Australian Army
Research Centre

Small Aircraft, Sizeable Threats: Preparing Army to Counter Small Uncrewed Aerial Systems

Dr Carl Rhodes

Australian Army Occasional Paper No. 24

Australian Army
Research Centre

Small Aircraft, Sizeable Threats: Preparing Army to Counter Small Uncrewed Aerial Systems

Dr Carl Rhodes

Australian Army Occasional Paper No. 24

Serving the Nation

ISSN (Print) 2653-0406
ISSN (Digital) 2653-0414

DOI: https://doi.org/10.61451/267507

All enquiries regarding this publication should be forwarded to the Director of the Australian Army Research Centre.

To learn about the work of the Australian Army Research Centre visit researchcentre.army.gov.au

Cover image: Three MAVIC 2 unmanned aerial systems at Edwards Air Force Base, California (Source: U.S. Department of Defense multimedia images). The appearance of U.S. Department of Defense (DoD) visual information does not imply or constitute DoD endorsement.

Contents

Abstract

In both international and intra-national conflicts conducted over the past decade, the increasing military capabilities of small uncrewed aerial systems (sUAS) have been firmly demonstrated. These systems pose a growing threat due to their ability to perform surveillance and reconnaissance, kinetic attack and other tasks. Methods to counter sUAS are increasingly important for military forces at all levels, but remain challenging due to the small signature, wide commercial availability and low cost of sUAS. This paper examines the growing threat of sUAS and how they have been employed by state and non-state actors over the past decade in selected conflicts. It also reviews technologies associated with sensing and affecting sUAS as part of the counter-UAS (CUAS) mission, highlighting strengths and weaknesses along with potential countermeasures. The status of counter-sUAS methods in Australian Army operations is also examined. Recommendations for the Australian Army and for agencies across the whole of government include investing in a layered approach for detecting and affecting sUAS, providing training to all Army soldiers around counter-sUAS methods, forming a counter-sUAS centre of excellence and assigning clear roles and responsibilities for countering sUAS on Australian territory. By incorporating these recommendations, the Australian Defence Force (ADF) and other Australian government agencies will be better positioned to counter the rapidly increasing threat posed by sUAS.

Introduction

United States Air Force (USAF) Predator operations in the Balkans during the late 1990s demonstrated that uncrewed aerial systems (UAS) have great utility on the modern battlefield. The MQ-1 Predator was a remotely piloted vehicle that was initially used solely in intelligence, surveillance and reconnaissance (ISR) operations but was equipped from 2001 with Hellfire missiles which allowed it to fly armed hunter-killer missions. Over the next decade, Predator and its successor, the MQ-9 Reaper, became essential tools in a range of US military operations including counterterrorism and counterinsurgency. Indeed this capability would log a total of 2 million combat flight hours by 2013.[1] The public's imagination was captured by full-motion videos of successful strikes carried out and recorded by Predators, and this publicity brought uncrewed aircraft into wider social discourse.

While many people were unfamiliar with UAS prior to the Predator's introduction, the employment of UAS in combat can be traced all the way back to 1849 with Austria's use of uncrewed balloons to deliver explosives against Venice.[2] In terms of powered flight, uncrewed target aircraft and cruise missiles were developed during the First World War[3] and the USAF made significant use of UAS (over 3,500 combat sorties) in reconnaissance missions during the Vietnam War.[4] One important early purpose served by uncrewed aircraft was to act as a drone target as part of training and technology development. For example, Australia's series of Jindivik jet-propelled target planes were first employed in 1952 as part of guided missile tests.[5]

While the military utility of UAS had been proven for decades, before the 21st century these systems were primarily used by militaries in niche missions playing a small role in the overall outcome of any conflict. Because of technological limitations and the demands of the missions being performed, UAS were relatively large until recent times and, as they operated at altitudes similar to crewed aircraft, their radar signatures were similar to those of crewed fighters or bombers.[6] This meant they could be effectively engaged by air defence systems designed to detect and defeat crewed military aircraft.

Advances in technology over the past two decades, including the

availability of space-enabled positioning, navigation and timing services and improvements in communications technology, have made UAS available to a broad range of users in increasingly smaller systems. Consistent with the US Federal Aviation Administration's *Aeronautical Information Manual*, in this paper a sUAS is defined as weighing less than 25 kg.[7] Today, sUAS are commonly available for sale to the public, with many units designed to be operated by hobbyists and casual users. sUAS are also being employed for a variety of commercial purposes including in agriculture, security, delivery and logistics, and inspections of critical infrastructure.[8] Given the wide availability of UAS in the public domain, militaries, insurgents and terrorist groups can also readily access and modify commercial UAS or purchase sUAS designed for military missions. Indeed, recent research shows that while only 60 nations were operating variations on military UAS in 2010, by 2020 that number had increased to 102.[9]

In the contemporary security environment, sUAS are not just an abstract threat. They have already proven to be a potent tool in military theatres of operation, including during the current conflict between Russia and Ukraine, between Hamas and Israel, in Syria, and during the Second Libyan Civil War from 2014 to 2020. At times, UAS operations have had devastating effects on land forces. Should the Australian Army, and the broader ADF, find itself in combat, it must be prepared to counter the threat of sUAS.

While many militaries possess long – and short-range air defence systems, most of these systems were built to defend against larger and faster crewed military systems like fighters, helicopters and bombers. Smaller uncrewed aircraft can be especially challenging to detect, based on their size and, for some systems, their low speed. The result is typically a relatively small signature. Small uncrewed aircraft can also operate at low altitudes and take advantage of terrain and foliage to hide their presence. Existing air defence systems with short-range capabilities have proven effective in downing some sUAS, but many of these systems are on the wrong side of cost imposition. The practice of repeatedly using an air defence missile which costs millions of dollars to shoot down an sUAS which costs thousands of dollars is unsustainable in a long conflict. Because sUAS are especially difficult to counter using systems currently in the Army's inventory, this paper focuses on the need for new capabilities to effectively deal with this proven threat.

Methodology

Based on analysis of open-source literature conducted at the unclassified level, this paper is presented in three parts. First, it provides a succinct review of sUAS technology to help elucidate the threat that such systems potentially pose to military forces. The paper then considers the literature associated with selected military operations involving sUAS and CUAS operations since 2010 and presents key lessons learned. Finally, the paper reviews CUAS technology literature. This part focuses on the 'sense' and 'effect' stages of engaging sUAS and highlights the strengths and weaknesses of selected technologies. The goal of the technology review is not to suggest that the Australian Army, or the ADF more broadly, acquire any specific system. Rather, it helps explain how various technologies and solutions could be implemented as part of an overall CUAS strategy. Following this analysis, the paper discusses CUAS doctrine, training and other considerations needed to systematically embed sUAS defences into Australian Army operations. To inform this aspect of the analysis, a series of semi-structured interviews were conducted with Army leadership to clarify the status of CUAS procedures, training, acquisition and experimentation. The final section of the paper contains a list of observations and recommendations for improving Army CUAS operations.

The research contained in this report was completed in December 2023. Ethical clearance for this project was provided by the Departments of Defence and Veterans Affairs Human Research Ethics Committee.

The Growing Threat from Small Uncrewed Aircraft Systems

The worldwide market for UAS has grown significantly over the past two decades. A recent report estimates that the size of the global market for all UAS is US$30.6 billion and predicts growth to US$55.8 billion by 2030.[10] While hobbyists were a large percentage of the initial users of sUAS, these systems are increasingly being employed to meet a variety of other needs including imaging, delivery, disaster response, security, agriculture and inspection of remote sites.[11] The number of sUAS models commercially available continues to grow, as do their capabilities. Commercial sUAS payload capacity, range, aerodynamic performance, automation, navigation tools and methods of control are continually improving. The capabilities of the Da-Jiang Innovations (DJI) Mavic 3 Pro give a sense of the state of the art for a UAS in its class. It has a 1 kg take-off weight, a maximum range of 28 km, a maximum endurance of 43 minutes and a maximum speed of 75 km/h.[12] This widely available system is equipped with a triple camera system and, in an uncontested conflict environment, would prove quite useful for surveillance and reconnaissance directly out of the box.

The number of nations using purpose-built military sUAS has also grown substantially. As of March 2020, 102 nations possessed military drones, of which 90 owned drones with a maximum take-off weight under 150 kg.[13] While the payload flown on an aircraft may distinguish a military sUAS from a commercial system, the performance of the aircraft itself is relatively consistent for both military and commercial sUAS.

It is important to remember that the overall uncrewed aircraft system consists of more than just the aircraft. For remotely operated UAS to fly safely and effectively, a basic system needs to consist of the aircraft, pilot, control station, sensors that provide situational awareness, and communications links for commanding the aircraft. For a fully autonomous UAS, navigation is a task that can be handled on board the aircraft. Communications are only required to change a predetermined autonomous plan. As this paper considers vulnerabilities of sUAS and their intended missions, the entire system will be examined rather than just the aircraft.

sUAS can be used across a range of missions including communications, electronic attack, cyber operations, and transportation of supplies. However, most reporting around sUAS employed in recent combat operations indicates a focus on two specific tasks: ISR and kinetic attack. Key aspects of these two tasks drive the desired characteristics of the platforms. In the ISR mission, endurance and survivability are key parameters when operating within sensing distance. Vital characteristics for such a mission include the ability to carry and effectively operate sensor payloads and to communicate data back to forces able to interpret that information.

In carrying out kinetic attacks, sUAS must be able to deliver an explosive payload accurately against a designated target (preferably exploiting a vulnerability). To be effective, the sUAS must be able to specify its target and survive to deliver its payload. Some UAS which carry out kinetic attacks may release a weapon and return to base to rearm, much like crewed fighter aircraft. In other missions, the UAS platform is sacrificed when it delivers the kinetic payload. In media reports, these types of UAS have been given a variety of names, including kamikaze drones and loitering munitions, but many of these technologies have been present in smart cruise missiles for decades. For example, the AGM-142E Raptor capability enables its operator to perform terminal guidance with the aid of an electro-optical/infrared (EO/IR) on the weapon. Similarly, the Block IV Tactical Tomahawk can loiter for hours and be retargeted in flight.[14]

There have been rapid recent advances in the degree to which weapons systems are able to operate autonomously. Several smart missiles utilise autonomy as part of terminal engagement, including the US AGM-158 Joint Air-to-Surface Stand-off Missile and German Taurus missiles, which both use imaging infrared seekers and internal algorithms.[15] Such systems can correct for guidance errors or for variations in target location. Other weapon systems rely more heavily on autonomy to find their targets. An example is the Israeli HARPY loitering munition, which can fly to a specified area, orbit for hours in search of specific radar emitters, and then attack autonomously.[16]

When paired with sUAS technology, autonomy has the potential to reduce the need for human operators and the communications links associated with those operations, increase efficiency, and enable whole new tactics. Over the past decade, commercial sUAS systems, such as the DJI Phantom 4, have come to feature advanced image-recognition algorithms to achieve

visual obstacle avoidance and active tracking of subjects.[17] The use of autonomy in this way not only reduces the workload on the pilot of the UAS; it also reduces the UAS's vulnerability to disruption, jamming or spoofing of its command links.

Researchers have suggested various ways to characterise the continuum of autonomy exhibited by different models of UAS. One useful characterisation is described in a 2021 Joint Air Power Competence Centre report, which defines six levels of automation involved with navigation. Level 0 has no automation and requires a human pilot to perform all navigation operations, while level 5 involves full automation with no need for human involvement. As the level of navigation automation increases, the level of pilot involvement decreases, with autonomous systems playing an increasing role in navigation and obstacle avoidance. One could imagine similar levels of automation also applied to UAS mission payloads.[18]

As automation continues to be developed and implemented at higher levels for UAS operations, humans will no longer be required to direct flight on a one-to-one basis. This advance will enable larger scale operations referred to as 'swarming'. The potential of swarming capabilities has been demonstrated by light shows which have included thousands of sUAS flying in close formation to create images in the sky.[19] In a military context, sUAS swarm tactics and operations can be enabled by emerging technology supported by cooperative operations in military missions.

While the concept of using sUAS in swarms can be traced to researchers at RAND Corporation in the late 1990s, the implementation of swarming techniques by sUAS has yet to be widely adopted. It remains, however, a topic of much interest.[20] For example, in a recent paper published on the Australian Army's *Cove* website, the author proposed the use of swarms for electronic warfare and anti-aircraft missions (including CUAS), and as a tool for surveillance and reconnaissance.[21] Significantly, in April 2023 joint demonstrations were conducted under AUKUS Advanced Capabilities Pillar 2 of Australian, UK and US AI-enabled assets working together as a collaborative swarm.[22]

Swarming creates two separate challenges for defenders. The first is that it enables a large number of unmanned aircraft to operate in the same airspace in a coordinated fashion to prevent collisions and fratricide. Mass can be generated to some extent by well-trained UAS pilots, but automated

technology to enable UAS swarms would be more effective. Such swarm tactics can overwhelm a defender's systems, creating significant challenges. Further, a swarm can also leverage the sensors, weapons, communications and autonomy of the entire fleet of UAS deployed to an area. By enabling coordinated tactics, the UAS swarm would be better able to carry out their mission or defeat defensive systems. In short, implementing swarming technologies may enable large numbers of relatively low-cost sUAS that are not very capable individually to work together to accomplish missions that would be far more challenging for larger, more expensive traditional airborne platforms.

A final important trend for sUAS is that the platforms are continuing to decrease in size while maintaining (or even increasing) system capabilities. This is due to a combination of factors including technological advances in batteries, sensors, processing and autonomy. Such trends make it feasible for smaller UAS to carry out missions that might have previously required a larger asset, including reconnaissance, electronic attack or targeting operations.[23] In examining advances associated with the DJI Phantom, researchers observed that, in just two years, a next-generation system was developed with similar performance specifications in a system 35 per cent smaller than the previous version. Such trends of increased capability per size and weight are expected to continue in the near term.[24]

UAS in Recent Combat Operations

sUAS are not just a theoretical concern for military forces—such systems have been employed extensively by both state and non-state actors over the past decade. While fielding a traditional crewed air force can be expensive, in terms of both acquiring equipment and training aircrews, less well-resourced groups and individuals can afford to buy and operate sUAS. In the hands of an innovative adversary, sUAS have proven to be an effective asymmetric weapon. This may explain why the Islamic State in Iraq and the Levant (ISIL) quickly adopted and adapted commercial sUAS technology to fly hundreds of sUAS sorties against US and allied troops across Iraq and Syria in 2016 and 2017. At the peak of their drone operations, in spring of 2017, ISIL was conducting between 60 and 100 drone bombing attacks against anti-ISIL forces in Syria and Iraq per month. According to General Raymond Thomas, Commander of US Special Operations Command during this time, ISIL drones enjoyed 'tactical superiority in the airspace under our conventional air superiority in the form of commercially available drones'. The only available response to the drone threat, according to Thomas, was small arms fire.[25]

The experience of ISIL's innovative employment of UAS provides a useful case study. ISIL first employed sUAS in 2013 for ISR purposes, heavily leveraging commercial off-the-shelf (COTS) technology. There was speculation that one of ISIL's UAS played a key role in supporting the targeting of a particularly well-aimed lethal Katyusha rocket attack against a US Marine base.[26] Subsequently, ISIL operations evolved to include the use of lethal kamikaze drones, first using a booby-trapped styrofoam model plane to kill a pair of Kurdish soldiers who picked up the device from the ground in October 2016.[27] By January 2017, propaganda videos appeared featuring ISIL munitions dropped accurately on targets from uncrewed quadcopters at altitude.[28]

A detailed examination of ISIL's drone program showed that the group required little technical sophistication to craft an effective military capability. Low-cost commercial drones were imported into the operational theatre and could be used immediately for surveillance and reconnaissance. For kinetic attack, COTS systems were modified with a bomb-drop mechanism

consisting of plastic tubes and a release mechanism that was described as something a 'sophisticated high schooler could put together'.[29]

Similar to the US and other anti-ISIL coalition forces, Russia experienced challenges from opposition forces employing sUAS during its operations in the Syrian civil war. Hmeimim air base, used by Russian forces in Syria, was attacked multiple times by sUAS in 2018. One attack led to the death of two Russian soldiers and seven destroyed aircraft. Another attack against that base later in the year utilised 'swarming tactics', with 13 UAS coordinating their flight pattern to penetrate Russian air defences around the base.[30] The scale of this new challenge led a Russian air defence researcher to claim that overcoming the threat from sUAS required a significant shift in thinking and operations, not unlike the response required to counter jet aircraft, which necessitated air defences to advance from anti-aircraft guns to surface-to-air missiles.[31] More recently, several states have achieved significant success employing sUAS against other states on the battlefield. For example, the ongoing conflict associated with Russia's illegal invasion of Ukraine has seen both sides employ uncrewed systems to great effect.

