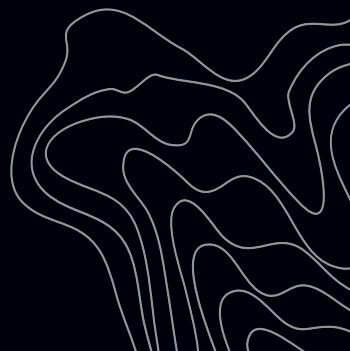


DRONES IN MODERN WARFARE: LESSONS LEARNT FROM THE WAR IN UKRAINE (2024–2026)



DR OLEKSANDRA MOLLOY

AUSTRALIAN ARMY RESEARCH CENTRE
/ Australian Army Occasional Paper No. 45





DRONES IN MODERN WARFARE: LESSONS LEARNT FROM THE WAR IN UKRAINE (2024–2026)

DR OLEKSANDRA MOLLOY

/ Australian Army Occasional Paper No. 45

© Commonwealth of Australia 2026

This publication is copyright. Apart from any fair dealing for the purpose of study, research, criticism or review (as permitted under the Copyright Act 1968), and with standard source credit included, no part may be reproduced by any process without written permission.

The views expressed in this publication are those of the author(s) and do not necessarily reflect the official policy or position of the Australian Army, the Department of Defence or the Australian Government.

ISSN (Print) 2653-0406

ISSN (Digital) 2653-0414

DOI: 10.61451/2675166

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
<https://researchcentre.army.gov.au>

Cover image: This photograph captures the silhouette of a person operating a multi-rotor drone against the backdrop of a setting sun. The General Staff of Ukraine (<https://empr.media/news/war/russia-ukraine-war-updates-key-developments-as-of-october-29-2025/>)

CONTENTS

Abstract.....1

List of Abbreviations 2

Introduction.....3

Methodology 7

 Participants..... 7

 Materials 8

 Data Analysis 9

The Evolution of Drone Warfare, 2024–2026 10

 FPV Drones: Expansion at Scale 10

 Fibre-Optic Drones 13

 Intelligence, Surveillance and Reconnaissance Drones..... 16

 Loitering Munitions 18

 Deep-Strike/Long-Range Drones 20

 Heavy Multirotors and ‘Night Bombers’ (Bomber Drones).....22

 Interceptor Drones or ‘Drone-on-Drone’ Warfare.....23

Drone Challenges 26

 Environmental Factors Complicate Operations.....26

 A UAS Cannot Hold Ground 27

 A UAS Has No Self-Defence 28

 Drone Production Depends on Chinese Components 28

 There Is No Perfect Weapon.....28

 The Drone Operator Is Target #1 29

Lessons from the Use of Drones in the War in Ukraine 30

PART I. Lessons on the Changing Character of Warfare 31

 Lesson 1: Learning the Right Lessons from Ukraine
 Requires Contextual Interpretation, not Mere Observation. 31

 Recommendations 33

 Lesson 2: Different Systems for Different Missions 39

 Employment of UAS Across the Levels of War.....45

 Recommendations 51

 Lesson 3: UxS Employment and Cross-Domain Integration.....55

 Maritime Drones 55

 Uncrewed Surface Vessels 55

 Uncrewed Underwater Vessels 58

 Uncrewed Ground Vehicles 60

 Cross-Domain Integration 62

 Recommendations 66

 Lesson 4: The Web of War—Operation Spiderweb
 and Multi-Domain Vulnerability 69

 Recommendations 72

 Lesson 5: Counter-UAS/EW—War Across the Spectrum 75

 National-Level Defence Against Shaheds Across the Country.....78

 Protection of the Front Line and Troops in Trenches and Vehicles ..80

 Fibre-Optic Drones and AI-Enabled Drones:
 How Do You Counter Them? 82

 Protection of Cities and Critical Infrastructure 83

 Drone Interceptors 86

 What’s Next? 88

 Recommendations 89

PART II. Lessons for Militaries: Adaptation and Preparedness 93

Lesson 6: Organisational Evolution—Change Is Needed.....	93
Women in Ukraine’s Drone War	95
Organisational and Workforce Challenge.....	97
Coordination Between Echelons Is Critical.....	98
Recommendations	101
Recommendations to Local Commanders	103
Lesson 7: Train Everyone, Train Rapidly, Train Continuously.....	104
The Shift in Authority and Training	108
Recommendations	109
Lesson 8: Adapt and Adopt at Speed	112
Combat Adaptation as a Fundamental Military Imperative.....	112
Ongoing Adaptation Cycle	114
Use Case	115
Recommendations	116
Lesson 9: Mass Matters.....	118
Mass Matters through the Lens of Defence	
Workforce and Defence Budget.....	120
Recommendations	123
Brave1	128
Brave1 Market.....	129
Test in Ukraine	129
Ukrainian Council of Defence Industry.....	129
Allyship and Strategic Partnership: the Global Sandbox.....	130
Drone Capability Coalition	131
Recommendations	132
Lesson 11: Build Resilient Defence Industry and	
Supply Chains—Component Localisation Is Key	135
Recommendations	138

PART III. Future Force Lessons 142

 Lesson 12: Future of Drone Warfare—Autonomy, AI and Swarming.. 142

 Rise of Autonomy and AI..... 142

 AI-Enabled Drone Warfare 145

 Drone Swarming 147

 Recommendations 149

Conclusion 153

 A Final Reflection 156

Disclaimer 159

Acknowledgements 159

ABOUT THE AUTHOR.....158

ENDNOTES.....160

ABSTRACT

Uncrewed systems (UxS) operating across air, land and maritime domains have added a new chapter to modern warfare. In Ukraine, UxS have become an important weapon for gaining an asymmetric edge over Russian forces. The lessons learnt from the use of UxS in Russia's war against Ukraine are almost innumerable, reshaping engagements from the individual soldier level through to tactical, operational and strategic command. This paper further extends and advances the findings of the first evidence-based research on UxS employment in the war in Ukraine (covering 2022 to mid-2024), providing updated analysis of developments and lessons learnt between 2024 and mid-2026.

Drawing on data collected between 2024 and 2026—the paper examines how multi-domain and cross-domain UxS have disrupted established concepts of warfare and accelerated cycles of technological adaptation and battlefield innovation. It argues that the pace and nature of UxS development observed in Ukraine is not a temporary wartime phenomenon but a structural shift in how military capability is generated, employed and contested—one with enduring implications for national defence planning worldwide.

This paper provides recommendations for the Australian Defence Force (ADF) and allied partners, including NATO member states, across four interconnected domains: doctrine development, training and workforce planning, capability investment, and acquisition strategy. These recommendations are grounded in the operational realities demonstrated in Ukraine and are structured to address both general lessons broadly applicable to national defence and those with specific relevance to Australia's strategic circumstances, force structure and geographic operating environment. The central finding is that nations willing to adopt an accelerated innovation cycle—learning from, and where appropriate partnering with, Ukraine's defence-industrial ecosystem—are best positioned to maintain a credible competitive edge against near-peer adversaries in both contemporary and future conflicts. For Australia, the window of time to integrate these lessons into capability development and doctrine is now.

/ LIST OF ABBREVIATIONS

ADF	Australian Defence Force
AFU	Armed Forces of Ukraine
AI	Artificial intelligence
BMS	Battlefield management systems
BOS	Battlefield operating system
C2	Command and control
C3	Command, control and communications
CSS	Combat service support
C-UAS	Counter-uncrewed aerial system
ECN	Employment category number
EMCON	Emission control
EMS	Electromagnetic spectrum
EW	Electronic warfare
FPV	First-person view
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HIMARS	High mobility artillery rocket system
DEW	Directed-energy weapons
DIU/HUR	Defence Intelligence of Ukraine, Main Directorate of Intelligence of the Ministry of Defence of Ukraine
HPM	High-powered microwave
IED	Improvised explosive device
ISR	Intelligence, surveillance, reconnaissance
LTE	Long-term evolution
MLRS	Multiple launch rocket systems
OSINT	Open-source intelligence
OWA	One-way attack
MANPADS	Man-portable air defence systems
NATO	North Atlantic Treaty Organisation
OODA	Observe, orient, decide, act
PME	Professional military education
PNG	Papua New Guinea
RF	Radiofrequency
SSU	Special Security Services of Ukraine (also abbreviated as SBU)
TTP	Tactics, techniques and procedures
UAS	Uncrewed aerial system
UAV	Uncrewed aerial vehicle
UCDI	Ukrainian Council of Defence Industry
UGV	Uncrewed ground vehicle
USF	Unmanned Systems Forces [of Ukraine]; unmanned systems forces [generic]
USV	Uncrewed surface vessels
UUV	Uncrewed underwater vehicle
UxS	Uncrewed systems

/ INTRODUCTION

In its fifth year, Russia's full-scale invasion of Ukraine has produced the most operationally significant evidence base for the employment of uncrewed systems (UxS) in the history of modern warfare. Across air, land and maritime domains, the operational integration of UxS has confounded early assessments of their utility as a transient or supplementary capability. Rather than diminishing as the conflict has matured, their proliferation has accelerated—expanding in platform diversity, payload capacity, operational range and multi-domain employment—generating measurable and consequential effects at the tactical, operational and strategic levels of war.

The empirical evidence of their battlefield primacy is unambiguous. Tactical uncrewed aerial vehicles (UAVs) are assessed to account for 60 to 70 per cent of all Russian materiel attrition (damaged and destroyed systems combined) while inflicting approximately 80 per cent of battlefield casualties and providing 86 per cent of all targeting data available to Ukrainian commanders.¹ By any metric of operational effectiveness, they are performing at twice the combined lethality and intelligence utility of every other weapons system in the Ukrainian arsenal. The widespread employment of UxS has fundamentally challenged existing assumptions across multiple domains of military thinking. Concepts of force protection, rear-area security, air defence architecture and the protection of military assets—built on doctrines developed for a different threat environment—have been exposed as insufficient in the face of low-cost, high-volume, precision uncrewed systems. The war in Ukraine is the first conflict in which UxS have been deployed at this scale, tempo and technological sophistication, making it an unparalleled source of operational evidence for defence planners worldwide.

In modern warfare, UxS have shifted from being 'passive observers' to 'active combatants', capable of conducting targeted strikes with pinpoint accuracy.² In fact, 70 per cent of recent armed conflicts globally have involved drone employment as a component of warfighting. In 2010, only three countries possessed armed drones; by 2024, this number had expanded to more than 40 countries.³ Today, 118 nations possess armed military drones. The role of UxS has shifted fundamentally—from that of passive intelligence, surveillance and reconnaissance (ISR) platforms to that of active combatants capable of delivering lethal effects with precision, at scale, and at minimal risk to operators. This proliferation trajectory and the operational lessons being generated in Ukraine carry direct implications for every nation planning for contemporary and future conflict. Ukraine has become the leading nation in rapid innovation, adaptation and industrial transformation of this domain.⁴ In 2022, seven Ukrainian companies were producing approximately 5,000 units annually. By 2025, more than 500 companies were producing

4.5 million first-person view (FPV) drones per year—a production increase of 900 per cent⁵—with the capacity to double output in 2026 should international funding be sustained, potentially reaching 20 million units annually.⁶ Monthly operational consumption by the Armed Forces of Ukraine (AFU) increased from approximately 10,000 units in 2024 to an average of more than 200,000 per month in 2025.⁷



Figure 1. A team of drone operators preparing to perform a mission. Photo credit: 12th Special Operations Forces Brigade Azov, First Corps Azov of the National Guard of Ukraine. Photo reproduced with the owner's permission.

In response to this operational reality, the AFU has undertaken a structural transformation without precedent. It has transitioned from having no formal drone operator specialisation to creating dedicated military occupational specialties for the operation and support of specific types of drones. The workforce structure has incorporated both uncrewed aerial system (UAS) / counter-UAS (C-UAS) units within the AFU (see Figure 1). Most significantly, it has established the world's first Unmanned Systems Forces (USF)—a separate branch of the AFU dedicated exclusively to uncrewed systems operations.⁸ The industry, meanwhile, has begun consolidating from an early proliferation of diverse platform types towards standardisation and modular architecture—a necessary evolution to sustain operational effectiveness at scale and avoid the capability fragmentation that accompanies an uncoordinated 'zoo of drones'.

These developments collectively represent more than tactical innovation. They signal a structural shift in the nature of military competition—one in which the ability to rapidly design, manufacture, field, adapt and counter uncrewed systems has become a core determinant of battlefield effectiveness. Drones represent the convergence of two long-term trajectories in military technology: the increasing precision of weapons systems and the rise of robotics and autonomy. When combined, they deliver lethal effects remotely, at no risk to the operator, and at a cost that fundamentally disrupts the traditional economics of warfare.

Despite the richness of this operational evidence, learning across nations remains largely unstructured and fragmented.⁹ Governments and military institutions are reassessing strategies, doctrines and capability frameworks in response to advanced technology warfare, yet the systematic extraction of lessons from Ukraine's UxS experience has not kept pace with the rate of operational change—hence the focus of this research. The findings of this research may confirm some existing assumptions by Western countries about the role and proliferation of UxS on the modern battlefield. In relation to future force structure and capability acquisitions, this research offers valuable insights into the implications of current and future uses of UxS. The findings are also relevant to the associated logistical demands of achieving survivability among a dispersed force. This paper makes a substantive contribution to the ongoing debate on drone and counter-drone technology and the changing nature and character of modern warfare.

This paper builds on and extends an earlier study, which identified 12 lessons from the employment of UxS in the Russia–Ukraine war between 2022 and 2024.¹⁰ The current research identifies a further 12 lessons from the period of June 2024 to June 2026, advancing the evidence base and updating the analytical picture in light of significant operational, technological and industrial developments during that period. Together, these bodies of research constitute the first longitudinal, evidence-based study of UxS employment in a major conventional conflict.

The overarching aim of this research was to understand how drone warfare has evolved from June 2024 to June 2026 in the Russia–Ukraine war, and to summarise the lessons that can be drawn from it for the ADF and allied partners, including NATO member states. For Australia in particular, the findings offer timely and operationally grounded insight into the capability investments, doctrinal adaptations, training requirements and workforce planning decisions that will determine the ADF's readiness to operate effectively in the uncrewed systems environment that now characterises modern conflict.

This research seeks to answer the following questions:

1. How has the employment of drones and counter-drone systems evolved in the Russia–Ukraine war between 2024 and 2026?
2. What lessons can be identified and learnt from the use of UAS/C-UAS in the Russia–Ukraine war?
3. What recommendations can be drawn from this analysis for the ADF and NATO partner nations?

For the purposes of this paper, the term *drone* is used to refer to an uncrewed aircraft and is used interchangeably with the terms UAV, UAS, remotely piloted aircraft and remotely piloted aircraft system. The term *uncrewed system* (UxS) is used as the overarching concept encompassing air, land and maritime uncrewed platforms. Given that the conflict analysed in this paper remains ongoing, the findings and assessments presented here should not be read as universal or definitive. The lessons identified reflect the evidence available at the time of research; they must be continuously observed, revised and—most critically—translated into the specific operational, doctrinal and strategic context of each nation applying them.

METHODOLOGY

Participants

In total, 38 participants took part in semi-structured interviews conducted as part of this research. All participants were over 18 years old and held either Ukrainian or Australian citizenship. They were drawn from both military and non-military domains, reflecting the interdisciplinary nature of uncrewed systems development and employment in contemporary conflict. Ukrainian participants comprised frontline warfighters with direct operational experience in the Russia–Ukraine war—including personnel who have conducted or directly supported UxS operations—as well as defence industry innovators engaged in the design, development, manufacturing and iterative adaptation of UxS platforms and C-UAS systems within Ukraine’s defence-industrial ecosystem. Australian participants comprised Defence officials, government representatives, and subject matter experts drawn from the UAS/C-UAS sector, the broader robotics and autonomous systems industry, and the fields of modern and future warfare analysis. This cohort provided the research with an informed allied-nation perspective on capability development, force structure planning, and the strategic implications of UxS proliferation—grounding the analytical findings in the specific defence context for which the recommendations of this paper are intended. Figures 2 and 3 show a summary of demographic information.

The research was approved by the Departments of Defence and Veterans’ Affairs Human Research Ethics Committee. All participants provided informed consent prior to their engagement in the research, with the condition of full participant anonymity; accordingly, no identifying information—including names, ranks, roles or institutional affiliations—is attributed to individual participants at any point in this paper. Participants are referenced throughout by their assigned participant number (e.g. P1, P12), consistent with the ethics approval conditions and established qualitative research practice for the nature of the research.



Figure 2. Demographic data: distribution of participants by country of residence.



Figure 3. Demographic data: distribution by area of work.

Materials

This study employs qualitative research methodology. A series of semi-structured interviews was selected as the most suitable approach. This method enabled more information to be elicited and clarification to be sought about the answers, examples and comments provided on the topics of interest. The interview method met the research aims and enabled multifaceted exploration of the lessons learnt from the use of UAS/C-UAS in Russia’s war against Ukraine. It has allowed the production of qualitative data that is sufficiently rich and nuanced to shed light on these complex issues.

Data collected as part of this research is classified as OFFICIAL—that is, available in the public domain. The interview sessions were conducted online or in person and took no longer than one hour to complete. The virtual platforms contained built-in recording functionalities that ensured accurate documentation of interview protocols during the sessions. Some participants preferred interviews to be recorded with written notes. Data from each interview was collected in a re-identifiable format, where any identifiers (e.g. name, workplace) were replaced with a participant number. In this paper, participants' responses are expressed as direct quotes, with reference to their participant number.

Data Analysis

On completion of each interview, the collected data was transferred to secure storage for transcription and translation (20 interviews were translated from the Ukrainian language). A further stage of data interpretation and analysis was conducted using NVivo 14 software for qualitative analysis. The data files were imported into NVivo 14 software, where they were coded. Thematic analysis was employed to identify recurring patterns, themes and insights within the dataset, following Braun and Clarke's six-stage approach.¹¹ This iterative process involved becoming familiar with the data, generating initial codes, searching for patterns, reviewing and refining themes, and writing up the thematic analysis. NVivo's visualisation features were used to generate word clouds and concept maps, which provided clarity around the presentation of results.

/ THE EVOLUTION OF DRONE WARFARE, 2024–2026

The period between mid-2024 and mid-2026 marked a tectonic shift in the character of UxS employment in the Russian war against Ukraine—a transition from what might be characterised as the ‘hobbyist era’ into the ‘industrialised autonomy era’ of systematic, high-tempo, multi-domain uncrewed systems warfare. This evolution was neither linear nor predictable; it was driven by the relentless operational pressure of a near-peer adversary engaged in continuous technological adaptation, forcing innovation cycles that were measured in weeks rather than months or years. Every day, the AFU employs thousands of platforms across the full spectrum of UxS categories—FPV strike drones, ISR systems, loitering munitions, deep-strike drones, heavy multirotor bombers and drone interceptors—each assigned to mission-specific roles within increasingly sophisticated and integrated employment frameworks. The emergence of drone-on-drone warfare that incorporates UxS interceptor platforms has introduced an additional layer to Ukrainian air defence architecture. Concurrently, the broader development trajectory of UxS has accelerated towards greater autonomy, obstacle avoidance capability, and artificial intelligence (AI) integration across guidance, targeting and navigation functions.¹²

An important strategic priority for Ukrainian defence manufacturers during this period has been the deliberate reduction of dependency on foreign-sourced components—most critically, Chinese-manufactured platforms and subsystems—in favour of indigenously produced equivalents (e.g., moving from Chinese DJI Mavic to Ukrainian Shmavik). This has become an important step towards technological sovereignty and sovereign industrial capability. This transition has been both operationally and strategically significant: it has reduced supply chain vulnerability, accelerated iterative platform development, and strengthened Ukraine’s capacity to sustain UxS operations at scale independent of external commercial supply chains. In parallel, tactical UAS employment has undergone continuous and rapid evolution, fundamentally challenging the doctrinal frameworks and procurement architectures of militaries worldwide—demonstrating that traditional, capital-intensive and temporally extended acquisition cycles are structurally ill-suited to UxS development and operational adaptation.¹³

FPV Drones: Expansion at Scale

FPV drones—compact, highly agile quadcopter platforms piloted via head-mounted display systems (goggles)—have become the ‘infantry’ of Ukraine’s drone force, acting as miniature loitering munitions to strike armoured vehicle hatches or chase enemy troops in

close battle. Their ubiquity across the forward line of troops has fundamentally altered the threat environment at the individual soldier level; Ukrainian soldiers have described FPVs as their ‘biggest threat’, citing the density of platforms in the operational airspace as a critical constraint on freedom of movement between and within defensive positions (i.e., to and from trenches).¹⁴

By late 2024, Ukraine had integrated FPV strike drone employment within its assault formations at scale. Dedicated drone companies now exist within brigades, and some assault units report that more than 60 per cent of their deployed assets are drones.¹⁵ FPV drones have become a central pillar of Ukraine's war effort, especially as artillery ammunition shortages have at times limited Ukraine's firepower.

An off-the-shelf Mavic can fly 3km, but with our modifications to the antennas and signal boosters, we can fly them 15km out and 15km back—a 30km round trip—if we are lucky and there is no EW [electronic warfare] interference. What was once my childhood hobby is now a primary means of destroying infantry and equipment. (P6)

The technical architecture of FPV systems has undergone substantial evolution across the period of study. Conventional radiofrequency (RF) control links, previously operating within a limited number of analogue bands, have progressively transitioned to digital video links incorporating frequency-hopping spread spectrum protocols, providing significantly enhanced resistance to interception and electronic countermeasures. Earlier analogue systems were inherently vulnerable—a hostile force aware of the operating frequency could intercept the video feed by tuning a portable receiver to the same band, effectively gaining access to the drone's sensor picture and revealing its intended target and flight path. Digital systems have substantially closed this vulnerability through algorithmic frequency hopping, though the electronic warfare (EW) competition between Ukrainian UxS operators and Russian countermeasures personnel has continued without pause.

Conventional radio-controlled FPV drones haven't lost relevance, however, radio links have changed from certain bands. We transitioned from purely analogue video to digital video links. Analogue video could be intercepted simply by tuning to the same frequency with a portable receiver—you could see the picture and determine the drone's target. One of the counter-drone tactics was that when a drone was detected and you knew which frequency it used (since most video links use one main frequency), you just switch on a receiver with an antenna at that frequency and can see where it's flying and what its target is. Digital is more complex because there can be built-in protection systems, including frequency-hopping spread spectrum, which makes interception significantly more difficult. Within one year of FPV use a lot has changed (i.e., hardware and software changes, different boards, switching to different frequencies). (P33)

The frequency migration of FPV systems between 2024 and 2025 has itself had significant second-order effects on the EW landscape. Operating frequencies dropped into the 300–400 megahertz range at the lower bound, extending to 1,200 megahertz at the upper bound—a substantial expansion from the two primary working bands of 868 and 915 megahertz that characterised operations in 2023. This spectral expansion has imposed considerable demand on EW manufacturers and operators, requiring substantially greater numbers of EW assets to achieve effective coverage across the widened spectrum. In practice, EW coverage along the front remains insufficient to address the full operational frequency range, creating persistent gaps in the electromagnetic protection architecture.

A significant additional development was the proliferation of fixed-wing FPV ‘kamikaze’ drones—systems where FPV-style operator control is applied to a fixed-wing airframe rather than to a multirotor configuration. These platforms represent an elevated threat category by virtue of their aerodynamic differentiation: they exhibit distinct flight characteristics, operate across different frequency bands and communication protocols, and are capable of carrying substantially greater explosive payloads than comparable multirotor FPV systems. An observed employment tactic involves the use of a fixed-wing platform as a carrier: a Russian Molniya fixed-wing drone transits to a designated release point, where it is either landed or suppressed by EW, before deploying a smaller multirotor FPV from its airframe, which then continues independently to prosecute the target. This composite employment method compounds the detection and interception challenge for defending forces. Additionally, a growing number of platforms have incorporated Ukrainian SIM card connectivity—utilising commercial mobile network providers including Kyivstar and Vodafone—to enable real-time operator control or target correction through mobile internet infrastructure, partially bypassing dedicated RF control links.

Shorter-ranged tactical fires have been shaped by Ukrainian improvements in EW employment and the expanded use of FPVs by both Russian and Ukrainian forces. In response to EW-induced guidance disruption, FPV systems have been progressively upgraded with autonomous terminal guidance capability and fibre-optic wire spools—the latter rendering platforms physically immune to electronic jamming by eliminating the RF control link entirely at the terminal phase of flight (see Figure 4).



Figure 4. A drone operated by the 12th Special Operations Forces Brigade Azov, First Corps Azov of the National Guard of Ukraine. Photo reproduced with the owner's permission.

Fibre-Optic Drones

Fibre-optic cables represent one of the most efficient data transmission mediums available, capable of carrying information at speeds approaching the speed of light (see Figure 5). Individual optical fibres can be drawn to diameters comparable to a human hair while retaining substantial tensile strength and delivering data throughput of approximately 32 terabytes per second—properties that, when applied to drone guidance architectures, produce a control link fundamentally impervious to EW disruption.¹⁶

The operational introduction of fibre-optic controlled FPV platforms in the Ukrainian theatre was first documented on 7 March 2024 by Serhiy Beskrestnov (Flash), a prominent Ukrainian military expert specialising in radio electronics and EW. Flash identified that Russian FPV kamikaze drone variants were operating via a thin fibre-optic cable rather than conventional RF broadcast signals—eliminating the electromagnetic signature that EW systems depend upon to detect, intercept and suppress. A week later, Ukrainians replicated this capability.¹⁷ Because control is transmitted through a physical hardwire connection rather than through the electromagnetic spectrum (EMS), no EW countermeasure is capable of disrupting the guidance link; the platform can only be defeated through physical interception or destruction. In January 2026, the typical operating range for Ukrainian and Russian fibre-optic FPV drones was between 15-25 kilometres. Reported cases indicate that the operational range of fibre-optic FPV systems has since increased to approximately 40–50 kilometres, while Russia are reportedly extending this range to as far as 65 kilometres to strike Ukraine's logistical nodes.¹⁸

Ukrainians first developed their own fibre-optic FPV drones in 2022. My company created our first fibre-drone 4 years ago. The problem was the cost of the spool—USD \$1000 for 500m of a cable, which was extremely expensive. Sourcing spools from China, same as Russia, and re-spooling them domestically. Only in 2024–2025, the line of producing optic fibre scaled up from zero. You must have a capable manufacturing line to produce this unique glass string at length of 30–50km from raw materials. (P30)



Figure 5. Launch of a fibre-optic drone. Photo credit: USF. Photo reproduced with the owner's permission.

The tactical implications of fibre-optic UxS employment are considerable and extend well beyond the EW dimension. The hardwired guidance link enables platform employment in environments that would otherwise deny or severely degrade RF-controlled systems—including subterranean operations, built-up areas with significant signal attenuation, and high-EW density environments. Fibre-optic platforms have demonstrated the capability to conduct clearing operations through structures, penetrating hallways, stairwells, and subterranean spaces—environments where RF-controlled FPV systems lose signal immediately upon loss of line of sight to the operator. This dramatically expands the threat envelope to which defending forces are exposed, eliminating the relative sanctuary previously afforded by hardened positions, underground shelters, and fortified structures.

We often send one drone to find and destroy the EW station first, then the rest of the FPV drones follows. Fiber-optic drones have the ability to search buildings, tunnels, downstairs into basements—environments where a non-fibre-optic FPV loses signal and ceases to function. If you have a fibre-optic cable, you can fly down a hallway, descend stairwells, and continue operating underground indefinitely as long as your cable remains attached. That creates an entirely new threat dimension for defending forces. I should just say not even defending the dug in forces, because where you used to be safe, we could have a respite. You just can't now. That has a massive morale and psychological effect. (P13)

The physical characteristics of fibre-optic spools introduce operational constraints that must be understood alongside their advantages. The added mass of the spool reduces available payload capacity and limits platform agility, particularly in densely vegetated terrain where the cable is susceptible to snagging on obstacles. Engagement in heavily forested or overgrown terrain has necessitated reduced airspeed to manage cable routing, increasing platform exposure to visual detection and physical interception by defending forces.

