems, rather than attempting to rely on the latter to cue in the C-UAS effectors deployed. In terms of the force planning assumptions, although the actual requirement for any given piece of terrain will be bespoke, providing a minimum viable point defence would likely need somewhere between a platoon (three to four platforms) and a company (9–12 platforms).

C2 for the C-UAS Fight

For a distributed array of comparatively short-ranged systems to be effective, it is necessary for them to be efficiently coordinated. Furthermore, since a range of the C-UAS techniques described can disrupt other C2 systems, it is important that the architecture for battlespace management is correct. Based on the functions at echelon described earlier in this chapter, a rational series of C2 relationships can be sketched out.

First, within the company, the ability to have a warning indicator for the presence of UAS as a flag raised and distributed via the company MANET would allow for all personnel to make informed judgements about their diligence in managing their signature and profile, or to determine that a threat justified being engaged by them. This simply requires the presence of the acoustic signature of rotors, silhouette or radio-control frequencies of a recognised UAS to be detected on a company platform associated with the company net, and for the fact of this detection to be shared. This could be done autonomously, with a human on the loop, to accelerate the process and free up cognitive capacity within the platoon from monitoring systems.

Second, the sensor that detected the UAS should collect the assessed characteristics, bearing and azimuth of the detection and hold this data available to be pulled by anyone requesting it. The most likely pull for this data would come from the platoon and company commanders, needing to make a decision about whether to apply or withhold electronic countermeasures, and from the dedicated C-UAS reconnaissance capability – which should pull the data automatically upon a flag being raised on the company MANET – intending to compare returns from multiple sensors, or to interrogate with their own, to classify the UAS. Another interested party would be the battalion EW team, who would want to gather directional data from multiple points to achieve triangulation and potentially

to begin using their own baselines, or other sensors, to look for the enemy control station. Again, much of this could be automated, with the EW specialists on the loop to intervene if required.

From this point, several additional C2 links become relevant. First, if the decision by the platoon or company commander is to apply countermeasures, those in the vehicles with this capability will need to be directed to activate their electronic protection capability. Second, the fact that this has been done will need to be communicated to the battalion EW team and thence to the brigade headquarters for the purposes of electromagnetic battlespace management. This could be automated by sending an alert as a function of turning on the electronic protection suite.

Another line of communications will need to pass the telemetry data, alongside the classification data, from the C-UAS reconnaissance teams to the battalion C-UAS and brigade command post. This is because the UAS could be interested in targets outside the company area of responsibility, and therefore capabilities need to be cued at higher echelon to be orientated and positioned to intercept. In this way, the subordinate companies become a distributed sensor net that allows limited C-UAS assets to be positioned to achieve hard kill against threats as they cross into the rear of the fighting echelon. As each echelon will have companies in reserve, which will also have their laydown of passive sensors, this creates a dense belt of sensors that can not only report the initial contact with a UAS but also, in fact, provide a track of its passage over time, without the need for dedicated communications architectures comparable to the air defence C2 infrastructure, which is too expensive and onerous to be kept at platoon level. Such a C2 structure would, however, require the dedicated hard kill C-UAS capabilities to be able to take the general plot of a UAS's progress and to then achieve a track-quality solution using organic sensors, as well as the ability to interrogate the target. The SPAAG and dedicated C-UAS systems at brigade would need to fall under the air defence command or at least have access to the common air picture to avoid fratricide, as they have the capability, but should not be primarily tasked, to engage a wider range of threats.

If such a system is to function on the standard tactical communications channels, it is important that raw data is not routinely moved from the sensors to a centralised point, but is instead interrogated on the platform so that the facts can be distributed in small data packets of text. The use of a structured language to conduct this reporting would make these reports usable by other C2 systems. This requires some analytical capacity to sit on the software-defined radios supporting the sensors. In principle, this is fairly straightforward. For classification, the onboard processing at the base of the sensor mast of the dedicated C-UAS ISR vehicles would be critical, as these would hold multiple

sensors and thus the ability to achieve high-confidence classification of targets, which could then be distributed as text. If the raw data were needed, it could be routed through an offset satellite communications link or other method, and thereby uploaded to a common portal from which higher echelon systems could pull it for analysis. One function of this pooling would be to create a library of signatures over time, which could then be used to refine both the software providing the classifications and the EW effects programmed into the distributed electronic attack antennae. This would therefore allow EW specialists at brigade to also upload software updates onto the same portal to be downloaded when the tactical situation allowed and thereby be distributed to the company's sensors.