In February 2022, Russian forces streamed into Ukraine across the Russian and Belorussian borders. The early months of the conflict featured the outstanding success of Ukraine's air force employing its tank-killing TB2 UAS. The TB2 is a Turkish-built medium-altitude long-endurance drone, larger and more capable in many ways compared to many of the sUAS systems discussed previously in this paper. In the opening months of the conflict, the TB2 was sent behind Russian front lines to successfully attack several kinds of targets including tanks, artillery, ships, logistical trains, rocket launchers and even air defence systems.[32] The early success of the TB2, documented in videos circulating on social media, led some commentators to call the system Ukraine's 'most valuable player'. Indeed, a few defence analysts went so far as to claim that these kinds of UAS would make armoured vehicles obsolete on battlefields of the future.

Unfortunately for Ukraine, Russia would find ways to nullify TB2 operations over the next four months. The shooting down of a TB2 in March 2022, allowing Russian exploitation of its recovered wreckage, led to a stronger understanding of the system's capabilities and vulnerabilities. The TB2 as designed is relatively slow and an easy target to engage once detected, quite similar to the MQ-1 Predator. Russia was already aware of this weakness and, once it better understood the system's electromagnetic

signatures and communications systems, found the TB2 even easier to detect, jam and engage. Russia also redistributed its air defences to better protect its forces against TB2 attacks.[33] The result of Russia's actions was a nearly complete disappearance of the TB2 from the battlefield. Colonel Valiukh, a commander in Ukraine's Main Intelligence Directorate, reported at a conference in October 2023 'For the TB2, I don't want to use the word useless, but it is hard to find situations where to use them'. The last TB2 mission Valiukh observed prior to this conference was airborne a mere 30 minutes before the US$7 million aircraft was shot down.[34]

With its most valuable player sidelined and ineffective, Ukraine was forced to evolve its operations and find other ways to effectively employ UAS. This initially required Ukraine to focus on leveraging commercial capabilities and low-cost military systems. In response, it acquired and employed COTS Chinese-built quadcopter drones from DJI and Autel.[35] These UAS are relatively easy to operate and thousands of Ukrainian UAS pilots have been trained during the conflict to fly them. One of the preferred systems is DJI's Mavic Pro 3, which costs under AU$7,000 even when fully equipped.[36] It is a system originally built for hobbyists or commercial users, yet is also an ideal tool for military surveillance and reconnaissance in an uncontested environment. A simple modification to the Mavic, implemented by Ukraine, allows it to drop a small explosive from the aircraft. Such explosives are being built in home-grown factories across Ukraine, with some versions including 3-D printed wing kits that improve accuracy.[37]

Another novel application of hobbyist technology by the Ukrainian military involves the use of first-person video (FPV) drones, originally built for racing, in performing kinetic attack. Flying one of these drones takes more skill because they can move at speeds approaching 250 km/h and are piloted using virtual reality goggles. Once mastered, however, the speed proves quite helpful in overcoming kinetic countermeasures and close-in jamming systems. In late 2023, Ukrainian suppliers estimated the military demand for FPV drones at 30,000 per month. The KH-S7, a drone built in Ukraine, was first used in combat in September 2023 and precisely carries a payload of 1 kg against targets at ranges up to 7 km.[38] FPV drones, acting as miniature cruise missiles, have been especially deadly when used against Russian ground forces. Operators estimate their success rate at 50 to 80 per cent per engagement at a cost of less than $1,000 per FPV drone.[39]

Ukrainian forces also have access to loitering munitions such as the US-provided Switchblade. The Switchblade was originally developed for airborne surveillance but was later equipped with a warhead which enables the operator to immediately engage a discovered threat. There are two Switchblade models, the 300 and the 600, which weigh 5.5 pounds and 33 pounds respectively, and both models employ cameras, global positioning system (GPS) navigation and image processing to assist in guidance. The larger model has a warhead built to be effective against armoured vehicles. Reporting indicates the system has object recognition features to assist an operator in finding and tracking targets.

Like Ukraine, Russia has used UAS extensively in the conflict, but it has been slower to adapt and employ COTS UAS. The Orlan-10, a medium-range sUAS (used for reconnaissance, jamming and other missions), has been in the Russian inventory since the early 2010s and has been employed extensively since the beginning of the conflict. It is a system built to military specifications with anti-jam datalinks and a maximum altitude of 5,000 m, which reduces the acoustic and visual signature of the platform. A variety of payloads can be carried on the Orlan-10, including imaging sensors, electronic intelligence sensors and electronic warfare emitters. Overall, the Orlan-10 is quite capable but is relatively expensive at a cost of roughly AU$150,000 per system.[40]

Another critical uncrewed system used by Russia is the Lancet loitering munition, which first appeared in 2019 defence trade shows. The Lancet has a range of 40 to 70 km and a 1 to 3 kg warhead, depending on the variant.[41] The Lancet is typically employed in conjunction with an Orlan-10 as a spotter and has proven to be a 'serious problem' according to a Ukrainian officer in the Zaporizhzhia region.[42] While early versions of the Lancet required operator guidance to a target up to impact, there are indications that a new version of the weapon may allow for autonomous target selection via pattern-matching algorithms. The new version may even allow for multiple Lancets to work together to deconflict targets during cooperative attacks.[43] This kind of system software enabling swarming would be a new military capability if implemented in combat.

Russia has significantly invested in one new UAS capability, the Iranian Shahed-136. The Shahed is a one-way 'kamikaze drone' with a take-off weight of 200 kg, making it larger than the sUAS class. The Shahed-136 would likely have been called a low-technology cruise missile prior to the

UAS revolution. The system has a range of 2,500 km, flies autonomously using satellite-based navigation and travels at 185 km/h carrying a 50 kg warhead.[44] The Shahed-136 has been employed to strike at strategic Ukrainian targets well beyond the front lines of the conflict. It appears that a new Shahed variant has been recently developed with an imaging sensor that improves targeting during terminal engagement.[45] Ukraine's development of the AQ-400 Scythe UAS, built by Terminal Autonomy, was a direct response to Russia fielding the Shahed. The Scythe, which entered service in December 2023, is a long-range kamikaze drone with an ability to carry 42 kg of munitions. It flies autonomously with a range up to 900 km and can use visual positioning techniques to overcome jamming of satellite navigation.[46]

Because of effective use of UAS by both Ukraine and Russia, both sides in the conflict have implemented new measures to counter UAS operations. Ukraine's methods include a variety of technologies; of which some are sovereign solutions while others are imported. One interesting approach involves using drones specifically designed to knock threatening drones out of the sky. These UAS operate by colliding with Russian quadcopter drones in a top-down attack to damage their propellers and bring them to the ground.[47] Several nations, including Australia, the US and other NATO countries, have sent Ukraine traditional air defence systems, such as Patriot and NASAMS, along with several recently developed counter-UAS systems. Some of the systems sent, like those built by DroneShield, are reliant on electronic warfare techniques and jamming for countering UAS. By contrast others, like VAMPIRE, are fitted with cost-effective air defence guns or small guided missiles.[48] The combined impact of these systems has reduced the effect of Russian UAS operations.[49]

Another interesting development for CUAS operations is a smartphone application called ePPO. This app is available to all Ukrainian citizens and was downloaded over 180,000 times in the first three weeks of its release. ePPO allows civilians to report seeing or hearing airborne threats like drones and missiles. The user simply points their phone in the direction of the threat and clicks on the type of system they hear or see. A report, including the phone's GPS location and compass direction, is then sent to the appropriate authorities. ePPO has been especially useful against Russian Shahed-136 drones, which are both noisy and slow, and the app is credited with enabling a Shahed kill.[50]

Electronic warfare has always been a strength of the Russian military and plays a critical role in their CUAS operations. Indeed, a May 2023 Royal United Services Institute (RUSI) report indicates that Russia placed a major electronic warfare system every 10 km along its front line in Ukraine, with a high priority placed on UAS defeat operations. The result of these actions was a loss rate of 10,000 Ukrainian UAVs per month.[51] Russia has also used the DJI AeroScope system and other electronic warfare techniques to determine the pilot location for several sUAS systems. The DJI AeroScope system, originally designed to allow government agencies to monitor drone use in potentially sensitive or prohibited areas, enables Russia to track Ukraine's COTS DJI drones in real time along with the pilot's location. This is accomplished by collection and interpretation of signals between the drone and its controller. This means that Ukrainian crews of these UAS are at risk of attack.[52] Commercial production of the AeroScope system was halted in 2023, likely over concerns about its use in the Ukraine conflict. However, hackers have published how someone might parse the DJI DroneID communications protocol to generate information similar to that gathered by AeroScope.[53] Given Russia's prowess with electronic warfare, it is likely that it has found ways to gather similar information about commercial DJI drones in the absence of AeroScope.

As a response to Russia's CUAS actions, Ukraine has built a sizeable indigenous drone production and modification capability. This has been funded by the Ukrainian government investing US$1 billion to support a new and rapidly growing sovereign Ukrainian UAS industry.[54] Building drones in-country helps mitigate the introduction, in September 2023, of Chinese export controls on Ukraine-bound UAS systems and parts. Ukraine makes changes to COTS drones including modifying radios and electronics to make aircraft more difficult to jam and detect. It also makes software changes that complicate tracking of aircraft and operators (noting, however, that Russian electronic warfare systems and operators have been relatively quick to adapt in response).[55] Just as impressive is the large number of artisanal drone factories that have popped up around Ukraine. While many electronic systems needed for Ukraine's UAS continue to be imported, the bodies of aircraft and other parts are increasingly being manufactured in Ukraine, which allows the nation to better customise these systems based on evolving mission requirements and threats to operations.

Notwithstanding the widespread use of UAS by both Ukraine and Russia, by late December 2023 neither side had achieved a significant increase in UAS autonomy. Some drones, like the Shahed, fly autonomously to their targets using satellite navigation. A subset of these drones, including the latest variants of the Lancet and Shahed, likely employ EO/IR sensors to fine-tune their terminal engagement using technology similar to that which has been employed on numerous smart missiles for decades. Automation could allow for better massing of forces and would negate the effectiveness of jamming techniques affecting the command link between pilots and uncrewed aircraft. The use of automation in Lancet during terminal engagement has already negated certain Ukrainian point defence systems on the battlefield.

Similarly, at the time of writing there had not yet been any deployment of sUAS designed to achieve automated swarming. Instead, to increase an attack's effectiveness, Ukrainian forces have typically coordinated attacks using multiple remotely piloted assets to create simultaneous time on target in order to confound Russian air defences. The employment of multiple operators using coordinated tactics is, however, a quite different method of warfare from employing automation to achieve a 'system of systems' swarm attack.

It should also be recognised that the threat from UAS does not only exist on distant battlefields during wartime. Explosive drones were used in an assassination attempt against Venezuelan President Maduro during a speech delivered in Caracas in 2018. In that incident, two commercial drones each carried and detonated a 1 kg explosive in the attempt against Maduro's life.[56] Drones in flight, even small ones, also pose a significant safety hazard to crewed aircraft. In 2018, for example, a civilian drone triggered a helicopter crash in the United States. Fortunately, the student and instructor pilots both survived. Drone incursions have also closed major airports in at least eight nations, with over AU$100 million in estimated economic losses associated with flight suspensions at Newark, Gatwick and Dubai international airports alone.[57]

Drones have also been suspected of conducting surveillance around numerous sensitive sites. For example, sUAS have been observed flying in sensitive airspace over US Naval Base Kitsap-Bangor (which hosts nuclear-armed submarines) and around nuclear facilities in the UK. In Australia, a drone crashed during an unsuccessful attempt to smuggle drugs and pornography into a Queensland prison.[58] This is just a tiny subset

of examples in which sUAS have either created a dangerous situation or harmed national security in various nations.

The conflicts and other security incidents outlined above offer several lessons that can inform efforts to meet the challenge of countering sUAS. For one, it is evident that a robust and rapidly advancing market for commercial drones has made it possible for unsophisticated users to access the aircraft, use them immediately, or easily adapt them for a variety of nefarious purposes. These systems are particularly accessible because they are designed to be easy to fly, so pilot training does not involve a significant investment. Any military deploying to an area where resistance is expected should be prepared to face threats from sUAS.

Additionally, sUAS are available off the shelf or can be built from parts for prices ranging from as low as hundreds to a few thousands of dollars. Being so cheap, they are highly expendable and so their survivability is of little concern. As a result, the prospect of losing large numbers of sUAS to achieve operational effects against adversary personnel (or against more expensive military equipment) is likely to be a rational and economically advantageous military tactic. Because of their low cost, innovation is occurring around sUAS systems used in combat within time frames that can be measured in weeks and months rather than in years. To counter this level of innovation, a defence force must be capable of responding with CUAS advances within similar time frames.

Methods and Technologies to Counter Uncrewed Aerial Systems

A review of technology and recent international combat operations demonstrates that sUAS pose a significant challenge for military forces. Most modern air defence systems were purpose built to defend against a very different kind of threat: fast-moving crewed fighter aircraft, rotary-wing aircraft and medium – and high-altitude bombers. Smaller UAS are especially challenging to detect because of their size and comparatively low speed. The combination of these factors results in a relatively small signature in many radar bands and in other phenomenology. sUAS are also able to operate at low altitude and can take advantage of terrain and foliage to hide their presence.

While some existing short-range air defence systems can effectively target UAS given the proper geometries, many of these systems are on the wrong side of any cost imposition strategy. For example, a Patriot missile has the capability to shoot down a Shahed-136, yet a Patriot missile costs $4 million dollars and the Shahed-136 costs a mere 1 to 3 per cent of that price. Additionally, the high cost of the detection systems and launchers associated with these kinds of exquisite air defence systems inevitably limits the numbers of such capabilities available to counter sUAS on any battlefield. These are a few of the reasons why alternative CUAS solutions must be explored.