The only way to destroy it is physical. You can't jam a cable. There is a huge demand for hunting shotguns now, because hitting a small object moving at 60 km/h at a distance of 300 meters with an assault rifle is nearly impossible. (P6)

When these systems were moving to strike Ukrainian positions in heavily vegetated areas of Kursk, they were forced to move much slower due to the risk of the fibre-optic cables getting caught or snagged on trees. Consequently, we saw a lot of footage of Ukrainian soldiers spotting these drones as they manoeuvred through the vegetation and simply using shotguns to shoot them down. This highlights that the environment remains a major factor in drone effectiveness. (P20)

Fibre-optic FPVs were employed by Russian forces in the Kursk direction to interdict logistics by bypassing EW coverage. Employment ranges have already exceeded 30 km, though the fibre spool is heavy and bulky. In high-intensity sectors around Pokrovsk, areas were covered with fibre lines—creating secondary mobility effects as cables wrap around vehicle running gear and halt movement; vehicles can move 100 metres and then stop. That is not the main problem, but it illustrates how many second-order effects emerge. Fixed-wing platforms are being adapted for fibre-optic control to exploit the extended range and payload advantages of the airframe over multirotor configurations, pushing operational depth further for both sides. (P33)

The operational versatility of fibre-optic platforms has expanded beyond their initial strike employment. Documented tactical applications include use as sleeping or ambush drones—platforms flown to a designated area, set down, and placed in an observation posture to wait for a target of opportunity before re-launching to engage. This patient, persistent engagement methodology significantly expands the operational utility of the platform beyond a single kinetic mission and imposes a continuous psychological burden on forces operating in or near the target area. Fibre-optic FPV drones are used not only to find and strike, but as ‘sleeping’ or ‘ambush’ drones—fly into an area, land, observe, wait, and when a target appears—vehicles or personnel—they take off and strike. (P17)

Intelligence, Surveillance and Reconnaissance Drones

UxS have proven indispensable for ISR operations across all echelons of the force—from strategic headquarters requiring deep-area persistent surveillance to section-level elements conducting close reconnaissance of adjacent terrain and enemy positions, and micro drones to scout enemy positions, direct fire and gather intelligence. These ‘eyes in the sky’ are now omnipresent over the front, and they have rendered effective concealment of troops and equipment extremely difficult across the depth of the operational area, providing continuous and persistent video feed of adversary dispositions, movement and activity to commanders at every level.

Practically every combat unit in the AFU now has access to live ISR feeds. Reconnaissance quadcopters routinely perform the role of forward observers—hovering over Russian positions to direct artillery and mortar fires with a precision that dramatically increases first-round effect probability and significantly reduces overall ammunition expenditure. This has dramatically increased lethality of artillery—Ukrainian gunners can adjust fire in real time, often using only a few rounds to destroy targets that would have taken dozens of unguided shots before. Small UxS platforms perform close

reconnaissance for dismounted infantry, enabling detailed observation of urban structures, building floors and close terrain without exposing personnel to direct fire. Thermal imaging platforms conduct persistent nocturnal surveillance to detect enemy infiltration, identify personnel in prepared positions, and guide offensive operations under conditions of limited visibility. Both Ukraine and Russia have fielded larger, fixed-wing, military-grade UAVs for operational-level ISR: Ukrainian Shark-M, Leleka-100 and Furia drones provide persistent wide-area surveillance at standoff ranges beyond audible detection thresholds (see Figure 6), while Russian platforms such as the Orlan-10—an 18 kilogram fixed-wing system—perform artillery spotting and targeting with day and night sensor payloads. Notably, drones have also been used as communications relays—hovering at altitude to extend radio links or datalink connectivity over terrain and beyond limitations of ground-based systems. This capability has maintained force communications under conditions of heavy EW, where ground-based radio infrastructure has been disrupted or degraded, and has sustained command and control (C2) connectivity for units operating in complex terrain that would otherwise impose significant communications denial.

The AFU has demonstrated the decisive operational effect achievable through coordinated ISR-to-effects integration. In one documented engagement, an AFU unit employed a fleet of commercial ISR drones to locate a massed Russian armour column, processed the intelligence picture, and coordinated a concentrated artillery barrage within minutes, halting the axis of advance. The Russian combined arms force demonstrated a mirror approach: ZALA ISR platforms conducting persistent surveillance of Ukrainian artillery positions vectored Lancet loitering munitions directly onto identified firing positions immediately following observed fire missions—with the ISR platform remaining on station to perform battle damage assessment and confirm destruction. This *hunter-killer* pairing of ISR and strike platforms—one detecting, one engaging, with continuous closed-loop assessment—has proven operationally effective for both sides and represents a significant evolution in the integration of unmanned ISR and fires at the tactical level.



Figure 6. Shark-M UAV. Photo credit: Ukrspecsystems. Photo obtained from Militarnyi, ‘Shark-M System Equipped with Simulator for Drone Pilots’.¹⁹

Loitering Munitions

Loitering munitions—UxS platforms designed to transit to a defined operational area, conduct autonomous or operator-directed target search, cruise over the targeted area and then strike targets through terminal kinetic attack—have emerged as one of the war’s most operationally impactful UxS categories in the conflict (see Figure 7).²⁰

Unlike small FPVs, loitering munitions typically incorporate significantly greater operational range, larger warhead capacity, and enhanced target acquisition capability, filling a niche between artillery and conventional airstrikes. The ZALA Lancet-3 is extensively used by Russia to compensate for artillery limitations, striking dozens of Ukrainian artillery pieces and even advanced Western tanks at standoff ranges. Similarly, one-way attack (OWA) drones like the Iranian-designed Shahed-136 (or Geran-2 in Russian service) and Ukraine’s indigenous long-range drones (e.g. AN-196 Liutyi or modified Soviet-era Tu-141s) are effectively low-cost cruise missiles. They carry larger warheads over hundreds of kilometres to hit energy infrastructure, and air bases deep in enemy territory. Ukraine’s own loitering munitions and OWA drone employment has achieved strategic-level effects, with documented strikes against targets across the depth of Russian territory—from airbase infrastructure in the Moscow region to fuel storage facilities in Crimea and oil refinery complexes supplying revenue and logistics to the Russian war effort—signalling Kyiv’s growing ‘deep strike’ capability via uncrewed systems.²¹ President Zelenskyy in 2023 hailed these long-range drones as ‘a clear and effective guarantee of Ukraine’s security’ after a series of spectacular drone attacks on Russian bases and even naval ships.²²



Figure 7. UAS SETH loitering munition in use by soldiers of the 12th Azov Brigade, March 2025.
Photo credit: Come Back Alive Foundation. Photo obtained from *Militarnyi*,
‘Ukrainian Defense Forces Hit Two Pantsir Anti-Aircraft Missile Systems With Drones’.²³

A notable case study in this category is Russia's Shahed drone campaign against Ukrainian critical infrastructure. Waves of Shahed-type OWA drones launched by Russia at Ukrainian cities and power stations (usually at night) have imposed a sustained attrition burden on Ukrainian air defence assets despite intercept rates being 92 per cent in May 2026, with plans being made to further increase this rate.²⁴ The residual penetration rate—even at 5 to 10 per cent of a large salvo—is sufficient to achieve a significant cumulative effect against power generation infrastructure and storage facilities. This has forced Ukraine and NATO to rethink air defence: firing a costly Patriot missile at a \$35,000 drone is a poor trade. In response, the AFU and its partners have progressively shifted towards cost-effective intercept solutions—including man-portable air defence systems (MANPADS), anti-aircraft artillery, EW systems capable of jamming or commandeering drone navigation links, and dedicated FPV interceptor platforms—to manage the threat within an affordable and sustainable defensive layering framework. On the battlefield, a vivid Lancet example occurred in June 2023 near Avdiivka: a Ukrainian BM-21 Grad rocket launcher had just finished a fire mission when it came under attack—first from a Russian S-300 missile (which missed) and then from a Lancet drone that 'chased' the vehicle. The Grad crew abandoned the truck and took cover; the Lancet narrowly missed a direct hit. The incident underscored how quickly loitering munitions can be dispatched to threaten artillery after firing. Such experiences have pushed Ukrainian gunners to adopt 'shoot-and-scoot' tactics and camouflage, knowing a loitering drone may be overhead.

Deep-Strike/Long-Range Drones

The growth curve of Ukrainian long-range drones has been extraordinary: from just 110 launched in January 2024 to 7,000 launched by March 2026, with the sharpest growth occurring in 2025, when Ukraine increased launches fivefold over the year. Deep-strike drones, or ‘long-range sanctions,’ have become a principal instrument for the execution of strategic-level tasks, enabling Ukraine to engage high-value targets across the full depth of Russian territory without the operational constraints and attrition risk associated with manned strike aviation (see Figure 8). Ukrainian long-range drone platforms have been tested at ranges exceeding 3,000 kilometres into Russian territory.²⁵

The strategic logic underpinning Ukraine’s deep-strike UxS campaign has been explicitly articulated at the highest levels of AFU command. General Oleksandr Syrskyi, Commander-in-Chief of the AFU, framed the operational rationale in unambiguous terms: disrupting Russian oil export revenue reduces the financial capacity to sustain the war effort; degrading Russian aircraft production facilities constrains the air superiority advantage that enables Russian aerospace operations over Ukrainian territory.²⁶

The technical cycle underpinning deep-strike platform development operates on a compressed timeline relative to more mature acquisition programs, though it remains longer than the extremely rapid adaptation cycles characteristic of FPV systems. Platform evolution across guidance architectures, survivability features and navigation redundancy has been continuous, with development cycles of four to six weeks for major modifications—within which further incremental changes affecting platform tactics and survivability are continuously introduced.

Tactics are more important than the drone itself when launching deep-strike missions. You must carefully map every possible route, assess terrain features, and analyse altitude at all critical points. You have to create a safe corridor for the drone to fly through. This tactical planning is critical. Without it, even the best technology will fail. (P30)

In 2025, the AFU conducted approximately 30,000 deep-strike sorties against Russian revenue-generating facilities (i.e., oil refineries and fuel processing infrastructure), operational ammunition stockpiles, and defence-industrial facilities—with strikes on logistics and transportation nodes—which had the cumulative effect of constraining the flow of materiel and personnel to the front line.²⁷ Between January and May 2026, Ukrainian strikes hit at least 15 Russian oil refineries, leaving nearly 40 per cent of Russia’s primary oil refining capacity offline. By May 2026, intensity had reached new highs: Russia’s defence ministry claimed to have shot down 9,418 Ukrainian drones in May alone, the highest monthly total it has reported since the start of the war.²⁸



Figure 8. Ukrainian long-range drones lined up at sunset before a mission. Photo obtained from UNITED24 Media, ‘Ukraine’s Long-Range Drones Cut Russian Artillery Use in Half, Forcing Warplanes Deeper into Russia.’²⁹

The Russian capital has become an increasingly frequent target and is now ringed by more than 100 air defence systems. Despite this, Ukrainian strikes are getting through with growing regularity, with the most audacious long-range strike on the Moscow oil refinery in the Kapotnya district taking place on 18 June 2026. This oil refinery processes over 11 million tons of oil annually and supplies approximately 40 per cent of Moscow’s total fuel market, including around 70 per cent of the gasoline consumed in the capital and surrounding region. President Volodymyr Zelensky directly stated in a voice message to journalists:

*We do not want this war and never did. But if Ukraine is going to burn, your Moscow will burn too ... it is time to end the aggression, time to end this war.*³⁰

The strategic calculus behind the refinery campaign is significant. Ukrainian officials and analysts estimate that cumulative drone strikes have now taken approximately one-third of Russia’s total oil refining capacity offline—roughly 2.14 million barrels per day. The downstream effects are already visible: fuel shortages have been reported across Russia’s Krasnodar Krai, with over 500 petrol stations in the region running low. Striking energy infrastructure simultaneously degrades Russia’s military logistics—cutting fuel supplies to frontline units—and erodes the export revenues that finance the war machine.³¹

Heavy Multirotors and ‘Night Bombers’ (Bomber Drones)

Night bomber drones (i.e. Baba Yaga, Vampire) have become one of the core components of combat capability, carrying payloads of up to 15 kilograms over a distance of up to 40 kilometres. According to the data from Ukraine’s ‘Army of Drones Bonus’ government program (the ePoints system), the Vampire bomber drone was the most effective strike system on the battlefield in 2025 (see Figure 9).³² These drones are resistant to EW and carry out tasks during both the day and the night. The bomber is employed for remote mining and for logistical tasks, including the delivery of water, food, medical supplies and equipment. Daytime bomber drones are used less frequently because larger platforms are visible and easier to engage with small arms. Hence, smaller bomb-drop platforms are more common during the day, but heavy multirotors can still be employed against high-value targets when required. Russia is also actively developing heavy multirotors.



Figure 9. Vampire bomber drone. Photo credit: SkyFall. Photo obtained with permission from Militarnyi, ‘VAMPIRE Bomber Drone Becomes the Most Effective Weapon on the Front Line in 2025’.³³

A particularly important task is remote mining: instead of striking a target, drones can place mines to deny terrain—especially in poor weather—so that enemy infantry cannot approach positions. This is a critical but under-discussed employment area. Units working at the line of contact understand that before the enemy infantry reaches you, you must saturate likely approaches with mines and disrupt movement as early as possible. (P33)

By 2024, large sections of the Ukrainian front had effectively become no-go zones for supply convoys due to pervasive Russian drone surveillance and fires—any visible movement of trucks drew immediate artillery or drone strikes. In response, some brigades stood up special ‘night drone resupply teams.’ Operating in darkness to evade enemy eyes,

these teams use heavy multirotor drones (e.g. Vampire, R18, Velykyi Banderyk) equipped with infrared sensors to fly supplies to frontline platoons. A single drone can quietly fly a few kilometres to a designated drop point, guided by GPS and the operator's night-vision feed. For example, drone teams can load 15 kilogram sacks of ammunition, food and water onto a Vampire drone each night, ferrying these essentials to infantry hunkered in trenches that trucks cannot reach. Upon reaching the unit, the drone drops the bundle by parachute or low hover and then returns for the next load. This method has kept isolated companies supplied during intense battles. In one case in 2025, a Ukrainian unit surrounded near Avdiivka survived for days on drone-delivered ammunition and rations until a relief operation arrived.³⁴ Another case showed delivery by drone of an electric bike to evacuate a wounded soldier.³⁵ Crucially, using drones for supply reduces risk to human life. Rather than sending a convoy of soldiers down a shelled road, the AFU can send a \$20,000 drone. In this manner, the armed forces risk only the cost of a drone instead of the lives of multiple soldiers. That drone can make multiple trips in a night, and if it is lost, no crew have been harmed. Ukrainian commanders have embraced this as a 'drone-based solution to a drone-caused problem'.

Interceptor Drones or 'Drone-on-Drone' Warfare

Ukraine's development of interceptor drones has rewritten the air war playbook.³⁶ Around 2023, a Ukrainian drone instructor pitched what sounded to troops like science fiction: flying drones to scout enemy drones midair. The soldiers thought it would be impossible to fly a small drone into a fast-moving target. However, truck-mounted and expensive surface-to-air missiles were not sufficient to counter the increasing number of Shaded strikes, escalating the urgency of acquiring an additional pillar of air defence. What seemed laughable has since become a low-cost and critical pillar of Ukraine's air defence.³⁷

In February 2024, warfighters from the unmanned Ayaks 126 systems destroyed a fixed-wing drone with an FPV for the first time. Since then, the tactics of interceptor drones have continued to expand and become a critical component of layered air defence.³⁸ The use of interceptor drones has reduced the saturation of Russian UAVs on the front line, reducing their situational awareness and targeting efficiency.

The enemy also developed its own system. That was expected. Their adaptation created new challenges for us (Ukrainians)—especially how to preserve our ISR capacity and ... [protect] our assets. The technological race is ongoing and characterised by constant change. This does not mean reviewing developments every few months; changes occur on a weekly basis. Lessons identified/ learned in one unit must be rapidly transferred and scaled across others. If something works well, our goal is to institutionalise and scale it across the force. (P33)

Interceptor drones have limited range and explosive power but are significantly cheaper than traditional air defence systems. The cost of an interceptor drone is between US\$1,000 and US\$5,000, whereas an air defence missile can cost hundreds of thousands to millions of dollars. A new, rapidly expanding field of UAS is now dedicated solely to intercepting other drones. The interceptor drones use various methods to down targets, including direct kinetic jamming, firing projectile-based systems or shotguns, and launching nets into the propellers of enemy aircraft. Hence, there has been a return to air-to-air conflict and dogfighting, but conducted entirely by uncrewed systems—‘drone-on-drone’ fights.

Ukraine has emerged as the global leader in the production of specialised interceptor drones. In 2025, Ukraine produced 100,000 interceptor drones, and production has grown eightfold since then.³⁹ Early in 2026, the average daily supply of FPV interceptor drones reached 1,500. The integration of interceptors with radar systems remains the fundamental cornerstone of Ukraine’s modern air defence network in countering massive night attacks by Geran/Shahed-type loitering munitions and other low-altitude threats. Radars provide long-range early detection, transmitting precise real-time coordinates to C2 systems. This enables the automated or semi-automated launch of FPV interceptors, mobile fire groups and other effectors. Without this integration, the efficacy of low-cost interceptor drones plummets, as operators struggle to locate targets at long distances in darkness or fog.⁴⁰

In early 2026, the employment of drone interceptors has evolved from manual operation through the EMS to remote operation. The first confirmed remotely operated drone-on-drone interception occurred during a large-scale Russian strike on the night of 24 March 2026, when remotely operated interceptor drones destroyed Shahed drones. Unlike conventional surface-to-air missiles, which are expensive and limited in supply, drone interceptors can be produced and deployed at scale, helping to address the cost imbalance that has long favoured the attacker. Another advantage lies in operational flexibility. Remotely piloted interceptors allow operators to visually track targets and adapt in real time, which is particularly useful against low-flying and slow-moving drones like the Shahed. This human-in-the-loop approach may complement radar-based systems that can struggle with such targets.⁴¹

In April 2026, Ukraine’s Defence Minister, Mykhailo Fedorov, announced that Ukraine was scaling up remote control technology for interceptor drones, enabling operators to shoot down enemy targets hundreds and even thousands of kilometres away. A key feature of this system is that an operator can operate an interceptor from secure environments—operators are no longer tied to frontline positions. This significantly reduces risks to Ukrainian operators and increases the effectiveness of air defence. Drones can now be operated from Kyiv, Lviv or even abroad.⁴²

In Ukraine, the interceptors are used to strike heavy Shahed-type drones, and light low-flying and slow ISR drones. There are different types of interceptors, as those for striking Shaheds cannot intercept slow ISR drones. Our brigade is using 14 interceptors, 13 of which are Ukrainian made. Whether fixed-wing type, or rocket FPV type, they rely on a combination of detection tools, targeting systems, skilled pilots and operators and, of course, the interceptor drone itself as a strike element. I would summarise that a successful mission in interception depends on pilots' training, not only with flying but also training in working with radar. When two crews—radar crew and main crew—are working together to find a drone, reading a radar and software between radar and ground station is the key to success. We just need a better radar as it allows to see your enemy and your plane and understand where you are and where your enemy is, and you can fly to that position. All producers are also working to full autonomous interceptor drones, but they are not there yet. (P38)

According to the 412th Nemesis Brigade—the top brigade against the enemy's air defence and in intercepting Russian air targets—one in every three Russian air targets destroyed over Ukraine is now brought down by interceptor drones costing less than a used car (see Figure 10).⁴³ Drone-on-drone warfare is evolving quickly.



Figure 10. A team of operators preparing for a night interception mission. Photo credit: 412th Nemesis Brigade. Photo reproduced with the owner's permission.

/ DRONE CHALLENGES

Between 2024 and 2026, drone warfare was reinforced as a constant adaptation contest under intense EW. Widespread jamming and spoofing drove rapid innovation in fibre-optic control, repeaters, alternative navigation methods and autonomy-assisted targeting. No technical advantage proved enduring without continuous modification. Despite the remarkable advantages of drone technology, it brings new challenges the adversary can exploit. Thousands of drones with operators dispersed across different units saturate the battlefield to the point where distinguishing between the friendly and enemy drones can be challenging. It requires careful planning and effective coordination. There are many factors that would affect success in a mission using UAS; however, some of the challenges associated with their use are shown below.

Environmental Factors Complicate Operations

Environmental factors—adverse weather conditions like high winds and heavy rain—further complicate operations. Rain, snow, fog, heat and terrain all influence the effectiveness of drone operations. Electronics react poorly to cold temperatures in winter, which quickly drain their batteries, allowing less airborne time. This is specifically important for Arctic countries, which need anti-icing protection for drones. A layer of ice forms on propellers and wings and destroys aerodynamics below 8 degrees Celsius.⁴⁴

Contrary to common assumptions, drones continue to operate in adverse conditions, including submersion and maritime environments, albeit at higher cost and complexity. Fog, for example, reduces wide-area ISR effectiveness and enables infiltration, while snow reduces foliage cover and increases detectability (see Figure 11). The lesson is that environmental adaptation must be designed into concepts of employment, not treated as an exception. For example, in November 2025, Russians launched an assault on Pokrovsk using a column of vehicles, which would normally have been wiped out by Ukrainian drones. However, dense winter fog obscured visibility for several days and impeded aerial reconnaissance.⁴⁵



Figure 11. A drone operator conducting a mission in snowy weather conditions. Photo credit: USF. Photo reproduced with the owner’s permission.

Snow is a great time to defeat [an] enemy because the leaves [fall] off the trees. Drones are adaptable and you can adapt them to the environment you are operating in. With drones now covering the battlespace, weather has regained its status as a critical factor in military planning. Fog, high winds, and heavy rain might be your ‘best friend’ when planning an attack, as most UAS platforms are currently too light and small to operate effectively in adverse conditions. If you want to conduct an attack, maybe you want to wait for a rainy day, when there are high wind levels and heavy rain and most UAS won’t be flying. (P34)

A UAS Cannot Hold Ground

It is an army cliché: a UAS cannot hold ground.⁴⁶ This requires a human being or at least a ground-based system, whether that be a vehicle, a robot or a person that physically occupies and holds ground. In the eyes of the army, without the ability to hold ground, it does not matter how many drones you have, how far those drones can project or what kind of warhead they can employ. If no one is there to occupy the ground, eventually the battle—and subsequently the war—will still be lost. Hence, a UAS does not completely replace that combatant.

A UAS Has No Self-Defence

A UAS has no self-defence, which can be exploited by the adversary in cyberspace. Two ways of doing this are hijacking drone software to access the data feed and locate enemy bases for strikes, and disabling a drone to make it easier for interceptors to destroy it. Some FPV drone exemplars have been fitted with counter-jamming devices as a result. But this add-on, as in the case of high-performance cameras, substantially increases the cost per drone. Drones only give combatants a decisive advantage until the adversary finds an effective way to counter them. Drone warfare in Ukraine is exceptional in terms of its fast adaptation cycles.⁴⁷

Drone Production Depends on Chinese Components

Unfortunately, a very large number of Chinese components still remain essential in drone production. For some components such as magnets, motors, microelectronics and processors, there is an almost total dependency on China, which retains the global monopoly on them. Although there are manufacturers who have moved to sovereign capability for at least 80 per cent of components,⁴⁸ for Ukraine overall it is still a large problem to find replacements for these components.

There Is No Perfect Weapon

Drones will absolutely perform a range of the roles of some of traditional weapons, but the 'scissors-paper-rock game' is where there is no perfect weapon. Technology always has a vulnerability and UAS are no exception. For example, drones have not taken over the need for combined arms warfighting where artillery, armoured vehicles and infantry are used; now drones just represent another tool.

Drones can't do everything. You still need people there to control the drones (See Figure 12). They're not going to decide themselves on choosing and engaging a target, despite autonomous decision-making, there are pretty substantial legal barriers to having them do that. (P7)



Figure 12. A drone operator performing a mission. Photo Credit: 12th Special Operations Forces Brigade Azov, First Corps Azov of the National Guard of Ukraine. Photo reproduced with the owner's permission.

The Drone Operator Is Target #1

Drone operations do not occur in a vacuum. The success of a drone mission is highly dependent on the skills of its human operator and the technology supporting the drone, such as navigation and communication satellites. Small FPV racing drones are able to glide into trenches or through windows to kill individual soldiers only if they are in the hands of a skilled operator. The most valuable asset in the battlespace is now a drone operator (see Figure 12). It is essential to separate the commander from the operator while maintaining communication. Furthermore, the ground station and antennas must be separated from the operator and the commander because they emit signals that make them targetable. It is similar to the situation in World War II, Vietnam and Korea where the radio operator was always the most targeted.⁴⁹ At present, the operator is separated from the rest of the team right from the start of a mission. If someone is well trained in camouflage and concealment, they can make themselves very difficult to see, though a trained operator can often recognise what another operator looks like through thermal imaging.

/ LESSONS FROM THE USE OF DRONES IN THE WAR IN UKRAINE

Ukraine's hard-won experience with drone warfare in 2024–2026 provides a trove of lessons for Western militaries. The conflict has shown that drones are transforming tactics and force structures, but also that adaptation—in procurement, doctrine and training—is crucial to fully exploit unmanned systems. Below, 12 key lessons, elicited from the expert interviews' most frequent themes, have been grouped into three parts. Part 1 answers the question of how drones are reshaping modern conflict, while Part 2 looks at how militaries should learn, adapt and prepare for war. The section concludes with Part 3 suggesting how forces can sustain combat power and prepare for the next phase of warfare. The discussion of the 12 lessons—all of which are interconnected—emphasises how Australia, its security partners and its allies can apply them.

/ PART I. LESSONS ON THE CHANGING CHARACTER OF WARFARE

Lesson 1: Learning the Right Lessons from Ukraine Requires Contextual Interpretation, not Mere Observation.

Lessons from military conflict do not always provide a template for other nations to follow. This is for reasons of geography, political factors and the strategic circumstances of each conflict. But it is possible to translate the insights from the war in Ukraine if one can define the key characteristics in different theatres through which lessons from Ukraine might be filtered.⁵⁰ Importantly, operational-level deception and the ‘noise’ of the information domain continue to shield critical vulnerabilities and strategic intent from view. While the ubiquity of uncrewed sensors has lowered the threshold for external observation, the strategic depth of the Ukraine conflict remains opaque. Military institutions must distinguish between tactical visibility—accessible via open sources—and operational reality, which remains shrouded by the inherent friction of high-intensity combat.⁵¹ Given the accelerated rate of technological obsolescence, military institutions must adopt a posture of ‘continuous adaptation’, integrating emerging trends into force design and professional military education (PME) in real time, acknowledging that waiting for historical certainty is a luxury that peer-level competition does not afford (see Figure 13).



Figure 13. A drone operator is conducting a mission in snowy weather conditions. Photo credit: Unmanned Systems Forces. Photo obtained with the owner’s permission.

In the 2026 security landscape, the ADF and its allies cannot afford to wait for the end of the war to achieve greater certainty about lessons that need to be incorporated into strategy, doctrine, training and other military affairs.⁵² Instead, we must learn with and from Ukraine and joint initiatives (e.g., the International Drone Capability Coalition, Operation Interflex / Operation Kudu, and Operation Legio) as well as filtering current, albeit incomplete, battlefield insights into our training and acquisition cycles now to maintain a competitive edge in the Indo-Pacific. There are many broader lessons from the war in Ukraine—beyond just lessons from innovations and technology—that must be observed, filtered and implemented in contemporary military endeavours.

In PME and strategic policy, ‘observing’ is passive; ‘learning’ is an active process of identifying the principles that can survive theatre-specific ‘filtering’. According to Major General (Ret.) Mick Ryan, having enhanced visibility of the war from outside Ukraine does not mean that the war is fully transparent to observers. There is much that remains hidden by the tempo of operations, the deliberate efforts of both sides to deceive their adversaries, and the age-old challenge of what Clausewitz described as ‘the fog of war’.⁵³

One of the key lessons is that one cannot apply the same uncrewed systems lessons across every battlefield. What is happening in Ukraine is different from what is happening in Gaza, and that is different again from what a Pacific conflict might look like. Context matters. We need to understand the environment we are operating in, identify and learn lessons from different conflicts, and then apply those lessons appropriately to the specific context. That said, the dominant trends are still small drones, explosive drones, and the ability to penetrate enemy positions. There is also a strong psychological dimension. The sound of a drone alone creates fear. Even if it is unarmed, people assume they are about to be killed. That psychological impact is significant and terrifying, purely from a noise and presence perspective.