Conclusion

Effective, layered and efficient C-UAS capabilities are not a luxury or a concept to be explored as part of an abstract 'future force'. They are basic elements of a land force that is suitable for operations today. Without C-UAS capabilities, a force will be seen first, engaged more accurately, and ultimately defeated by an opposing force that fields UAS and has the ability to counter them. For NATO members, the aiming mark set by the Alliance's senior leadership is to be ready to deter Russia by 2028.[48] This does not leave time to design and develop new capabilities from scratch. Fielding C-UAS capabilities – which are absent in any structured sense from most NATO land force elements – is therefore an urgent operational requirement.

At the same time, simply procuring expensive and standalone C-UAS systems will not lead to an efficient or coordinated system for protecting the force. At best it will provide limited protection against specific classes of UAS, which will rapidly become obsolete as the threat evolves. This paper has sought to outline the balance of capabilities needed at echelon to provide effective and enduring protection. The following recommendations endeavour to translate this into specific capabilities needed by the British Army. The capability mix articulated may be said to be generalisable to all NATO militaries, but its articulation in terms of specific systems and programmes requires reference to a particular force, and so the British Army is used here as a reference force.

Recommendations

First, the British Army needs to mount EW antennae and software-defined electronic protection suites, passive radar and acoustic sensing across its vehicle fleets. The electronic protection suites should be capable of both directional RF and GNSS jamming. Where systems already exist – as with the acoustic sensors on Ajax – software updates must allow them to be used to accurately detect UAS, drawing on available libraries of data from Ukraine. The software solution

48. For examples of this 2028 aiming mark, see statements about the two- to three-year window to prepare, from Norwegian Chief of Defence Eirik Kristoffersen, in Ott Umelas, 'Norway Army Chief Sees Short Window to Boost NATO's Defenses', *Bloomberg*, 3 June 2024; the statement on the need to double lethality in three years from British Chief of the General Staff Roly Walker, in Alex Candlin, 'New Chief of the General Staff: British Army Needs to be More Special Forces', *Forces Net*, 28 June 2024, <https://www.forces.net/services/army/new-chief-general-staff-british-army-needs-be-more-special-forces>, accessed 6 July 2024; and the statement about the Russian threat to NATO within three years from Danish defence minister Troels Lund Poulsen, in Richard Milne and Marton Dunai, 'Russia Could Attack a NATO Country within 3 to 5 Years, Denmark Warns', *Financial Times*, 9 February 2024.

should be common across the force, rather than separate for each platform or sensor type.

Second, the British Army should develop a passive multi-sensor mast with a software solution that allows its sensor returns to be cross examined to classify objects. These should be mounted as a modular unit on existing fleets of vehicles, optimised for Jackal and Cayote, and procured in sufficient density to have two per company group.[49] Dismounted light infantry should receive the mast as a deployable kit, since the sensors themselves are largely man-packable and can be connected to a buried generator or a light tactical vehicle to be powered. If this is to be done by 2028, the Army will need to risk existing trials processes for its integration on vehicles. The current process of assurance will drive delays and cost up to the point of mission failure.

Third, the British Army must field hard-kill C-UAS capabilities. Software updates to existing RWS on British vehicles should be used to enable them to engage UAS. More importantly, the effective C-UAS interceptors developed and fielded in Ukraine should have their production scaled through the international drone coalition, which the UK leads.[50] This is beneficial to Ukraine now. But the scale of production should also be used to equip British forces at the same unit price as Ukrainian forces are equipped. These interceptors should be given to British support weapons companies.

The acquisition of a SPAAG system for the UK to provide dedicated hard-kill C-UAS coverage at battalion level does require a more deliberate acquisition programme. However, the new Labour government has previously suggested that strengthening Anglo-German defence and industrial collaboration is a priority.[51] The acquisition of a SPAAG turret module for the Anglo-German Boxer would be a possible area for such cooperation, given proven German expertise in SPAAG design. An important consideration for the UK is that using the wheeled Boxer for ground manoeuvre alongside armour will require troops to dismount off the objective and advance on foot, rather than fighting, like a tracked infantry fighting vehicle, onto the objective. In this context, however, a suitable cannon with high elevation angles could allow Boxers to hold back and provide both direct suppressive fire against ground targets with the vehicle hull down, and C-UAS protection over troops moving forward. This is probably the fastest and most plausible route to regenerating a sufficient density of C-UAS/SHORAD

49. This has already been done in trials. Author observation of vehicle at Army Warfighting Experiment 2018, Salisbury Plain, November 2018.
50. MoD, 'UK to Supply Thousands of Drones as Co-Leader of Major International Capability Coalition for Ukraine', 15 February 2024, <https://www.gov.uk/government/news/uk-to-supply-thousands-of-drones-as-co-leader-of-major-international-capability-coalition-for-ukraine>, accessed 6 July 2024.
51. Cristina Gallardo, 'UK Labour Would Seek Security and Defense Treaty with Germany', *Politico*, 16 May 2023.

systems in the relevant timeframe, and would fit well within Boxer's inherent capabilities and limitations.