CUAS solutions tend to fall into two distinct categories—active defences, which counter the UAS directly; and passive defences, which reduce the likelihood and impact of UAS operations without needing to engage the UAS itself. Passive defences include a range of measures such as camouflage and concealment, deception, dispersion, displacement and hardening. Both active and passive defences are useful for any unit that encounters sUAS, and both will be explored in this section. It should also be noted that it is possible for commercial UAS manufacturers to code geographic fences which prohibit flight in certain areas or beyond certain altitudes or distances into their software. This is a form of capability denial for commercial systems, but such restrictions can easily be removed via hacking or other techniques (at least for DJI drones).[59]

The US Headquarters, Department of the Army, first published a document detailing techniques to 'deny enemy uncrewed aircraft from accomplishing their mission' as part of the Army Techniques Publication (ATP) series in 2017, with an update released in August 2023. The publication, titled *Counter-Unmanned Aircraft System (C-UAS)*, ATP 3-01.81, is aimed at the brigade level and below. It includes a review of threat UAS, planning measures that can be taken to mitigate the threat, along with offensive and defensive measures available to units in the event that UAS are encountered.[60] Recognising that no single defensive measure is foolproof, ATP 3-01.81 emphasises a layered approach to the CUAS mission and examines both active and passive measures for defence.

Passive UAS Defences

Passive defences in the CUAS mission include methods that avoid detection, avoid targeting, and mitigate the effectiveness of any attacks associated with threat UAS. It should come as no surprise that many passive measures resemble methods that date back to World War I efforts to defend against attacks from the air. Similar methods can still be effective against crewed aircraft, cruise missiles, ballistic missiles and uncrewed aircraft.[61] Passive measures fall into categories that include camouflage, concealment and deception (CCD), dispersing forces, hardening, and providing shelters.

CCD involves making it more difficult for the threat sUAS to detect and identify their target with their sensors. Having a knowledge of the enemy's sUAS capabilities will help focus any CCD efforts. Developing an effective plan for CCD must also account for the environment in which friendly forces will be operating. While distinguishing signatures of land forces from those of an sUAS may be problematic enough in an unpopulated environment, it may be still more challenging in urban environments cluttered by multiple other vehicles, civilians and radiofrequency emitters. Obscurants, such as smoke, or the use of decoy systems can also be useful to disguise the location of high-value vehicles from optical sensors.

Decoys can also dilute the effectiveness of enemy attacks by forcing the opponent to expend weapons on worthless targets and thereby reveal their location. Decoys have been a part of Ukraine's strategy from the outset. For example, Ukraine has fooled Russian UAS and other sensors with wooden

decoys of High Mobility Artillery Rocket System (HIMARS) that have been attacked by Russian forces.[62] Further, inflatable decoys that are easy to move and deploy and that replicate Ukrainian armoured vehicles have been effectively used on the battlefield. Notably, inflatable decoys of Leopard tanks have included components that create heat and radar signatures in order to better represent the multispectral aspects of an operational tank.[63]

Dispersion is another time-proven tactic utilised to increase survivability by moving friendly units apart from one another. This strategy helps reduce their overall signature and makes forces less vulnerable to attack. If an attack is called in on a specific location, dispersion helps to limit the number of friendly assets exposed to fire. Such measures have proven useful against reconnaissance systems that have called massed fires involving unguided or cluster munitions upon discovered troop locations. While effective in this context, it is less clear that dispersion would be a useful response to an adversary's release of large numbers of loitering munitions that individually and autonomously select their own target. For these situations, dispersion could be counterproductive as individual dispersed units may not be able to mount an effective defence against attacks from loitering munitions (due to limits on numbers of CUAS equipment) or from opposing ground forces.[64] While dispersion improves survivability against most types of airborne attack, it can make active CUAS efforts more challenging, due to limits on their area of effects.

Hardening, or the use of shelters, is another measure that can reduce the impact of delivered munitions. Because of their small size, sUAS have a limited ability to deliver a kinetic payload, so hardening can make a significant difference to the targeted assets' survivability. Hardening can include low-technology techniques like adding metal screens to the tops of armoured vehicles, a measure which can reduce the damage caused by sUAS airdropped munitions. Such 'cope cages' have been implemented by Ukrainian, Russian and Israeli forces in recent years, but there has been little reporting on their effectiveness.[65] Hardening at fixed sites could include specialised construction and the use of shelters to protect high-value vehicles.

Active UAS Defences

Active defences against sUAS involve methods to sense, decide and effect as part of the kill chain. These three phases of engagement provide a useful basis upon which to conduct an evaluation of the various technologies available to perform the CUAS mission. As such, these stages will provide the structure for analysis in this part of the paper as it examines the technologies involved in the 'sense' and 'effect' phases of CUAS operations and evaluates the vulnerabilities of specific types of sUAS. The 'decide' phase will be discussed in less detail, recognising that command and control involves a close working relationship between humans and information processing systems. The paper will, however, outline the characteristics needed for a system to perform this phase of the engagement cycle.

The significant threat posed by UAS has driven growth in the global market for CUAS systems. Research shows that, as of March 2021, there were 581 CUAS products on the market, produced by 282 manufacturers with 39 countries of origin.[66] Active defences take advantage of the vulnerabilities of various components of any uncrewed aircraft *system*—the word 'system' is emphasised purposely. For remotely operated UAS, the overall system consists of the operator(s), the control station, the aircraft, communications links and any associated payloads. Autonomous UAS may not require operators, control stations or communications while in flight, but they nevertheless rely upon on-board processing while airborne. In examining methods to counter UAS, understanding the individual components that make up the overall system can help disclose methods that can exploit the capability's most vulnerable components.

To 'sense' sUAS aircraft is quite challenging for a variety of reasons. First, the aircraft itself is relatively small and, as a result, has a small signature as compared to other aircraft, both during flight and on the ground. The aircraft can also fly close to the ground or tree lines to make use of terrain and foliage masking. Other tactics to reduce the signature of the platform include flying upwind towards targets (to minimise acoustic signature), and making use of natural phenomena like the brightness of the sun or cloud cover to mask operations. If the aircraft is remotely operated, it will likely need to communicate some type of position information back to its operator unless it only operates inside line of sight. The platform's on-board sensors may also communicate back to a remote location.

Sensing the sUAS operator and associated control station also tends to be quite difficult as neither needs to be co-located with the aircraft. However, to command an aircraft which is not fully autonomous, an operator will need to communicate with it. Many early commercial sUAS used narrow-band communications which made detection of the control station relatively easy. More recent commercially available systems use spread-spectrum techniques instead to reduce the impact of interference which could disrupt flight operations. This development poses an added challenge to CUAS efforts in that these communication systems are also more difficult to detect than narrow-band systems. New communication options in commercial sUAS are starting to become available, including the use of fifth-generation (5G) cellular networks or wideband commercial satellite communications networks. Because of the large number of users of these networks across applications, identifying sUAS among the massive number of transmitters would prove particularly challenging.[67] Further, purpose-built military sUAS, like the Orlan-10, typically feature hardened radio datalinks, making them more difficult to jam or intercept.[68]

Turning to the 'decide' phase, once a suspected threat sUAS is detected, it may be identified and then a decision must be made about how to act in response to that threat. The identification process might include determining the source of the threat, the specific model, the intent, or other details needed to inform any potential operational engagement. If a decision is made to engage a part of the system (the operator, the control station, communication links and/or the aircraft), an effector must be tasked. At times, such as when an individual soldier sees and engages a small uncrewed aircraft using small arms fire, the sensor, decision-maker and effector are all co-located. At other times, multiple sensors may report back to a single location for fusion and interpretation. In either event, the decision-making process will most likely involve a human or a computer (or some combination of the two) tasked to integrate sensor data, to classify threats and to task/re-task sensors and effectors in order to deal with the threat.

To enhance both the 'sense' and 'decide' phases of the engagement cycle, it is useful for friendly UAS to implement 'identification, friend or foe' (IFF) technology. Such systems involve the use of encrypted transponders on aircraft and interrogation systems to allow a quick determination whether an incoming aircraft is friendly or a potential threat. NATO requires all military aircraft to use IFF Mode 5 capabilities, including UAS. IFF transponders as small as 190 grams have been developed for use on sUAS.[69]

The ‘decide’ phase of the engagement must account for several additional factors. Forces must comply with their operational rules of engagement as well as any specific directives associated with the engagement of sUAS. Any decision to engage an aircraft must also account for other friendly aircraft, both crewed and uncrewed, along with other friendly forces in the area that could be affected by engaging a hostile aircraft. If jamming techniques are used, forces must be careful to avoid self-jamming or other collateral effects affecting friendly forces. Further, decisions must be compatible with any airspace control directives. It should be noted that the use of IFF transponders or similar technology on friendly uncrewed aircraft would simplify the identification process and reduce the workload on any forces dedicated to CUAS.

NATO has selected the ‘Sensing for Asset Protection with Integrated Electronic Networked Technology’ (SAPIENT) protocol to regulate CUAS decision-making. This protocol, originally developed by the UK Ministry of Defence, defines open standards that can be used for fusion of information used in the CUAS mission. SAPIENT was utilised in the September 2023 NATO CUAS Technical Interoperability Exercise to feed information into 12 different command and control applications.[70]

The final phase of the engagement cycle, the ‘effect’ phase, involves methods to defeat the sUAS itself or the overall military capability provided by its payload. A range of effectors is possible including kinetic and non-kinetic solutions that could leverage directed energy, jamming or spoofing techniques, anti-aircraft artillery, missiles, entangling nets or friendly sUAS built to collide with and damage other UAS. It is important to consider both the effectiveness of these systems and their potential to cause collateral effects.

Sensor Technologies

This section will examine various technologies for sensing sUAS. Each technology examined will be described along with its utility in detecting various types of sUAS. While such sensing technology has considerable military utility, it is worth remembering that humans have some unaided ability to detect sUAS via visual and acoustic means. Relevantly, researchers from the University of Defence in the Czech Republic ran a series of experiments at a military training area to determine the visibility and audibility of a DJI Phantom 2 Vision aircraft. Under ideal conditions, a human could

visually detect the Phantom aircraft against a specific section of blue sky out to 700 m. Against more challenging backgrounds, 500 m is a realistic maximum range for detection by the human eye. Audibility was strongly correlated with the altitude of the aircraft and whether it was climbing (i.e. the engine output was higher). Under ideal conditions, the acoustic signature could be detected by a human out to 700 m maximum range when above 50 m altitude. Inevitably, increased background noise and lower altitude flight operations degraded that level of performance.[71]

Acoustic

Acoustic UAS detection systems employ microphones to listen for UAS noises, typically from aircraft propulsion systems. The engine and propellers of the small aircraft generate sounds which are typically in the range of 20 to 20,000 Hz. Different models of sUAS generate specific acoustic signatures across the frequency spectrum which, when compared to a precompiled library of acoustic signatures, may allow the UAS model to be identified. Acoustic sensors are passive, meaning that they do not emit signals that disclose their presence. Additionally, an array of microphones with processing capability can utilise time difference of arrival techniques to determine an aircraft's location to GPS-level accuracy.[72]

Detection range is limited as sound pressure attenuates with the inverse square law. That is, sound pressure reduces by 6 decibels with every doubling of distance to the source. The reported effective range of acoustic systems varies quite substantially in the scientific literature, anywhere from 5 m to 600 m. One advantage of acoustic detection over other methods is that it does not necessarily require line of sight between the sensor and the aircraft. Acoustic methods for sUAS detection are not, however, effective in high-noise environments (such as commercial airports) and are quite susceptible to disruption by weather (such as rain and wind). Recognising these limitations, researchers recommend the use of acoustic sensors in conjunction with other sensors for detection and identification.[73]

Noise reduction features, like improved propeller shapes and quieter engines, are relatively easy to implement on sUAS. In addition, there is demand from commercial users to reduce the noise associated with sUAS. Needless to say, sUAS operators taking videos of events or of nature prefer not to disrupt the environment in which they are filming.[74] The combination

of a small detection range and the disruptive effects of weather and external noise, as well as expected technological improvements to reduce sUAS aircraft acoustic signatures, will continue to limit the utility and effectiveness of acoustic detection systems.

Electro-optical and Infrared

EO and IR sensors primarily work in the visual or infrared frequency ranges, with infrared typically divided into short-wave (1.0 to 3.0 μm), mid-wave (3.0 to 5.0 μm) and long-wave (8.0 to 14.0 μm). EO and IR sensors are passive and do not typically rely on illumination for effective operation (although EO sensors are far less effective during hours of darkness). Under amenable conditions and with appropriate magnification, imaging sensors can detect, identify and track targets. Visual images may also prove useful for forensic applications in the aftermath of an encounter with an sUAS.

In contrast to imaging sensors, non-imaging systems tend to have a larger field of regard, but they do not provide information about the shape or type of target. As a result, non-imaging systems are typically used for detection and tracking. An example of a non-imaging sensor is the IR search and track (IRST) sensor present in some fighter aircraft that allows quick detection and tracking of potential aircraft threats at distance.[75]

Advanced computer vision technologies can be used in conjunction with EO/IR sensors to detect, track and identify drones, as well as to estimate distance from the sensor to the threat.[76] When training these algorithms, it is important to include likely 'confusers' (such as birds) in the training data. Computer vision techniques could likely make use of arrays of EO/IR sensors to improve distance estimates. However, it remains challenging to detect and identify uncrewed aircraft mixed with clutter (such as weather, dust or birds) or in front of a cluttered background. Challenging backgrounds might include trees, other kinds of vegetation, or buildings in an urban environment.[77] EO and IR sensors are also affected by adverse weather, such as rain, snow or fog, and there is a remarkable reduction in their detection range in the worst environmental conditions.

It is difficult to make broad, sweeping statements about the range and performance of EO/IR sensor systems as performance can depend on the quality and resolution of the sensor, along with the optics used by the system. Nevertheless, it is safe to say that one should prefer a sensor with more

pixels and higher sensitivity despite its higher cost. For a fixed sensor array, resolution is generally improved by reducing the sensor field of view via the choice of optics. In practice, this means that high-resolution EO/IR imaging sensors, which are able to detect and identify sUAS at distance, have a relatively small field of view and often need to be cued by other systems.[78]

The output of a representative EO/IR system can be seen in a YouTube video documenting range testing of Aaronia's AARTOS long-range EO/IR sensor for CUAS.[79] The video shows a small commercial drone being detected, and tracked, out to 1,000 m range using both a visual and a thermal camera in good weather conditions. Using the visual camera, the aircraft can be identified by a trained observer at a range out to 100 to 200 m based on the resolution observed. The thermal camera provides better tracking at longer ranges, and tracks out to 1,000 m. Aaronia also offers a higher performance Ultra Long Range Thermal / Optical Tracking System for CUAS with a listed maximum tracking range of 8 km, although the field of view at this range is not provided.[80] Applying the Johnson criteria, this corresponds to identification at a maximum range of approximately 1.5 km.[81]

Non-imaging IR sensors can detect and track, but not identify targets. IRSTs in fighters can detect other fighter aircraft at long range because the target is much hotter than the background sky. Most sensors in this class use mid-wave and long-wave IR bands to detect heat coming from sUAS batteries or engines. Such sensors can be quite sensitive. In clear conditions with a warm sky, theoretical calculations show that a typical sUAS (a Sky Viper was used in the example considered here) could be detected and tracked out to 6.9 km using a non-imaging long-wave IR sensor with a 30-degree field of view. The IRST would also be able to detect and track sUAS against a more challenging background of dense foliage out to 4 km.[82]

Overall, higher end EO/IR systems can provide detection of sUAS out to roughly 8 km as well as the capability to provide high-quality identification of sUAS out to an approximate maximum range of 1.5 km. Thanks to their large field of view, non-imaging sensors seem particularly well suited to detection outside urban environments. By contrast, due to their relatively small field of view, imaging sensors may be most useful for identifying threats when cued to a given area by other sensors. EO/IR sensors can also play a role in characterising new sUAS threats relatively quickly, because images can help indicate to an analyst monitoring the feed whether the aircraft is carrying an explosive or other types of payloads. EO/IR sensors are also

able to handle multiple targets and the sensor's capability is unaffected by aircraft autonomy. EO/IR sensors will, however, be affected by poor weather conditions like rain or fog, and EO sensors will be most effective during daylight hours.