Another lesson that needs to be learned is just do it, just do it, just do it! If we want to think about how the Chinese will use FPV and other drones against us (Australia), there's a good way and a bad way to think about that. The bad way is to just think about it. You know, observe how China might be using them against other people and try and learn lessons on a desktop, reading about it or watching videos. The good way is to buy that gear, give it to your own red team so that when you go on exercise, your red force uses it against you. That is the best way, the ‘just do it way’. (P3)

Recommendations

Recommendations to the ADF and Military Leaders

1. Formalise a mandatory ‘identify-translate-learn-implement’ lessons cycle.
 - Move beyond ad hoc, individually held observation towards a formalised, mandatory and institutionally owned lessons cycle to bridge the gap between individual-level awareness and institutional change, and to showcase how current conflicts are informing strategies, policies and training. At present, learning from contemporary high-intensity conflict remains fragmented across the force, retained at the individual or unit level, and lacks any systemic mechanism to ingest, validate and operationalise operational insight at scale.
 - Create or advance a centralised, continuously updated lessons register—accessible across all services and security-appropriate echelons—that tracks each lesson through the full cycle from identification to implementation, with clear accountability assigned at each stage and visible reporting on where lessons have stalled. Critically, this is not a knowledge management exercise; it is a transition from observer status to active implementer status. Validated insight from Ukraine and other contemporary conflicts must be directly and traceably integrated into tactics, techniques and procedures (TTPs) and force structure plans, with a named owner accountable for each integration outcome.
 - Establish a standing analytical function—whether within Army Headquarters, the Australian Army Research Centre, or a dedicated joint cell—tasked specifically with translating Ukrainian lessons through the filter of Indo-Pacific geography, adversary capability and Australia’s own strategic circumstances. Lessons should never be adopted as direct templates; the analytical product must explicitly distinguish between universally transferable principles (e.g., drone saturation effects, EW-driven adaptation cycles) and context-bound tactical detail that does not translate.
 - Adopt a doctrine of continuous adaptation rather than waiting for post-conflict certainty. Doctrine, force design and PME curricula must be structured for live, iterative updates as battlefield evidence emerges from Ukraine, rather than awaiting a definitive historical assessment for which peer-level competition does not afford us the luxury of waiting.
2. Deepen direct engagement with AFU command.
 - The ADF should pursue a tiered, deliberately sequenced engagement model with the AFU to ensure Australian doctrine and training reflect the contested reality of the modern battlefield—not a doctrinally filtered approximation of it.

- Facilitate the secondment of Ukrainian combat commanders (or veterans) to Australian PME institutions to assist with doctrine and training development, so that the ADF can ensure that its training reflects the contested reality of the modern battlefield. Leveraging Ukrainian expertise in co-designing and advising on training development could also be of great benefit to the ADF in keeping up with the pace of changing tactics of UAS use in offence and defence.
 - Tier 1 (gold standard / highest priority): Embed technical advisors in-theatre, subject to political risk mitigation, to capture real-time tactical and technological innovation as it emerges.
 - Tier 2 (enhanced liaison / near-term priority): Expand the scope of Operation Legio (or similar) to include dedicated ‘lessons capture cells’ that prioritise Ukrainian tactical innovations in command, control and communications (C3) and UxS/C-UAS systems employment. This knowledge should feed directly into ADF acquisition and training cycles.
 - Tier 3 (inbound expertise / foundational, immediate action): Formalise the secondment of Ukrainian combat commanders and veterans into Australian PME institutions and doctrine-writing cells, ensuring Ukrainian operational expertise directly shapes—rather than merely informs—ADF training and doctrine development.
3. Appoint a ‘two-star champion’ with a unified mandate and authority to act.
- Five years into this war, the absence of centralised, accountable leadership for the ADF’s uncrewed systems transformation is no longer a tolerable gap—it is a strategic liability. The government and the ADF should appoint a major general (two-star) who can champion this complex area and lead with an unambiguous mandate to synchronise funding, strategy, capability development, resources and industrial engagement across all services. Current efforts remain bottom-up, fragmented and dependent on individual initiative; this must be replaced with top-down, accountable leadership empowered to direct, not merely coordinate. The question remains whether there is centralised leadership at the top level that would be dedicated to care enough about it.
 - The above appointment must carry real authority to resolve the ‘airworthiness paradox’ that continues to throttle capability fielding: small, tactical, attritable UAS should not be subject to the same regulatory and legislative burden as crewed aircraft. The two-star champion must be empowered to define where these systems sit within the Defence regulatory framework and to cut through governance settings that were never designed for a high-volume, attritable systems environment—and to do so with urgency, not through another multi-year review.

4. Close the ‘drone gap’ as a strategic capability priority.

- Rebalance force structure from high-cost, low-volume platforms towards a high-low capability mix as an urgent strategic imperative, not a future aspiration. Mass is now a determinant of battlefield survivability and lethality; a force structure that cannot generate and sustain mass in the uncrewed domain will be at a decisive disadvantage against any peer or near-peer adversary in the Indo-Pacific. This requires the immediate development of comprehensive, service-wide UxS doctrine—not single-service or experimental frameworks—to ensure interoperability with allies and to close current vulnerabilities in coalition and multinational operating environments. Doctrine development should not wait for capability acquisition to mature; the two must proceed in parallel.

5. Leapfrog to the 2026 capability baseline.

- Reject any modernisation pathway that begins at the 2022 baseline of the Ukraine conflict. To do so would be to deliberately repeat a costly and unnecessary learning curve that partner nations have already paid for in operational evidence, and in some cases in lives. Military leadership and capability managers must prioritise immediate adoption of current 2026-validated capability—tactical data links, AI-enabled targeting, EW-resistant drone architectures, communication software and long-range uncrewed systems across all domains. Given the validated maturity of these technologies in active combat use, fielding at the current baseline should be treated as an immediate force generation priority.

Recommendations to Local Commanders

1. Leverage the accessibility of TTP evolution via open-source intelligence (OSINT) to drive bottom-up change.
 - Units should formalise how they observe, document and disseminate OSINT-derived tactical lessons, ensuring that observations are written up, validated and published through appropriate channels to directly influence higher-echelon capability requirements—not left as informal knowledge held by individuals who may post or move on. Learning should be filtered through the commander’s specific operational context—‘train for the fight tonight’. Lessons drawn from Ukraine, Gaza or any other contemporary theatre must be filtered explicitly through the commander’s own operational context before being adopted. Commanders should not passively observe; they must proactively experiment with available UAS/C-UAS technology within current training cycles to close the immediate ‘fight tonight’ capability gap, rather than waiting for formal capability programs to deliver validated

systems years from now. While accessible, OSINT can be biased. Commanders must apply rigorous analysis to ensure that tactical anecdotes and/or myths from social media are not generalised into systemic doctrine without verification.

6. Adopt the ‘just do it’ principle as standing practice, not aspiration.
 - Commanders should not treat observation of adversary drone employment (e.g. Chinese FPV and UAS tactics) as a desk-based, open-source research exercise. Commanders should procure available commercial and military-equivalent drone systems and integrate them directly into red team / red force activity during exercises, ensuring their own units experience adversary-representative drone employment under realistic conditions rather than learning about it second-hand.
7. Integrate the psychological dimension of drone threat into training design.
 - Commanders should explicitly train personnel to manage the psychological effect of drone presence—including the documented fear response triggered by drone noise alone, independent of whether the platform is armed. Training should address this as a distinct readiness requirement, not merely as a by-product of technical or tactical training, given its demonstrated impact on troop behaviour and decision-making under threat.

Recommendations to Government

1. Revise procurement and acquisition models to enable accelerated UxS capability development.
 - To accelerate capability development, the government should move from an ‘expedient acquisition’ model to a ‘deliberate, requirements-based’ model supported by high-quality analytics.
 - Introduce transparent procurement frameworks that focus on standalone modules and can be rapidly acquired, based on standardised technical requirements. This would provide clear funding pathways for sovereign companies.
 - Provide stronger, top-down direction to the Department of Defence to bypass conventional, slow-moving procurement processes, recognising that modern drone warfare is an urgent problem that cannot be resolved through standard multi-decade cycles. Leadership should champion rapid, disruptive change at the ministerial level.

- Review acquisition frameworks and approval thresholds to ensure capability decisions informed by Ukrainian lessons are not delayed by acquisition cycles designed for a pre-drone era of military procurement, recognising that the operational tempo of relevant adversaries will not wait for traditional government procurement timelines.
8. Strengthen regional and international cooperation via partnerships, coalitions, joint research and development, and production with allied partners.
- Government should reframe public and parliamentary communication regarding Australia's contribution to mechanisms like the International Drone Capability Coalition, Operation Legio and similar programs to make explicit the direct return: in addition to supporting Ukraine, it is accelerated, evidence-based learning that strengthens ADF readiness for Indo-Pacific contingencies. This reframing will also support sustained funding commitments amid competing budget priorities.
 - Australia and other member states should deepen their involvement in and contribution to the International Drone Capability Coalition to develop sovereign capability and support joint cooperation. While geographic distances in the Indo-Pacific differ from those in Europe, Australia should seek to offset its industrial weaknesses by specialising in niche areas (e.g. maritime UxS or specific sensor payloads) within the allied industrial base.
 - The government should acknowledge that the 'Ukraine model' of high-volume, low-cost strike is directly applicable to the Indo-Pacific. All types of drones are highly relevant to Australia, specifically across air and sea, including long-range drones, interceptor drones, naval drones, and combined cross-domain drone use. Investment should reflect the reality that drones with 3,000 kilometre range are essential for island-chain control where traditional logistics for platforms like the F-35 are highly vulnerable.
9. Invest in research and development initiatives for defence and national security.
- Establish and fund a Centre of Excellence (CoE) for UAS/C-UAS for defence and national security where innovation can be developed, tested and evaluated in a fast and effective manner. Private startups and defence industry can test prototypes, obtain feedback, and work together with the ADF to refine capability as required.
 - Further strengthen the relationship and feedback loop between defence and industry to accelerate the development, adaptation and adoption of innovations that matter. This would involve standardising reporting, conducting statistical field studies and providing evidence-based assessments to de-bias decision-making. It would allow for research and development, and testing and evaluation of the systems according to the defined problems with agility and at scale.

- Support independent, rigorous analytical capacity separately from single-service or single-agency reporting. Government should ensure funding flows to academic, think-tank and research institutions (including Australian Army Research Centre-commissioned research of this kind) that are positioned to apply the contextual filtering this lesson identifies as essential rather than relying solely on internal military reporting, which may be subject to institutional bias or operational tempo constraints.

Lesson 2: Different Systems for Different Missions

UAS deliver effects across most categories of the battlefield operating system (BOS) spectrum—the framework for how the Army categorises and organises the effects it delivers in the battlespace. The BOS provides a structured way to understand how different capabilities contribute to combat power. These effects range across manoeuvre; C3; ISR; offensive support; information and deception; and combat sustainment. UAS are now capable of contributing meaningfully across this entire spectrum. Importantly, these systems now shape, enable and disrupt every functional component of the battlespace, and conduct various missions at the tactical, operational and strategic levels.

1. Manoeuvre. This encompasses the primary fighting elements—most notably infantry and armoured forces. These are the forces responsible for seizing, holding and controlling ground. Manoeuvre warfare is enabled through integration with sensors and supporting systems that provide situational awareness and targeting information. Manoeuvre warfare in contemporary high-intensity conflict has transitioned from massed combined arms formations to highly distributed, signature-managed force employment. Traditionally, manoeuvre aimed to achieve positional advantage through shock, speed and mass. However, the persistent ISR environment created by ubiquitous UAS has fundamentally altered this paradigm.

In Ukraine, armoured thrusts and battalion-sized manoeuvre elements have proven exceptionally vulnerable to detection by small ISR drones. Once identified, these formations are rapidly engaged through coordinated strike complexes integrating artillery, loitering munitions, and FPV attack drones. As a result, manoeuvre forces have adapted through dispersion, micro-manoeuve and the employment of small assault detachments (3 to 10 personnel) conducting infiltration tactics, often at night and under EW cover. Motorcycle infantry, light vehicle columns and foot infiltration now dominate manoeuvre actions in contested sectors such as Donetsk and Zaporizhzhia.

UAS have become organic to manoeuvre elements, embedded at platoon and company level. Drone operators provide immediate ISR, flank security and target acquisition. This has enabled manoeuvre units to conduct sensor-enabled movement, where every bound, displacement and assault is preceded by drone reconnaissance. The effect is a near-real-time tactical common operating picture at the lowest echelon of command, reducing reliance on higher headquarters and enabling decentralised initiative.

Control of terrain is increasingly achieved through ‘fires dominance’ rather than through physical occupation. Units deny ground by maintaining persistent drone overwatch and strike coverage, creating lethal engagement zones extending 5 to 15 kilometres behind the forward line of troops. Manoeuvre now occurs within this expanded kill web, forcing forces to prioritise concealment, terrain masking, subterranean movement and rapid displacement. Thus, manoeuvre warfare has evolved into ISR-constrained movement under persistent surveillance, fundamentally redefining tempo, mass and survivability.

A persistent myth is that UAS are better than soldiers. That is not the case. The soldier on the ground remains the decisive element of combat power. Soldiers seize and hold terrain; they endure, adapt and persist under conditions that machines cannot. The operational ‘sweet spot’ is therefore not UAS instead of soldiers, but UAS integrated with soldiers in a complementary manner. UAS deliver effects—ISR, precision strike, deception, targeting—that enable the soldier to manoeuvre, survive, and dominate the ground fight. UAS are constrained by battery life and technical limitations. Soldiers, by contrast, are sustained through logistics and discipline, enabling them to endure over time. That endurance remains central to victory. In short, UAS enable effects; soldiers deliver decisive outcomes. (P20)

2. Command, Control and Communications. This function underpins all other operating systems, ranging from the dissemination of orders prior to an operation to the technical communications networks that integrate platforms and enable coordination between individuals and units. Effective C3 is essential for synchronising combat power across the force. In Ukraine, C3 systems operate under constant pressure from EW, cyber operations, kinetic strikes, and EMS denial.

UAS are now deeply embedded within C3 architectures. Live drone feeds are integrated into battalion and brigade command posts, digital battle management systems (e.g. Delta) and artillery fire direction centres. This enables commanders to conduct dynamic targeting, battle damage assessment and real-time force re-tasking. The decision-action cycle of ‘observe, orient, decide, act’ (OODA loop) has compressed dramatically, allowing engagement of time-sensitive targets within minutes rather than hours. However, this digital integration has produced new vulnerabilities. Drone ground control stations, relay nodes and satellite terminals (e.g. Starlink) have become priority targets.

To mitigate this, forces employ redundant communications pathways, including mesh networks, civilian long-term evolution (LTE) infrastructure, fibre-optic tethered drones and courier-based data transfer. Commanders must assume intermittent communications, degraded situational awareness and delayed reporting. These conditions reinforce the importance of commander’s intent, pre-delegated authorities and autonomous subordinate leadership.

3. Intelligence, Surveillance, and Reconnaissance. ISR focuses on detecting and understanding the adversary. This includes collecting indicators and information that feed into intelligence analysis, typically conducted by intelligence cells. The resulting assessments inform the commander’s understanding of enemy intent, capabilities and likely courses of action, shaping decision-making and execution.

ISR in Ukraine has undergone a paradigm shift from episodic reconnaissance to persistent battlespace surveillance. UAS operate continuously across tactical, operational and

strategic levels, creating unprecedented transparency. Small quadcopters conduct close reconnaissance, while fixed-wing UAVs provide deep ISR out to 100-plus kilometres. ISR has become fully integrated into strike operations through the sensor-to-shooter kill chain.

The traditional separation between reconnaissance and strike has collapsed. FPV drones increasingly perform dual ISR-strike roles, conducting target confirmation before executing terminal attacks. This has produced a 'reconnaissance-strike complex' where detection almost guarantees engagement. However, ISR dominance has triggered an active counter-ISR battle. Adversaries employ decoys, camouflage, multispectral concealment, terrain masking and deception operations to degrade drone effectiveness.

4. Offensive Support. This is another core operating system. Traditionally, it refers to the employment of high-explosive fires to engage enemy forces or cannon artillery, but it now includes rocket systems such as multiple launch rocket systems (MLRS) and high mobility artillery rocket systems (HIMARS). In Ukraine, offensive support remains dominated by artillery fires, reinforcing its continued relevance in high-intensity conflict. Despite this, UAS are increasingly fulfilling roles within offensive support. Offensive support remains dominated by artillery, which continues to account for the majority of battlefield casualties. Tube artillery, MLRS and precision rocket systems (HIMARS, Tornado-S) deliver massed and precision fires across depth. What has changed is that UAS now form the backbone of artillery employment. Drone observers conduct target acquisition, fire adjustment, post-strike assessment and counter-battery spotting. This has increased artillery lethality and reduced ammunition expenditure through precision correction. The introduction of loitering munitions and FPV strike drones has further expanded offensive support options, allowing commanders to engage armoured vehicles, bunkers, EW systems and infantry positions with high precision and low cost. Ukraine has effectively created a distributed fires network where FPV drones function as micro-precision strike systems. These are employed to destroy armoured vehicles, neutralise artillery pieces, suppress infantry positions and conduct deep interdiction strikes. This 'drone artillery' complements traditional fires and allows engagement of targets that are masked, mobile or beyond the reach of conventional systems. The fires domain has also become highly contested. Both sides conduct counter-battery radar operations, drone-enabled artillery hunting, targeting of ammunition depots, and strikes on drone operators and fire direction centres. Offensive support has therefore evolved into a multi-layered fires ecosystem, integrating cannon artillery, rocket systems, loitering munitions and FPV strike drones into a single kill web.

5. Information and Deception. UAS have emerged as a critical enabler of information and deception operations, fundamentally reshaping how military forces influence adversary perceptions and decision-making processes. Their value extends well beyond kinetic effects, as they increasingly operate as cognitive and informational weapons that shape the behaviour of opponents across tactical, operational and strategic levels of warfare.

Persistent ISR enables forces to track enemy movements and identify command nodes, logistics hubs and patterns of life, while simultaneously imposing psychological pressure on adversaries who are aware—or strongly suspect—that they are under constant surveillance.

UAS also play a central role in deception operations by functioning as decoys and false signatures. They simulate strike packages, trigger air defence systems and expose radar positions. By presenting fabricated threats, forces can manipulate adversary responses, compel premature engagements and exhaust interceptor stocks. This deliberately distorts the enemy's situational awareness, causing commanders to misallocate defensive resources and react to false attack axes while real manoeuvres unfold elsewhere. In this way, UAS actively engineer enemy decision-making rather than merely observing it.

The psychological dimension of UAS employment is equally significant. Persistent drone presence over frontline units, harassment flights, and deep-strike demonstrations into rear areas reinforce a sense of vulnerability and inevitability. The publication of strike footage further amplifies these effects, eroding morale and reinforcing narratives of technological superiority. The battlefield becomes increasingly transparent and psychologically contested, where fear of detection shapes behaviour as much as physical threats.

6. Combat Sustainment, or Combat Service Support (CSS). This is the BOS responsible for generating, maintaining and regenerating combat power throughout the conduct of operations, enabling sustainment, resupply and logistics. While manoeuvre and offensive support deliver kinetic effects, sustainment determines whether a force can remain in contact, exploit success and endure protracted engagements. Doctrinally, CSS is a warfighting function, not an enabling afterthought. Without assured sustainment, combat power rapidly culminates. CSS encompasses the full spectrum of logistics and support functions. Support functions primarily relate to logistics and sustainment—the enablers that allow all other BOSs to function. This includes supply, transport, maintenance and medical support. Without these elements, manoeuvre, fires and command systems cannot be sustained.

In Ukraine, CSS has transitioned from a rear-area function to a contested forward battlespace activity. Logistics hubs, ammunition points, fuel farms and maintenance areas are persistently targeted by long-range fires, loitering munitions and ISR drones. As a result, sustainment nodes are forced to operate in a highly dispersed posture, relying on mobility, camouflage, deception, and emission control (EMCON) to survive. Uncrewed systems have become a critical enabler of sustainment under these conditions. Small multirotor UAS are now routinely employed for last-tactical-mile resupply to platoon- and section-level positions. This includes delivery of small arms ammunition and grenades, FPV batteries and payloads, medical supplies and tourniquets, rations and water, and communications equipment.

Uncrewed systems can augment conventional logistics, improving battlefield resilience. They also illustrate the need for new doctrine and training for ‘drone logistics operators,’ who blend aviation, signals and supply expertise. Recognising this, Ukraine in 2023 began integrating drone operations into its logistics command structure, and Western armies are observing closely. NATO allies have even trialled Ukrainian drones for their own resupply use cases—for instance, Ukrainian technology firms demonstrated drone delivery of medical supplies to NATO observers in 2024 exercises.

Since late 2024 to early 2025, uncrewed ground vehicles (UGVs) have been very actively used in logistics—specifically when delivering supplies to dangerous and high-risk areas for both soldiers and vehicles. UGVs are small and low profile, and have a high success rate. There are positions where soldiers may remain for 90 to 120 days and resupply cannot be done by crewed vehicles. In these scenarios, drones deliver ammunition, water and food in small loads repeatedly. Drones are also essential for certain river-crossing environments, where delivery is conducted primarily by drones. Evacuating wounded personnel is a major problem. In some cases, wounded personnel may remain for days because evacuation vehicles cannot reach them without being struck by drones. Ground robotic platforms equipped with EW, intended to suppress the channels used by kamikaze drones and drop drones, can drive to a position, load a casualty onto a trailer, and extract them while providing EW protection. Such robots can also deliver supplies and ammunition and can carry substantial payloads.

The land domain remains the most challenging. While UGVs struggle with tactical manoeuvre in complex terrain (jungle, urban or mud), they are finding immense success in non-combatant roles such as casualty evacuation and logistics resupply (moving food, water and fuel), reducing the risk to soldiers by performing ‘the last 300 metres’ of a dangerous task. Currently in Ukraine, logistics resupply is done by uncrewed systems (i.e. ground logistics robots), while casualty evacuation is carried out exclusively by ground robotic systems. The main purpose of these UGVs has been to minimise participation of Ukrainian forces on the battlefield, helping to preserve the lives of Ukrainian soldiers. Anything that is large can be easily detected and destroyed. Furthermore, bringing a heavy vehicle to the front line is a logistics challenge as it requires fuel or batteries to charge. Due to the increased number of UAS, the kill-chain distance has increased to up to 30 to 40 kilometres from the front line. Uncrewed systems represent a shift in logistics and resupply processes by supporting warfighters in high-risk missions.

The use of logistics drones is still evolving, but Ukraine’s experience has highlighted both possibilities and limits. On the positive side, drones have greatly increased the flexibility and resilience of supply lines. Ukrainian logisticians have had to ‘think outside the box’—literally deploying civilians’ octocopters as military transports. The army has worked with drone manufacturers to boost the payload capacity and range of logistics UAVs (e.g., developing drones that can lift 20 to 30 kilograms and travel dozens of kilometres).

They have also established procedures for coordinating drone deliveries: drop zones are selected carefully and timed with frontline units to avoid exposing soldiers (e.g., units are alerted via radio to retrieve a drop only when enemy observation is minimal). On the downside, current drones can only carry limited weight—a 15 kilogram payload might equate to a ‘middling stream of rifle ammunition, some sausages, energy drinks, and cigarettes’ for troops (P4). Heavier equipment (like artillery shells or fuel) still demands ground transport or crewed aviation. Weather is another constraint; high winds or freezing rain can ground drones, whereas a truck might still drive through. Thus, Ukraine continues to use traditional trucks and helicopters when feasible, but drones have become a critical adjunct especially for the ‘last mile’ to units in contact.

In war, in humanitarian operations—logistics is the foundation. Australia is enormous geographically. Your postal system must work perfectly, or you must have alternative delivery methods. I know you have railway networks, but there is only one main line running from the east coast to the north. This creates vulnerabilities. Logistics wins wars. Not technology alone—logistics. (P30)

Drones also support medical sustainment. While rotary-wing medical evacuation remains doctrinally preferred, contested airspace and MANPADS proliferation have limited its employment. UAS are increasingly used for forward medical resupply, including trauma packs and blood products, and for route reconnaissance prior to casualty evacuation. This enhances casualty survivability by reducing response time and enabling risk-informed extraction. From a sustainment intelligence perspective, ISR drones enable logistics battlespace management. Commanders use UAS to conduct route clearance reconnaissance, identify interdiction threats, monitor convoy movement, assess damage to main supply routes, and detect enemy attempts to interdict supply lines.

This creates a sustainment paradox: UAS reduce risk to human logisticians but dramatically increase the technical sustainment footprint. The Ukrainian experience demonstrates that logistics tempo dictates drone tempo, and drone tempo dictates combat tempo. Units that lose sustainment continuity rapidly lose persistent ISR coverage, fires cueing capability, early warning, Counter-UAS capacity. This degradation cascades across all BOS elements—manoeuvre, offensive support, and C3—often within hours. The decisive advantage lies with the force that can regenerate capability under attrition. Combat Sustainment has therefore become a frontline warfighting function, central to endurance, tempo, and operational success in modern high-intensity conflict. (P20)

Employment of UAS Across the Levels of War

Table 1 provides a summary of UAS employment at tactical, operational and strategic levels.

Tactical Level

An important development of 2024–2026 was the simultaneous employment of drones across all levels of war. At the tactical level (i.e., squad, platoon and company), Ukrainian troops have been using FPV drones for OWAs and as disposable ammunition that can loiter prior to striking their target (see Figure 14). This type of human-guided munition conducts real-time video transmission to its operator—first-person control that enables precision and responsive manoeuvring. In 2025, specifically, fibre-optic variants became dominant in ambush, close combat and point-target strike roles. Weaponised quadcopters with hand grenades, mortar shells and anti-tank missiles have become anti-personnel and anti-tank/anti-armour weapons.⁵⁴



Figure 14. A drone operator sets up an FPV drone at an improvised airstrip. Photo credit: USF. Photo reproduced with the owner's permission.

At the tactical level, UAS performs nearly any role a frontline combatant would. This includes ISR and strike (traditionally achieved by mortars and artillery) or air power, C3 (establishing relay links and providing direct situational awareness to commanders), and mobility/counter-mobility (using infrared cameras at night to identify the heat signatures of landmines—which hold heat longer than the ground—and placing precision landmines).

In Ukraine there are many mobile FPV tactical groups, who operate 10–20kms behind the zero line (see Figure 15). When needed, they move forward and deploy their ground control stations that consist of large antennas and are used to control drones deep into enemy territory. If the enemy is close, or if there are no terrain obstacles such as earth curvature, hills, or urban structures, operators can work directly. If not, Ukrainians use a relay model, called a repeater. In this model, a relay drone stays in the air and re-broadcasts the signal from the ground station to the FPV drone. For this task, you need a dedicated reconnaissance group operating scouting drones and a separate relay group operating repeater drones. A single pilot alone is not sufficient. Effective operations require team support, coordination, and multiple specialised roles. You need a team to cover you, a driver, a vehicle fully equipped with jamming systems, when operating closer to the zero line. You need a technician who installs the antennas and connects all cables. You need an FPV pilot. You need a specialist who prepares the grenades and warheads. You need a commanding officer who maintains situational awareness, understands what is happening on the battlefield, and makes decisions in real time. So, it takes many people to accomplish a single mission—for example, destroying Russian positions in a trench. This is a highly complex operation, and it demonstrates the true nature of tactical drone employment. (P30)



Figure 15. Magyar's 'Birds' team performing a mission. Photo credit: Magyar Birds. Photo reproduced with the owner's permission.

A drone equipped with electro-optical (EO) and infrared (IR) cameras, as well as unmanned ground vehicles (UGVs), represents a different tactical application altogether. These systems require separate operational concepts, different training programs, and distinct performance metrics. Each platform is designed for specific mission profiles. Different drones are optimised for different target sets, and therefore each requires its own tactical employment model. In other words, mission success depends on matching the right platform to the right task and applying the appropriate doctrine, training and operational procedures for each system. (P30)

Operational Level

At the brigade and battalion levels, the Ukrainian defence forces use fixed-wing drones for long-range reconnaissance or OWA strike (see Figure 16). These drones significantly enhance target acquisition due to their range and reduce time between detection and an attack to three minutes in some cases. The long-range reconnaissance drones are most useful for strategic planning and precision strikes on high-value targets, as they can conduct surveillance and intelligence with high-resolution cameras for up to 24 hours.

This involves targeting and ‘shaping in the deep.’ Ukraine uses UAS to strike logistics hubs and headquarters nodes tens of kilometres behind the front. A widely applied example is the use of small drones far behind enemy lines to target exquisite deep-strike aircraft on Russian runways. This destroys the enemy’s ability to provide standoff air bombing and shapes the battle space. Operationally, dedicated drone formations have emerged with the depth and endurance to conduct sustained campaigns rather than episodic strikes. These units focus on counter-UAS, logistics interdiction and the degradation of enemy drone ecosystems.