For brigade and point defence C-UAS capability, the fielding of directed-energy weapons appears to be an increasingly practical proposition. The translation of a capability such as Dragonfire onto a land platform should be a priority.[52] Integration of such a system is, however, likely to take time. In the meantime, a more immediate solution would be the acquisition of Supacat HMT vehicles carrying AIM-132 ASRAAM for UK forces. Tried and tested in Ukraine, this is a cheap option, not so much because of the cost of the ASRAAM missiles, but because increasing the stockpile of these missiles is of direct benefit to the RAF, which uses the ASRAAM as its primary within-visual-range air-to-air missile for Typhoon and F-35B.[53] Therefore, investment in additional missile procurement tranches as a C-UAS stopgap will not be wasted if/when the British Army ultimately pivots away from the platform towards a more mature future SHORAD and medium-range air defence (MRAD) capability. The Supacat HMT is also a vehicle that can have a range of useful roles within the army beyond the utilisation of that particular weapons system. The deliberate development of a low-cost interceptor to augment higher-performance anti-aircraft missiles on a future deployable MRAD system should be a longer-term priority.

For higher-echelon EW, the highest payoff area of priority is likely to be localisation defeat, or the ability to determine a UAS's self-localisation process and disrupt it. The equipment and effects involved in this are not the primary bottleneck. The most significant bottleneck will be personnel with appropriate training and expertise. The priority, therefore, should be to expand the number of personnel in this field.

Finally, fielding any significant C-UAS capability – and in particular the EW effects necessary to protect the force – depends on realistic training. The inability to use EW effects on exercise areas is a major impediment to the readiness of the army. The MoD should aim to establish areas where EW capabilities can be experimented with during live exercises, and if this cannot be done in physical training, it should be replicated in a synthetic environment. It is especially important that formations practise and understand how to use and deconflict their sensors, communications and EW without saturating their own frequencies. Although the need to confront commanders with EMS deconfliction and balance-of-risk judgements between connectivity and electronic protection is something

52. Defence Science and Technology Laboratory and MoD, 'Advanced Future Military Laser Achieves UK First', 21 March 2024, <https://www.gov.uk/government/news/advanced-future-military-laser-achieves-uk-first>, accessed 6 July 2024.
53. MBDA, 'ASRAAM', <https://www.mbda-systems.com/product/asraam/>, accessed 6 July 2024.

that can be trained in simulators to some extent, the practical testing of all relevant systems at echelon requires live exercises.

An effective C-UAS capability across the force is a non-discretionary requirement to be able to sustainably operate on the modern battlefield. A force that has not prepared for this challenge risks finding itself in the position of the Armenians in 2020 – unable to resupply, rotate units, concentrate forces for manoeuvre or achieve operational surprise without taking unsustainable casualties.[54] Defeating current and likely future classes of battlefield UAS, including those with high levels of autonomy, is not intrinsically complex, nor is it difficult compared with developing ballistic missile defences or space capabilities; the requisite sensors, effectors and TTPs all exist and are mostly available off the shelf. There is no justification for complacency, or delay.

54. Watling, 'The Key to Armenia's Tank Losses'.

About the Authors

Jack Watling is the Senior Research Fellow for Land Warfare at RUSI. He works closely with the British military on the development of concepts of operation and assessments of the future operating environment, and conducts operational analysis of contemporary conflicts. Jack's PhD examined the evolution of Britain's policy responses to civil war in the early 20th century. Jack has worked extensively on Ukraine, Iraq, Yemen, Mali, Rwanda and further afield. He is a Global Fellow at the Wilson Center in Washington, DC.

Justin Bronk is the Senior Research Fellow for Airpower and Technology in the Military Sciences research group at RUSI, and Editor of the *RUSI Defence Systems* online journal. Justin holds a Professor II position at the Royal Norwegian Air Force Academy and is a member of the Editorial Board of the scientific and technical journal *Weapons and Equipment* at the Central Scientific Research Institute of Arms and Military Equipment of the Armed Forces of Ukraine. His PhD from King's College London examined 'Balancing Imagination and Design in British Combat Aircraft Development'. Justin is also a private light aircraft and glider pilot.