One potential drawback of EO/IR detection methods is that, to detect an aircraft, the sensor needs an unobstructed line of sight. A smart sUAS operator could therefore avoid detection by making use of terrain and conducting a low-altitude flight into the target area. Additionally, the maximum detection range could be reduced by decreasing the signatures in both the EO and IR frequency bands. This is a technique that has been applied to larger aircraft and could equally be applied to sUAS.[83] A UAS design that employed more efficient battery and engine technology, for example, would likely run cooler and would also likely have a lower IR signature.

Radar/LADAR

Radar is the predominant tool used for detecting and tracking traditional commercial and military aircraft. Most radars are active sensors which emit electromagnetic waves and detect an object by receiving the waves reflected off the target. Passive radars, which make use of emissions from other transmitters, also exist but they lack the performance needed to replace active radars.[84] Modern integrated air defence systems typically use a variety of radars for different purposes, with some radars specialising in early warning / wide-area surveillance while others are used for focused tracking of threats and target engagement. Due to the Doppler frequency shift and other characteristics of a radar return signal, radar processing can capture information about an aircraft's radar signature, its speed, and the distance to it.

The size of the return from an illuminated target at a given range will vary by frequency, viewing angle, environmental conditions and other factors. The metric describing target return is typically called the radar cross-section (RCS) which is often measured in square metres. Some examples of RCS values at microwave frequencies for non-stealthy aircraft are 0.01 m^2 for a bird, 1 m^2 for a small, single-engine aircraft, 6 m^2 for a large non-stealthy fighter and 100 m^2 for a jumbo jet.[85]

Researchers from the University of Defence in the Czech Republic performed several experiments on a DJI Phantom 2 Vision to measure various signatures of the aircraft. In X-band, a radar band of 8 to 12 GHz (commonly used for air traffic control around an airport or for military fire control), the RCS of the Phantom 2 Vision was between 0.03 and 0.1 m^2.[86] This size of signature tends to be difficult to detect for many existing X-band radars, especially in an operational environment contaminated by environmental clutter. Tuning a radar to detect a target of this size will likely result in an unacceptably high false alarm rate.

Most military radars tend to have system characteristics which are optimised for a threat larger and faster than most sUAS.[87] For this reason, higher frequency radars are often proposed for sUAS detection, with Ku and Ka band (at frequencies of 12-18 GHz and 26.5-40 GHz respectively) being especially attractive.[88] The disadvantage of moving to such higher frequencies is that atmospheric attenuation increases, especially when it is raining, which reduces the maximum range of the system.[89] Reported effective ranges for radar systems against commercial sUAS tend to vary in the literature, as theoretical maximum ranges may result in unacceptably high false alarm rates when implemented in real-world conditions. Nevertheless, commonly reported numbers range from 2 to 8 km in ideal conditions, assuming the radar has line of sight to the target.

One potential way to decrease false alarm rates would be to employ a method that helps distinguish sUAS targets from noise-based false alarms or confusers (like birds). Uncrewed aircraft that employ rotors for propulsion generate a micro-Doppler signature which can be used to help detect and classify the target.[90] Additionally, each type of system will have its own micro-Doppler signature. Radar systems with the ability to capture this signature have the potential to more consistently reject false targets and might even be able to use specific signatures to detect desired targets.

Because of the large number of design parameters associated with any given radar (frequency, power, field of regard, revisit rate, etc.) it is challenging to make sweeping generalisations about expected performance. One drawback of a radar is that it is an active system which is at risk of being detected by an adversary when operating. A second downside of radar systems is that flight tactics which utilise terrain masking will continue to be effective. Additionally, sUAS could be designed, like crewed aircraft, to include counter-radar jamming systems and radar-reducing stealth designs

that would make them even harder to detect. Such actions would increase the cost of the aircraft and would be technically challenging to build and integrate, thus limiting this specific concern to sophisticated adversaries. Despite these limitations, radars nevertheless continue to improve, as do signal processing techniques associated with capturing information. Radars, which are not reliant on aircraft emissions, also have the benefit of being applicable against autonomous aircraft.

A laser detection and ranging (LADAR) system is like a radar but uses laser light to illuminate its target. Much like the EO/IR systems discussed previously, such systems are severely impacted by rain and fog. Indeed, recent experiments show that LADAR systems cannot achieve high success rates against sUAS aircraft beyond a maximum range of 30 m.[91] While such ranges are unlikely to be of much utility in support of contemporary CUAS missions, improvements are expected over time with the development of better laser and processing technologies.

Radiofrequency Detection

The communication signals between the aircraft and its control station are a key exploitable vulnerability of many remotely operated sUAS. Radiofrequency (RF) detectors operate by capturing these signals in a passive manner to detect and, potentially, geolocate uncrewed aircraft and/or their associated control station. Once collected, the emissions can be analysed using techniques known as 'bearing of arrival' or 'time/frequency difference of arrival' (if multiple sensors are installed) to locate the emitter with reasonable accuracy (potentially under 100 m).[92] If the only possible emitter in the region were to be an sUAS, detection would be straightforward. However, in a conflict zone or within a populated region the RF environment tends to be active and contested.

The difficulty in distinguishing the RF of an sUAS from the latent environment means that RF detectors need to be well informed about the communications frequencies and protocols used by specific sUAS. For this reason, most RF detectors (much like most electronic warfare systems) use libraries of known signatures to aid in detection and identification of UAS. The process of detection involves scanning specific frequencies and modulations and matching those emissions in the target area with known threats. Allowing the RF detection system to search beyond known UAS emitters risks high false alarm rates. Equally, an sUAS operating at new

frequencies or with new protocols may not be detected if its signature is not already resident within the threat library. To maintain the effectiveness of RF detectors, the library of known UAS communications must be continually updated with new threat information as and when it becomes available.[93]

Efforts to exploit aircraft communication systems face an emerging challenge. Specifically, commercial sUAS are evolving to leverage wi-fi, cellular, or even satellite networks. This development will make it increasingly difficult to pick out the UAS communications from the large number of other systems operating with similar frequencies and protocols. In such cases, the RF detection may need to gain access to the data in transmissions to help achieve identification.[94] Another option would be to narrow the search for emitters to specific areas where the sUAS threat is expected to be present.

Some systems have been built to exploit the data from transmission of specific sUAS, including the now discontinued DJI AeroScope system discussed previously in the context of Russia's illegal invasion of Ukraine. That system operates by collecting the information present in communications between specific DJI sUAS ground stations and aircraft. Someone in possession of one of these systems, or utilising the information collected by hackers about DJI communications protocols, would be able to collect sUAS self-reporting about the GPS-identified location of the aircraft and ground station.[95] Given GPS coordinates, it would therefore be quite easy to attack the ground station with artillery or other precision strike capabilities. Additionally, it might also be possible to intercept and exploit datalinks from the sensor payload on the aircraft (like full-motion video) that would assist in determining the aircraft's location.

It is difficult to generalise maximum ranges for the effectiveness of RF detection, as much of the performance will depend on the power and characteristics of the signals being emitted by the aircraft and the control station. There are, however, several providers offering CUAS systems that use RF detection. A brief review of their specifications suggests detection ranges of 5 to 10 km (with the disclaimer that results are dependent on the sUAS threat system). This performance seems reasonable given that, in ideal conditions, sUAS systems like the DJI Mavic 3 Pro can be controlled and can transmit video to a ground station up to 15 km away. It is notable, however, that this maximum control distance would drop to 1.5 to 3 km in an urban environment or in other locations where strong interference is expected from other RF emitters.[96]

One obvious counter to RF detection is to build autonomy into the aircraft so it is not required to communicate with its ground station. Depending on the mission to be carried out, achieving such autonomy would likely involve the use of satellite navigation for guidance, among other measures. Flying a fixed route while collecting imagery would be an easy task for an autonomous system, whereas finding specific vehicles on a battlefield to strike would be more challenging. Despite such limitations, the use of autonomy could open new vulnerabilities that could be exploited by CUAS capabilities.

Another method of countering RF detection systems is to use frequencies and protocols that are not in the library of the detection system or that resemble non-threatening systems. To stay ahead of the RF detection system's threat library, an adversary would need to regularly invest in software (and potentially hardware) upgrades. Another way to deceive and potentially overwhelm RF sensors would be through the use of RF-emitting decoys. To reduce their RF signature, sUAS systems could also utilise low probability of detection communications waveforms and directional phased array antennas to reduce emissions in those directions assessed by an adversary as likely to result in detection.

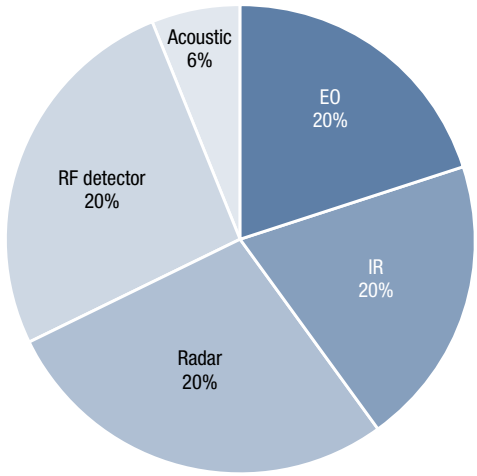
In summary, RF detection techniques are extremely well suited to defeating remotely piloted sUAS, and they effectively support the targeting and identification of both the aircraft and the control station (along with the pilot of the sUAS). The technique, however, has some limitations. Specifically, while this detection method works at a comparatively long range, it is only effective if the threat library is regularly updated. Further, while RF detection systems have an identification capability, they may not be effective against autonomous UAS.

Summary of Sensor Technologies

It is difficult to suggest any single type of sensor which would be preferred over others for detecting sUAS aircraft. All solutions have advantages and disadvantages, and the various sensors tend to complement one another. For example, radars are capable of accurate detection by scanning broad areas at distance, whereas optical systems have a narrower field of view that, if cued, can examine a specific part of the sky to identify and collect forensic information. This complementarity of capabilities is why many CUAS systems on the market use multiple sensors.

A 2020 review of 545 commercial CUAS products that are capable of detecting and/or affecting UAS shows that roughly half of the UAS detectors used more than one type of sensor, with 12 per cent of systems employing four or more sensors. Figure 1 shows the breakdown of sensor phenomenology used by these detection systems. It is notable that acoustic sensors tend to be used far less often than the other options.[97]

Figure 1—Sensor types employed by detection systems[98]



Effector Technologies

Once an sUAS is detected and a decision is made to engage, options to disable or destroy the system will be needed. In the next section, this paper focuses primarily on affecting the aircraft and its communications links. This approach recognises that, if the control station is located, it will be vulnerable to attack just like any other ground target. A variety of targeting methods will be evaluated here, along with a description of their strengths and weaknesses.

Kinetic Options

Air defence systems built to engage traditional military targets (like helicopters and fighter aircraft) typically use missiles or artillery. Some weapons in this class can be operationally effective against sUAS but tend to be quite expensive. According to US General David Perkins when he relayed the story of an ally's actions to a 2017 military symposium, 'That

quadcopter that cost 200 bucks from Amazon.com did not stand a chance against a Patriot'.[99] Economically, however, trading $3 million missiles against $200 drones is not a sustainable strategy.

Artillery, cannons and machine guns have been modified to more effectively target uncrewed aircraft in the air, and some manufacturers are pursuing low-cost guided missiles designed specifically to engage sUAS. The Raytheon Coyote is one example of a tube-launched missile that uses a seeker and warhead to intercept drones. It was successful in downing drones that attacked a US base in Syria in January 2023.[100] At a reported US$100,000 per missile, the Raytheon Coyote is an order of magnitude less expensive than a Patriot missile, but it is still very expensive compared to the threat.[101] The US also successfully employed the Centurion counter rocket, artillery and mortar (C-RAM) system to down uncrewed systems at an air base in Iraq in 2022. That system is a land-based version of the Phalanx close-in weapon system used by the US Navy and others, with a cost per engagement of around US$8,000.[102]

While missiles and artillery fire can be extremely effective at destroying drones, it would be challenging to use these weapons outside a combat zone due to the high potential for collateral damage. Even in a combat zone, arcs of fire and airspace control would need to be coordinated to avoid potential friendly incidents on the ground or in the air when engaging sUAS with missiles and artillery. Further, these kinds of weapons usually focus on destroying a single aircraft, which could limit their utility against future swarms of UAS. Deep magazines, quick engagements, and warheads that provide area effects may help improve performance against swarms of drones.

Other kinetic options designed specifically to target sUAS include entangling nets. These could be fired into the air or carried into the sky by friendly UAS. Alternatively, kinetic responses could constitute airborne assets designed to collide with a threat UAS and damage its ability to fly. For example, UAS have been designed and employed by Ukraine to perform a top-down collision attack.[103] Interestingly, birds of prey have been employed in the Netherlands to capture threatening uncrewed aircraft from the sky and return them to the bird's trainer.[104]

Jamming, Spoofing and Hacking Techniques

Jamming is a widely used effector against sUAS targets. A jammer operates by transmitting RF signals towards the aircraft that interrupt transmissions to or from it (and it is also feasible to carry out jamming operations against the control station if its location is known). When an uncrewed aircraft loses contact with its control station, it is typically programmed to respond in one of four ways: hovering in place, landing in place, returning home to its launch location, or travelling to a pre-specified landing area. However, some aircraft fall out of the sky or fly erratically when jammed. Medium-power jamming systems are reported to operate out to ranges of a few kilometres; however, the power of the jammer and the hardness of the sUAS communications play a large role in determining the maximum range.[105]

'Control link jamming' targets the communication signals between the control station and the uncrewed aircraft. This method is effective against threats with a remote operator but will not necessarily defeat autonomous sUAS. Several control jamming methods have been proposed and employed by many defence manufacturers and militaries. One is to broadcast noise over an entire portion of the frequency band that could be employed by threat sUAS. This technique requires some knowledge of the frequency bands being used by sUAS, but does not require information about specific frequencies. By lowering the signal-to-noise ratio at the receiver, this method introduces errors into the communications and, if the noise is strong enough, the aircraft will drop its link with its control station. A second, more targeted, form of control link jamming involves jamming only specific frequencies being used by the sUAS. This technique has the potential to deliver more jamming power. A third approach is to use 'sweep jamming', which involves stepping noise transmissions through a library of narrow frequencies used by all potential threat systems. This approach does not necessarily require identification of a specific sUAS system during an encounter, but it does depend on the frequency of all potential threat systems being stored in the library and it inevitably takes time to sweep through the large quantity of frequencies held in this repository.[106]

Several other advanced 'smart jamming' techniques can also be employed against the control link. Although beyond the scope of this paper, these techniques allow for more effective and focused attacks against threat systems using spread-spectrum communications techniques, as well as other methods to mitigate jamming that will be discussed later. The effective

employment of smart jamming requires either exploitation of a captured threat system or detailed forensic analysis of communications signals between the control station and the aircraft to discover weaknesses to attack.[107]

As an alternative to jamming or spoofing an aircraft's control frequencies, satellite navigation signals may be targeted instead. This approach can be useful against autonomous aircraft that rely on satellite signals for guidance, although most UAS have an inertial navigation system that could enable an autonomous aircraft to continue its mission for some length of time. Satellite navigation jamming of commercial sUAS typically results in vehicle drift and makes it impossible for the aircraft to return to its launch site. By actively generating a signal that spoofs satellite navigation coordinates to control the aircraft's perceived location, it may even be possible to cause the aircraft to land at a position selected by the spoofer.[108]

Another jamming technique involves transmitting signals that take control of the aircraft itself. This technique requires detailed knowledge of the communications link used by the drone along with the protocol used to control it, or administrator-level access to its processor. One method that has been effectively used to take control of commercial sUAS involves replay attacks that repeat recent command signals via broadcasts to the aircraft.[109] There are also other exquisite jamming methods that are highly system dependent. These include the use of ultrasound signals to disrupt miniaturised gyroscopes and accelerometers, causing the sUAS aircraft to land.[110]

A drawback of jamming is that it can have unintended collateral effects by interfering with friendly or civilian communications, especially if carried out over a wide range of frequencies and for long periods of time. Jamming or spoofing of satellite navigation signals could also result in the failure of friendly or other nearby systems reliant on those services. Directional jamming can reduce collateral effects but will not totally eliminate the possibility of unintended consequences.