One of the biggest disruptions we observed from drones was not actually right on the front line, but just behind it. Often, the soldiers on the front line—at the zero line—are in cover and are reasonably well-concealed, which makes them quite difficult to target with drones. Instead, the greatest impact was occurring in the area roughly between 5kms to 15kms behind the front line. This had a major disruptive effect, particularly on force rotation. Previously, Ukrainian forces would typically spend about a week on the front line before rotating back. However, it became so dangerous to move personnel to and from the front that, combined with personnel shortages, those rotation periods were extended again and again. This was largely because it had become extremely dangerous to move people in that environment. (P25)

At the operational level, the focus shifts to targeting. The operational level in a military construct, in regard to striking, targeting and ‘shaping in the deep’, is associated with the logistics nodes and caches as well as C2 or headquarters nodes in the deep. The focus at operational level is to destroy those and use the long-range fires capabilities. Ukraine is moving its headquarters nodes tens of kilometres rearward because there is a threat of being targeted by Russian UAS.

Operationally, this is enabling strikes in depth against logistics nodes and command and control elements. We are also seeing increasingly deliberate targeting of ground control stations. As a result, drones are not only being used to strike ground targets, but also increasingly being used against other drones. This dynamic is having a significant operational impact. Drones have been used as a primary logistics means to resupply isolated forces on the islands. We saw up in Kursk, when Russians were able to disrupt Ukrainian logistics up the highway. Drones have become a major source of logistics just even for quite large-scale forces. (P25)



Figure 16. A drone operator preparing a drone for launching. Photo credit: USF. Photo reproduced with the owner’s permission.

Strategic Level

Drones may impact the way the war is being conducted, but they do not shape its outcomes. Strategically, long-range drones were used to strike infrastructure, oil refineries, air bases and symbolic targets deep inside enemy territory, linking battlefield action to economic and political pressure (see Figure 17).

Whoever can generate and maintain a drone advantage will maintain momentum. However, the strategic effects of such strikes remained contested, reinforcing the lesson that drones alone do not decide wars, but shape the conditions under which broader strategies succeed or fail. (P34)



Figure 17. Preparing a heavyweight drone for a night mission. Photo credit: USF. Photo reproduced with the owner's permission.

One strategic employment of UAS is the targeting of critical national infrastructure (though it is arguable whether this is operational or strategic). In daily reports there is news about deep strikes of hundreds of Shahed drones and ballistic missiles targeting Ukrainian cities and Ukrainian infrastructure. Ukraine is also targeting Russian oil facilities, training depots and ammunition depots: a strategic use of a larger UAS with the same capability. Experts mentioned several examples of the strategic use of drones, as shown in Table 1.

Table 1. UAS technology application at tactical, operational and strategic levels

Level	Functions	Examples	Requirements	Limitations
Tactical (from squad to battalion)	• Tactical ISR in real time • Fire correction • Local strikes (FPV) • Patrolling, control of terrain sectors • Communications • Logistics	• FPV attack on armour and personnel • Night ISR for artillery correction • C3 relays • Delivery of ammunition and other cargo to forward positions • Placement of precision landmines; use of infrared cameras to detect mine heat signatures	• Rapid operator training • Reliable communications or autonomous modes • Mobile logistics (spare batteries, motors, controllers, video cameras etc.)	• Limited range • Vulnerability to EW • Weather and terrain constraints
Operational (brigade, operational group)	• Coordination of swarms/packages • ISR in operational depth • Synchronisation with artillery/aviation • Strikes on logistics nodes • Integration into C2 (BMS)	• Reconnaissance swarm detection of supply node → package of strike drones + artillery • Coordinated strike on a railway segment • Targeting logistics caches and headquarters nodes tens of kilometres behind the front	• Centralised/distributed C2 systems • Compatible comms protocols and ISR integration • Backup channels and autonomous modes in EW	• Need for tight coordination • Vulnerability of critical communications • Risk of decision-making • Delays
Strategic (higher Headquarters, theatre)	• Strategic strikes on critical infrastructure • Mass operations to exhaust enemy logistics • Deterrence support • Building of national industrial base • Geopolitical influence	• Strikes on oil facilities, energy infrastructure, airfields, strategic aircraft, air defence, fuel/ammunition depots • Maritime drones to disrupt sea logistics • Mass operations undermining enemy supply	• Strategic production infrastructure • Coherence between industry, intelligence and policy • Legal/ethical assessment of deep-rear operations	• Political/legal escalation risks • High dependence on supply chains • International consequences of rear-area attacks

Recommendations

Recommendations to the ADF and Military Leadership

1. Integrate UxS across all BOS formally, not as a bolt-on capability.
2. Select the relevant UxS capability with explicit reference to which BOS function(s) a given platform is intended to support. Force design must account for the fact that a single class of platforms (e.g. FPV strike drones) can simultaneously deliver ISR, fires and deception effects. Identify relevant capability tiering for the theatre of operation: different systems for different missions.
 - Conduct detailed, theatre-specific analysis to identify gaps and opportunities for the employment of different uncrewed systems against different mission sets within the Indo-Pacific theatre of operation specifically, rather than adopting a generic or one-size-fits-all UxS capability model. This requires acquisition of uncrewed systems across all relevant domains and levels of war—UAS for the air domain, UGVs for the land domain, and uncrewed surface and underwater vessels (USVs/UUVs) for the maritime domain—tiered explicitly for tactical, operational and strategic mission requirements.
 - A central priority within this tiering could be the expansion of long-range UxS capability that is cheap enough to scale, precise enough to matter, and numerous enough that some platforms will always penetrate adversary defences. Producing and fielding thousands of long-range strike drones can generate credible deterrence without requiring the force structure or cost base of a superpower-sized air force. Critically, it creates the ability to impose cost on an adversary from the first minute of aggression. Given Australia's strategic geography, UxS should be explicitly framed and resourced as a critical tool for island-chain control, particularly in scenarios where traditional crewed assets may be grounded or denied by logistical disruption.
3. Develop dedicated doctrine and force structure for combat sustainment via uncrewed systems.
 - Given that combat sustainment has shifted from a rear-area function to a contested forward battlespace activity, the ADF should develop dedicated doctrine, training pathways and force structure for drone logistics operators—a discipline blending aviation, signals and supply expertise that does not currently exist as a formal specialisation. This should include integration of small multirotor UAS for last-tactical-mile resupply and UGVs for casualty evacuation and resupply to high-risk forward positions, recognising that sustainment tempo now directly dictates combat tempo. Given Australia's geographic scale and limited inland logistics redundancy

(rail, road), this lesson carries particular weight for ADF force design and should be prioritised accordingly rather than treated as a lower-tier capability investment behind strike systems.

4. Implement the ‘rifle section’ model of drone teaming.

- The Ukrainian experience demonstrates conclusively that there is no single ‘silver bullet’ drone and that uncrewed systems are most operationally effective when integrated as a combined arms team mirroring the proven structure of an infantry section. The ADF should adopt this teaming construct as a standard force structure and training model, comprising:
 - the **scout**: long-endurance air and naval sensor platforms (including solar- or wave-powered systems for extended persistence) functioning as the team’s primary detection and situational awareness asset
 - the **automatic weapon**: high-volume FPV strike drones employed for suppression and mass effect, mirroring the role of a section’s automatic weapon in generating sustained suppressive fire
 - the **grenadier**: short-range ‘dropper’ drones for immediate tactical disruption, analogous to a grenadier’s role in close-quarters disruption of enemy positions
 - the **sniper**: long-range precision loitering munitions reserved for high-value target engagement, mirroring the selective high-value engagement profile of a section’s designated marksman.
- This model should directly inform unit establishment, training design and equipment scaling at section and platoon level, ensuring UAS capability is fielded as an integrated team function rather than as individual, disconnected platforms.

5. Redesign C3 architecture for assumed degradation, not assumed connectivity.

- Redesign C3 architecture on the explicit assumption that ground control stations, relay nodes and satellite terminals (including commercial systems such as Starlink) will be priority enemy targets and will be degraded or denied during operations. This requires institutionalising redundant communications pathways—mesh networks, civilian LTE infrastructure, fibre-optic tethered systems, and courier-based data transfer—as standard operating architecture, not contingency planning. Critically, this should be matched by a cultural and doctrinal shift towards pre-delegated authorities and decentralised command, since commanders should be able to fight effectively through intermittent communications and degraded situational awareness rather than assuming continuous connectivity to higher headquarters.

Recommendations to Local Commanders

1. Treat UxS employment as platform specific, not generic.
 - Recognise that different UxS platforms—electro-optical/infrared equipped ISR drones, FPV strike drones, fibre-optic variants, fixed-wing long-range systems, USVs/UUVs and UGVs—require distinct operational concepts, training and performance metrics, and cannot be treated as interchangeable ‘drone capability’. Commanders should ensure mission planning explicitly matches platform type to task, applying the specific doctrine and procedures relevant to each system rather than defaulting to a generic UxS employment model.
2. Build and train dedicated multi-role drone teams, not individual pilots.
 - Recognise that effective tactical-level UxS employment requires a coordinated team—including reconnaissance/scout operators, relay (repeater) operators, a vehicle and security element with jamming capability, a technician, a payload specialist, and a commanding officer maintaining real-time situational awareness—rather than a single pilot operating in isolation. Local-level training and exercise design should reflect this team-based reality, and force generation planning should resource and train for the full team structure rather than individual operator qualification alone.
3. Institutionalise sensor-enabled movement as standard practice.
 - Embed UxS as organic to manoeuvre elements at platoon and company level, ensuring every bound, displacement and assault is preceded by drone reconnaissance. This ‘sensor-enabled movement’ approach should become standard operating procedure, enabling a near-real-time common operating picture at the lowest echelon and reducing dependency on higher headquarters for tactical decision-making.
4. Apply disciplined EMCON and signature management to C3 and sustainment nodes.
 - Apply rigorous EMCON, camouflage, dispersion and deception discipline to ground control stations, command posts and logistics/sustainment nodes, recognising these as priority targets under persistent ISR coverage. Commanders should plan resupply and casualty evacuation with explicit reference to enemy ISR and strike coverage, including timing drone drop-offs and pickups to periods of minimised enemy observation.
 - Resource and rehearse UAS-enabled casualty evacuation and resupply now. Given documented cases of wounded personnel remaining static for days due to the danger of conventional evacuation, commanders should proactively integrate UGV-

and UAS-based casualty evacuation and ‘last 300 metres’ resupply capability into current training and contingency planning, rather than waiting for these capabilities to be issued through formal force generation cycles.

Recommendations to Government

1. Prioritise sovereign development of cross-domain, multi-echelon UxS capability with clear strategic-level application.
 - Invest in direct sovereign capability development towards systems with demonstrated strategic-level utility—particularly long-range strike and deep ISR platforms capable of targeting critical infrastructure and high-value nodes at extended range, recognising that strategic-level UxS employment can be considered most directly relevant to Australia’s strategic circumstances. This should be paired with deliberate investment in the supporting C3 and ISR architecture required to compress the sensor-to-shooter decision cycle, without which strike capability alone delivers limited operational value.
2. Fund dedicated training pathways for drone logistics and multi-role drone team specialisations.
 - Resource the establishment of formal training pathways and trade structures for ‘drone logistics operators’ and multi-role tactical drone teams (reconnaissance, relay, technical and command roles), recognising that these are now distinct professional disciplines requiring dedicated career and training pipelines rather than ad hoc, on-the-job skill development.

Lesson 3: UxS Employment and Cross-Domain Integration

The use of technology in the war in Ukraine began with aerial drones and will continue with maritime and ground-based ones. Further innovative uses of drones may herald the proliferation of multi-domain drones and may even introduce a third drone age defined by full-spectrum drone warfare. While UAS were well discussed in the sections above, the focus of this lesson is on their integration with other domains and their employment in multi-domains.

Maritime Drones

Uncrewed Surface Vessels

Despite lacking large operational warships, Ukraine has successfully employed USVs and cruise missiles to harry Russia's Black Sea Fleet. In late 2024 and early 2025, Ukraine began arming naval drones with missiles and anti-air weapons, essentially turning unmanned boats into mobile launch platforms.⁵⁵ In a world-first feat, a missile-equipped Ukrainian naval drone reportedly shot down several Russian helicopters over the Black Sea in January 2025.⁵⁶ In May 2025, Ukrainian officials announced that naval drones carrying anti-aircraft missiles had even downed two Russian fighter jets—a remarkable extension of drone capabilities across domains.⁵⁷ These developments highlight Ukraine's innovative use of drones at sea to offset Russia's numerical advantages.

Ukraine primarily uses two USV families: the agile Magura V5 multi-purpose USV, developed by Ukraine's Main Directorate of Intelligence (HUR) intelligence service (Figure 18), and the Sea Baby, developed by the Special Security Services of Ukraine (SSU) and built for heavy kamikaze payloads. Between 2024 and 2025, the primary evolution was weaponisation of USVs and subsurface maturation. The new generation of Sea Baby are equipped with an advanced navigation system and are capable of covering over 1,500 kilometres with up to two tons of cargo. The first variant is equipped with a gyro-stabilised machine-gun mount featuring automatic target acquisition and recognition (Figure 19). The second variant carries heavy armament—a 10-round, 122 mm Grad multiple-launch rocket system—turning it into a mobile naval artillery platform (Figure 20). The success of these small, low-cost USVs were demonstrated in sinking Russian warships as well as During the operation to strike the Crimean Bridge [in June 2025], the drones delivered explosives directly to the detonation point, causing serious damage to the structure's supports.⁵⁸ The success of these small, low-cost USVs were demonstrated in sinking Russian warships.



Figure 18. Magura v5 and Magura v7 with AIM-9M missiles. May 2025. Photo credit SSU. Obtained from *Militarnyi Defence Intelligence of Ukraine Reveals Capabilities of Magura v7 Marine Drones*.⁵⁹



Figure 19. Ukrainian Sea Baby naval drone with a machine-gun mount. October 2025. Photo credit SSU. Obtained from *Militarnyi SSU Presents New Generation of Sea Baby Naval Drones: Range Exceeds 1,500 km*.⁶⁰



Figure 20. Ukrainian Sea Baby naval drone with a 122 mm rocket launcher. October 2025. Photo credit SSU. Obtained from Militarnyi SSU Presents New Generation of Sea Baby Naval Drones: Range Exceeds 1,500 km⁶¹

Sea Baby and Magura were very effective. It is a key point when you can eliminate and block every Russian and other enemy ships in our seas. This is a unique technology with synthetic data and satellite communication. This technology improves our GNSS model, which is installed in Starlink satellites and receivers, and it helps to communicate using Starlink technology. It allows our drones to operate anywhere on Earth. This is really unique technology. When you use classic Starlink, you can jam it easily. Why? Because it is a satellite system. It moves around the Earth in space, and it is actually not that hard to jam. It is hard to jam the satellites themselves, but it is easy to jam the small GNSS modules that are built into it and receive the data. These small GNSS modules are needed for synchronisation with the global satellite system. What Ukrainians do is they inject synthetic data into this GNSS module and feed it false information about its actual position. It is like hacking. We hack Elon's system and hack the network. It is a not rocket science. (P30)

If we had a number of long-range one way attack drones launched at us—if we could deploy a number of USVs that had interceptor drones on them out into the ocean and go and meet that incoming threat—that would be very, very relevant for us. (P7)

While Uncrewed Surface Vessels (USVs) are tactically useful, they are technically limited. Anything on the ocean surface should be relatively detectable, especially if it is moving and leaving a wake. These systems have a significant Infrared (IR) signature compared to the ocean, making them visible to a range of sensors. The fact that the Russians failed to detect them—and frankly, our Navy likely couldn't either—suggests they were simply unprepared. It would be a mistake to assume these same tactics would work against a prepared adversary. For instance, while the US has proposed a 'hellscape' theory for the defence of Taiwan, a prepared adversary in that scenario will likely be ready to counter USVs without much complexity. The Ukrainians utilised the element of surprise to great effect, impacting morale and Russian control of the Black Sea. However, the likelihood of repeating this success in a conflict two or three years from now is limited The subsurface domain is where future battlespaces will become much more contested. (P12).

Uncrewed Underwater Vessels

On 15 December 2025, Ukraine's SSU announced that it had carried out an attack with a Sub Sea Baby UUV that damaged a Russian Improved Kilo-class diesel-electric attack submarine with land-attack capability (see Figure 21). The SSU reported 'critical damage' to the rear section housing the propulsion, causing a mobility casualty that necessitated extensive repairs for the targeted submarine.⁶² A Ukrainian government statement asserts that the UUV attack is the first ever use of the Sub Sea Baby and was conducted jointly by Ukraine's Navy and the 13th Directorate of the SSU.⁶³ In fact, this may mark the first ever combat use of an attack UUV, though operational use of mine-countermeasure UUVs dates back to at least the 2003 invasion of Iraq. Previous uses by Ukraine of UUVs had been evident since 2022, including the 6 metre long Marichka by AMMO non-profit, and the Toloka family of UUVs by Brave1.⁶⁴



Figure 21. The explosion of a Russian submarine in the port of Novorossiysk by a Ukrainian submarine drone, Sub Sea Baby. December 15, 2025. Photo credits: SSU (Obtained from Militarnyi: Ukrainian Underwater Drones Blow Up Russian Submarine).⁶⁵

Whether or not Ukraine's UUV attack on Novorossiysk inflicted substantial damage, it will impose additional burdens on the Black Sea Fleet as Russia's Navy can no longer treat UUVs as future hypothetical. Likely the service will develop and deploy a host of new anti-submarine defences and patrols as a defensive response to the Ukraine's UUV capabilities. Australia, China, Japan, Russia, Taiwan and the US (among others) are all moving towards introducing combat-capable UUV designs into operational service for roles ranging from anti-ship and counter-UUV missions armed with mini-torpedoes to laying smart mines and even delivering coastal-attack nuclear weapons. The development of sea denial via autonomous underwater systems is the next frontier for 2026.

Sea drones are extremely important in the Black Sea because they evolve the problem. You evolve the task, and you create side missions for these drones, that go beyond just as kamikaze FPV systems. For example, Magura and Sea Baby can work as motherships for FPV drones. They go close to the Crimean coast carrying 5 to 10 FPV drones. These FPV drones communicate with the mothership USV via satellite link. From this platform, the FPV drones launch and fly toward targets. They operate not far from the coast, around 20–30 km, but this is more than enough. Russian jamming systems and radars are positioned behind the front line, behind the main combat area. This method allows the drones to bypass those systems. Now the technology has become a platform—a platform that shows how these systems can be used in different ways. (P30)

Subsurface autonomy is more complex than surface systems, but over time autonomous underwater systems are likely to perform most tasks now done by crewed platforms—better, cheaper, and at far lower risk. They will not replace nuclear submarines in raw performance; a system like Speartooth cannot match the endurance or speed of a nuclear boat. But for missions such as sea denial, large numbers of autonomous systems could be highly effective. Operating in ‘wolf pack’ configurations, they could threaten adversary shipping at scale, potentially with greater impact than a single crewed submarine. The key difference is risk: a crewed submarine becomes vulnerable once it reveals its position, whereas autonomous systems can be attritable and expendable. While nuclear deterrence will remain the domain of crewed submarines, autonomous underwater systems are poised to assume many other roles more cost-effectively and, in some cases, more effectively. (P12)

Uncrewed Ground Vehicles

The use of UGVs has become increasingly important across various missions in Ukraine. These have been used for combat, logistics, casualty evacuation and mining. The impact of UGVs on the battlefield is quite profound.

In terms of combat roles, the main trend of this year in UGV employment is moving from a supporting role to an active role in combat operations, mainly for defence operations. The shift in paradigm is seen as the robot goes first—while humans operate from a safe distance. In late 2025, Ukrainians made military history by deploying a single UGV armed with a mounted machine gun to hold a frontline position for almost six weeks, with undergoing maintenance and reloading every 48 hours. According to Ukrainian government officials, ‘the development and scaling of ground robotic systems form a systematic, human-centred approach focused on protecting personnel.’⁶⁶

In terms of non-combatant roles such as logistics, UGVs were supplying approximately 90 per cent of all supplies to the Ukrainian front line in 2025 on some axis (i.e. Pokrovsk).⁶⁷ In 2026, the Ukrainian defence minister Mykhailo Fedorov stated that the aim is to shift 100 per cent of frontline logistics to be handled by robotic systems.⁶⁸ This is reportedly one of the fastest-growing areas in defence technology; while the sector barely existed in 2022, by mid-2026 there are over 280 companies and over 550 solutions.⁶⁹ UGVs are being used extensively for logistics resupply; they are moving casualties, ammunition, food, water and fuel backward and forward so that there is less risk to combatants. It is slightly easier to drive a remote-controlled car along a road for 5 kilometres up to an area to drop off ammunition and then drive back than it is to try to break into a pit or actually seize an objective or a building.

However, the ground is perhaps the most problematic of the three domains. Ukraine has attempted to field dozens of different UGVs of different designs and different capabilities, and the continual problem they come across is that maintaining a communications link and effectively manoeuvring a platform in the land domain is incredibly difficult (see Figure 22).



Figure 22. Two soldiers conceal a UGV. Photo credit: 12th Special Operations Forces Brigade Azov. Photo reproduced with the owner's permission.

There's also a lot of ability for UGVs to do supporting tasks. In my mind, breaching is one of the most tactically challenging tasks that a combatant will undertake in the land domain. Actually, trying to get up to an established obstacle, such as a tank gap, a minefield, a wall, or even a river—trying to get across or through that is breaching. In Australian Army doctrine, we expect anyone involved in a breach to take 80% casualties. If we can remove the human element from that tactical action through the use of UGVs, that is a huge opportunity that hasn't fully been exploited yet. Both Australia and the US are experimenting with that now, but I haven't seen it done successfully yet. I think it's a big area of growth and opportunity. (P19)

Very small UGVs that are being employed at the lowest tactical level in the front line still have value. Whether I'm fighting in [an] Eastern European farm or in a densely

urban Philippine city, or in the jungles of PNG [Papua New Guinea], the ability to use a small UGV to project forward just a few hundred meters (i.e., 300 to 400 m) will keep the soldier out of the direct line of fire, can provide the opportunity we wouldn't otherwise have. (P19)

Right now, in the Australian Army, there are a few key units or a few key people in the Army that hold the vast majority of our UAS skills, experience, knowledge and tactical application. That is insufficient. We need to rapidly spread or diversify that skill across the entire organisation. If we have a workforce that understands employees and is qualified in UAS, then they will use them in more diverse and interesting ways. In our UAS experimentation, training and employment at the combatant level, the focus is on the individual combatant, the soldier engaged in direct combat, but not broadly. There is no reason that our logisticians should not be as capable on UAS because if they become capable and qualified on it, they will then think of new ways to use those assets that support their mission and that is only going to make the Army and the broader ADF more capable across the full board. They're here to stay. Everyone needs to be competent and qualified, and we need to diversify and expand our training so that everyone has that and know what that means. (P29)

Cross-Domain Integration

The collaboration of uncrewed systems across domains is a significant shift in the field of robotics that enables a combination of aerial mobility and ground or maritime endurance and interaction that neither system could achieve alone. This synergistic approach not only enhances operational outcomes but also provides greater flexibility in adapting to dynamic environments. Cross-domain integration is understood here as drones' employment across several domains of operations that are combined to perform a specific mission (e.g. UAV-USV, UAV-UGV etc.). Although in its infancy, this integration is experiencing challenges associated with communication network instability, environmental adaptability, EW, coordination and operational efficiency in complex scenarios.⁷⁰

UAV-USV Combinations

Several navies are developing warships specifically for launching drones.⁷¹ The Ukrainian Navy, without large ships, got there first and launched FPV drones with explosives for strikes on coastal targets. Early in Russia's war on Ukraine, the USVs exclusively targeted Russian warships—and only on one-way sorties. In 2024, the Ukrainian Navy, security services and intelligence directorate armed some of the USVs with surface-to-air missiles and remotely aimed machine guns. A USV equipped with R-73 air-to-air missiles

retrofitted for surface launch ('Sea Dragon') engaged two Russian Mi08 helicopters.⁷² The ability of Ukrainian USVs to act as FPV drone motherships was first demonstrated in December 2024. On 7 December, the Ukrainian Navy executed a strike on Russian-occupied oil platforms in the Black Sea. This operation introduced USVs equipped with FPV UAVs. Each USV carried at least four FPV drones, each armed with a small payload of explosives. These drones were launched mid-mission to strike Russian surveillance equipment and personnel stationed on the platforms.⁷³ The Ukrainian Navy conducted a series of FPV drone strikes, reportedly destroying two Pantsir-S1 (US\$15 million each) and one Osa short-range air defence system (up to US\$5 million) in the Kherson Oblast region.⁷⁴

Ukraine has developed a new type of USV capable of carrying multiple fibre-optic FPV drones. On 24 September 2025, a Ukrainian USV attacked Russia's port city of Tuapse in Krasnodar Krai, southern Russia, a key transport and logistical port. The USV contained four FPV drones, each tethered to a spool of fibre-optic cable. This marks the first confirmed use of sea-launched, fibre-optic-controlled FPV drones. This attack is becoming increasingly complex for Russians, as they have to counter not only the 'surface threat' but also FPV-drone attacks that are immune to EW systems.

Ukraine's success in integrating USVs and UAVs underscores the importance of innovation and adaptability in modern warfare. With the potential to further extend the capabilities of these platforms, the AFU is not only defending its sovereignty but also setting a precedent for the future of combat operations worldwide. The adaptation of the maritime platform (i.e. USVs) to carry air-to-air missiles—reportedly R-73 short-range infrared-guided missiles in this case—represents a major leap in offensive capability. On 31 December 2024, a MAGURA V5 modified with an R-73 air-to-air missile shot down a Russian Mi-8 helicopter near Cape Tarkhankut and damaged another one.

World's First Strike of a Fighter Jet by a USV and Missile

On 2 May 2025, Defence Intelligence of Ukraine (DIU/HUR) reported that it had downed a US\$50 million Russian Su-30 fighter jet using AIM-9 Sidewinder air-to-air missiles fired from a Ukrainian Magura-7 naval drone (see Figure 23). 'This is the first time in the world that a combat aircraft has been destroyed by [a missile from] a marine drone', the GUR said in an official statement.⁷⁵



Figure 23. Footage from the missile's seeker head captures the moment it locks onto and strikes the Russian Su-30 fighter jet, launched from a Ukrainian Magura-7 naval drone in the Black Sea. Photo credit: Ukraine Defence Intelligence Service., Photo obtained from Army Recognition Group.⁷⁶

In defensive operations, on 19 April 2026 the world saw another excellent 'world's first' by the operators from the 412th Nemesis Brigade of the USF. The operators shot down a Russian Shahed drone by an interceptor drone launched from a USV in the Black Sea. If Ukraine can attack Russian Shaheds from the Black Sea, this reduces pressure on urban air defence and avoids the risk of shooting down explosive drones directly above populated areas.⁷⁷

UAV-UGV

On December 2024, the AFU conducted their first fully uncrewed operation near Lyptsy, a village north of Kharkiv. The attack involved dozens of UGVs and FPVs drones, with no infantry participation. UGVs equipped with machine guns and munitions performed tasks such as mine clearance and direct fire. FPV drones supported the operation from the air, creating a coordinated multi-domain assault. Following the attack, the surviving uncrewed systems returned behind the Ukrainian positions. The tactical air–land operation successfully destroyed Russian military positions. Although still controlled by drone

operators, this operation brings Ukraine closer to implementing the vision of the future battlefield, which will increasingly utilise AI-enabled autonomous capabilities.

A central takeaway is that drones now structure the land battle rather than merely supporting it (see Figure 24). Drones are ushering in a transformation of how the land tactical battle functions. This transformation has rendered many traditional assumptions about combined arms increasingly obsolete, particularly those relying on massed manoeuvre, predictable logistics and uncontested observation.



Figure 24. UAV-UGV mission. Photo credit: 12th Special Operations Forces Brigade Azov, First Corps Azov of the National Guard of Ukraine. Photo reproduced with the owner's permission.

By 2024–2025, both Ukrainian and Russian forces accepted that persistent aerial observation at low altitude was the default condition. The front line became saturated with drones to the extent that ‘nothing flies apart from drones’ (P34). Static positions, logistics convoys and command nodes became continuously observable and therefore targetable unless actively protected or dispersed. To achieve ground manoeuvre, forces must first seek to achieve local tactical air dominance through counter-UAS, EW and persistent strike, thereby isolating a defined piece of terrain. This approach focuses on achieving a ‘correlation of effects’ in the air domain before translating it into a ‘correlation of force on

the ground’ (P34). Only once enemy ISR and strike drones are sufficiently degraded does limited manoeuvre become viable. This reflects the growing importance of battlefield aerial interdiction as a prerequisite for ground action.

Recommendations

Recommendations to the ADF and Military Leaders

1. Revise terminology and establish a mission-based classification framework for uncrewed systems.

For example, the term ‘USV’ is too broad. Classify systems by employment method rather than just ‘uncrewed’ status (ISR, decoys, logistics, mine countermeasures, port protection etc.). This classification framework should directly inform acquisition policy, training pipeline design and doctrinal development, ensuring that capability investment and employment concepts are tied to specific operational functions rather than to generic ‘uncrewed’ categories.

2. Conduct a comprehensive, theatre-specific mission analysis for uncrewed systems in the Indo-Pacific.

The ADF should commission and resource a dedicated, comprehensive analysis of how different categories of uncrewed systems can most effectively complement both offensive and defensive operations within the specific geographic, environmental and strategic context of the Indo-Pacific theatre. This analysis must go beyond generic capability assessments to produce operationally specific employment concepts tailored to the region’s defining geographic and strategic characteristics—*island chains, narrow maritime chokepoints, vast open-ocean distances and limited land-based infrastructure*. A number of high-priority mission sets should be examined within this analysis as immediate priorities:

- **Chokepoint defence using USVs.** USVs are demonstrably most effective in constrained maritime environments where land geography limits the manoeuvre space available to larger surface combatants. In narrow, shallow waterways—such as the Malacca Strait, the Lombok Strait, the Torres Strait and analogous chokepoints across the Indo-Pacific—conventional surface vessels cannot manoeuvre effectively to evade small, fast-attack uncrewed platforms. USVs employed in massed, coordinated formations in these environments can impose disproportionate cost on adversary naval forces at a fraction of the platform cost of conventional maritime assets.
- **Long-range maritime ISR using UAS.** Given Australia’s vast exclusive economic

zone and the distances involved in the Indo-Pacific operating environment, persistent long-range aerial surveillance using UAS platforms is essential for threat detection and maritime domain awareness at ranges and persistence levels that crewed aviation cannot sustain cost-effectively.

- **Island-chain control and denial using long-range strike drones.** Consistent with Lesson 2, the analysis should specifically examine how long-range, low-cost strike UAS can be employed to establish and sustain denial effects across island chains in scenarios where conventional logistics supporting crewed platforms (e.g. F-35, P-8) are disrupted or denied.
 - **Cross-domain integration.** The analysis should explicitly examine combined USV-UAV, USV-missile/turret and UGV-UAS employment options, reflecting the multi-domain integration patterns already operationally demonstrated in the Ukrainian maritime and land theatres. This analysis should be conducted in close partnership with allied nations operating in the region (i.e., the United States, Japan, the Philippines), and its findings should feed directly and traceably into ADF capability planning, force structure decisions and acquisition priorities.
3. Embed multi-domain and combined drone operations into regular ADF exercises and training cycles.

Understanding how uncrewed systems can be employed in multi-domain and combined operations is insufficient at the desktop or analytical level; it should be rehearsed, tested and refined through regular, realistic and operationally demanding training and exercises. The ADF should embed multi-domain UxS operations—integrating air, land and maritime uncrewed systems in combined offensive and defensive scenarios—into its standing exercise program as a mandatory and recurring activity rather than treating such exercises as ad hoc events or technology demonstrations. Exercise design should be explicitly tailored to the Indo-Pacific operating environment, including:

- **large-scale swarm employment and counter-swarm exercises**, replicating the high-volume, massed drone operations documented in Ukraine, adapted to the maritime and island-chain context of the Indo-Pacific
- **combined USV-UAV operations**, including chokepoint defence, maritime strike and ISR relay scenarios in geographically representative environments
- **contested electromagnetic environment exercises**, replicating the EW conditions documented in Ukraine—jamming, spoofing, frequency-hopping and fibre-optic workarounds—to ensure operators and commanders are trained to maintain effectiveness under realistic degraded communications and navigation conditions

- **red team / blue team UxS exercises**, in which ADF units face realistic adversary drone employment (modelled on Chinese and Russian doctrine and equipment) from a dedicated red force equipped with representative platforms, consistent with the ‘just do it’ principle articulated in Lesson 1
- **joint and coalition integration exercises**, bringing together ADF, US, Japanese and other regional partner UxS capabilities to identify interoperability gaps, develop common TTPs, and build the multinational operational fluency required for coalition operations in a contested Indo-Pacific environment.

Exercise outcomes should feed directly into the lessons identification and implementation cycle recommended in Lesson 1, ensuring training insights are captured, validated and incorporated into doctrine and force design rather than remaining at the unit level.

Lesson 4: The Web of War—Operation Spiderweb and Multi-Domain Vulnerability

The outstanding Operation Spiderweb is a lesson in itself for all militaries to watch and learn from. On 1 June 2025, the daring and wildly successful operation Pavutyna (Spiderweb) was carried out by the SSU, showcasing how a relatively small country can successfully damage the strategic capabilities of a larger nuclear state.⁷⁸ The plan of one year, six months and nine days was conducted in secrecy and supervised by the head of the SSU on behalf of President Volodymyr Zelenskyy. The plan emerged in November 2023 when the enemy began to shell peaceful Ukrainian cities, hospitals and energy facilities. The operation targeted five air bases deep within Russian territory: Olenya (Murmansk region, approximately 1,900 kilometres north of the Ukrainian border), Belaya (Irkutsk region, approximately 4,300 kilometres east of the Ukrainian border), Dyagilevo (Ryazan region, approximately 600 kilometres north-east of the Ukrainian border) Ivanovo (Ivanovo region, approximately 800 kilometres north-east of the Ukrainian border) and Ukrainka (Amur region, approximately 6,000 kilometres east of the Ukrainian border).

First, the SSU transported approximately 117 combat FPV drones to Russia, and then modular wooden houses. Once in Russia, the drones were hidden under the roofs of the houses, which were placed on trucks. To carry out the operational plan, the SSU created a front company in Russia—a logistics company in Chelyabinsk. They subsequently purchased five trucks, and the drivers they hired transported various cargoes, thus reinforcing the cover story. The drones were covertly delivered to launch sites (installed in the roofs and loaded onto trucks or construction trailers) and launched simultaneously to strike strategic aviation. The drones looked like ordinary FPVs but were unique, with several types of communication and a special explosive mixture developed specifically for this operation—a 1.6 kilogram special cumulative high-explosive charge—to burn through the aircraft's fuselage and cause an explosion inside.⁷⁹ The drones were configured to operate without GPS (inertial navigation, visual guidance) and used international SIM cards and specialised software for coordination. Launches were synchronised from multiple points: a mass simultaneous strike to reduce the effectiveness of air defence.

The total losses of the Russian Air Force amounted to 41 destroyed and damaged aircraft, including A-50, Tu-95, Tu-22M3, Tu-160, An-12 and Il-78, with approximately US\$7 billion of damage, at four out of the five originally planned Russian airfields. According to NATO estimates, the attack destroyed 34 per cent of Russia's long-range missile carriers.⁸⁰ The only base not reached was Ukrainka in the Amur region, because the truck carrying drones to the area caught fire and exploded en route. The operation demonstrated the ability to inflict significant damage on enemy strategic aviation using inexpensive FPV drones and a high degree of innovation in planning, and the vulnerability of even high-value military infrastructure deep in the rear. It illustrates a structural shift in contemporary conflict: warfare increasingly unfolds as an interconnected web rather than along

linear fronts (see Figure 25). In this web, dispersed nodes—uncrewed systems, digital communications, ISR networks, cyber capabilities and information operations—interact across domains to generate cumulative effects that exceed the scale of individual tactical actions. The concepts of friction and uncertainty described by Carl von Clausewitz remain central, yet technological acceleration has transformed their manifestation. Enhanced visibility through commercial satellite imagery, OSINT and social media has not eliminated the ‘fog of war’. Rather, it has compressed decision cycles and amplified the speed at which tactical disruption produces operational and strategic consequences.⁸¹ Operation Spiderweb demonstrates that enhanced global visibility does not eliminate uncertainty; instead, it accelerates the feedback loop between tactical action and strategic consequence. ‘Anytime, anywhere, under any circumstances’ is an operational condition enabled by distributed technologies, networked coordination and adaptive adversaries.



Figure 25. Operation Spiderweb. Photo credit: SSU. Photo obtained from Militarnyi.⁸²

Operation Spiderweb combined human control with elements of autonomy and AI. The role of AI was supporting flight stability and targeting on aircraft. The FPV drones used in the operation were remotely controlled through Russian mobile telecommunications networks, including 4G and LTE connections. To enable stable long-distance control over mobile networks, the drones relied on a software-hardware system built around ArduPilot—a widely used, open-source autopilot framework designed for UAVs. ArduPilot provides advanced flight stabilisation, waypoint navigation, failsafe routines and programmable mission profiles. In this case, each drone was integrated with a compact onboard computer

(e.g., a Raspberry Pi), connected to a webcam and an LTE modem via Ethernet. The camera feed was used for visual navigation, while control signals were routed through ArduPilot's UART interface, allowing operators to pilot the drone remotely with stabilised, responsive input—even when faced with significant signal latency.⁸³

A central lesson is the growing vulnerability of high-value military assets to attritable, low-cost systems. By employing inexpensive FPV drones guided by open-source software and commercial networks, Ukraine inflicted disproportionate damage on strategic aviation platforms that are costly, scarce and—in some cases—irreplaceable. The operation exposed critical shortcomings in rear-area defence and force protection. Traditional air defence systems optimised for high-speed or high-altitude threats were ineffective against small, low-flying drones launched from close proximity. This reinforces the need for integrated, low-tech and high-tech defensive solutions, including EW, infrastructure protection and persistent monitoring of civilian-adjacent spaces near military installations. In addition, it highlights that creativity, professionalism and uncrewed systems can generate strategic effects deep within an adversary's rear areas. The operation requires thinking differently about securing supply chains and equipment far from front lines. It also challenges longstanding assumptions that strategic impact requires expensive platforms, advanced industrial capacity or uncontested access to high-end communications. Instead, it highlights how accessibility, creativity and systems-level targeting can offset traditional advantages in scale and resources.

It was very important operation that showed to all countries that their strategic capabilities can be actually threatened by those drones which are small systems, but they still can be significantly damaged by FPV drones. (P29)

If something like a spiderweb operation occurred in Australia tomorrow, would the ADF be able to protect against it and respond? We'd likely identify it beforehand through domestic intelligence services. However, if it reached the stage where it got past all of that, we would not ... (P20)

The lesson from the Operation Spider Web is clear—you need to preserve your high value assets, as anything can happen anywhere at any time. We should also focus less on a small number of large platforms and more on many smaller systems. At the moment, far too much money is being spent on long-term projects that are already obsolete by the time they enter service. Yet low-cost drones have destroyed billions of dollars' worth of Russian aircraft. (P22)

Recommendations

Recommendations to the ADF and Military Leadership

1. The ADF should move away from legacy static defence models towards a framework of systemic resilience.
 - Defence should acknowledge that physical, digital and cognitive domains are now inextricably linked. Disruption in the EMS or a cyber-interference event should be anticipated to cascade into operational paralysis in the land or air domains.
 - Invest in adopting a layered approach of systems to identify, detect, track and destroy drone threats to protect important assets and infrastructure.
 - To survive the ‘web’, the ADF should prioritise:
 - distributed bases—moving away from concentrated ‘super-bases’ towards smaller, dispersed and mobile footprints that deny adversaries the high-value, single-strike targeting opportunities that large, fixed installations present
 - redundant mesh communications—implementing self-healing mesh network architectures that can maintain C2 connectivity even when primary satellite or fibre links are severed or degraded
 - hardened digital architecture—prioritising the cyber-resilience of UxS command links, data systems and battle management networks against persistent interference, recognising that an adversary targeting the digital backbone of drone operations will simultaneously blind ISR, degrade fires cueing and collapse sustainment coordination.
2. Address the anti-deterrence risk posed by attritable drone swarms.
 - The proliferation of low-cost, high-volume UAS represents a paradigm shift and underappreciated challenge to traditional deterrence theory. If an adversary can threaten high-value strategic assets—airfields, port facilities, command nodes, submarine berths—through massed, attritable drone swarms costing a fraction of the targets they attack, the conventional logic of deterrence (the capacity to absorb a strike and retaliate) is materially undermined. The ADF should treat this ‘anti-deterrence’ risk as a first-order strategic planning consideration, not just a technical problem.
 - The ADF should invest in sovereign swarm-based defensive layers that impose sufficient cost and operational uncertainty on an adversary to deny them a ‘cheap win’ against expensive, limited and strategically irreplaceable assets. Additionally, the ADF should explore the development of a persistent drone-based sensor network

deployed across the Indo-Pacific approaches—providing the low-altitude, persistent early-warning coverage that satellite-based systems, constrained by orbital geometry and revisit rates, cannot deliver—to ensure incoming threats are detected with sufficient lead time to initiate effective defensive responses.

3. Maintain meaningful human oversight across increasingly automated kill chains.

- As highly automated and semi-autonomous systems become the connective tissue of networked multi-domain operations, the ADF should maintain a disciplined focus on meaningful human oversight to manage the ethical, legal and operational risks inherent in high-speed, networked warfare. This is not an argument against automation—the speed of modern drone-on-drone engagements and swarm interception demands automation at the tactical level—but a recognition that the rules of engagement, target classification authorities and escalation thresholds governing these systems must be defined, tested and enforced by human commanders before autonomous execution begins.
- Defensive adaptation should itself become increasingly adaptive and anticipatory, incorporating AI-driven analytics to identify patterns of adversary drone activity, pre-position defensive assets, and cue intercept systems before a strike is launched rather than reacting to it after detection. The ADF should invest in the development and testing of AI-enabled threat anticipation tools and embed these into C2 architectures at the appropriate echelon.

Recommendations to Local Commanders

- Commanders should plan all operations on the assumption that primary communications will be intermittently denied and that ground control stations, relay nodes and command posts emit targetable electromagnetic signatures requiring rigorous EMCON discipline.
- Units should rehearse multi-domain disruption scenarios—simultaneous cyber, EW and kinetic attack on C2 nodes—to develop the command culture and pre-delegated authorities required to operate effectively through degraded connectivity.
- Commanders should integrate counter-drone detection and response into all exercise scenarios as a default condition, not a specialist training event.

Recommendations to Government

- Government must fund and mandate the transition of ADF basing architecture towards distributed, dispersed footprints, accepting the associated infrastructure cost as a necessary investment in strategic survivability.
- Government should direct investment in a sovereign persistent drone-sensor network for Australia’s northern approaches, to be treated as a national early-warning infrastructure investment rather than a Defence-only capability program.
- Government should establish clear legal and policy frameworks governing autonomous defensive responses to high-volume drone swarms—recognising that engagement timelines in such scenarios may exceed the capacity of traditional human-in-the-loop kill chains—while ensuring human authorisation of mission parameters, engagement rules and target profiles prior to autonomous execution.

Lesson 5: Counter-UAS/EW—War Across the Spectrum

EW has existed for more than a century, with its role primarily focused on the detection, interception and analysis of adversary communications.⁸⁴ In Ukraine, this paradigm shifted dramatically. Both Russian and Ukrainian forces began treating the EMS as a manoeuvre space—actively shaping it to degrade adversary C2, disrupt drone operations and influence targeting cycles. The contest evolved from temporary spectrum denial to an ongoing cycle of measure and countermeasure in which frequencies, waveforms and system architectures are constantly modified in response to adversary interference.⁸⁵ The EMS has emerged as a primary domain of warfare, where strategic advantage could determine the outcome of broader operations. Both Ukraine and Russia have profoundly transformed their approaches, giving rise to an entirely new model of spectrum warfare: a coordinated spectrum of offensive, defensive and intelligence support activities designed to produce tactical, operational and strategic effects.⁸⁶

A central lesson of the Ukraine conflict is that modern forces are deeply dependent on the EMS. Communications, ISR, targeting and logistics systems rely on uninterrupted spectrum access. As forces become more networked and integrated, they simultaneously become more vulnerable to electromagnetic interference. Mastery of EW now directly affects a force's efficiency, survivability and cohesion across echelons. This integration simultaneously creates increased vulnerability to adversary interference and inadvertent fratricide in the spectrum (see Figure 26).

As early as 2024, the electromagnetic environment at the front was extremely dense, with overlapping jamming zones that sometimes even impeded an army's own drones. By 2024–2025, EW/C-UAS efforts increasingly reflected layered integration rather than standalone systems. Soft-kill measures—such as jamming and spoofing—were combined with kinetic short-range air defence to counter saturation attacks. The economic asymmetry of the threat (low-cost drones versus high-cost interceptors) further incentivised scalable, cost-effective EW solutions.

EW integration at the tactical level is now a must—every platoon might need an EW specialist or at least access to jamming devices to survive in drone-saturated battles. Ukrainian forces have effectively embedded EW into ground units (e.g., an assault company might go into battle with a dedicated EW vehicle supporting it). NATO militaries, which traditionally keep EW in higher-level formations, are taking note that electronic protection is now as fundamental as armour or cover on the modern battlefield. (P38)



Figure 26. Mobile EW platform for point-defence in contested environments. Hymo XL C-UAS system. Photo credit: Serhyi Prytula Charity Foundation. Photo reproduced with the owner's permission.

Electronic jamming has proven the most effective way to stop drones mid-flight. Ukrainian and Russian forces saturate the front lines with EW systems that jam GPS signals or drone radio links, causing UAVs to lose control or video feed. As soon as drones shift to alternative control frequencies or encryption to evade jamming, adversaries adjust their EW tactics in response. Ukrainian drone pilots report that enemy jammers have forced them to constantly hop to new, less common frequencies and to employ signal repeaters to maintain control beyond line of sight. At the infantry level, both sides use portable 'anti-drone guns'—these devices emit directional jamming signals to down or disable small quadcopters threatening frontline troops. Companies began ordering modules for the frequencies where drones appeared. As links became more resilient, higher power became necessary. If in 2022–2023 a 20-watt module could be effective, in 2026 anything below roughly 50 watts per channel is often not worthwhile. This makes EW much more demanding in power supply: higher consumption means either larger battery stocks or other energy solutions. A smaller portion of the sector is moving towards 'smart EW'. This means EW that does not jam an entire broad spectrum continuously, but detects what is flying, identifies the precise operating frequency corridor, and then jams narrowly within that corridor. This reduces the need to blanket huge bandwidth and can reduce power requirements. With directional antennas, lower-power modules can achieve far longer neutralisation distances compared to conventional white-noise jamming.

We are producing and using different types of jamming systems. We jam every frequency band from 100 MHz up to 6–7 GHz. These are very powerful systems—about 100 watts per channel. We have around 15–16 models. They are very expensive, but the Russians are not stupid. They understand what must be done to solve this problem, just like we do, and they use mostly the same technology. They also install jamming devices on their tanks. (P30)

To overcome the jamming threat, next-generation drones that can operate with a high degree of autonomy or via unjammable control links are being developed. One approach is drones being guided by AI for target recognition and attack, so that no continuous radio control is needed during the terminal phase. Both sides have begun fielding a small number of drones with onboard AI that can identify a target (e.g. a vehicle) and then home in on it without further operator input.

We (Ukrainians) use inertial navigation systems. These are sensors built into FPV drones. If you visually lock onto a target and focus on it, the drone can continue flying toward that point even without GNSS and even without video signal—as long as the target is not moving. Another method is object-based navigation. When you create a map, when you perform satellite reconnaissance, you already have data from satellites. You also have reconnaissance drones flying over the area in advance. You already have photos of where the target was located. You can upload this data into the drone, and the drone can fly fully autonomously—not using GNSS, not using its FPV camera, but using a downward-facing camera that analyses the terrain below the drone. (P30)

In 2025, Russia produced thousands of Shahed-type systems and millions of FPV drones to overwhelm Ukrainian defence systems at the front line and back at the rear. However, Ukraine has demonstrated its ability to innovate and to allow those innovations to continuously evolve, adapt, iterate and find effective solutions under pressure, often with intermittent electricity supply, and compensate shortages of manpower and ammunition against such a large-scale force. Shahed drones also continued evolving. One major evolution is the CRPA antenna (a controlled reception pattern antenna) supporting satellite navigation resilience through Russian and non-Russian constellations. If in 2023 this was often 4–6 channels, now most are at least 12 channels and sometimes 16. These antennas are difficult to jam with EW. Their positioning and the geometry of satellite-antenna interaction also makes them harder for EW to influence. The only way to stop it is to physically shoot it down or cut the cable. We are seeing a high demand for ‘pump-action shotguns’ (hunting carbines) because hitting a drone moving at 60 km/h at 300 meters with a standard assault rifle is nearly impossible. (P6)

The broader trend is also organisational. EW is a relatively young tactical domain, and Ukraine is only now building layered EW defence in a more systematic way. Today there are many manufacturers providing ad hoc systems. They are installed on vehicles and positions in a scattered manner. The direction of travel is towards EW being fully accounted for in a common situational awareness system, displayed on a map that shows what EW is active, what sectors it covers and in what direction it is working—so EW commanders at battalion, brigade and corps levels can see what is operating where. This is critical.

The idea is an integrated networked EW ecosystem: detection, identification and coordinated response, rather than isolated standalone devices. Interceptors, air defence, mobile fire groups and EW must work together. AI terminal guidance drones remain immature and unreliable at scale. In a 1–5 year horizon, solutions may mature, but at present it is not the dominant problem. Importantly, systems that worked a few months ago are no longer operational; they are continuously evolving and adapting to adversaries' adaptation. The rise of drones, however, has driven the emergence of a new class of tactical EW capabilities, including:

- operational-tactical EW (15–20 kilometre class)
- mid-range tactical EW (3–5 kilometre class)
- close-range tactical EW (200–300 metre class).

In addition, in Ukraine (broadly speaking), counter-drone and EW efforts can be grouped into three major mission sets, and will be further explored in detail:

- national-level defence against Shaheds across the country
- protection of the front line and troops in trenches or vehicles
- protection of cities and critical infrastructure.

National-Level Defence Against Shaheds Across the Country

In 2024, Ukraine started employing and scaling interceptor drones as part of defensive capabilities in response to the large salvos of Shahed-type drones that Russia was launching against Ukraine every night in hundreds.⁸⁷ In summer, Russia significantly increased both the size and the frequency of its drone and missile strikes (i.e., 100 in 2024 versus 400 in 2025). The largest strike, which involved 999 drones, was on 24 March 2026.⁸⁸ The overall interception rate of drones in March 2026 surpassed 90 per cent, and according to Ukraine's war plan, the aim is to identify 100 per cent of aerial threats in real time and intercept at least 95 per cent of drones and missiles.⁸⁹ Hence, interceptor drones have emerged as an integral part of the layered defence system, along with mobile firing brigades, surface-to-air missiles, air-to-air missiles, EW and helicopter crews. One in every three Russian aerial targets destroyed over Ukraine is now brought down not by a missile

or a gun but by an interceptor drone.⁹⁰ In addition, as they cost between US\$1,000 and US\$5,000, they are more economical options for countering Russian Gerans (\$35,000 to \$45,000), compared to expensive missiles.⁹¹

Ukraine has shown the efficiency of interceptor drones to eliminate Shaheds, when you are not using \$6mln rockets for this, with a \$500 FPV drones that with extreme efficiency eliminate Russian drones. We call it 'economy of the war' when you use cheap technology and make the biggest impact in the war. (P30)

The methods employed are either fly the drone directly into another drone, or strap either a shotgun or some sort of projectile-based system. We've seen drones that shoot nets into the propellers of other drones, drones with shotguns, drones with rockets on them. But these are deliberately designed to target other UAS, and I think that's something that no one really expects. I'm almost certain that field will continue to grow. I think that's a huge area we don't yet understand but is going to become relevant in the next 18 to 24 months. (P19)

The most critical factor remains the continuous mass deployment of Shahed-type UAVs, which rapidly exhaust Ukraine's air defence resources. In January 2026, even with fewer launches (i.e., on average 143 per day) the combination of technological improvements, harsh winter conditions and accumulated infrastructure damage produced a significant strategic effect, underscoring the urgent need to further strengthen Ukraine's air defence and counter-drone capabilities.⁹²

The most efficient means of shooting down Geran-2 and Gerbera UAVs flying at a higher altitude include helicopters and combat air patrols. Generally, Ukraine endeavours to wear down the waves of UAVs over a significant distance using a distributed defence, so that the point defences at the eventual target—ranging from self-propelled anti-aircraft guns and mobile fire teams with heavy machine guns, to MANPADS teams and surface-to-air missile systems—have to engage as few targets as possible. These methods have proven successful, with the vast majority of OWA-UAVs intercepted.⁹³

Helicopters could be a good option to shoot down Shaheds. Apache is an ideal means because it has a radar, and it can see Shahed 30–50km. It can identify where to move the positions to expect it. (P35)

There should be a coordination—friendly-enemy forces. Helicopters could be good 5 groups—with each sector 80–90 km and could intercept drones outside of the cities.

The focus of 2025 for Ukrainian manufacturers was not only long-range drones (1,000km+), but also on middle strike drones (i.e., 100–200 km). Developing a platform that can fly long distance is not a rocket science. We build a dedicated platform that integrates the engine and the entire tactical communications suite, including optical navigation and GNSS-denied navigation capabilities. This combination is the key to mission success. (P30)

Protection of the Front Line and Troops in Trenches and Vehicles

The widespread use of reconnaissance drones and FPV strike systems has fundamentally altered frontline survivability. Trenches, fighting positions and vehicle concentrations are routinely observed, targeted, and struck with minimal delay. As a result, protection is no longer solely about shielding against indirect fire; it now accounts for vertical threats and real-time targeting. Units have increasingly incorporated overhead cover, camouflage netting, multispectral concealment and rapid relocation drills to reduce exposure. Armoured vehicles, logistics trucks, and even civilian vehicles used near the front have undergone extensive field modification. Improvised ‘cope cages’ or slat armour have been added to counter top-attack munitions and FPV drones. However, these modifications often increase weight and reduce mobility, creating trade-offs between protection and manoeuvre.

Portable and vehicle-mounted jammers are used to disrupt drone control links and GNSS signals. EW assets are frequently deployed alongside manoeuvre elements to create temporary protective bubbles against small UAS. This integration reflects a broader shift in which spectrum control directly contributes to troop survivability. Systems mounted on a tracked robotic platform are designed to support casualty evacuation and demining, provide cover during assault operations and protect logistical routes (see Figure 27).



Figure 27. Mobile electronic warfare system Kvertus AD Berserk. Photo reproduced with the owner's permission.

There are multiple levels of jammers, ranging from so-called 'trench jammers', which cover individual positions, to larger pieces of EW kit, with jammers mounted on individual vehicles and individual boats.

At the line of contact, we cannot actively use classic radar because anything emitting becomes a target—it 'lights up' and gets hit. So, detection is hard. We need passive radar and passive electronic intelligence systems. (P4)

I guess EW planning and liaison is important, so the units were able to conduct EW mapping, understand where the corridors are, and moving through them, whether that's understanding signal propagation, terrain shielding. Obviously, EW, but drones are still effective, so clearly, they are still able to get through. Putting spectrum fratricide aside, the inadvertent jamming of your own systems is a serious problem. Whether that's your radio communications, your drone communications, or your GPS signals, which a lot of modern equipment relies on. That's a serious issue. (P25)

In terms of countering or suppressing drone elements, we're seeing both sides increasingly target the other side's drone operators, which I think is a bit of a change from earlier phases of the war. Whether that's targeting their ground control stations, their GCSs, their launch locations, or likely positions where operators

are expected to be operating from. I think that's an important element of counter-UAS. Also, just different patterns of movement, limiting movement, particularly in that dangerous five to fifteen kilometres behind the front line, the use of cover and concealment, all those basic Army techniques—I think sometimes the best countermeasures are the simplest ones. Both sides are heavily using basements for protection from artillery, but also protection from drones, as well as other buildings. Hence, there is the countering side, but then there's also the avoiding side, and the hardening of positions as well. I think both of those are really important. (P25)

Fibre-Optic Drones and AI-Enabled Drones: How Do You Counter Them?

Fibre-optic drones are immune to jamming because control does not rely on radio waves and does not emit electromagnetic radiation.⁹⁴ Practical countermeasures against fibre-optic drones include nets and shotguns or other kinetic solutions. Their slower speed gives soldiers more time to react if they see or hear the threat.