Countermeasures to jamming and spoofing of the command link include communications systems that employ frequency hopping or spread-spectrum techniques. Frequency hopping involves rapidly jumping between various frequencies known to the transmitter and the receiver to overcome jamming on any single frequency. Spread-spectrum techniques involve spreading a signal across a wider frequency band in order in reduce detectability and increase the resistance to jamming. To stay ahead of the

adversary when employing sUAS, agility may be required in the employment of frequencies and protocols. For example, the conflict in Ukraine has involved a continual move/countermove process between the command links employed by Ukraine's sUAS and the Russian electronic warfare systems performing CUAS missions.

Directed Energy—High-Energy Lasers and High-Power Microwaves

Directed energy effectors show promise for the CUAS mission due to their effectiveness, ability to act quickly, relatively small logistical requirements and low cost per shot once fielded. Importantly, lasers and high-power microwaves (the two major types of systems in this class) have the potential to minimise collateral damage associated with UAS engagements. In the US, directed energy weapons have been the subject of continual research and billions of dollars of investment since the 1960s. Nevertheless, it took until 2014 before the US was in a position to field its first operational weapon of this type, when a prototype 30 kW laser was installed on the US Navy amphibious vessel USS *Ponce*.[111] Since that time, there has been significant progress in directed energy weapons, making them potentially suitable for the CUAS mission.

High-energy lasers have many benefits, the first of which is fast and precise engagements. Assuming it has an unobstructed line of sight, the light from a laser will reach its target at the speed of light (albeit that it usually takes time to transmit enough power from a beam onto a target area to cause damage). Most laser weapons are built to maintain a beam on target even if the aircraft manoeuvres, and this feature allows for precision engagement. Additionally, by reducing the power or firing time, a laser might be able to dazzle the imaging sensor on an uncrewed aircraft, resulting in a mission kill rather than destroying it. The effectiveness of lasers can, however, be negatively affected by poor weather and obscurants in the air, like smoke or dust. Further, some laser wavelengths are attenuated by water vapour, which leads to degraded performance in humid environments.

A high-energy laser is extremely precise against targets in its immediate area and can confidently illuminate a target. However, a target disabled by a laser falls from the sky in an unpredictable fashion, resulting in the potential for unintended collateral damage. In addition to considering such risks, concepts of operations for high-energy lasers must also consider

their potential collateral effect on distant sensors (for example, on aircraft sensors in the area) as well as the risk posed to humans exposed to a laser's specular reflection from the target while it is engaged. Temporary or permanent damage to the human eye associated with scattered laser energy is a significant concern, and the kinds of modelling required to estimate the potential for collateral damage are very different for lasers than for more conventional weapons like missiles or artillery.[112]

The effective range of a high-energy laser will be strongly dependent on its power, system design and dwell time on target, and on the environmental conditions and the hardness of the target. Nevertheless, a 10 kW laser, tested from the back of a military dune buggy, has been proven to have an effective range of 3 km against sUAS in ideal conditions.[113] The cost per shot of these systems is relatively small. For example, Israel's Iron Beam, a laser-based system designed to shoot down uncrewed aircraft, reportedly costs $3.50 per shot to operate.[114]

Along with lasers, high-powered microwave weapons are the second category of directed energy effectors. They can be delivered by RF-generating equipment (from a fixed site or a mobile vehicle) or from single-use, specially designed explosive systems. The effects achieved by microwave weapons can be delivered close to the threat, using a fired explosive round, a missile or a UAS.[115]

High-powered microwave weapons produce electromagnetic interference or damage by releasing large amounts of energy and they are usually intended to disrupt or destroy electronics. The currents generated by high-powered microwave CUAS systems have an effective range against uncrewed aircraft of a few hundred metres and are unaffected by environmental conditions.[116] High-powered microwaves can be either narrow-band (if the power is focused around a single frequency) or wideband (which involves short pulses of intense energy spread across a band of frequencies).[117] While these weapons are directional, they are less precise than lasers. Specifically, while the beamwidth from a high-energy laser at a distance of 1 km would be millimetres in size, a high-powered microwave system would have a beamwidth of roughly 100 m.[118]

Unlike laser weapons, which attack a single target at a time, high-powered microwave weapons are well suited to delivering effects against multiple targets. This characteristic makes them useful against sUAS swarms if

aircraft are gathered closely. As is the case with laser weapons, however, the use of high-powered microwaves entails a risk of unintended consequences, particularly to electronics in the area. And because of beam dispersion, the area of potential collateral effect will be larger than for a high-energy laser, although collateral effects will be limited to much shorter ranges. Further, while the high-powered microwaves that are likely to be fielded in battle are non-lethal to humans, few academic articles address the medical implications of human exposure to these RF weapons.[119]

Countermeasures are available against both laser and high-powered microwave weapons. In the case of lasers, these measures include the use of smoke or other obscurants, or hardening a target vehicle against laser threats. Hardening may involve using materials that better reflect energy in the frequency of the laser (which will typically slow, rather than halt, the laser's effects). Another countermeasure involves overwhelming the laser system with large numbers of UAS. This technique succeeds because lasers eventually need cooling and/or recharge time between shots. High-powered microwaves can be countered using hardened UAS electronics and smart aircraft design, such as shielding that keeps pulse energy from entering the aircraft.[120] Similar techniques are used to harden nuclear-capable manned aircraft, like the B-52H bomber.[121] Such changes typically add to the size, weight and cost of the aircraft, however, making them less useful for asymmetric attack.

Summary of Effector Technologies

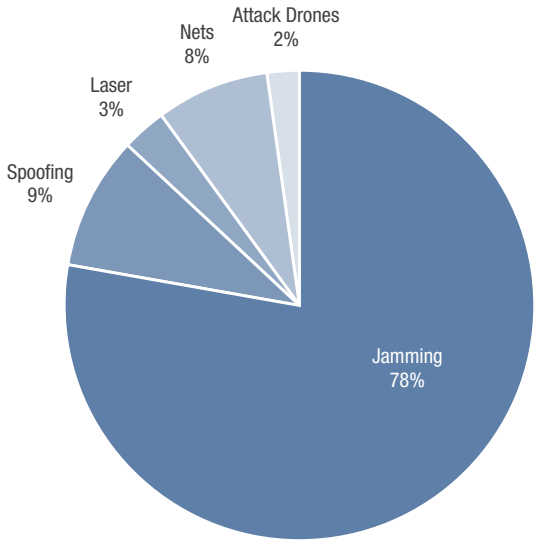
A 2020 review of commercial CUAS products with effectors shows that roughly 40 per cent of the systems use a single mitigation technique, with the remaining products using multiple techniques. Figure 2 shows a breakdown of effector phenomenology used. The predominant methods are jamming either of the command link or of the satellite navigation signals.[122] Some of the jamming systems available are portable and directional (like the DroneGun systems produced by DroneShield), whereas others are fixed and/or omni-directional.[123] The remaining systems marketed specifically for CUAS involve other methods, with spoofing attacks and entangling nets being most used.

No single effector is guaranteed to bring down every threatening sUAS, so a layered approach using multiple types of effectors is preferred for defence

in high-threat environments. In all situations, selecting the most suitable type of effector will likely depend on the nature of the operating environment and the likelihood of collateral effects. For example, using cost-effective missiles to down sUAS via kinetic means may be acceptable in a remote location during wartime but might not be feasible for force protection during peacekeeping in an urban environment. As another example, deploying high-powered microwaves to defend an airfield against sUAS could result in collateral damage to air traffic control systems or the systems of passenger aircraft operating out of the field.

Fundamental differences in the vulnerabilities of different kinds of UAS, along with the variety of environments in which CUAS effectors might be employed, suggest that it would be worthwhile for the Department of Defence and others to invest in a variety of effector technologies (if funding allows). In the near term, jamming is an effective solution against many commercial sUAS systems that might be employed by less sophisticated actors. The collateral effects of jamming, if targeted in a focused manner, can also be appropriately mitigated.

Figure 2—Effector types employed by sUAS engagement systems[124]



Integrating CUAS Thinking and Operations into the Australian Army

The Australian Army faces a significant challenge in responding to the threat posed by sUAS. The low cost and wide availability of these systems makes it feasible for an adversary to use them to threaten forces at all levels, including dismounted infantry and lightly armoured vehicles. Tanks and other vehicles may also prove vulnerable to the kinds of top-down attack that sUAS can deliver. Because of their effectiveness and the challenges entailed in defeating these threats, in recent conflicts sUAS attacks have become ubiquitous across many battlefields. For example, the conflict in Ukraine has witnessed a continual process of 'move' and 'countermove' between Ukraine's drones and the detection and jamming countermeasures brought to bear by Russian electronic warfare systems.

Unlike air defence against fighters and bombers, defences against sUAS threats cannot remain at the theatre level. Solutions need to be distributed to units at the tactical level. To make this happen, tactical-level units need to understand the sUAS threat as well as the various methods available to counter the threat in order for them to continue to operate effectively. This means that procedures are needed across the force to institutionalise CUAS capabilities. Simply put, the sUAS threat cannot be a concern only for air defence units. All units, at home or deployed, may find themselves targeted by sUAS and therefore need to understand methods to mitigate and/or defeat the threat.

Interviews with Army leadership conducted in preparation of this paper indicate that some specific units have developed CUAS tactics customised to their individual situations, but no systematic approach exists across the Army.[125] Rather than relying on initiatives at unit level, the Army needs to develop a systematic force-wide approach to countering sUAS. Moreover, this approach should not just focus on destroying or disabling uncrewed aircraft. Instead, its primary focus should be on keeping the sUAS from accomplishing its intended mission. sUAS missions might include the spectrum of surveillance and reconnaissance (optical or electronic), kinetic attack, communications relay and cyber operations, along with a range of other missions.

Because of their low cost and ease of replacement, destroying large numbers of small uncrewed aircraft may not totally mitigate the threat. While attrition is a proven tactic for engaging crewed aircraft, replacement of sUAS can occur much more quickly than replacement of larger aircraft with crew. This is why Ukraine's sUAS operations can continue unabated, even with a loss rate of 10,000 aircraft a month.

Countering sUAS should be viewed through the same lens as countering terrorist tactics—because all forces could be exposed to the threat, all forces must know how to react. While destruction of an sUAS aircraft may be a desirable outcome in many situations, jamming the sensor feed from an sUAS performing a targeting mission may prove just as effective. This is why strategies that defeat the sUAS mission may be preferred over tactics focused on destroying individual aircraft.

Having good intelligence about adversary sUAS capabilities prior to the conflict (including knowing which specific systems might be employed) will make future operations against those forces far more effective. If the adversary is known to have the capacity to utilise commercial sUAS, it would be prudent to possess (well ahead of any potential conflict) a database of the characteristics, communications methods (datalink frequencies, protocols and data formats) and vulnerabilities of assets available on retailers' shelves. Such a process could be ongoing during peacetime and would assist in growing the skills needed to quickly exploit and discover vulnerabilities of modified commercial or military-specific sUAS in times of conflict. Because of the nature of those systems, they might only become available for exploitation after being shot down over friendly territory in conflict. Being able to act quickly to discover vulnerabilities associated with new threat UAS could save lives.

In writing tactics and doctrine around CUAS, guidance should be provided about how to organise and employ methods to conduct the CUAS mission. ATP 3-01.81 *Counter-Unmanned Aircraft System (C-UAS)* provides a useful reference and could serve as a starting point for the Australian Army.[126] This document provides a brief overview of threat systems and the individual components that typically make up such systems. Planning considerations are identified next. While remaining a valuable source of reference, the publication does not provide much implementable guidance in critical areas such as forming an airspace control plan (which will need to account for friendly aircraft) or an area defence plan. However, the document does argue

for a layered approach, which calls for early engagement and defence in depth. Given the likely detection and engagement ranges for many systems discussed previously, this approach would likely necessitate carrying out and coordinating the CUAS mission across multiple units.

The US Army Field Manual FM 3-01 *U.S. Army Air and Missile Defense Operations* reviews UAS threats and provides some useful guidance regarding actions that can be taken to counter them. The manual highlights that all Army forces participate in air and missile defence, which includes the CUAS mission. The document proposes delegating engagement of sUAS to the lower levels of command to account for the time-sensitive nature of the threat. Paragraph 9-38 of FM 3-01 directs that 'Virtually all rotary-wing, smaller class UAS, and RAM [rocket, artillery and mortar] engagement authorizations are decentralized to platoon level'.[127] Procedural controls and fire direction orders provide guidance for these engagements. Paragraph 11-4 of FM 3-01 describes how all forces participate in CUAS and air and missile defence, and it includes examples about how manoeuvre, aviation, special operations, field artillery and intelligence forces might contribute.

Complementing its doctrine, the US Army will soon include counter-drone training at boot camps, ensuring that all specialties understand the threat. This includes being able to identify and react to it. The US Department of Defense also offers a more comprehensive two-week course at Yuma. Further, Fort Sill recently reopened the Joint Counter Small Unmanned Aerial Systems University for operators and maintainers.[128]

As of October 2023, reports indicate that NATO is also close to implementing its first-ever counter-drone doctrine. The doctrine builds on a 2019 handbook on the topic and is expected to be between 70 and 80 pages long. According to report, the document will detail the operationalisation of CUAS and training standards for operators while describing the importance of layered, multi-domain solutions.[129]

While no funded Department of Defence program exists in Australia to acquire CUAS equipment, a handful of systems have been purchased for experimental development, demonstration and testing purposes. Examples include Agile Shield (a Lockheed Martin Australia built battle management systems), UAS detection and defeat equipment from DroneShield, and the EOS-built Slinger one shot, one UAS kill capability based on the EOS R400 Remote Weapon Station.[130] Notably, in August 2023 the Australian Army

hosted a counter robotics and autonomous systems focused innovation day aimed at 'showcasing Australian Defence Industry and academia's ability to use innovative concepts to address capability gaps and grow the project pipeline'. Several providers involved in developing and building CUAS capabilities participated in the event with the hope of entering contractual discussions with the Department of Defence.[131]

CUAS is a rapidly emerging mission for the Australian Army. The time is therefore ripe for the ADF to develop its own guidance for countering sUAS before the relevant technology enters the force's inventory en masse. The reality is that these aircraft threaten forces of all types. Further, sUAS threats are observed and act at a uniquely local level. These characteristics make sUAS fundamentally different from the threat posed by larger crewed and uncrewed aircraft, which tend to be of higher value and which can be detected and engaged across a broader part of the battlefield due to their operations at medium or high altitude. When dealing with sUAS, sensing from remote locations is not feasible and many effectors have limited range. In response, the sense, decide and effect tasks will need to be conducted at the platoon or section level. In developing guidance for the Army, it should be remembered that the simple act of detecting sUAS can provide some level of protection from the threat. Further, such detection can, to a degree, be carried out by human eyes and ears. Accordingly, with sufficient warning procedures in place, units may be able to take passive defensive measures to respond to a detected threat, even if no methods to defeat it are available. Reporting methods will also need to be specified in Army guidance so that the overall force can maintain situational awareness about extant threats on the battlefield.