Nothing really works against them. Electronic warfare does not. At present, only guns—kinetic measures. But that is a problem, because you cannot shoot everything down. Sometimes it is just that there are already a large number of those drones, and they are getting tangled and destroying each other. Now, in that kill zone, all the steppes and fields of Ukraine are already covered with fibre-optic cables. It is becoming disadvantageous for other fibre-optic drones to operate, because they can get tangled. Other fibre-optic or regular drones can simply cut the cable and stop the connection between the pilot and the drone. (P29)

A shortage of traditional air defence systems drives the development of laser weapons in Ukraine. Laser systems are considered a promising component of a layered air defence network, primarily for countering short-range kamikaze drones and reconnaissance UAVs. In early 2026, Ukraine publicly unveiled trials of a new domestically developed laser air defence weapon, 'Sunray', representing a significant advance in C-UAS and directed-energy capabilities. The system is designed to counter low-cost Russian UAS, including tactical reconnaissance and strike drones, by using a high-energy laser beam to ignite or disable targets mid-air. The development of Sunray follows earlier Ukrainian efforts to field laser weapons trialled by the USF, such as the Tryzub (Trident) system since April 2024 – which was claimed to engage aerial targets at altitudes of up to 2 kilometres, suggesting a broader and evolving laser weapons program. The military claims that this laser can destroy attack drones, guided bombs, cruise missiles and ballistic missiles at distances of up to 3,000 metres, and helicopters, aircraft and reconnaissance drones at distances of up to 5,000 metres.⁹⁵

Such systems are part of a larger domestic push to build an ‘anti-drone dome’ of layered defences capable of countering mass UAS attacks and protecting critical infrastructure. The combination of low unit cost, mobility almost limitless ammunition capacity, and directed-energy lethality positions laser weapon systems as a pragmatic, battlefield-driven C-UAS solution tailored to the high tempo of modern air attack campaigns.⁹⁶ Ukraine could become one of the few countries in the world to deploy laser weapons in real combat conditions as a means of countering drones.

However, powering the laser requires a substantial 50 kilowatts of electrical power. This means stationary energy facilities or ships equipped with large diesel generators are currently the only viable platforms capable of powering such a laser air defence system. In active combat zones, where reliable electricity access can be limited, this power requirement becomes a critical logistical factor for the weapon’s effectiveness. In addition, the effective engagement range of laser weapons can drop to mere hundreds of metres, which severely limits their tactical utility.⁹⁷

Protection of Cities and Critical Infrastructure

A key issue is that Ukraine cannot resource everything simultaneously. The state must prioritise urgent needs, and protection of frontline cities often depends on external partners, donors and investments, rather than sufficient state resources. For example, cities close to the front or border are being terrorised by drone attacks, including attacks on emergency vehicles and civilian transport. Russian UAV attacks carrying grenades, improvised explosives, anti-tank mines and rocket-propelled grenade (RPG) warheads have intensified dramatically. Between August and November 2024, Kherson alone endured 9,500 ‘kamikaze-style’ drone attacks, which resulted in 531 civilian deaths and hundreds more injuries.⁹⁸ The enemy is actively scaling the use of drones for attacks on Ukrainian cities, and this is yielding a grim result for Ukrainians with energy infrastructure—suffered critical damage during the winter.

For protection of civilian and military infrastructure, Ukraine mainly uses interceptor drones, mobile fire groups and radar systems. Systems such as Giraffe radar are used to detect long-range Russian strike drones, including Shahed, Zala, Gerbera, and other medium-range and long-range UAVs. These detection systems provide early warning, allowing air defence and mobile groups to engage the drones before they reach critical infrastructure.

The key point is detection and the creation of protective ‘bubbles’ through jamming and early-warning systems. Detection comes first. Then, if necessary, destruction follows. However, destruction itself is a major challenge—especially when we are trying to minimise civilian harm. Intercepting drones must be done in locations

and ways that reduce collateral damage to civilian infrastructure. This is the harsh reality of war... When you intercept a Shahed or similar strike drone, it often loses control after being hit. Once that happens, you cannot predict where it will fall ... Unfortunately, this means that even when a drone is successfully destroyed, it can still crash into civilian buildings or populated areas. This is something Ukraine faces constantly. While interception is necessary, it always carries risk. There is no completely safe way to neutralise airborne threats over urban areas—only risk mitigation, not risk elimination ... (P30)

EW systems alone do not guarantee the destruction of enemy drones. Therefore, manufacturers are developing networked scenarios where EW interacts with radars, early-warning systems and command posts. This approach, according to the manufacturers, enables wider area coverage, better sector coordination and faster response to emerging threats.

In 2025, the concept of the ‘anti-drone wall’ emerged in Ukraine to span the front line, using its EW technologies. The initiative is expected to utilise EW and electronic reconnaissance technologies to save the lives of countless soldiers and civilians while protecting critical infrastructure from the escalating threat of UAVs. A large-scale networked EW system combines electronic intelligence, automated detection and jamming into an integrated counter-drone defence. Using smart algorithms, it can detect UAVs at extended ranges, identify operating frequencies and directions, and enable remote disruption of hostile drones while reducing friendly-fire risk. Designed as a scalable anti-drone wall, such systems can link large numbers of EW units to protect frontline forces, civilians and high-value assets such as artillery from increasingly pervasive drone threats (see Figure 28).⁹⁹



Figure 28. Atlas system. Photo credit: Kvertus. Photo reproduced with the owner's permission.

Ukraine currently uses many different detection platforms, such as Tsukorok, Tenet, Chuika and Zhelezniak. These devices detect drone communication signals. It is important to clarify that drones do not transmit navigation signals. They receive control signals from the remote controller, and transmit video, using separate frequency bands—typically 1.2 gigahertz, 2.4 gigahertz, 3.3 gigahertz, 4.9 gigahertz and 5.8 gigahertz. Detection systems scan these video transmission bands. These are portable devices that soldiers can carry. They warn when an enemy drone is approaching, allowing troops to take cover or activate jamming systems. Most European jammers use software-defined radio methods, but they are not always effective. Why? Because drones now use frequency hopping. For example, if a drone is operating on 900 megahertz and detects jamming, it automatically switches to another frequency. It may hop across hundreds of frequencies. At that moment, the jammer becomes ineffective.

The Russians use a system called Shtora, which jams for 15 seconds, then pauses, then jams again. Our pilots understand this pattern and exploit it. We know how to bypass it using our own technology and ground control systems, such as Dronarnia. (P30)

First, when we talk about EW and C-UAS and the way to defend against a drone we need to clarify which drones, we are talking about—frontline or rear cities? It won't be the same. For rear cities, a drone is not a difficult target by itself—the problem is the mass of drones. You can shoot down an FPV with a shotgun.

But on the frontline, you can't stand up in a trench to do that. We need automated turrets and automated systems. In any case, defence against aerial threats—deep-strike drones or FPVs—requires an integrated approach using EW. EW is not only jamming command links or GPS. On the line of contact GPS often doesn't exist. EW also includes directed energy: laser weapons and electromagnetic pulse systems. Those are counter-measures too. Also, deception: simulating unit activity, simulating radar emissions and other signatures to divert the enemy. And kinetic solutions; plus, passive physical protection—nets, chains, external cages ('cope cages') on vehicles—first on turrets, later across the whole vehicle. It's a layered approach of a complex of measures: EW, kinetic defence, and physical protection—tailored to where you are. At 'zero' (line of contact), there is one set of systems; in the 10 km zone, more operational-tactical EW coverage; for fibre-optic drones, laser/EMP; for rear cities, classic air defence systems, man-portable air defence systems (MANPADS), mobile fire groups, and interceptor drones. (P30)

Australia's approach is more maritime defence. That makes some aspects easier because coastal systems can be built to deny any attempts 20 km away. Hence, a different approach is needed. Land war and maritime war are different problems. That is why it's easier for the UK, the US, and Australia because of maritime defence and geography. If we had a sea on the Kharkiv border, I wouldn't object. Any weapon that can destroy an aerial object is effective. The question is how you employ it. Laser weapons are less effective in fog, snow, rain. Pulse weapons are effective. Kinetic weapons are effective. (P33)

Drone Interceptors

In Ukraine, different types of interceptors have been designed to: (1) strike heavy Shahed-type drones, and (2) strike light low-flying and slow ISR drones. This is because those for striking Shaheds cannot intercept slow ISR drones, and vice versa. One of the top AFU's brigades in drone interception are using 14 interceptors, 13 of which are Ukrainian made. Whether fixed-wing type, or rocket FPV type, they rely on a combination of detection tools, targeting systems, skilled pilots and operators and, of course, the interceptor drone itself as a strike element. (P38)

More than four years since Russia's full-scale invasion, and with hundreds of Shahed-type drones flying over Ukrainian territory daily, Ukraine has become the world leader in developing and using innovative drone defence capabilities. Interceptor drones have become a cost-effective game changer in countering air defence threats (i.e., Shahed-type and other ISR drones). Ukraine's expertise and capability are highly valuable. For example, since the outbreak of the conflict in the Middle East in late February 2026, both Ukrainian expertise and capability have been indispensable for Gulf countries and the US to defend against Iranian drone attacks.¹⁰⁰ In early March 2026, 11 countries, including the United States, requested Ukraine's assistance in countering Iranian Shahed drones. Ukraine's low-cost interceptor drones, such as the Sting by Wild Hornets (Figure 29), cost as little as US\$1,000 and could change the economics of the ongoing conflict in the Gulf.



Figure 29. Drone interceptor sting by wild hornets. Photo credit: Serhyi Prytula Charity Foundation. Photo reproduced with the owner’s permission.

Ukraine is the most combat-experienced, doctrinally up-to-date and innovative partner in the Western world. In July 2025, at the LANDEURO international meeting, Robert ‘Magyar’ Brovdi, Commander of the Ukrainian USF, stated that ‘four of our drone crews could destroy your NATO base in 15 minutes, from 10 kilometres away’. While many dismissed this message, in February 2026 there were reports on NATO’s Hedgehog exercise with near-identical headlines, such as ‘Within half a day, the 10-person Ukrainian team with drones eliminated two NATO battalions who were unable to effectively counter the drone teams during the scenario.’¹⁰¹ If Australia and NATO countries recognise this reality soon, they will be better prepared for the next major war.¹⁰²

EW is now an arms race. Drones may prevail today—but counter-drone systems will decide who wins tomorrow. The EW battle in Ukraine is pervasive and dynamic. The cat-and-mouse between drones and EW in Ukraine has led to several emerging best practices. One is the need for resilient C2 networks: the AFU, for instance, leveraged SpaceX’s Starlink satellite internet to ensure that drone operators could communicate and send back video even when local communications were jammed. This use of satellite links has big implications—NATO and ADF planners are now looking at how to integrate satellite communications and redundant links for their uncrewed systems in high electromagnetic interference environments.

Finally, the Ukraine war has exposed capability gaps in counter-drone defence. Many advanced militaries (NATO included) did not have large stocks of cheap anti-drone weapons, or enough tactical EW units, going into this conflict. Stopping drones cannot rely on one silver bullet—it requires radar detection, jamming, spoofing and point-defence weapons working in concert.

Each soldier is a sensor/target on the battlefield. As uncrewed systems are continuously developing, the measures to counter these technologies are also developing in a cycle of rapid innovation. Media often talks about how effective Russian electronic warfare systems are. But the reality is, the beauty of these drones is they don't care about external signals. They aren't transmitting. They rely on airspeed and a compass—old-school navigation, just done by a computer. If they can't receive GPS, it doesn't matter. They continue the mission. It's practically impossible to jam a system like that. If you knew exactly where it was, you could theoretically destroy it—maybe with something like an EMP—but that causes a lot of collateral damage to other systems, so it's not something that would be used routinely. If you can't see the drone, you don't know where it is to target it. (P38)

What's Next?

In September 2025, Ukraine reportedly became the first nation in history to deploy an autonomous drone swarm in combat, believed to be able to coordinate, adapt and strike with minimal human input.¹⁰³ Drone swarms, whether utilising AI or not, cannot be countered by limited-ammunition C-UAS platforms due to the inherent redundancy of individuals within the swarm. For example, a C-UAS system that relies upon conventional surface-to-air projectiles will be unable to eliminate entire swarms and so is unable to cripple the adversary's operational effectiveness. This weakness is driving investment in directed-energy weapons (DEW) solutions. Lasers (light amplification by stimulated emission of radiation) are a form of DEW that can destroy vital segments of a drone's airframe, causing it to fall to the ground. Lasers offer a low-cost-per-shot option to operators, requiring only electrical energy rather than chemically propelled munitions.

Much like laser-powered DEWs, high-powered microwave (HPM) systems offer solutions to drone threats that have emerged or developed during the war in Ukraine. The HPM weapons are DEWs that direct pulses of high-intensity microwave energy at the drone, disabling the aircraft's electronic systems. These weapons carry similar benefits to lasers, being low cost per shot. Current versions of HPMS, which are being tested or in prototyping, can operate within a limited range and power. These systems are anticipated to be effective for terminal defence against some types of swarm attacks or could be mounted forward on mobile platforms that intercept and incapacitate swarms further away from the area, personnel and assets being defended.

Directed microwave weapons can be useful, but again, they're easy to counter—for example, with reflective materials. That might increase radar signature, but you could even use that deliberately. You could fly multiple drones, let defenders shoot the wrong one, while the real drone has minimal reflection. All of those techniques are now pretty standard. (P22)

I think laser weapons make the most sense. They are the most cost-effective counter-UAS solution. I think they are probably going to be more effective than shotguns and certainly a lot cheaper than missiles or other types of ammunition used to bring drones down. For me, laser weapons make sense as the most effective counter-UAS option, but I didn't see anything regarding their actual use in Ukraine, based on open-source information, but I know they are exploring mounting them on ships and other major platforms, whether as a counter-missile or counter-UAS capability. Obviously, the power available on a ship is very different from what you would have in a trench. I saw that there is the Australian company EOS, like electro-optical system, and they have developed a laser that apparently works, 100 kilowatt high-powered laser, but we'll see. (P25)

The challenge also remains to counter drones that are continuously increasing in numbers and advancing in its capability. Each conflict for the last year involved missiles and drones as the key offensive capabilities. According to the Commander of the USF:

Our [Ukrainian] experience will be invaluable for the entire rational world, because any country could face a similar scenario. I don't know of a single NATO country [to date] capable of defending its cities if faced with 200–300 Shaheds every day, seven days a week. Your national security urgently requires a strategic reassessment.¹⁰⁴

Recommendations

Recommendations to the ADF and Military Leaders

1. Elevate EMS and EW literacy from a niche specialisation to a universal soldier competency.

Modern warfare is defined by the contest for EMS dominance, yet the ADF continues to treat EW as a niche signals corps capability rather than a foundational combat skill. This must change. Every soldier in the ADF—not only signals and EW specialists—must possess a working understanding of their own EMS signature, the signatures emitted by their equipment, and the implications of those signatures for survivability and operational security. The ADF should:

- establish **all-arms EMS education** as a mandatory competency embedded in initial and continual training, raising baseline EMS awareness across the force to a level where tactical commanders can integrate EMS management into mission planning as naturally as they integrate fire support or logistics
 - develop **joint EW integration** frameworks through close collaboration between the Air, Land and Maritime Warfare Centres, producing joint tactics that account for the distinct EMS challenges and interdependencies of each domain
 - mandate **EMS deconfliction planning** between friendly EW teams and UxS operators at all echelons, recognising that friendly EW emissions can and do suppress friendly drone operations if not planned and coordinated with the same rigour as fires deconfliction.
2. Build realistic, adversarial C-UAS architecture and move beyond scripted demonstrations.

C-UAS is a fundamentally difficult physics and engineering problem, and its solution cannot be validated through scripted, pre-announced demonstrations conducted under controlled conditions. The ADF must move towards rigorous, unscripted, adversarial C-UAS testing that replicates real-world threat behaviours—including unexpected flight profiles, multi-axis attack, frequency agility and swarm saturation—rather than proof-of-concept events announced months in advance that fail to simulate the unpredictable, adaptive nature of drone swarm employment. It must be clearly acknowledged that some systems currently being presented and evaluated in Australia are already tactically obsolete or insufficiently developed relative to the current battlefield standard.

Systems at different levels are needed to protect individual soldiers, cities, critical infrastructure, etc. in ways that vary in their effects. A layered architecture should be built for sensing and effecting to include an ecosystem of kinetic and non-kinetic solutions (e.g., kinetic interceptors, electronic jamming and directed-energy weapons). Training for all systems should be pushed down to every combat unit rather than remaining centralised at specialist establishments.

The cost-exchange ratio principle must be embedded in all C-UAS acquisition decisions: counter-drone systems must be demonstrably cheaper to produce and operate than the systems they are designed to defeat, or they do not represent a viable long-term solution against a high-volume, low-cost threat.

The ADF should accelerate Project Land 156 and establish rapid iteration cycles for C-UAS capability. Given the pace of UxS threat evolution—where a tactical advantage can become obsolete within weeks rather than years—the ADF must explore every available avenue to accelerate Land 156 (tactical UAS) timelines, ensuring the force trains on, experiments with and fields systems that are current rather than legacy.

Capability programs for C-UAS should be structured around rapid iteration cycles modelled on the basis of a 24-6-6 framework: continuous tactical adaptation (frequency changes, employment adjustments) on a daily basis; hardware and software upgrade every six weeks; and full capability updates every six months. This cycle is incompatible with traditional multi-year acquisition timelines and requires a dedicated rapid acquisition pathway for C-UAS systems classified as attritable or expendable.

The ADF should develop a variety of very low-cost hard-kill and soft-kill systems to be used against drones and missiles. These systems should be at lower cost than the drones or missiles they are sent to defend against.

3. Operationalise a sovereign ‘drone wall’ as a deterrence-by-denial instrument.

In alignment with the 2026 National Defence Strategy and its emphasis on ‘deterrence by denial’, the ADF should operationalise a high-low capability mix in its northern approaches that integrates high-end platforms such as the MQ-28A Ghost Bat with thousands of low-cost, sovereign-produced systems—including Syraq, Quantum Systems tactical UAVs, and Speartooth USVs.

4. Establish clear policy, legal and ethical frameworks for lethal autonomy.

The speed of drone-saturated battlespaces requires a fundamental reassessment of command authority and rules of engagement for autonomous and semi-autonomous systems. The ADF and the Australian Government should develop clear, unambiguous policy, legal and ethical frameworks governing human-in-the-loop, human-on-the-loop and human-out-of-the-loop configurations across multi-domain operations—recognising that these distinctions have direct operational, legal and ethical implications that cannot be resolved by default during a conflict.

Rules of engagement should be reviewed and updated to permit autonomous or semi-autonomous responses to high-volume drone swarm attacks in scenarios where the speed of engagement exceeds the capacity of a traditional human-centric kill chain, while ensuring human authorisation of mission parameters and engagement rules prior to autonomous execution.

5. Protect vulnerable assets.

Even the most advanced autonomous systems are vulnerable while they are on the ground being refuelled or maintained. Defence should prioritise the physical and electronic protection of the ‘hubs’—logistics nodes and runways—recognising that large, high-end assets are easily detected via radar and transponder emissions during their most vulnerable operational phases.

Recommendations to Local Commanders

- Commanders should integrate EMS management into every mission planning process, treating electromagnetic signature as a targetable vulnerability requiring the same discipline as physical concealment and camouflage.
- Every combat unit should train regularly on available C-UAS systems, treating counter-drone defence as a core section- and platoon-level skill rather than a centralised specialist function.
- Commanders should advocate strongly for realistic, unscripted C-UAS testing in their unit's training cycle—including adversarial red team drone employment—to develop genuine rather than scripted counter-drone proficiency.
- Physical and electronic protection of ground control stations, relay nodes and communications infrastructure should be treated as a primary force protection task, equivalent to the protection of crew-served weapons or command posts.

Recommendations to Government

- Government should fund the development and procurement of a layered, sovereign C-UAS architecture spanning kinetic interceptors, electronic jamming and directed-energy systems at every echelon of the force.
- Procurement policy for C-UAS systems should embed cost-exchange ratio as a mandatory acquisition criterion—no C-UAS system should be procured if its unit cost exceeds the cost of the threat systems it is intended to defeat at realistic attrition rates.
- Government should resource an accelerated timeline for Land 156 and establish a dedicated rapid acquisition pathway for expendable C-UAS systems operating outside legacy airworthiness certification frameworks.

/ PART II. LESSONS FOR MILITARIES: ADAPTATION AND PREPAREDNESS

Lesson 6: Organisational Evolution—Change Is Needed

In the context of the war in Ukraine, the organisational structure of the AFU has undergone significant adaptation, highlighting the need to formally integrate both drone and counter-drone functions into the structure. With thousands of drones and dollars incurred daily, formalised staffing models, procurement processes, training procedures and asset write-off procedures need to adapt. The Ministry of Defence of Ukraine has approved a list of 32 authorised positions related to operating uncrewed systems. Among them are FPV drone operators, operators of fixed-wing combat and special UAVs, multirotor uncrewed complexes for combat and special purposes, and operators of ground robotic systems, to name a few.¹⁰⁵ Being at war gives Ukraine an advantage, as changes can be made much more quickly. The AFU can identify a need and a location and ‘just do it’.

A good historical parallel is the machine gun companies of the First World War. Rarely used prior to the First World War, machine guns became industrial-scale machines of destruction during the war, requiring their own specific planning and logistics due to their massive ammunition consumption. Initially, the military developed one specialised machine gun company per battalion. Over a short period, they realised they could break these units up and push the capability down to the platoon level, placing it under a lower level of command.¹⁰⁶ Ukraine has approached drone warfare in a similar way. Initially, the battlefield was very dynamic in 2022 and 2023, but it has since devolved into a static front line. As this happened, drones became increasingly vital. In the early stages, when there were fewer platforms and operators, drone assets were held at the brigade level. However, as the number of platforms and operators increased, that capability was pushed down to the company level. Now there is a company commander who has the ability to prioritise drone efforts in direct accordance with their specific mission sets.

Ukraine has achieved this evolution on an incredibly compressed timeline—doing in three years what would typically take us (Australia) ten. They have successfully decentralised a high-tech capability to where it is needed most on the ground.

(P13)

Since 2022, there has been an evolution in the AFU force employment. The need for the role of a drone operator evolved initially out of infantry needs rather than through a single top-down decision. Drones supported small units to provide tactical ISR and immediate support to infantry manoeuvre, giving infantry ‘eyes in the sky’. If a unit had a drone operator, a small quadcopter (e.g. a Mavic) could be launched to check for threats out approximately a kilometre, which significantly improved situational awareness, reduced risk, and simplified infantry tasks. Over time, commanders at higher levels recognised the value and began forming dedicated units to conduct reconnaissance and strike in support of their units.

Within months, commanders at platoon, company and battalion levels saw the value and began formalising specialist units for ISR and strike purposes. First there were strike platoons, then these rapidly grew into dedicated drone strike units equipped with FPV systems. At that time, Ukraine already had specialised ISR units, such as artillery reconnaissance with fixed-wing UAVs supporting indirect fires. Artillery—‘the gods of war’—was the primary striking arm in 2022, so long-range ISR was largely shaped around artillery requirements. Through 2023, the balance shifted as infantry-centric drone employment expanded, and then the special units scaled into battalions.

On 11 June 2024, the USF was created to reduce the burden on infantry formations and enable dedicated units to operate with greater freedom across the battlespace.¹⁰⁷

The USF is the first independent military branch globally that is dedicated to developing and deploying uncrewed systems capability (See Figure 30). This is because the first year of full-scale invasion introduced battlefield transparency to some extent, and pervasive sensor networks have made tactical surprise almost impossible.

The massive, decentralised integration of drones units across all branches required an urgent structural response for coordination, doctrinal support and standardised training. The USF was initially established as a department within the General Staff with a focus on managing localised units and developing basic doctrinal documents for the AFU. In 2026, it transformed into a multi-domain ecosystem to conduct cross-domain operations seamlessly across air, land and sea—and not just in the contested zone but deeply integrated across operational and strategic depth. Structurally, the USF has a number of brigades, regiments, battalions and other units (e.g., recruitment, research and development, support, logistics, intelligence, workshops). The USF now makes up to 2.2 per cent of the AFU (approximately 20,000 personnel) and there are plans to increase it to 5 per cent to cover the entire front line at tactical, operational and strategic levels.¹⁰⁸

Our role was created to be less tethered to a single battalion's line and to operate at operational depth. That operational depth is a core focus now: infantry cannot reach or influence many targets, but we can. At the operational level, you arrive, coordinate support and corridors, execute, and move on. Strategic missions

may operate with different deconfliction arrangements—often requiring sensitive corridor management. We have the expertise, experience, and systems. We need more platforms and more mass across the force to deliver sustained effects. (P33)

Acknowledging the increasing role these systems play in contemporary conflict, Russia mirrored the USF and established a dedicated branch of the Russian Armed Forces focused on drone warfare on 11 November 2025.¹⁰⁹



Figure 30. Control point of the USF of the AFU. Photo credit: USF. Photo reproduced with the owner's permission.

Women in Ukraine's Drone War

According to the defence ministry of Ukraine, there are over 75,000 women serving in the AFU, including 48,000 military service members and more than 5,500 fighters deployed in the combat zone as of 2026. The Ministry of Defence noted that women in the AFU have equal rights with men to hold positions, advance in their careers and attain military ranks.¹¹⁰

Technology has been a major equaliser that has brought a significant shift in entrenched attitudes to gender roles. Competence, not gender, defines success in drone warfare. According to Ukraine's 'mother of drones', Mariia Berlinska, drone warfare demands focus, precision and emotional resilience rather than physical strength, which has opened up this combat domain to women. Women often show strong analytical skills, composure under pressure and teamwork, which make them highly effective drone operators (see Figure 31).¹¹¹



Figure 31. A female drone operator, call sign Yunha, operates FPV drones on the front line in Ukraine's Rubizh Brigade. Photo credit: Rapid Reaction Brigade. Photo accessed via Forbes, 'A Woman's Place Is in the Drone War: How Technology Changes Attitudes.'¹¹²

In April 2025, a new women's unit, 'Harpies', was opened under the USF. While men are still part of the unit, only female drone pilots in this unit can deliver a final strike (see Figure 32). Harpies describe their unit as 'an environment for women who seek revenge on the enemy, protecting their children, families, and the country using unmanned and robotic systems.'¹¹³

This is a historic change in Ukraine's military culture, where 'technical skill trumps physical prowess' and capable female drone operators are recognised as combat aces alongside their male counterparts. The social impact of the drone revolution is already being felt in Ukraine's military. Hand-to-hand combat looks like a relic of the distant past. Getting within rifle range or even seeing the enemy face to face is a rarity. As one Russian prisoner mentioned, on the battlefield he did not see a single Ukrainian soldier—only drones.¹¹⁴



Figure 32. ‘Harpies’ preparing the Vampire drone for a mission. Photo credit: USF. Photo reproduced with the owner’s permission.

Organisational and Workforce Challenge

Experience from Ukraine highlights that integrating uncrewed systems is primarily an organisational and workforce challenge. While senior leadership may articulate the need for drones and counter-drone capabilities, the difficulty lies in implementation at battalion and brigade level within existing organisational structures. The introduction of dedicated uncrewed systems elements, such as platoons, companies, regiments, battalions and brigades, is in continuous progress in Ukraine. As noted by the Commander of the USF of the AFU, the main goal is to increase strike capabilities, strengthen deep strike capabilities and enhance the ability to act against strategic enemy targets. At least several regiments were reformatted into brigades and special USF centres, and battalions were reformatted into regiments, to complete assigned UAS/C-UAS missions.

At battalion level, the establishment of a dedicated uncrewed systems platoon typically requires approximately 30 personnel. When replicated across multiple battalions, this creates a cumulative demand that must be supported at brigade level with additional specialists for coordination, logistics and C2. In practical terms, three battalions can require close to 100 additional personnel at brigade level. For smaller armies, this represents a

substantial burden in terms of recruitment, training, funding and sustainment, particularly when coupled with broader force-structure reforms such as the reconstitution of brigade headquarters, as seen recently in parts of Europe.

Organisational transformations take place among other domains of operation. For example, the 20th Separate Battalion of Unmanned Ground Complexes (K-2) has announced the formation of the world's first battalion of UGVs, a milestone that further strengthens Ukraine's innovative approach to modern warfare, as was reported on 3 August 2025. This new battalion will focus on enhancing Ukraine's battlefield capabilities, improving logistical support, and expanding the use of autonomous systems to protect and assist soldiers on the ground in high-risk environments. By pioneering the deployment of unmanned ground systems, Ukraine is positioning itself at the forefront of military innovation, setting a new precedent for the future of autonomous warfare.¹¹⁵

Ukraine's experience further demonstrates that scaling drone operations exposes critical administrative and sustainment challenges. High attrition rates of relatively low-cost systems quickly generate significant financial losses at unit and state level, necessitating formalised procedures for procurement, accountability, and write-off of destroyed equipment. In Ukraine, initially the absence of such mechanisms led to reliance on volunteers and ad hoc solutions until formal roles were established, such as designated non-commissioned officers or officers responsible for materiel accountability and internal investigations. These processes are often invisible at lower tactical levels but become unavoidable as drone losses scale into the tens or hundreds at brigade level.

Coordination Between Echelons Is Critical

UAS capability is necessary at multiple echelons and coordination remains critical. Today, every competent unit across the Army, Navy and Air Force has its own drone operators. This reflects an evolutionary process driven by battlefield necessity. As participants mentioned, relying entirely on neighbouring units is risky because units may redeploy at short notice, and there is a time gap before coordination is established. A significant proportion of drone survivability depends on interaction with friendly forces to avoid fratricide or electronic interference. Boundaries are set through combat orders and defined responsibilities. Brigades have assigned areas/lines of responsibility depending on the intensity of combat. Adjacent boundaries are 'seams' between units, and combined units may be positioned there. UAV employment beyond one's boundary requires interaction and deconfliction between units.

If you want to fly into a neighbouring unit's sector, you must coordinate so you are not engaged by friendly forces. In practical terms, effective coordination with friendly units can be half of your platform's survivability. If neighbouring units can

provide coverage, that is helpful, but you cannot rely on it because units move. There is a gap while you establish relationships with new neighbours. This is tied to the battlefield management system. It is usually formalised through combat orders. There are standing regulations and doctrinal approaches defining how each service operates. For example, brigades are assigned areas of responsibility (AORs) and boundaries. Depending on combat intensity, a brigade might hold 3–5 km, or more; in extremely intense sectors, frontage can be compressed dramatically. Usually, a brigade might be responsible for a much larger frontage (exact figures vary widely by theatre and force density). Corps headquarters now assign and manage multiple brigades. Adjacent units operate side-by-side along contact lines. Drones may operate at 3 km for immediate effects, or further for ISR and strike. The key is coordination and deconfliction: if you want to fly through another unit's airspace or sector, you must coordinate so you are not engaged by friendly forces. This is a major determinant of survivability. We joke amongst ourselves that 'the only thing worse than enemy EW is friendly EW'. The same applies to C-UAS engagement and fires. (P33)

An ideal situation for Australia would be: obtain own internal reconnaissance and at least some strike UAS capability. This is advantageous for two reasons: (1) it's a force multiplier in terms of the effect you can have on the enemy; (2) the amount of situational awareness that this grants a dismounted or mounted manoeuvre commander is incredible. It will provide battlefield awareness and enable coordination—which is significant. For example, a section commander launches their drone, flies it over the next hill, and identifies a mechanised company moving forward in the distance. This is a generalised example, but immediately from there, they can raise that information very quickly. They can provide a grid reference; they've got live video feed and can start cueing assets to strike those targets. If this capability exists at a section level, that is ideal. Realistically, where the Australian military is at the moment, if we can even get a dedicated section of UAS operators within each company, that would be achievable in the short term. But that requires recognition that change is needed. People need to get ambitious quickly, because this isn't being ambitious about something unproven. This is ambition based on something that is already tried, tested, and has only positive outcomes. (P29)

In operational reality, therefore, the decisive shift in drone warfare lies not only in the proliferation of platforms but, importantly, in the restructuring of forces to accommodate them. Drones must be treated as integral elements of the combined arms system—resourced, commanded, and sustained as such—rather than as bolt-on technologies. Failure to institutionalise UxS risks misjudging both their contribution to combat power and the scale of investment required to sustain them in high-intensity conflict.

Across NATO countries, the proliferation of UAS and the rapid escalation of EW have driven a reassessment of how militaries organise and sustain their forces. Operational lessons from Ukraine have demonstrated that drones and counter-drone activities generate persistent demand for trained operators, analysts, EW specialists, maintainers and planners. It is now well recognised that these functions cannot remain ad hoc tasks absorbed by traditional combat arms but instead require dedicated workforce structures embedded across the force. Several NATO members have already initiated structural changes. Countries such as the United Kingdom, Germany, Poland and several Baltic states are expanding dedicated UAS and EW billets while strengthening brigade-level headquarters to better manage drone effects across the battlespace. In some cases, this has coincided with the reconstitution or expansion of brigade structures, recognising that modern high-intensity conflict requires both mass and technical specialisation. Workforce growth at command and staff levels has been necessary to plan, coordinate and synchronise UAS, EW and counter-UAS activities alongside manoeuvre forces.

The United States has expanded UAS and counter-UAS roles across the army, marine corps and joint forces, creating dedicated military occupational specialties and career pathways for drone operators, EW personnel and multi-domain effects coordinators. UAS and EW functions are increasingly positioned at battalion, brigade and higher headquarters levels to enable coordination across depth rather than remaining tied solely to manoeuvre units. This reflects a shift towards recognising drone and EW operations as continuous, staff-intensive activities requiring permanent organisational ownership.

In Canada, the Canadian Armed Forces are similarly adapting workforce models to integrate UAS operators and EW specialists more formally within land, air and joint structures. Rather than treating drones as niche enablers, Canada is investing in training pipelines, simulation, and specialist roles that support both UAS employment and counter-UAS protection of forces and infrastructure. This includes closer integration of drone and EW personnel within intelligence, fires, and C2 functions, acknowledging the importance of sensor-to-shooter integration in modern operations.¹¹⁶

Australia is facing similar pressures, and this underscores the need for the ADF to adapt its workforce structure to accommodate dedicated drone operators, EW specialists and counter-UAS roles. According to Major General (Ret.) Mick Ryan, as part of strategic adaptation, the ADF as an institution will need to be able to rapidly adapt its force structure to take into account the large-scale penetration of uncrewed systems in the land, air and sea domains, noting that there is no one-size-fits-all solution. Different environments and missions will demand different balances of crewed and uncrewed systems. This will also demand adaptations to force structure and, at a minimum, the formation of multiple new drone and counter-drone units in the army, navy and air force and their reserve components.¹¹⁷

Recommendations

Recommendations to the ADF and Military Leadership

1. Establish a formal unmanned systems force with a unified mandate and senior leadership.

The proliferation of UAS and EW is no longer a niche technical challenge—it is a prerequisite for operational relevance in any peer or near-peer conflict. The ADF should establish a formal, dedicated USF—or an organisational equivalent—providing unified senior leadership, strategic prioritisation, central direction and coordination, doctrine development, and guidance for investment in both uncrewed systems and counter-drone capability, training and sustainment. Current efforts remain fragmented, bottom-up, and dependent on individual initiative; these must be replaced by top-down, accountable institutional leadership with the authority and resources to drive change across all services. Initially, this structure could be embedded within Joint Forces Command, but its workforce development pipeline must be fundamentally reimaged rather than grafted onto existing structures.

2. Establish a centre of excellence for UxS and C-UxS.

Working in direct partnership with the newly established USF, the ADF should establish a dedicated centre of excellence for UxS and C-UxS that enables rapid research and development, test and evaluation, and deep collaboration between Defence and the defence industry on specific, operationally defined problems.

This centre should maintain large-scale ‘sandbox’ testing areas utilising Australian national territory—offering realistic operational conditions across diverse terrain and maritime environments—to drive innovation in uncrewed and autonomous systems at the pace the threat demands. Where a sovereign centre of excellence is not immediately achievable at full capability, the ADF should actively explore formal collaboration with established international equivalents, including the UK Uncrewed Systems Centre of Excellence and the Latvian Autonomous Systems Competence Centre.

3. Introduce robotic warfare brigades and formalise drone units at every echelon.

The ADF should introduce dedicated robotic warfare brigades—or equivalent formations—integrating regular, reserve and volunteer workforces to accelerate the fielding of UxS capability at scale. Every brigade should incorporate drone companies and, ultimately, a drone battalion as organic elements, with specific problems identified and worked through directly with defence industry partners in realistic operational environments. The whole of force—from individual soldiers to senior commanders—must be prepared to integrate the UxS threat layer into all operations: in international waters, in contested and congested EW environments, and in GPS-denied conditions.

Training approaches must change to replicate the rapid skills obsolescence cycle that characterises drone warfare, ensuring operator currency is actively maintained rather than treated as a one-time qualification. Regulatory frameworks must be revised to enable uncrewed systems training, experimentation and operation to occur without the administrative burdens that currently constrain the ADF's ability to develop this capability at pace.

4. Formalise career pathways and workforce structure for UxS specialisations.

The ADF should acknowledge that a modern combat regiment may no longer be composed entirely of infantry in the traditional sense. A target workforce mix of 20 to 30 per cent of a regiment holding specific drone qualifications should be established as a planning benchmark, with clear Employment Category Numbers (ECNs) and officer specialisations created for UAS and C-UAS operators, analysts and maintainers to ensure long-term retention, expert development, and institutional knowledge accumulation. Specific ECNs should distinguish between fundamentally different skill sets—for example, a small UAS operator qualified in FPV strike and loitering munitions employment requires different training and qualifications from a traditional ISR operator. New specialisations should be considered across all services, including dedicated Mission Aircrew educational pathways at the University of New South Wales (UNSW) Canberra and at the Australian Defence Force Academy (ADFA) and structured engagement with the ADF Cadet program and FPV drone racing community to build the pipeline of future operators from the earliest career stages.

5. Expand operational scope from ISR to complex strike, and decentralise command.

The ADF should transition its regulatory, doctrinal and governance frameworks from their current focus on ISR-dominated UAS operations to encompass the full range of complex strike capabilities—loitering munitions, FPV attack drones and semi-autonomous strike systems—that now characterise the operational employment of uncrewed systems in peer conflict. This requires revised doctrine, updated rules of engagement and revised safety regulations governing autonomous and semi-autonomous strike platforms, alongside a fundamental shift in operator training from passive observation to active, integrated lethality.

In parallel, C2 must become significantly more decentralised. In a drone-saturated environment, traditional vertical C2 hierarchies are too slow; the OODA loop of higher headquarters consistently lags behind the pace of frontline decision requirements. The ADF should shift towards more horizontal C2 structures that grant lower-level commanders greater autonomy to act on real-time UAS data, actively testing decentralised C2 models in exercise environments to identify the optimal balance between commander's intent and tactical initiative.

Recommendations to Local Commanders

- Commanders should actively advocate for drone company and battalion structures within their own formations and resist the ad hoc assignment of drone responsibilities to existing roles without dedicated training, resources and time.
- Unit commanders should push for decentralised authority to act on real-time UAS data without requiring higher-echelon approval for time-sensitive engagements and should exercise this authority routinely in training scenarios to develop the cultural and procedural fluency required in combat.
- Commanders should build and maintain a ‘drone community’ within their units—structured around continuous training, knowledge sharing and daily flying practice—to ensure operator skills remain current against the rapidly evolving threat.

Recommendations to Government

- Government should legislate and fund the establishment of a formal USF as a discrete-capability organisation within the ADF, with the authority, resources and senior leadership required to drive cross-service coordination and reform.
- Regulatory frameworks governing UxS training, certification and operation should be revised to remove administrative burdens that are structurally incompatible with the pace of uncrewed systems development. Treating expendable tactical systems under the same regulatory framework as crewed aircraft is operationally and institutionally untenable.
- Government should fund dedicated UxS career pathways, including new ECN structures and educational programs at UNSW Canberra and at ADFA, as a long-term workforce investment rather than a discretionary training expense.

Lesson 7: Train Everyone, Train Rapidly, Train Continuously.

All ‘sensible’ partner countries must begin preparing more actively and learning the lessons paid for with Ukrainian lives—because, in time, they too will be drawn into war.

USF Commander Magyar Brovdi, 2025 International LANDEURO meeting, Wiesbaden¹¹⁸

In addition to an ever-growing drone industry, the rise of UxS has necessitated a new education and training approach. Since 2022, dozens of private UAV pilot training centres have emerged in Ukraine, but until recently there was no unified system regulating their activities. A key achievement in 2025 was the establishment in Ukraine of a nationwide network of certified training centres for drone operators. A broad range of training programs is offered to both civilian and military participants, combining theoretical instruction, practical flight experience, and specialised combat and reconnaissance skills. These programs include basic multirotor, fixed-wing, and FPV drone courses for combat conditions, as well as special operations and EW fundamentals. Courses vary from two-day weekend sessions to four-week programs.¹¹⁹ Training courses are continuously redesigned to meet the evolving needs of the military based on frontline experience and requirements. Practical training is conducted with the systems and in locations that replicate the real battlefield (i.e., fast-moving UAV, contested EW, GNSS-denied environment).¹²⁰

Drone operator training remains a significant investment. Even with simplified control systems, effective operational proficiency takes time. While basic training may take approximately 30 days, true competency requires continuous improvement and operational experience. Training on military-grade systems differs substantially from civilian platforms and involves learning military procedures, communication protocols and mission planning. Although the controls may be simpler than traditional aviation, operators still need tactical awareness, target identification skills and coordination with other units. This means that readiness is not simply about flying a drone but understanding its role within the wider battlefield system.

Western militaries are looking to Ukraine’s training models to inform their own capability development.¹²¹ Western forces, including the British Army, have adapted Ukrainian training curricula based on lessons from the battlefield. For example, emphasis on substantial practical drone flight time, around 60 hours of combined simulation and live flying, has been adopted to raise proficiency to combat-relevant standards. This knowledge was gained during their support of Operation Interflex, the UK-led effort with 13 other countries, including Australia, to train Ukrainian soldiers in Western and NATO-style fighting. The British Army has also made other changes based on Ukrainian advice, including adding anti-drone nets to training and using 3D printing to quickly and cheaply produce

drone parts.¹²² The US Army has also been learning from Ukraine about the value of simulators in drone training, designed to help the service catch up on drone warfare. Other Western militaries are seeking similar guidance. Poland and Norway have looked to Ukraine for help with training operators, while Ukrainian specialists have travelled to Denmark to participate in counter-drone exercises.

*Interflex doesn't actually train new operators from scratch; instead, we take existing operators and enhance their skills through exposure to tactical missions and advanced flying. My own qualification within the Australian Army for multi-rotor UAS was focused heavily on civil aviation rules, such as maintaining a 30-meter distance from people and understanding basic regulations. In contrast, training Ukrainian pilots is entirely different. They start with approx. 40 hours on a computer-based flight simulator—using apps like Liftoff from Steam that serves as their gateway. For FPV, they complete 40 hours of simulation, undergo testing, and then move on to 40 hours of live flying with instructors, provided they demonstrate the necessary skills and abilities. As a side note, the Australian Army recently sent its drone racing team to Military International Drone Racing Tournament (a global Defence Forces competition). The Australian team won, which is remarkable! Interestingly, most were 16-year-old cadets rather than full-time soldiers. They were just kids in training.*¹²³

Interesting, Ukrainians are not taught how to fly to win a drone competition. That type of flying isn't particularly relevant to the front lines. According to a Ukrainian operator who flew there, the focus is on tactical flying. This involves maintaining low speeds and low signatures, so the drone is harder to find, see, or hear. It is essentially 'stalking'. You identify a target, confirm it, align yourself, and only in the final minute do you accelerate to 180 km/h to strike. That is the perfect scenario. (P13)

I saw a clear contrast in the UK (Interflex) from 2 pilots in the unit I worked with for training we were doing. They had gone to a UAS school where the training was much more sports-oriented—flying fast through obstacles. These soldiers were very capable, but they had never flown tactically. We spent two days having Ukrainian operators train them on tactical flying. At the end of those two days, the soldiers told us it was the most valuable training they had ever done. Their commanding officer sat in and took notes on how to change their TTPs and SOPs (Standard Operating Procedures). And they actually were drawing information from his operators who had been trained by Ukrainians on how to use FPV tactically, and went to their OC [officer commanding]. That proved to me that this tactical approach is exactly what we need to be doing. It works. (P13)

A significant observation I made while training Ukrainian soldiers was their extreme hesitancy to move anywhere before drones were airborne. A major friction point we encountered in training was trying not to break their reliance on drones, but rather to reinforce basic soldier skills first, and then provide them with drones to enable the foundational skills we were teaching them. We were cautious that an over-reliance on UAS for everything presents a risk. There are strengths and weaknesses to the way we were training. I think we (Australians) should also have been learning more ourselves. The big point is how UAS complements soldier manoeuvre. One important factor is that UAS has been pushed down to lower levels, that gives autonomy to junior commanders to have their own UAS conducting reconnaissance, rather than having to request it from higher headquarters. Because when you have to request it: (1) it takes time, and (2) your mission may not get priority—and then you're at a disadvantage. Instead, they have organic UAS at section and platoon level. So, we're talking about squads of around 8 to 12 soldiers, and platoons of up to 30 to 33 personnel. These UAS are used to complement manoeuvre, and they have the ability to synchronise it when you're conducting an offensive action. (P25)

The ADF needs to get comfortable with bottom-up initiative and pushing authority lower. In the AFU, a corporal might see a high-value target and strike it immediately without asking permission. We need to be comfortable giving that authority to a corporal. Also, we must accept higher risks in training—to people, equipment, and budgets—to make it realistic. If you mitigate risk to zero, the training isn't effective. (P13)

Every frontline soldier must be able to operate a drone just like they can operate weapons and be aware of counter-drone systems to protect against them. We (Australians) were trained to use multiple weapons—grenade launcher, rifle, pistol and so on. Now the drone becomes another 'weapon system' every soldier must be able to use. (P14; See Figure 33.)



Figure 33. Training of drone operators in the real-world environment, in the ‘field’. Photo credit: Volyn Falcons. Photo reproduced with the owner’s permission.

Ideally, a drone operator should have infantry or artillery battlefield experience. Even a very smart person seeing a group of infantry needs to interpret whether they are moving to reinforce, assault, conduct MEDEVAC; how competent they are; or whether they are high-value specialists. If you can only engage one group with fires, you must prioritise correctly. That judgement is competence- and experience-based. (P3).

The Australian Army’s Land Combat College has recently introduced the first course on multi-role drones, ‘Modify and Operate Attack Drones (FPV)’, where trainees are taught to employ stabilised drones predominantly as a reconnaissance platform, but also as a platform to drop munitions or carry other payloads. The instructors recently came off Operation Kudu where they were directly mentored by AFU drone specialists, and they are leveraging that battlefield experience to give the best possible instruction to trainees (see Figure 34).¹²⁴



Figure 34. Soldiers receive a theory lesson during the Modify and Operate Attack Drones (FPV) course. Photo credit: Department of Defence. Photo obtained from Defence, ‘Army Accelerates Drone Training’.¹²⁵

The Shift in Authority and Training

Going forward, everyone in the military must be exposed to these platforms and understand how their individual actions affect the tactical, operational, and strategic levels. However, there is a major difference between the ability to use drones and the authority to use them. In the AFU, we see a structure where:

- Sections have ISR drones.
- Platoons have dropper drones.
- Companies hold FPV assets to allocate as needed.

That system works really well, but it requires understanding that you have to delegate strike authority—potentially even down to the level of a corporal. A corporal might identify a high-value target, such as an artillery piece, and decide to strike it immediately using their own assets and pilot without waiting for permission ...

Regarding Australia's specific changes, my focus was on the company-sized element in the UK. The integration of FPV drones into tactical training within Interflex was an Australian-led initiative. Australian team did the groundwork to make that happen with support from Dutch and British counterparts. When the Chief of Army visited us in the UK, we made sure to have FPVs in the air. Given that he is the patron of the Army's drone racing team, he was highly engaged and was interested in our methodology and has since asked to provide a briefing in Canberra on how we can adjust policies, safety procedures, and regulations to formally integrate this capability into the Australian Army. Having that level of support from the Chief of Army is a very positive sign for the future of the force. (P13)

To adapt, we must make training realistic. This means accepting a higher level of risk to our people, equipment, and budgets. You cannot mitigate risk to zero; if you do, the training is no longer realistic or effective. (P4)

Recommendations

Recommendations to the ADF and Military Leadership.

1. Professionalise the UAS workforce as a core combat trade.

The ADF must formally acknowledge that UAS operation is no longer a peripheral or supplementary skill but a core combat trade requiring professional mastery, dedicated career pathways, and institutional investment equivalent to that afforded to other primary combat specialisations. The current model—in which drone duties are informally absorbed by existing roles without dedicated training, time or career recognition—is operationally inadequate and institutionally unsustainable.

The ADF should establish a formal UAS Operator trade and non-commissioned officer stream with clear career progression, professional mastery benchmarks and retention incentives. This will create the conditions for the development of genuine expertise rather than the perpetuation of amateur-level competence in a domain that is now among the most consequential on the modern battlefield. A 'pilot mindset' should be cultivated across the infantry. The cognitive load on the modern soldier—requiring digital situational awareness, EMS literacy and real-time ISR-to-strike coordination—has increased to a level previously associated only with aircrew and special operations forces. Training must reflect this fundamental shift in intellectual and reactive demands.

2. Compress the decision-to-effect cycle through horizontal C2 and empowered junior leaders.

In a battlespace where the time from drone observation to artillery impact can be

measured in seconds, traditional vertical command structures—in which a soldier must await a commander's decision before acting on ISR data—impose lethal delays that an adversary will exploit. The ADF should move deliberately towards a horizontal C2 model in which the individual soldier and section commander are empowered to act immediately on ISR data within pre-authorised engagement parameters, rather than routing every time-sensitive decision upward through a command post.

Senior leadership across all corps—particularly air and infantry—should receive directed, data-driven education on current casualty attribution from peer-level conflict. The evidence from Ukraine is unambiguous: small arms account for approximately 4 per cent of casualties, while drones account for approximately 80 per cent. Mines and artillery account for the remainder. ADF doctrine must pivot to address these primary lethality drivers rather than continuing to optimise training and force structure around a threat distribution that no longer reflects the contemporary battlefield.

3. Transition training from civil certification standards to tactical combat standards.

Current Western UAS training frameworks have been heavily shaped by civil aviation certification models—emphasising racing skills, safety distances, and controlled environment 'gates' that have no operational relevance in a contested, GPS-denied, EW-saturated battlespace. While building a community of FPV enthusiasts and maintaining the engagement of civilian drone practitioners is valuable for the long-term talent pipeline, military UAS training must be fundamentally restructured around tactical combat standards.

The ADF should transition to a 'tactical stalking' training methodology emphasising low-speed terrain masking, GPS-denied navigation, EW signature management and the avoidance of signature-generating reconnaissance behaviours (e.g., 'live kamikaze' reconnaissance approaches) that would result in immediate operator targeting in a peer conflict environment. The ADF should collaborate directly with AFU veterans and active operators to establish, refine and jointly evaluate standard operating procedures and training programs for UAS and C-UAS employment—ensuring training is built on current threat behaviours and operational reality rather than idealised peacetime safety parameters.

4. Break institutional silos through cross-corps UAS education.

Different corps must break out of their traditional operational silos to develop a shared, operationally accurate understanding of the changed air-land-sea interface that UxS now define. Artillery, engineer and infantry officers should be routinely rotated through joint UAS and C-UAS cells to develop first-hand understanding of how drones have restructured battlefield operations across every functional domain.

This cross-corps education must also address the broader force design context: while high-end strategic assets such as nuclear submarines are essential for island defence

and strategic deterrence, they must be complemented by a force that is trained, equipped and structured to fight and win against mass-attrition drone threats at the tactical level—ensuring that an adversary never reaches the point of prosecuting a breach of Australia’s maritime and littoral approaches unchallenged.

Recommendations to Local Commanders

- Commanders should immediately begin transitioning drone training within their units from civil certification standards to tactical stalking and combat employment standards, drawing on available AFU-derived standard operating procedures and open-source combat footage analysis.
- Unit commanders should establish regular, mandatory drone flying practice as a standing training activity—treating drone operator currency the same as weapons maintenance and fitness—to prevent the skills decay that occurs when drone training is conducted episodically.
- Commanders should ensure that training scenarios include realistic EW conditions, GPS denial and adversarial counter-drone activity, rather than operating in the permissive electromagnetic environment that characterises most current Australian training.

Recommendations to Government

- Government should fund the establishment of a formal UAS Operator trade structure with associated career pathways, education programs and retention mechanisms, treating this as a foundational workforce investment rather than a discretionary training initiative.
- Government should resource AFU veteran and instructor exchange programs that directly support ADF UAS training development, recognising these as the most direct and cost-effective source of combat-validated training expertise available to Australia.

Lesson 8: Adapt and Adopt at Speed

Adaptation is the mechanism to build advantage in many areas of warfighting concurrently, while at the same time negating enemy advantage by attempting to interfere with their learning and adaptation. Learning and Adaptation does not just happen, it must be led and driven by leaders.

Major General (Ret.) Mick Ryan, 'The Adaptation Battle Intensifies'¹²⁶

The Ukraine war has demonstrated that battlefield success increasingly depends on the ability to innovate rapidly, adapt continuously, and adopt at scale. These three actions form a cycle rather than isolated steps. Innovation generates new technical or tactical solutions under urgent operational pressure. Adaptation refines those solutions in response to adversary countermeasures and environmental constraints. Adoption institutionalises successful practices across units, doctrine and industry. In a sensor-saturated, drone-dominated battlespace characterised by EW and compressed decision cycles, this innovation–adaptation–adoption loop has become a decisive component of combat power. The side that can shorten this cycle—moving from prototype to battlefield integration more quickly than its opponent—gains cumulative advantage, not through technological perfection but through operational agility and learning velocity. The rapidly evolving nature of modern warfare in Ukraine necessitates an accelerated cycle of innovation, which currently ranges from a week to approximately three months. New solutions or significant modifications to existing technologies are continuously required to maintain a competitive edge over the adversary. Important, a military institution that learns more slowly than the threat evolves is already falling behind.¹²⁷

Combat Adaptation as a Fundamental Military Imperative

The ability to adapt is crucial in modern warfare, where the pace of change is rapid and the consequences of failure are severe. Adapting is not only about leveraging new technology but also about rethinking how we employ existing systems and organisational structures, and how that informs our doctrine. It requires a mindset that is open to new ideas, willing to challenge conventional wisdom and able to learn from experience. As we continue to analyse the ongoing conflict in Ukraine, it is clear that adaptation must be driven by a culture that values innovation, learning and experimentation.¹²⁸

Effective learning and adaptation extend well beyond the introduction of new technology. The technologies employed in Ukraine would not have produced decisive effects without deliberate human intervention. These interventions have typically taken one or more of three forms: the generation of new concepts, the creation or evolution of organisational structures, and the development of new training frameworks (see Figure 35).

However advanced the technological systems may be, their operational impact ultimately depends on how effectively military institutions integrate them through updated doctrine, reorganised structures and purposeful training. This mindset must therefore be embedded within institutional adaptation processes and incorporated into leadership development models to ensure sustained organisational agility.

As eloquently indicated by Major General (Ret.) Mick Ryan, effective adaptation must be led. Military leaders must nurture people who are actively learning and capable of changing quickly. Such a culture is enabled by clear statements about leadership tolerance for risk and new ideas. What leaders should do at all levels to observe, collect and share lessons about combat and non-combat aspects of military affairs must be defined and disseminated widely.

Leaders must recognise that military adaptation occurs in three distinct forms: peacetime adaptation, adaptation during the transition to war, and adaptation in wartime. Peacetime adaptation is typically constrained by limited resources, extended timelines for experimentation and analysis, and significant bureaucratic friction. Wartime adaptation, by contrast, is driven by existential necessity and therefore proceeds at a far greater tempo. However, the scale, complexity and simultaneity of challenges encountered during war far exceed those faced in peacetime, requiring leaders to place heightened emphasis on learning and adaptation as core elements of their wartime responsibilities. The transition from peace to war constitutes a separate and unique form of adaptation, demanding rapid organisational, doctrinal and cultural shifts under conditions of uncertainty and escalating risk.¹²⁹



Figure 35. A drone operator in the workshop adapting, changing and assembling a drone.
Photo credit: 12th Special Operations Forces Brigade Azov. Photo reproduced with the owner's permission.

Rapid adaptability is critical. For example, we might select something like the Mavic 4 as our medium drone, buy a thousand of them, and then by the time they actually enter service—12 to 18 months later—new versions are already on the market. Then we use them for two years, and suddenly we realise we have been operating with outdated technology for four years. We need to be in a world where we are constantly adapting—constantly adopting new technologies and learning how to take risks with them. That includes experimenting with multiple technologies at once: fitting different antennas, making software modifications, attaching different payloads and pieces of equipment. At the same time, there is a danger. You can burn a lot of money doing this—buying drones, using them for a short period, and then discarding them as technology. So, there should be a balance between rapid adaptation and responsible investment. (P38)

Ongoing Adaptation Cycle

We continue to see ongoing adaptation cycles. Both sides are getting better at using UAS, and they are also getting better at countering them. One critical observation is that almost no drone is used in its original configuration. Every brigade or unit has a technical team that disassembles, modifies and rebuilds drones to suit specific mission requirements. This happens because procurement cycles are slow, supply chains are rigid, and battlefield conditions change more quickly than production timelines.