To implement Army guidance, units will eventually need to be equipped to perform CUAS-associated tasks. In allocating capabilities, the potential complexity of the CUAS equipment will need to be matched with the ability of a unit to properly utilise that system. For example, there may be some cases in which a dedicated CUAS crew might need to be assigned to support another unit in a high-threat environment. Army should also consider what capabilities may be required to technically exploit intercepted signals, or to deal with captured (including downed) aircraft and control stations. Such capabilities would be especially important in supporting efforts to effect threats through RF detection or jamming, spoofing or hacking. An exploitation capability would also prove useful in determining

UAS system vulnerabilities and in establishing methods to slow the supply of UAS systems or components. While such capabilities cannot be built quickly, performing exploitation of commercial drones during peacetime may help equip units to develop the capacity to execute this mission during times of conflict.

Training is an important fundamental input to capability in the CUAS mission. As previously outlined, limited tests and experiments have been performed, but no systematic training across the Army currently exists. Because all units are at threat from sUAS, all units should receive training about general methods to identify, mitigate or defeat them. Further, because the sUAS threat is continually evolving (as evidenced by ISIL operations and the conflict in Ukraine), training needs to be updated and offered on a regular basis. Indeed, course-based training would be useful across the ADF, and even across the whole government sector as police and intelligence organisations may have domestic responsibilities to respond to UAS threats. As part of its effort to prepare for the CUAS mission, it may be worth sending Army representatives to attend US advanced courses so that they are able to develop suitable course materials for force-wide and specialist training back in Australia. In addition, field training and exercises must be conducted that include realistic sUAS threats developed by red teams equipped with the latest technology. Engaging with this technology during training will provide soldiers and officers with the skills and knowledge necessary to help overcome this emerging battlefield threat.

Beyond policy guidance, technical capability and training, in order to counter sUAS, Army (and the ADF in general) needs to maintain its intellectual currency around this rapidly evolving threat. This requires an ongoing focus on the evolution of technology and operational art, which can happen quickly in wartime. Additionally, Army needs to understand how certain potential adversaries might employ sUAS in the future. Achieving the requisite level of knowledge will involve a combination of good intelligence collection on adversary sUAS technology and operations, study of open-source documents from adversaries' military journals (and other sources), and a strong understanding of potential technological advances. A comprehensive set of lessons learned from combat and terrorist use of UAS should also be maintained.

Beyond the Army's remit, one point of concern is the issue of sUAS regulations inside Australian territory. While Australia was ahead of the

world in its original regulations around UAS, this legislation warrants reconsideration given rapid advances in technology and the remarkable growth in number of hobbyists and commercial users of sUAS. Remotely piloted aircraft were originally a rarity but are becoming an increasingly common sight. In Australia, the Civil Aviation Safety Authority is responsible for ensuring the safe use of airspace by uncrewed aircraft via the Civil Aviation Safety Regulations, Part 101. If flying a UAS under 25 kg for sport or recreation, a pilot must follow certain rules but does not require a remote pilot licence or other approvals to fly. A stricter set of accreditation and licensing approvals applies when a UAS is flown for work purposes. Breaking the rules and unsafe flying can attract fines, with the most serious offences potentially leading to prosecution.[132]

In the UK, a whole-of-government approach is described in the UK Counter-Unmanned Aircraft Strategy. Produced by the Home Office in October 2019, this recognises the public safety threat posed by uncrewed aircraft. The document defines a strategy based on mitigating malicious and criminal use of drones that might threaten national security and critical infrastructure. The strategy includes a four-phase approach to reducing these risks. Specifically, it focuses on understanding the threat; using a full-spectrum approach to deterrence, detection and disruption; building relationships with industry to help meet security standards; and empowering professionals to access counter-drone capabilities. While the strategy sets a framework for CUAS operations, access to counter-drone capabilities by police, for example, may require changes to UK legislation.[133]

Processes and regulations are reportedly being developed in Australia to help keep communities safe by ensuring that relevant agencies can act against and respond to drones that may cause harm. The Australian Communications and Media Authority has made an exemption to the *Radiocommunications Act 1992* to allow Australian police to access counter-drone equipment.[134] Additionally, the increased threat from UAS near airports has resulted in Airservices Australia posting a request for information on AusTender associated with an upcoming procurement of UAS surveillance services.[135] While contemporary law enforcement efforts inside Australia are primarily a question for domestic civilian authorities, thought will need to be given to the potential role that military CUAS capabilities might play in the future. Such consideration is especially important given the potential for state or non-state actors to carry out attacks or ISR operations

from within Australian territory. Especially close attention will need to be given to risks posed to sensitive Defence bases and infrastructure where the Defence Security and Estate Group typically has lead responsibility for protective security. Understanding key roles and accountabilities will become ever more important as sensitive technology associated with AUKUS Pillars 1 and 2 are developed, tested and fielded.

Observations and Recommendations

Based on the preceding analysis, this final section provides overall observations about the threat of sUAS, as well as proposing methods for countering the harmful employment of these systems. It also makes recommendations for Army and other Australian government agencies to consider in their efforts to prevent the malicious use of sUAS to harm the ADF and other elements of Australia's national security capabilities.

Observations

The first observation is that the sUAS threat which has emerged over the past decade is a significant and new challenge for military forces that shows no signs of abating. Rapid technological advances, primarily occurring in the commercial world, have improved batteries, propulsion, sensors and control stations—all of which make sUAS increasingly capable and easy to fly. The nature of these assets makes them especially well suited to a variety of military missions including surveillance and reconnaissance, targeting, and precise delivery of small payloads. This last point means that many uncrewed aircraft can be converted into small, guided cruise missiles or bomb-dropping assets for use against their intended targets. Just as challenging is the low cost of these systems, which allows sUAS to be placed in the hands of many militaries, groups and even individuals who may wish to harm Australia's military forces or its national security more broadly.

Trends towards component miniaturisation and performance improvement mean that sUAS capabilities will continue to grow. Increasingly powerful sensors and new types of sensors (like radars) are set to become a feature of more small aircraft in the future. Communication methods that are more resistant to disruption should also be expected. In response, two implementations of sUAS technology should be monitored particularly closely by the Army: autonomy and swarming systems. Autonomous sUAS that do not require a link back to a control station will become invulnerable to a number of contemporary control detection and jamming techniques. Further, these systems will be operable in much larger numbers than is possible today as each aircraft no longer needs its own remote operator. By virtue of their numbers and the use of autonomous coordinated tactics,

swarming sUAS could simply overwhelm or outsmart much of today's CUAS technology. Countering a swarming threat will likely require new thinking around sensors and effectors.

The second observation is that sUAS are not only a threat for the future. Since conflicts dating back to 2016, they have already been proven to be effective against some of the world's leading military forces, including the US and Russia. sUAS have successfully been used in attacks that have caused casualties and have destroyed aircraft, armoured vehicles, trucks, fixed sites and several other types of targets. sUAS have also contributed to intelligence-gathering efforts. Military forces unprepared for the threat of sUAS have found themselves without options to effectively respond, leaving them susceptible to the threat of attack at times and places of the adversary's choosing. In Russia's case, reducing the threat demanded significant changes to tactics, along with the dedication of high-value electronic warfare resources. However, even with its emphasis on defeating Ukrainian sUAS, and its ability to down thousands of aircraft per month, the threat has not yet been eliminated.

Lessons about the changing nature of warfare are emerging daily from the Russia-Ukraine conflict. Driven by the availability of large numbers of sensors (including sUAS), the difficulty in massing and generating surprise on the modern battlefield is becoming increasingly evident. This fact was astutely observed by David Johnson in an August 2022 article.[136] Suddenly it has become quite challenging for forces to generate the effects of massed fire and manoeuvre that have conventionally been required during offensive operations. Further, the fact that sUAS make it possible to deliver small explosives accurately against vehicles and individuals has reduced force morale and force effectiveness in new and confronting ways. To overcome such challenges, military forces in the future will need to find ways to create temporary zones of freedom from sUAS and more sophisticated means of detection and attack.

The third observation is that there are no silver-bullet solutions to deliver either 'sense' or 'effect' consequences against sUAS, both of which are needed for completing CUAS engagements. Thanks to its ability to provide militarily useful capability at a low cost, the sUAS is a truly asymmetric capability. As sUAS look and behave in a manner totally different to larger, crewed military aircraft, most militaries are not currently trained or equipped

to counter these threats. Indeed, a review of CUAS technology shows that there exists no low-cost, foolproof solution for eliminating the threat.

For sensing, the best solution based on current technology involves fusing information together from EO/IR sensors, RF detectors and radars. Radars can detect sUAS at longer ranges but will be increasingly challenged by miniaturisation and potential countermeasures. Assuming that RF libraries are continuously maintained, RF detectors can be effective against many commercial systems where the communication frequencies and protocols are known. The effectiveness of RF detectors may, however, degrade in the future as sUAS move to 5G networks and other more robust communications methods. Additionally, sUAS communications can easily be modified through software or hardware changes to help avoid RF detection. Nevertheless, EO/IR sensors, especially non-imaging ones with wide fields of view, can be useful for detection in some situations. Imaging EO/IR sensors are especially useful for short-range identification, if cued to the target, but are affected by poor weather and clutter.

For effectors, the choice of system will be strongly influenced by issues of military utility and cost-effectiveness, as well as concerns about the system's capacity to cause collateral damage. Missiles and artillery are a proven approach for air defence that are effective against sUAS attacks, but weapons currently in the inventory typically cost far more than the target they are meant to shoot down. These systems are also the most likely to create collateral damage or unintended effects, which will inevitably limit their utility in certain situations. Jammers, spoofing and hacking techniques require knowledge about the communications being used by the opposing threat systems. This renders them less useful when little is known about the sUAS system. Equally, jamming will likely be of little utility against autonomous sUAS. By contrast, based on tests, new directed energy solutions appear promising, but these are just starting to be deployed in combat. High-energy lasers work at long range under good weather conditions but could be ineffective due to fog, smoke or other poor weather. High-powered microwaves seem to be well suited to defeating sUAS swarms, but their effects tend to be limited in range.

The last observation is that the threat posed by sUAS exists beyond battlefields and times of war. sUAS could be used inside Australia today by terrorists, criminals or malicious foreign actors to gather intelligence, perform electronic jamming, enable cyberattacks, carry out kinetic attacks

and/or deliver other lethal payloads. Using sUAS to harm national security, to damage critical national infrastructure or to shut down airports is a relatively easy task, even for a hobbyist. Government agencies dedicated to generating the methods and technology necessary to detect, understand and counter the sUAS threat inside Australia are needed just as much as those that are focused on defeating the threat posed to our expeditionary forces.

Recommendations

The first recommendation for the Australian Army is to develop a training program for **all** soldiers around the sUAS threat, along with methods to counter those systems. The threat from sUAS will be ubiquitous on battlefields for the foreseeable future, and a peacetime threat already exists at Defence bases and installations within Australia. Conducting successful CUAS operations requires a basic understanding of sUAS technology and its potential applications. A single situation report about sUAS surveillance at a sensitive site, or a warning about an impending kinetic attack by a group of sUAS aircraft on the battlefield, could enable threat mitigation and save lives. Training will also prove immensely useful when CUAS systems are introduced into service within the ADF. As these systems come online, procedures and doctrine around CUAS operations need to be implemented in parallel.

The second recommendation is for Army to invest in a layered approach in its efforts to detect and effect sUAS. The technology associated with both the sUAS threat and the methods to counter that threat are evolving rapidly, so it is too early to focus investment into a single technology. Army, and the ADF more broadly, should therefore invest in a range of technologies for research and development of sensors and effectors, either through AUKUS Pillar 2 or the new Advanced Strategic Capabilities Accelerator. The ADF should also rapidly agree upon CUAS data standards and protocols for sensors, like NATO's SAPIENT standards, to enable data fusion now and into the future in a sensor agnostic fashion. Reasonable investment should immediately be made to provide a limited CUAS capability to Army should combat operations be needed over the next three years.

As the sUAS threat is not limited to foreign combat zones, the third recommendation involves building a CUAS centre of excellence focused on sUAS, either inside the Department of Defence or at a whole-of-government

level. This centre should focus on four missions to improve CUAS capability investments and operations: technology forecasting; gathering global lessons learned from nefarious use of sUAS; maintaining databases of sUAS capabilities and vulnerabilities; and foreign material exploitation of captured sUAS. To help focus investments, forecasting should consider advances in both sUAS and CUAS technology. As demonstrably effective tactics tend to be mimicked and shared, lessons-learned studies should focus on how sUAS are being employed by militaries, insurgents and terrorists around the world. Building and maintaining databases of sUAS capabilities and vulnerabilities will help feed libraries needed to exploit specific UAS signatures in the RF, radar or other domains. A foreign material exploitation capability would prove extremely useful to inform Australia's understanding of new sUAS threats in conflict, but any such capability must also be exercised during peacetime to maintain currency. If foreign sUAS systems are not available to exploit, commercial systems could be used to help inform domestic CUAS needs.

The last recommendation focuses on the fact that sUAS are not just a threat that exists outside Australia's borders. sUAS could be employed from Australia's territory in ways that harm our national security. Forming a strategy to mitigate the harmful use of sUAS on Australian soil requires a whole-of-government approach, much like the UK Counter-Unmanned Aircraft Strategy. Roles and responsibilities for domestic CUAS need to be assigned, along with equipment and other resources, before national security is compromised.

Conclusion

This paper has reviewed the growing threat posed by sUAS to military forces and to national security in general. While UAS have been a prominent feature of combat operations for decades, there have been significant advances in the availability of continually smaller sUAS systems to an ever broader range of users. These systems are readily available in the commercial market and have proven quite effective on the battlefield when employed by militaries and insurgent forces over the past decade, especially in ISR and kinetic attack mission tasks. In recent conflicts, military forces including those of the US and Russia have been successfully attacked by sUAS resulting in casualties and losses of military equipment.

Unfortunately, there are no 'silver bullet' solutions to address the sUAS threat. Current air defence systems are either not well suited to these small aircraft targets or are far more expensive to employ per engagement as compared to the sUAS that they may shoot down. The signatures associated with sUAS are also small, so technology improvements to 'sense' and 'effect' these systems are needed. The Australian Army, like many other militaries, currently lacks the doctrine, training and systems needed to counter sUAS.

The most important conclusion associated with this work is the fact that sUAS are not a future threat. The wide availability of these systems and the ease with which they can be modified to cause harm to the ADF and Australian national security interests more broadly necessitates urgent action to mitigate the threat. The Australian Army should therefore immediately develop concepts and acquire systems that provide the minimum viable CUAS capability needed for combat operations in the 2020s and beyond. A new strategy for countering the harmful use of sUAS inside Australia is also needed and requires a whole-of-government approach. The formation of a CUAS centre of excellence would allow the government to keep track of the rapidly evolving threat posed by sUAS and to improve CUAS capabilities and operations.

About the Author

Dr Carl Rhodes, director and founder of Robust Policy, has over 25 years of experience delivering policy analysis and actionable recommendations for senior government and military leaders in Australia and the United States. Carl has experience as a research leader and manager of policy analysis efforts and is active across several portfolios including defence technology and acquisition and national security strategy. Carl is currently a non-resident Senior Fellow with the National Institute for Deterrence Studies and worked at RAND Corporation from 1997 to 2021, including as director of RAND Australia. Carl earned a PhD in chemical engineering from Caltech.

Endnotes

1 Senior Airman James Thompson, 'Sun Setting the MQ-1 Predator: A History of Innovation', Air Combat Command, 14 February 2018, at: https://www.acc.af.mil/News/Article/1442622/sun-setting-the-mq-1-predator-a-history-of-innovation

2 'Foreign News: Bravo!', *Time*, 25 July 1949, at: https://time.com/archive/6791346/foreign-news-bravo/l

3 'A Brief History of Drones', Imperial War Museums, accessed 30 October 2023, at: https://www.iwm.org.uk/history/a-brief-history-of-drones

4 Thomas P Ehrhard, *Air Force UAVs: The Secret History* (Arlington VA: The Mitchell Institute for Airpower Studies, 2010), at: https://mitchellaerospacepower.org/air-force-uavs-the-secret-history/

5 'Jindivik', Defence Science and Technology Group, accessed 19 February 2024, at: https://www.dst.defence.gov.au/innovation/jindivik

6 Joint Air Power Competence Centre, *A Comprehensive Approach to Countering Unmanned Aircraft Systems* (Kalkar, 2021), at: https://www.japcc.org/books/a-comprehensive-approach-to-countering-unmanned-aircraft-systems

7 Federal Aviation Administration, *Aeronautical Information Manual: Official Guide to Basic Flight Information and ATC Procedures* (U.S. Department of Transportation, 2023), Chapter 11, Section 2.

8 Faiyaz Ahmed, JC Mohanta, Anupam Keshari and Pankaj Singh Yadav, 'Recent Advances in Unmanned Aerial Vehicles: A Review', *Arabian Journal for Science and Engineering* 47, no. 7 (2022): 7963–7984, at: https://doi.org/10.1007/s13369-022-06738-0

9 Dan Gettinger, *The Drone Databook* (The Center for the Study of the Drone at Bard College, 2019), at: https://dronecenter.bard.edu/files/2019/10/CSD-Drone-Databook-Web.pdf; Dan Gettinger, *The Drone Databook Update: March 2020* (The Center for the Study of the Drone at Bard College, 2020), at: https://dronecenter.bard.edu/projects/drone-proliferation/drone-databook-update-march-2020/

10 Nessa Anwar, 'World's Largest Drone Maker Is Unfazed—Even If It's Blacklisted by the U.S.', CNBC, 8 February 2023, at: https://www.cnbc.com/2023/02/08/worlds-largest-drone-maker-dji-is-unfazed-by-challenges-like-us-blacklist.html

11 Bradley Wilson, Shane Tierney, Brendan Toland, Rachel M Burns, Colby P Steiner, Christopher Scott Adams, Michael Nixon, Raza Khan, Michelle D Ziegler, Jan Osburg and Ike Chang, *Small Unmanned Aerial System Adversary Capabilities* (Homeland Security Operational Analysis Center operated by the RAND Corporation, 2020), at: https://doi.org/10.7249/RR3023

12 'Mavic 3 Pro—Specs', DJI, accessed 7 December 2023, at: https://www.dji.com/au/mavic-3-pro/specs

13 Gettinger, *The Drone Databook Update*.

14 'Tomahawk Cruise Missile', Raytheon, accessed 9 December 2023, at: https://www.rtx.com/raytheon/what-we-do/sea/tomahawk-cruise-missile; Carlo Kopp, 'AGM-142E Raptor: The RAAF's New Standoff Weapon', Air Power Australia, 2014 [1996, 2005], at: https://www.ausairpower.net/TE-AGM-142-SOW.html

15 Douglas Barrie, 'Trends in Missile Technologies', International Institute for Strategic Studies (IISS), 11 March 2019, at: https://www.iiss.org/online-analysis/online-

analysis//2019/03/trends-in-missile-technologies

16 'HARPY: Autonomous Weapon for All Weather', IAI, accessed 9 December 2023, at: https://www.iai.co.il/p/harpy

17 National Academies of Sciences, Engineering, and Medicine, *Counter-Unmanned Aircraft System (CUAS) Capability for Battalion-and-Below Operations: Abbreviated Version of a Restricted Report* (National Academies Press, 2018).

18 Joint Air Power Competence Centre, *A Comprehensive Approach to Countering Unmanned Aircraft Systems*.

19 'Guinness World Record for Largest Drone Show Owned by Genesis Motors', The Droning Company, 14 June 2023, at: https://www.thedroningcompany.com/blog/guinness-world-record-for-largest-drone-show-owned-by-genesis-motors

20 David R Frelinger, Joel Kvitky and William Stanley, *Proliferated Autonomous Weapons: An Example of Cooperative Behavior*, Documented Briefing (Santa Monica CA: RAND Corporation, 1998), at: https://www.rand.org/pubs/documented_briefings/DB239.html

21 Andy Le, 'Swarm: UAS Swarming Technology and "Future Ready" for the 20th Regiment', The Cove, 20 December 2021, at: https://cove.army.gov.au/article/swarm-uas-swarming-technology-and-future-ready-20th-regiment

22 Robert Dougherty, 'UK Hosts First AUKUS AI and Autonomy Trial', Defence Connect, 29 May 2023, at: https://www.defenceconnect.com.au/land-amphibious/12055-uk-host-first-aukus-ai-and-autonomy-trial

23 J Philip Craiger and Diane Maye Zorri, *Current Trends in Small Unmanned Aircraft Systems: Implications for U.S. Special Operations Forces*, JSOU Press Occasional Paper, September 2019, at: https://commons.erau.edu/publication/1472

24 Wilson et al., *Small Unmanned Aerial System Adversary Capabilities*.

25 Don Rassler, 'The Islamic State and Drones: Supply, Scale, and Future Threats' (Combating Terrorism Center at West Point, July 2018), at: https://ctc.westpoint.edu/islamic-state-drones-supply-scale-future-threats

26 Michael S Schmidt and Eric Schmitt, 'Pentagon Confronts a New Threat From ISIS: Exploding Drones', *The New York Times*, 12 October 2016, at: https://www.nytimes.com/2016/10/12/world/middleeast/iraq-drones-isis.html

27 '"Booby-Trapped" ISIL Drone in Deadly Iraq Attack', Al Jazeera, 12 October 2016, at: https://www.aljazeera.com/news/2016/10/12/booby-trapped-isil-drone-in-deadly-iraq-attack

28 Rassler, 'The Islamic State and Drones'.

29 Ibid.

30 Kerry Chávez and Ori Swed, 'Off the Shelf: The Violent Nonstate Actor Drone Threat', *Air & Space Power Journal* 34, no. 3 (2020): 29–43.

31 Mason Clark, 'The Russian Military's Lessons Learned in Syria', Military Learning and the Future of War Series (Washington DC: Institute for the Study of War, January 2021), at: https://www.understandingwar.org/report/russian-military%E2%80%99s-lessons-learned-syria

32 Vikram Mittal, 'The Ukrainian Military Is Changing Its Tactics with Bayraktar TB2 Drones', *Forbes*, 23 June 2022, at: https://www.forbes.com/sites/vikrammittal/2022/06/23/ukrainian-military-is-changing-its-tactics-with-the-bayraktar-tb2-drones/

33 Ibid.

34 Elisabeth Gosselin-Malo, 'Are the Once-Vaunted Bayraktar Drones Losing Their Shine in Ukraine?', *Defense News*, 31 October 2023, at: https://www.defensenews.com/global/europe/2023/10/31/are-the-once-vaunted-bayraktar-drones-losing-their-shine-in-ukraine/

35 Mitchell Institute for Aerospace Studies, 'The Air Battle for Taiwan: Lessons Learned from Ukraine's Drone Operations', *The Aerospace Advantage*, 8 April 2023, at: https://mitchellaerospacepower.org/episode-123-the-air-battle-for-taiwan-lessons-learned-from-ukraines-drone-operations/

36 Elisabeth Gosselin-Malo, 'Ukraine Continues to Snap up Chinese DJI Drones for Its Defense', *Defense News*, 23 October 2023, at: https://www.defensenews.com/global/europe/2023/10/23/ukraine-continues-to-snap-up-chinese-dji-drones-for-its-defense

37 'Ukraine's Latest Weapons in Its War with Russia: 3D-Printed Bombs', *The Economist*, 1 August 2023, at: https://www.economist.com/science-and-technology/2023/08/01/ukraines-latest-weapons-in-its-war-with-russia-3d-printed-bombs

38 Sofiia Syngaivska, 'The New Ukrainian KH-S7 Drone Has Undergone Its First Real Combat Trials and Received Feedback', *Defense Express*, 14 September 2023, at: https://en.defence-ua.com/news/the_new_ukrainian_kh_s7_drone_has_undergone_its_first_real_combat_trials_and_received_feedback-7938.html

39 'How Could FPV Drones Change Warfare?', *The Economist*, 4 August 2023, at: https://www.economist.com/the-economist-explains/2023/08/04/how-could-fpv-drones-change-warfare

40 James Byrne, Jack Watling, Justin Bronk, Gary Somerville, Joe Byrne, Jack Crawford and Jane Baker, *The Orlan Complex: Tracking the Supply Chains of Russia's Most Successful UAV* (Royal United Services Institute for Defence and Security Studies, December 2022), at: https://static.rusi.org/SR-Orlan-complex-web-final.pdf

41 Bohdan Tuzov, 'Analysis: Russian Lancet Kamikaze Drone in Ukraine: An Overview', *Kyiv Post*, 12 November 2023, at: https://www.kyivpost.com/analysis/23923

42 Alistair MacDonald and James Marson, 'This Russian Suicide Drone Is Blunting Ukraine's Advance', WSJ, 3 November 2023, at: https://www.wsj.com/world/this-russian-suicide-drone-is-blunting-ukraines-advance-8241a0e4

43 David Hambling, 'Russia Boosts Production and Displays New "Swarming" Version of Lancet-3 Kamikaze Drone', *Forbes*, 18 July 2023, at: https://www.forbes.com/sites/davidhambling/2023/07/18/russia-boosts-production-and-displays-new-swarming-version-of-lancet-3-kamikaze-drone/

44 Jeremy Binnie, 'IRGC Confirms Specs for Shahed-136 Attack UAV', Janes, 17 May 2023, at: https://www.janes.com/osint-insights/defence-news/air/irgc-confirms-specs-for-shahed-136-attack-uav#:~:text=The%20Shahed%2D136%20weighs%20200,speed%20of%20185%20km%2Fh.

45 'Iran's Shahed-136 Drone Evolves with Jet Propulsion and Targeting "Eyes"', *Militarnyi* (blog), 13 November 2023, at: https://mil.in.ua/en/news/iran-s-shahed-136-drone-evolves-with-jet-propulsion-and-targeting-eyes

46 David Hambling, 'Scythe Attack Drone Is Ukraine's Answer to Russia's Shaheds', *Forbes*, 17 December 2023, at: https://www.forbes.com/sites/davidhambling/2023/12/17/scythe-attack-drone-is-ukraines-answer-to-russias-shaheds/

47 'How Drones Dogfight above Ukraine', *The Economist*, 7 February 2023, at: https://www.economist.com/the-economist-explains/2023/02/07/how-drones-dogfight-above-ukraine

48 Ethan Walton, 'Here's the Counter-Drone Platforms Now Deployed in Ukraine', C4ISRNet, 21 November 2023, at: https://www.c4isrnet.com/opinion/2023/11/21/heres-the-counter-drone-platforms-now-deployed-in-ukraine/#:~:text=Electric%20Optic%20Systems%20based%20in,moving%20targets%20beyond%20800%20meters.; Anthony Albanese, the Hon Richard Marles MP and the Hon Pat Conroy MP, 'Australian Capabilities to Continue Supporting Ukraine' (media release), Department of Defence, 25 October 2023, at: https://www.minister.defence.gov.au/media-releases/2023-10-25/australian-capabilities-continue-supporting-ukraine

49 Ukrainian air defences reported destroying all but one Shahed drone in an attack wave of 75 UAS in November 2023. Samya Kullab, 'Russia Launches Largest Drone Attack since Start of Ukraine Invasion', C4ISRNet, 25 November 2023, at: https://www.c4isrnet.com/unmanned/2023/11/25/russia-launches-largest-drone-attack-since-start-of-ukraine-invasion/

50 Dan Sabbagh, 'Ukrainians Use Phone App to Spot Deadly Russian Drone Attacks', The Observer, 29 October 2022, at: https://www.theguardian.com/world/2022/oct/29/ukraine-phone-app-russia-drone-attacks-eppo; 'The ePPO Application Has Started Working in Ukraine: How to Notify the Armed Forces of Ukraine about a Missile or a Drone', Visit Ukraine, 27 October 2022, at: https://visitukraine.today/blog/1083/the-eppo-application-has-started-working-in-ukraine-how-to-notify-the-armed-forces-of-ukraine-about-a-missile-or-a-drone

51 Jack Watling and Nick Reynolds, *Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine*, Special Report (Royal United Services Institute for Defence and Security Studies, 19 May 2023), at: https://www.rusi.org/explore-our-research/publications/special-resources/meatgrinder-russian-tactics-second-year-its-invasion-ukraine

52 Sean Hollister, 'DJI Drones, Ukraine, and Russia—What We Know about AeroScope', The Verge, 23 March 2022, at: https://www.theverge.com/22985101/dji-aeroscope-ukraine-russia-drone-tracking

53 Emma Roth, 'DJI Quietly Discontinues Its Drone-Detecting AeroScope System', The Verge, 5 March 2023, at: https://www.theverge.com/2023/3/5/23626057/dji-discontinues-aeroscope-drone-detecting-system; Andy Greenberg, 'This Hacker Tool Can Pinpoint a DJI Drone Operator's Exact Location', *Wired*, 2 March 2023, at: https://www.wired.com/story/dji-droneid-operator-location-hacker-tool

54 Dina Temple-Raston, Sean Powers and Daryna Antoniuk, 'Exclusive: Inside Ukraine's Secret Drone Factories', Click Here (podcast), The Record. Recorded Future News, 12 October 2023, at: https://therecord.media/ukraine-secret-drone-factories-click-here?utm_source=substack&utm_medium=email

55 David Hambling, 'Jam Buster: How Ukraine's "Secret Weapon" Shrugs off Russian Radio Interference', Popular Mechanics, 17 February 2023, at: https://www.popularmechanics.com/military/a42922481/tricopter-drone-atlaspro-resists-russian-jamming

56 Chávez and Swed, 'Off the Shelf'.

57 Georgia Lykou, Dimitrios Moustakas and Dimitris Gritzalis, 'Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies', *Sensors* 20, no. 12 (2020): 3537, at: https://doi.org/10.3390/s20123537

58 Rex Martinich, 'Drone Loaded with Drugs "crashed" during Prison Flight', *The Canberra Times*, 22 September 2023, at: https://www.canberratimes.com.au/story/8360817/drone-loaded-with-drugs-crashed-during-prison-flight

59 Hollister, 'DJI Drones, Ukraine, and Russia'.

60 Headquarters, Department of the Army, *Counter-Unmanned Aircraft System (C-UAS)*, ATP 3-01.81 (August 2023), at: https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN38994-ATP_3-01.81-000-WEB-1.pdf61 Alan J Vick, *Air Base Attacks and Defensive Counters: Historical Lessons and Future Challenges*, Research Report (Santa Monica CA: RAND Corporation, 2015), at: https://www.rand.org/pubs/research_reports/RR968.html

62 John Hudson, 'Ukraine Lures Russian Missiles with Decoys of U.S. Rocket System', *Washington Post*, 30 August 2022, at: https://www.washingtonpost.com/world/2022/08/30/ukraine-russia-himars-decoy-artillery

63 Nicholas Fiorenza, 'IDET 2023: Inflatable Leopard 2A4 Decoys Sent to Ukraine', Janes, 26 May 2023, at: https://www.janes.com/defence-news/news-detail/idet-2023-inflatable-leopard-2a4-decoys-sent-to-ukraine

64 For military vehicles on the move under air attack by area effect weapons, increased spacing will result in lower losses and a higher rate of advance. If the attacks employ one-on-one weapons, such as Hellfire or loitering sUAS munitions, decreased spacing increases the rate of advance. This situation is discussed in detail in David A Ochmanek, Edward R Harshberger, David E Thaler and Glenn A Kent, *To Find, and Not to Yield: How Advances in Information and Firepower Can Transform Theater Warfare*, Monograph Report (Santa Monica CA: RAND Corporation, 1998), at: https://www.rand.org/pubs/monograph_reports/MR958.html

65 Joseph Trevithick, 'Israeli Merkava Tanks Appear with "Cope Cage" Armor', The Drive, 16 October 2023, at: https://www.thedrive.com/the-war-zone/israeli-merkava-tanks-appear-with-cope-cage-armor

66 Chenyang Lyu and Renjun Zhan, 'Global Analysis of Active Defense Technologies for Unmanned Aerial Vehicle', *IEEE Aerospace and Electronic Systems Magazine* 37, no. 1 (January 2022): 6–31, at: https://doi.org/10.1109/MAES.2021.3115205

67 Wilson et al., *Small Unmanned Aerial System Adversary Capabilities*.

68 Byrne et al., *The Orlan Complex*.

69 Dawn MK Zoldi, 'IFF Technology Aims for a Safer Battlefield—Military Embedded Systems', Military Embedded Systems, 6 May 2021, at: https://militaryembedded.com/unmanned/sensors/iff-technology-aims-for-a-safer-battlefield

70 Olivia Savage, 'NATO to Adopt SAPIENT as C-UAS Standard', Janes, 25 September 2023, at: https://www.janes.com/osint-insights/defence-news/defence/nato-to-adopt-sapient-as-c-uas-standard#:~:text=NATO%20will%20adopt%20the%20SAPIENT,2023%20(TIE23)%20in%20Vredepeel%2C

71 Jan Farlik, Miroslav Kratky, Josef Casar and Vadim Starý, 'Radar Cross Section and Detection of Small Unmanned Aerial Vehicles', *2016 17th International Conference on Mechatronics—Mechatronika (ME)* (Prague: IEEE, 2016), at: https://ieeexplore.ieee.org/document/7827857

72 Lykou, Moustakas and Gritzalis, 'Defending Airports from UAS'; Wahab Khawaja, Vasilii Semkin, Naeem Iqbal Ratyal, Qasim Yaqoob, Jibran Gul and Ismail Guvenc, 'Threats from and Countermeasures for Unmanned Aerial and Underwater Vehicles', *Sensors* 22, no. 10 (2022): 3896, at: https://doi.org/10.3390/s22103896; Vittorio Ugo Castrillo, Angelo Manco, Domenico Pascarella and Gabriella Gigante, 'A Review of Counter-UAS Technologies for Cooperative Defensive Teams of Drones', *Drones* 6, no. 3 (2022): 65, at: https://doi.org/10.3390/drones6030065

73 Lykou, Moustakas and Gritzalis, 'Defending Airports from UAS'; Castrillo et al., 'A Review of Counter-UAS Technologies for Cooperative Defensive Teams of Drones'.

74 Wilson et al., *Small Unmanned Aerial System Adversary Capabilities*.

75 Ibid.

76 Lykou, Moustakas and Gritzalis, 'Defending Airports from UAS'.

77 Castrillo et al., 'A Review of Counter-UAS Technologies for Cooperative Defensive Teams of Drones'.

78 Wilson et al., *Small Unmanned Aerial System Adversary Capabilities*.

79 'AARTOS DDS Camera Rangetest' (video), Aaronia AG YouTube channel, 2018, at: https://www.youtube.com/watch?v=Jnmypd09HJ8

80 *Specifications of AARTOS Ultra Long Range Thermal / Optical Tracking System* (AARTOS, 2023), at: https://downloads.aaronia.com/datasheets/solutions/cameras/AARTOS_ultra-lr-thermal-optical-camera.pdf

81 GM Koretsky, JF Nicoll and MS Taylor, *A Tutorial on Electro-Optical/Infrared (EO/IR) Theory and Systems* (Alexandria VA: Institute for Defense Analyses, January 2013), at: https://apps.dtic.mil/sti/citations/ADA586864

82 Robert W Nicholas, Ronald Driggers, David Shelton and Orges Furxhi, 'Infrared Search and Track Performance Estimates for Detection of Commercial Unmanned Aerial Vehicles', *Infrared Imaging Systems: Design, Analysis, Modeling, and Testing XXIX, Orlando, United States* (SPIE, 2018), at: https://doi.org/10.1117/12.2305559

83 Wilson et al., *Small Unmanned Aerial System Adversary Capabilities*.

84 Wiesław Klembowski, Adam Kawalec and Waldemar Wizner, 'Passive Radars as Sources of Information for Air Defence Systems', in *Passive Radar, Challenges Concerning Theory and Practice in Military Applications* (NATO, S&T Organization, 2013), at: https://studylib.net/doc/25624496/mp-set-187-10

85 Merrill Ivan Skolnik, *Introduction to Radar Systems*, 2nd edition (New York: McGraw-Hill, 1980).

86 Farlik et al., 'Radar Cross Section and Detection of Small Unmanned Aerial Vehicles'.

87 Lykou, Moustakas and Gritzalis, 'Defending Airports from UAS'.

88 Matthew Henderson, 'Detection and Classification of Small UAS for Threat Neutralization', *DSIAC Journal* 7, no. 3 (2020), at: https://dsiac.org/articles/detection-and-classification-of-small-uas-for-threat-neutralization

89 For satellite communications, this phenomenon is typically called 'rain fade'. Wilson et al., *Small Unmanned Aerial System Adversary Capabilities*.

90 Huiling Hou, Zhiliang Yang and Cunsuo Pang, 'Rotor UAV's Micro-Doppler Signal Detection and Parameter Estimation Based on FRFT-FSST', *Sensors* 21, no. 21 (2021): 7314, at: https://doi.org/10.3390/s21217314

91 Castrillo et al., 'A Review of Counter-UAS Technologies for Cooperative Defensive Teams of Drones'.

92 Ibid.

93 Wilson et al., Small Unmanned Aerial System Adversary Capabilities.

94 Castrillo et al., 'A Review of Counter-UAS Technologies for Cooperative Defensive Teams of Drones'.

95 Hollister, 'DJI Drones, Ukraine, and Russia; Greenberg, 'This Hacker Tool Can Pinpoint a DJI Drone Operator's Exact Location'.

96 'Mavic 3 Pro—Specs'; Lykou, Moustakas and Gritzalis, 'Defending Airports from UAS'.

97 Lykou, Moustakas and Gritzalis, 'Defending Airports from UAS'.

98 Ibid.

99 Details of the encounter, such as the nation or groups involved, were not disclosed. Chris Baraniuk, 'Small Drone "Shot with Patriot Missile"', *BBC News*, 15 March 2017, at: https://www.bbc.com/news/technology-39277940#

100 Chris Gordon, 'Coyote Air Defense Weapon Shoots Down Drones Attacking US Outpost', *Air & Space Forces Magazine*, 20 January 2023, at: https://www.airandspaceforces.com/coyote-air-defense-weapon-shoots-down-drones-us-syria

101 Joseph Trevithick, 'Drastic Increase in Army Coyote Drone Interceptor Purchase Plans', The Drive, 20 December 2023, at: https://www.thedrive.com/the-war-zone/drastic-increase-in-army-coyote-drone-interceptor-purchase-plans

102 Joseph Trevithick, 'Video Shows Missile, Vulcan Cannon Fire Reportedly Shooting Down Drones in Iraq', The Drive, 4 January 2022, at: https://www.thedrive.com/the-war-zone/43736/video-emerges-of-centurion-cannon-and-missile-repelling-drone-attack-in-iraq; 'Defeating the Cost Curve in Ukraine', Missile Defense Advocacy Alliance, 25 October 2022, at: https://missiledefenseadvocacy.org/alert/defeating-the-cost-curve-in-ukraine

103 'How Drones Dogfight above Ukraine'.

104 'Dutch Police Fight Drones with Eagles', *BBC News*, 12 September 2016, at: https://www.bbc.com/news/world-europe-37342695

105 Lykou, Moustakas and Gritzalis, 'Defending Airports from UAS'.

106 Castrillo et al., 'A Review of Counter-UAS Technologies for Cooperative Defensive Teams of Drones'.

107 Ibid.

108 Lykou, Moustakas and Gritzalis, 'Defending Airports from UAS'.

109 Lyu and Zhan, 'Global Analysis of Active Defense Technologies for Unmanned Aerial Vehicle'.

110 Ibid.

111 Kelley M Sayler, Andrew Feickert and Ronald O'Rourke, *Department of Defense Directed Energy Weapons: Background and Issues for Congress* (Congressional Research Service, 13 September 2022), at: https://crsreports.congress.gov/product/pdf/R/R46925/5

112 Aaron Angell, 'The High-Energy Laser: Tomorrow's Weapon to Improve Force Protection', *Joint Forces Quarterly*, no. 64 (January 2012): 115–121, at: https://apps.dtic.mil/sti/citations/ADA562311

113 Kelsey D Atherton, 'What It's Like to Fire Raytheon's Powerful Anti-Drone Laser', *Popular Science*, 31 October 2022, at: https://www.popsci.com/technology/firing-raytheon-laser-weapon/

114 This cost does not appear to include acquisition of the laser system itself. B David Zarley, 'Israeli and US Navy Lasers Successfully Shoot Down Drones, Rockets, Artillery', *Big Think*, 1 May 2022, at: https://www.freethink.com/technology/laser-defense-iron-beam

115 These types of weapons are also referred to as electromagnetic pulse (EMP) weapons. Steven C Furlong and Timothy M Lang, 'Counter UAV drone system using electromagnetic pulse', United States US11378362B2, patent filed 15 May 2020 and issued 5 July 2022, at: https://patents.google.com/patent/US11378362/en

116 Lyu and Zhan, 'Global Analysis of Active Defense Technologies for Unmanned Aerial Vehicle'.

117 Castrillo et al., 'A Review of Counter-UAS Technologies for Cooperative Defensive Teams of Drones'.

118 'Shooting Drones out of the Sky with Phasers', *BBC News*, 14 October 2019, at: https://www.bbc.com/news/business-49984415; Mark Gunzinger and Chris Dougherty, *Changing the Game: The Promise of Directed-Energy Weapons* (Washington DC: Center for Strategic and Budgetary Assessments, 2012), at: https://csbaonline.org/research/publications/changing-the-game-the-promise-of-directed-energy-weapons

119 Bruce A Wright, Eric Powell and William W Dodson III, *Directed Energy: Medical Effects of Radio Frequency Exposure (Microwave & Millimeter Wave)—A Literature Review* (Wright Patterson AFB OH: Air Force Research Laboratory, 711th Human Performance Wing, January 2013).

120 Major Coningsby J Burdon, 'Hardening Unmanned Aerial Systems' (Master of Operational Arts and Sciences research report, Air Command and Staff College, Air University, 2017), at: https://apps.dtic.mil/sti/pdfs/AD1042082.pdf

121 Christian Tabak, 'B-52H Undergoes First Electromagnetic Pulse Hardness Testing at Tinker', Tinker Air Force Base, 18 May 2020, at: https://www.tinker.af.mil/News/Article-Display/Article/2204895/b-52h-undergoes-first-electromagnetic-pulse-hardness-testing-at-tinker/#:~:text=Electromagnetic%20pulse%20testing%20of%20the,major%20milestone%20for%20the%20program.

122 Lykou, Moustakas and Gritzalis, 'Defending Airports from UAS'.

123 'DroneShield—Products', DroneShield, 2023, at: https://www.droneshield.com/products

124 Lykou, Moustakas and Gritzalis, 'Defending Airports from UAS'.

125 Multiple Australian Army senior leaders, semi-structured interviews around current and future Army counter-UAS capabilities, December 2023.

126 Headquarters, Department of the Army, *Counter-Unmanned Aircraft System* (C-UAS), ATP 3-01.81.

127 Headquarters, Department of the Army, U.S. *Army Air and Missile Defense Operations*, FM 3-01 (December 2020), at: https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN31339-FM_3-01-000-WEB-1.pdf

128 Shaan Shaikh, Tom Karako and Michelle McLoughlin, *Countering Small Uncrewed Aerial Systems: Air Defense by and for the Joint Force* (Washington DC: Center for Strategic and International Studies, November 2003), at: https://www.csis.org/analysis/countering-small-uncrewed-aerial-systems; Todd South, 'Army Boot Camp Will Soon Include Counter-Drone Training', *Army Times*, 15 November 2023, at: https://www.armytimes.com/news/your-army/2023/11/15/army-boot-camp-will-soon-include-counter-drone-training/

129 Elisabeth Gosselin-Malo, 'NATO to Adopt First-Ever Counter-Drone Doctrine for Member Nations', *Defense News*, 20 October 2023, at: https://www.defensenews.com/unmanned/2023/10/20/nato-to-adopt-first-ever-counter-drone-doctrine-for-member-nations/

130 Max Blenkin, 'More on EOS' New Counter-UAS Weapon System' *Australian Defence Magazine*, 18 May 2023, at: https://www.australiandefence.com.au/news/more-on-eos-new-counter-uas-weapon-system; Gerrard Cowan, 'Australian Army Acquires DroneShield RfOne MKII C-UAS Sensors', Janes, 22 July 2021, at: https://www.janes.com/osint-insights/defence-news/australian-army-acquires-droneshield-rfone-mkii-c-uas-sensors; Philip Butterworth-Hayes and Tim Mahon, 'Lockheed Australia Agile Shield Battle Management System Passes Counter-Drone Operational Test', *Unmanned Airspace* (blog), 25 October 2023, at: https://www.unmannedairspace.info/latest-news-

and-information/lockheed-australia-agile-shield-battle-management-system-passes-counter-drone-operational-test

131 'Army Innovation Day 2023', Australian Army Research Centre, accessed 21 February 2024, at: https://researchcentre.army.gov.au/event/army-innovation-day-2023

132 Department of Infrastructure, Transport, Regional Development, Communications and the Arts, Drones (website), accessed 24 December 2023, at: https://www.drones.gov.au/homepage

133 HM Government, *UK Counter-Unmanned Aircraft Strategy* (October 2019), at: https://www.gov.uk/government/publications/uk-counter-unmanned-aircraft-strategy

134 Department of Infrastructure, Transport, Regional Development, Communications and the Arts, 'Security Policy', Drones, accessed 20 November 2023, at: https://www.drones.gov.au/policies-and-programs/policies/security-policy

135 Airservices Australia, 'Managed Airspace Surveillance Solution RFI', AusTender, 19 September 2023, at: https://www.tenders.gov.au/Atm/ShowClosed/d1d6eb27-e18e-445d-b5f6-f8ffbe8c559e?PreviewMode=False

136 David Johnson, 'Ending the Ideology of the Offense, Part II', War on the Rocks, 25 August 2022, at: https://warontherocks.com/2022/08/ending-the-ideology-of-the-offense-part-ii. Unfortunately, Dr David Johnson passed away in October 2022. He was a friend, a colleague and a brilliant analyst on military history and security issues.

researchcentre.army.gov.au

CG APR030/24