By the time a drone is delivered—often six months after procurement—the operational environment has already shifted. This forces frontline units to adapt systems locally. As a result, nothing truly works ‘out of the box’. This is not a failure of engineering but a structural reality of modern warfare. (P26)

Militaries must build systems that allow rapid modification, experimentation and iteration at the tactical level. Traditional procurement cycles are incompatible with the pace of modern conflict. From a strategic perspective, democratic nations face a particular challenge. There is hesitation to experiment aggressively due to political, ethical and bureaucratic constraints. However, innovation in this domain cannot be risk free. If we avoid experimentation, we will fall behind.

We need more people, more innovation, and faster adaptation cycles. Defence organisations must find safe but effective ways to test, fail, learn, and improve. Catching up requires institutional flexibility, funding mechanisms that support rapid prototyping, and closer collaboration between operators, engineers, and policymakers. In short, future success will not come from perfect technology, but from systems that can evolve faster than the threat. (P26)

Use Case

The FPV drone battle has been a textbook case of rapid adaptation. To counter jamming by EW units, both Ukraine and Russia began deploying fibre-optic guided FPV drones in 2024. These wired drones trade range for reliability, allowing strikes in high-jamming environments. Ukraine has also introduced AI-assisted targeting for FPVs—e.g. automatic recognition of vehicles in the video feed—to improve hit rates despite enemy interference, reportedly boosting terminal strike success to around 70 per cent by 2024 (up from around 30 per cent early in the war).¹³⁰ Meanwhile, Russian forces increasingly disperse or cover equipment to mitigate the omnipresent FPV threat. The FPV drone has truly become a ‘force multiplier’ for Ukraine’s infantry, dramatically increasing the firepower and reach of small units. It illustrates how a low-cost technology, rapidly iterated, can offset a numerically superior enemy by ‘extending the operational range of soldiers’ and allowing a smaller unit to cover more area with lethal effect.¹³¹

The high attrition of ISR drones forced Ukraine to innovate in sustaining its ‘drone eyes’. Crowdfunding initiatives like the ‘Army of Drones’ enabled Kyiv to distribute thousands of commercial UAVs down to the company level, training scores of new operators. Ukraine also leveraged its tech sector: within a year, the number of domestic drone makers exploded from just seven to over 200 manufacturers, thanks to streamlined procurement and public–private partnerships. This fusion of civilian tech and military need meant troops at the front could request custom modifications (better zoom cameras, silent props etc.) and see them prototyped in weeks. A notable adaptation in 2024 was the deployment of interceptor drones. Both sides started fielding these ‘drone-on-drone’ hunters to protect high-value assets from surveillance.

Finally, heavy Russian signal jamming necessitated robust countermeasures: Ukraine adopted frequency-hopping and multi-channel controls for its quadcopters, so that ‘modern FPV drones operate across 11 or 12 different frequency bands’, foiling any single jammer. Ukrainian EW units also set up centralised counter-drone jamming zones at the front, freeing individual soldiers from having to carry personal jammers. These measures have kept ISR drones in the fight despite a dense EW environment.

Importantly, the war in Ukraine—and recently in the Middle East—has shown that perhaps the most transformative aspect of modern conflict has been the power of new, technology-supported learning and adaptation systems. As Major General (Ret.) Mick Ryan states:

The foundation to rapidly adapt a military institution and its society to a time of war must be set down in peacetime ... The adaptation battle in Ukraine alone is moving at a pace that is incomprehensible to the low-risk bureaucrats and politicians in Australia. A larger ‘adaptation war’ has emerged with Russia, China and North Korea sharing insights in near real time. The most critical element of military institutions ... may well [be] the enhancement of nation’s adaptive capacity in a rapidly changing world.¹³²

Recommendations

Recommendations to the ADF and Military Leadership

1. Establish adaptation as a core military competency and institutionalise it across all operational phases.

Adaptation is not a wartime emergency measure—it is a permanent, structured military competency that must be cultivated, resourced and measured in peacetime if it is to be available at the speed required in conflict. The ADF must move beyond treating adaptation as an ad hoc, leadership-dependent response to operational surprise, and instead institutionalise it as a formal organisational capability with defined processes, accountable owners, and measurable outputs at every echelon.

Adaptation should be explicitly categorised by its operational phase and resourced accordingly:

- Peacetime adaptation: deliberate, strategy-driven evolution of doctrine, force structure and capability—structured, evidence based, and informed by continuous observation of contemporary conflicts, including Ukraine.
- Transition-to-war adaptation: rapid scaling of production lines, training pipelines and ‘warm’ industrial capacity that has been pre-positioned and exercised in peacetime, ensuring the force can surge without starting from zero.
- War adaptation: the ultra-fast, iterative cycle of tactical and technical modification required to survive and counter an active, adaptive adversary—measured in days and weeks, not months and years, and dependent on the cultural and procedural foundations built during peacetime.

2. Address Australia’s adaptation and procurement speed gap as a strategic vulnerability.

Ukraine’s ability to identify a threat, develop a response, test it in operational conditions, and scale it across the force in weeks represents a model of adaptation velocity that the ADF currently cannot match. As Participant 17 observed from direct operational experience in Afghanistan, the ADF’s inability to out-adapt the Taliban’s cheap, rapidly evolving IED threat—despite the technological and resource disparity—cost Australian lives. The same structural failure of institutional rigidity against a cheap, adaptive threat is now the defining challenge in UxS warfare. Australia cannot afford to repeat that failure at a strategic level.

The ADF must create a mechanism for testing, validating and acquiring defence capabilities at a speed commensurate with the threat—modelled on Ukraine’s Brave1 initiative, which creates a tight, closed-loop feedback cycle between frontline users and defence industry, enabling hardware iteration every two to four weeks. This is not a

marginal improvement to existing procurement processes; it is a structural overhaul that treats speed of adaptation as the primary capability metric for the UxS domain.

3. Improve the ADF's capacity to identify and exploit enemy critical vulnerabilities in near-real time.

Adaptation is not only about defending against threats; it is equally about exploiting adversary vulnerabilities more quickly than they can be closed. Leaders at every level should be trained and empowered to recognise adversary critical vulnerabilities—in their drone employment patterns, EW signatures, logistics chains, and operator behaviours—and to develop, test and implement exploitation strategies at tactical speed. In peacetime, military institutions must build the analytical capacity to draw lessons from combat, develop solutions, and ensure those solutions are disseminated across the entire organisation within days, not months.

Recommendations to Local Commanders

- Commanders should actively create conditions for bottom-up innovation within their units—establishing clear, formal pathways for soldiers to escalate novel TTPs or technical modifications to higher echelons for rapid evaluation and scaling, rather than allowing good ideas to remain at the unit level.
- Commanders should document and publish every operationally relevant adaptation their unit develops, however incremental, contributing to the institutional lessons cycle and ensuring that what works in one unit reaches others before the threat changes again.

Recommendations to Government

- Government must fund Brave1-equivalent infrastructure in Australia—innovation sandboxes with direct defence industry and frontline unit integration—as a permanent institutional capability rather than a pilot program.
- Government should overhaul peacetime procurement regulations for expendable UxS to create 'wartime-equivalent' agility in a peacetime setting, with clear legal and policy frameworks that allow rapid fielding of systems that meet operational performance standards rather than full legacy compliance with airworthiness frameworks designed for crewed aircraft.

Lesson 9: Mass Matters

You could conduct most if not all of the airpower roles for the price of a drone, a laptop, and some imagination.

Air Marshal Stringer, CSIS interview series¹³³

In the context of contemporary warfare, scale is manifested in the rapid development, mass production and continuous iteration of uncrewed aerial systems. Drone warfare in Ukraine illustrates how scaling processes influence not only manufacturing output but also doctrinal integration, force employment and tactical adaptation. This section examines drone operations in the Russia–Ukraine war through the analytical lens of economies of scale and operational scaling, demonstrating how mass production, accelerated innovation cycles and system integration are reshaping battlefield dynamics and altering the character of modern conflict.¹³⁴

The ‘ubiquity of massed, uncrewed systems across the land, sea, air and space domains’ has ushered in a ‘new era of mass warfare in Ukraine’, complementing the large-scale use of conventional forces and artillery.¹³⁵ In practice, Ukrainian units employ networks of drones as an extension of their combat power—spotting targets for artillery, dropping small munitions on enemy trenches, or swarming enemy defences (see Figure 36). These drone swarms are highly attritable but are rapidly replaced thanks to domestic production and a pipeline of commercial drone imports.

Quantity has a quality of its own in drone warfare. Ukraine’s strategy of deploying ‘high-volume, low-cost technology’ has paid off, overwhelming Russian defences at times and ensuring redundancy. Western forces, which traditionally favour a few high-end platforms, might need to adjust their mindset to include a high volume of inexpensive drones (and plan for significant losses). The war highlights that a modern military should be as comfortable buying \$500 off-the-shelf quadcopters by the thousands as it is buying a handful of \$5 million UAVs—both have their place.

Western militaries should be prepared to integrate unmanned systems at scale into their force structure. This entails procuring large numbers of drones (from micro drones to larger UAVs) and developing the doctrine to employ them in swarms and as part of combined arms teams. NATO observers highlight that ‘this war has seen remote and autonomous systems of various types operated at a scale not seen before’ and that NATO forces need to adapt accordingly. ‘Mass is the watchword. In 2023 Ukraine was making around 800,000 drones a year. ... This year, we think it’s on track to make millions of them.’¹³⁶ For the ADF, which operates in vast Indo-Pacific distances, uncrewed systems offer a way to extend surveillance and strike reach without risking pilots or large manned platforms.

NATO and its member states are continuing to learn defence capability and operational lessons from the Russia–Ukraine war. The Ukraine war has often been likened to a 21st century ‘industrial war’ for the staggering scale of resources consumed. After decades of low-intensity conflicts, Western militaries were confronted by an enemy firing thousands of artillery shells per day and fielding massed armoured formations—a style of attritional, high-volume warfare many thought consigned to the past. Ukraine had to mobilise its entire economy and society to sustain the fight. As a senior NATO official put it, the conflict has highlighted ‘the need for faster production of weapons in significant mass amid a race to develop new technology through constant innovation.’¹³⁷ Countries such as Japan, Taiwan and the United States have demonstrated a proactive approach by integrating lessons derived from Ukraine into their security policies and procurement strategies.

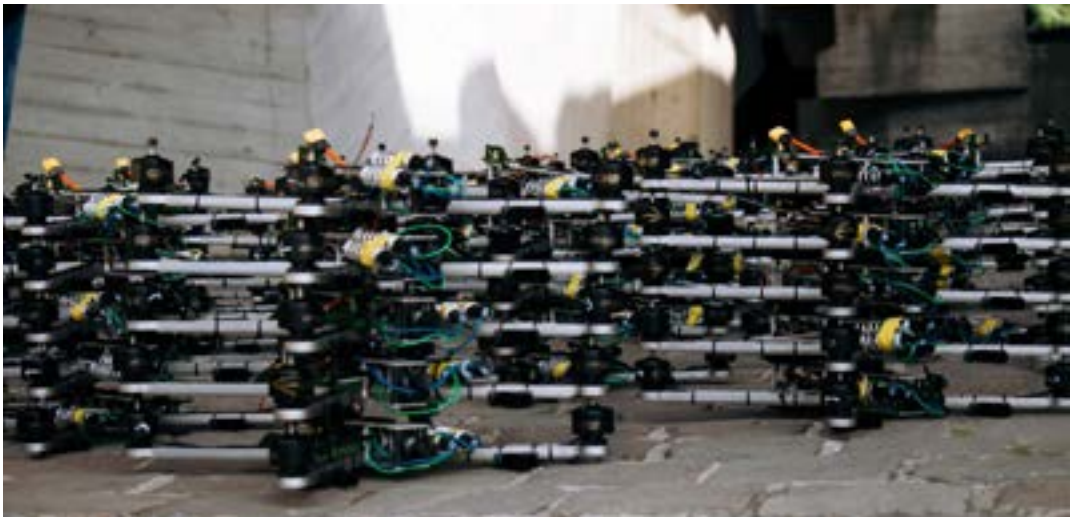


Figure 36. FPV drones prepared for military use by Putyla’s foundation. Photo credit: Serhyi Prytula Charity Foundation. Photo reproduced with the owner’s permission.

Munitions consumption in Ukraine has been astonishing. Both sides have expended artillery ammunition at rates that dwarf NATO’s planning assumptions. In fact, Western stockpiles were quickly depleted as NATO countries rushed to supply Ukraine; this exposed serious shortfalls in ammunition manufacturing capacity. For example, the United States discovered that its pre-war production of 155 mm shells (around 14,000 per month) was woefully inadequate—a fraction of what Ukraine was firing in a similar period.¹³⁸ European allies likewise found their inventories of rockets and missiles shrinking more quickly than they could be replenished. These strains forced a belated surge in industrial output: multiple NATO nations have now launched crash programs to reopen assembly lines, expand factories and fund ammunition manufacturers. A NATO report in early 2025

noted that ‘after decades of underinvestment, nations on both sides of the Atlantic seem to have awoken to the need for a reinvigorated defence-industrial base.’ The war has essentially revalidated the importance of having a ‘war economy’ footing available—the capacity to ramp up production of key military goods (munitions, spare parts, vehicles) on short notice and to sustain that output for months or years.¹³⁹

Ukraine's own experience drives this point home. Blockaded from many foreign arms in 2022, Ukraine undertook a major effort to boost domestic arms production. By late 2023, Prime Minister Denys Shmyhal announced that Ukraine's defence industry output had tripled compared to the previous year.¹⁴⁰ Every second artillery shell being fired at the front was by then Ukrainian made. Factories that once made tractors or machine tools were converted to produce mortar bombs and drones. As a result, Ukraine's annual production of ammunition soared—from roughly 1 million rounds in 2022 to 2.5 million rounds in 2023, a 150 per cent increase. Similarly, production of armoured vehicles quadrupled, and new lines for anti-tank weapons and drones came online. This wartime industrial mobilisation, supported by emergency laws and funding, has been a crucial factor in keeping Ukraine's army supplied. It underscores that capacity for mass production (and the logistics to deploy it) is a strategic asset. Notably, Ukraine's drone manufacturing has exploded: by one estimate, Ukraine was making only a few hundred drones per month in 2022 but is now producing over 4 million drones annually—an explosive growth driven by necessity.¹⁴¹

Mass Matters through the Lens of Defence Workforce and Defence Budget

The renewed salience of ‘mass’ is not just about hardware; it is also about workforce (manpower and unit quantities) and defence spending. Russia mobilised over 300,000 additional troops in late 2022 and 2023, accepting high casualties to hold territory. In 2026, Ukraine mobilises 30,000 to 34,000 a month, while Russia mobilises 10,000 recruits more than Ukraine.¹⁴² Ukraine likewise expanded its forces significantly and created a large territorial defence force—reminiscent of mid-20th century wars in scale.¹⁴³ In such an environment, having depth (in personnel reserves, equipment reserves, and production capacity) is crucial to outlast the adversary. Precision weapons and superior training provide an edge, but without ample stocks and the ability to replace losses, that edge could be fleeting in a long war.

Figure 37 shows the change in defence workforce (i.e., active military personnel) in Australia and NATO countries between 2023 and 2026 (as per projected numbers). Poland, Romania and Greece show the most substantial expansion of defence workforce. The United States remains overwhelmingly dominant, reaching a force level above 1.3 million active duty personnel. Meanwhile Australia records modest growth over the period, increasing from just under 59,673 active military personnel in 2023 to a projected 61,049 in 2026.¹⁴⁴

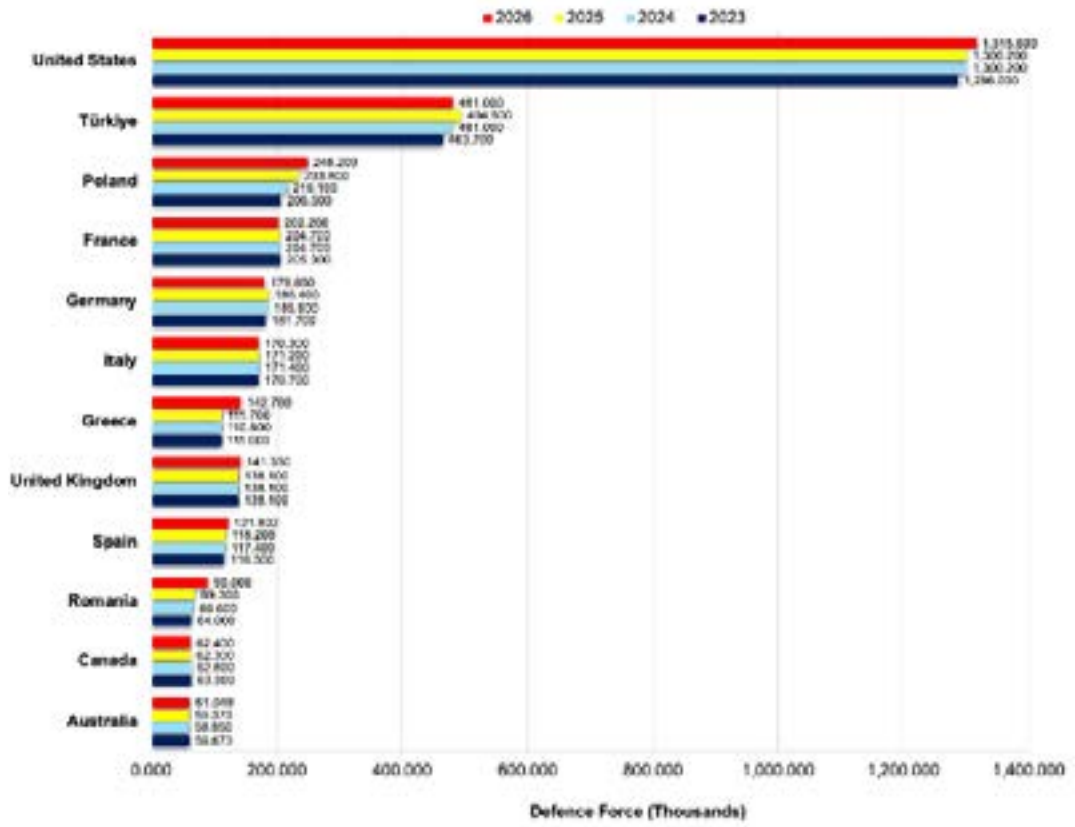


Figure 37. Defence forces of top 10 NATO countries and Australia from 2023 to 2026. This figure presents only active military personnel.^{145 146}

The salience of ‘mass’ is also in the ability of the country’s defence spending to sustain the defence needs. Ukraine’s military expenditure grew by 20 per cent in 2025 and by 1,501 per cent over the decade 2016–2025. At \$84.1 billion, Ukraine’s estimated military spending was at its highest ever level and represented 40 per cent of its GDP and 63 per cent of government spending. Both shares increased in 2025, remaining the highest in the world for the fourth year in a row. In 2025 Russia’s military expenditure reached an estimated \$190 billion, following a year-on-year increase of 5.9 per cent. This marked the slowest annual rate of growth in Russian military spending since the full-scale invasion of Ukraine in 2022. In particular, Russia’s use of UAS has expanded rapidly, partly compensating for earlier losses of more expensive equipment such as aircraft and armoured vehicles.¹⁴⁷

Table 2 highlights the 20 countries with the highest military expenditure in 2025.¹⁴⁸ NATO countries and Australia show the most change in defence effort when measured as

percentage of GDP between 2023 and 2026 (as per predicted numbers). In June 2025, the NATO member states agreed to raise the alliance’s military spending target to 5.0 per cent of GDP by 2035, a substantial increase since reaching 2.0 per cent of GDP in 2024. Of the 5.0 per cent of GDP, 3.5 per cent is expected to be allocated to core military spending, while the remaining 1.5 per cent can be allocated to defence and security-related spending, such as spending to protect critical infrastructure, ensure civil preparedness and resilience or strengthen the arms industrial base.¹⁴⁹

Table 2. The 20 countries with the highest military expenditure in 2025¹⁵⁰

2025 rank	Country	Spending (\$b) 2025	Change (%) 2024–2025	Change (%) 2016–2025	GDP share (%) 2025	GDP share (%) 2016
1	United States	954	-7.5	11	3.1	3.4
2	China	[336]	7.4	62	[1.7]	[1.7]
3	Russia	[190]	5.9	96	[7.5]	[5.4]
4	Germany	114	24	118	2.3	1.1
5	India	92.1	8.9	39	2.3	2.5
6	United Kingdom	89.0	-2.0	32	2.4	2.0
7	Ukraine	[84.1]	20	1 501	[4.0]	[3.7]
8	Saudi Arabia	[83.2]	1.4	12	[6.5]	[9.2]
9	France	68.0	1.5	21	2.0	1.9
10	Japan	62.2	9.7	61	1.4	0.9
11	Israel	48.3	-4.9	120	7.8	5.2
12	Italy	48.1	20	57	1.9	1.3
13	South Korea	47.8	2.6	30	2.6	2.3
14	Poland	46.8	23	207	4.5	1.9
15	Spain	40.2	50	122	2.1	1.1
16	Canada	37.5	23	77	1.6	1.1
17	Australia	35.3	3.0	18	1.9	2.1
18	Türkiye	30.0	7.2	94	1.9	2.0
19	Netherlands	28.9	14	133	2.2	1.1
20	Algeria	25.4	11	89	8.8	5.7

In essence, Ukraine’s experience reaffirms that wars between peer adversaries become tests of industrial and societal endurance. NATO and Australia must regenerate some of the dormant skills of mass mobilisation and industrial warfare to ensure they are not outpaced in a prolonged conflict. Western defence establishments need to reconfigure for an era where industrial preparedness and sheer mass are key to deterrence and warfighting. The Ukraine war serves as a stark warning that NATO’s and Australia’s ‘just-in-time’, small-inventory model is inadequate for peer conflict.

Recommendations

Recommendations to the ADF and Military Leadership

1. Rebalance force mass calculus from exquisite to high-low mix.

Australia's current force structure—concentrated in a small number of high-value, exquisite platforms including Tier-1 submarines and fifth-generation aircraft—is insufficient for a sustained war of attrition against a peer adversary capable of deploying mass. The ADF must complement these high-end strategic assets with a high-volume, low-cost attritable layer that can generate mass, impose cost, and sustain operational tempo independent of the availability of exquisite platforms, which will be conserved for their highest-value strategic roles.

The ADF should establish a persistent 'drone wall'—an autonomous defensive mesh across Australia's northern approaches—utilising thousands of expendable platforms (in the cost range of \$50,000 to \$100,000 per unit) to create a persistent sensor and strike screen that complicates adversary approach, imposes cost on maritime and air incursion, and provides the persistent low-altitude surveillance coverage that satellite systems cannot deliver. This is not a future aspiration; given the pace of threat development documented in this paper, it is an immediate planning priority.

2. Shift from 'just-in-time' to 'just-in-case' stockpile logic.

The 'small inventory' sustainment model—designed for peacetime efficiency—is structurally inadequate for the ammunition and materiel consumption rates characteristic of peer-level high-intensity conflict. The ADF must reassess stockpile levels across all categories of munitions, interceptors and UxS platforms for sustained high-intensity operations in the Indo-Pacific, holding substantially larger reserves that provide genuine insurance against the supply scarcities that constrained NATO and Ukrainian operations in the early phases of the conflict.

3. Build domestic surge production capacity as a strategic investment.

Ukraine's ability to scale from approximately 5,000 drone units annually in 2022 to 4.5 million FPV drones in 2025 illustrates with operational clarity the strategic importance of sovereign surge production capacity. Australia must invest in domestic production capacity—or reliable, diversified allied supply chains—capable of generating uncrewed systems in the quantities required to sustain high-intensity operations. This should include the establishment of rapid-assembly production lines (including 3D-printed and commercial-off-the-shelf assembly capability) and the maintenance of strategic stockpiles of critical sub-components (chips, batteries, motors and airframes) that cannot be rapidly manufactured on demand.

4. Develop robust C-UAS and air defence capabilities to defeat drone swarms.

Mass drone swarms—already demonstrated at operational scale in Ukraine—represent a threat category that the ADF's current air defence architecture is not configured to defeat at scale and at acceptable cost. The ADF must develop and field robust counter-drone measures spanning EW jamming, dedicated interceptor drones, laser and directed-energy systems, and conventional projectile air defences, drawing directly on the counter-drone innovations developed and operationally validated in Ukraine. Every element of this architecture must be designed with cost-exchange ratio as a primary design criterion.

5. Embed mass and attrition planning into force design and exercises.

Military force design must explicitly account for high equipment loss rates and rapid platform attrition as a baseline planning assumption for peer conflict—not as a catastrophic edge case. The ADF should procure sufficient platforms across all categories to equip initial forces and rapidly replace expected battlefield losses, and should develop the doctrinal and organisational flexibility to rapidly establish new formations—including volunteer-integrated drone battalions modelled on the Ukrainian experience—in a transition-to-war scenario. Training exercises must incorporate drone swarm employment as a standard operational condition, teaching junior leaders to exploit unmanned scouts, autonomous resupply, and attritable strike platforms as primary tools of manoeuvre rather than specialist augmentation.

Recommendations to Local Commanders

- Commanders should train their units to plan and operate under assumptions of significant platform and equipment attrition, rehearsing rapid capability regeneration and cross-training across roles to maintain combat effectiveness as individual assets are lost.
- Commanders should advocate through the chain of command for realistic stockpile levels of UxS platforms, batteries, payloads and consumables within their formation, rather than accepting 'just-in-time' resupply models that will fail under operational conditions.

Recommendations to Government

- Government must fund a comprehensive reassessment of ADF strategic stockpile levels for munitions, interceptors and UxS sub-components, with a commitment to achieving and sustaining inventory levels adequate for sustained high-intensity conflict in the Indo-Pacific.

- Government should invest in domestic surge production infrastructure, treating this as a strategic national security investment equivalent to the AUKUS submarine program rather than a discretionary industry support measure.
- Government should introduce multi-year, demand-certainty contracts with sovereign manufacturers of UxS sub-components to enable the industrial scaling required for surge production, recognising that industry cannot invest in production capacity without the demand signal that only government can provide.

Lesson 10: Innovation Ecosystem—Domestic Initiatives, Allied Integration and Strategic Mateship

Technology alone does not win wars; the ability to innovate quickly, integrate private-sector expertise and field solutions at scale is what shifts the balance of power.¹⁵¹ This rapid development has been made possible by Ukraine's agile and decentralised approach to defence innovation, where startups, engineers and volunteer groups play a key role in military adaptation. The rapid evolution of the Ukrainian battlespace has demonstrated that technological superiority is not a static achievement but a continuous process of adaptation. This innovation is driven by a unique synergy between three pillars: grassroots domestic initiatives, structured allied partnership, and the informal but powerful bonds of strategic 'mateship' that bypass traditional bureaucratic bottlenecks.

War accelerates innovation. A system that might take 3–4 years in peacetime can be built in a year under wartime pressure. Innovation did not slow; priorities shift—at times the focus is drones, then EW, then ground robotic systems, then back again—depending on where breakthroughs occur. (P1)

It is very much a war of innovation—that's a big thing to recognise. Personal anecdotes and a lot of open-source reporting talk about particular frequencies Ukraine might be using—for example, employing one specific frequency for a number of drones. Then, within a couple of days, Russia catches on, and there's an electronic warfare defensive action that denies use of that particular spectrum. There's so much back-and-forth, tit-for-tat activity happening. The cycle is: you come up with something new; it gives you a very short window of effectiveness, and then a counter emerges. (P20)

In late 2024/early 2025, fibre-optic drones use was a significant step forward, aimed at defeating the EW vulnerabilities of UAS. What we're seeing now is a much more layered defensive approach to counter those systems. Because the drone has a fixed cable, defenders are using layered obstacles and positioning to deny the drone access to its target. Additionally, there's a lot of footage showing concealment—defensive positions, particularly in areas where fibre-optic UAS are heavily employed. (P29)

In the Kursk region in Russia, fibre-optic drones were used extensively. Ukrainian positions there were heavily concealed in vegetation, essentially using natural terrain to deny UAS access to their targets. When fibre-optic drones tried to strike Ukrainian positions in heavily vegetated areas, they had to move much more slowly

because of the risk of the cable snagging on trees. There was a lot of footage showing Ukrainian soldiers spotting these slow-moving drones and literally pulling out a shotgun and shooting them down. (P25)

The lesson is that the production of unmanned systems should be very agile, and state procurement also should be focused on the needs of the battlefield, and the needs of the military. That is something that in Ukraine is functioning very well just because of the war. So simplified access to procurement, and importantly military units can participate in procurement—something that you don't see anywhere else. Listening to militaries what they need—and to determine those needs faster is important. Also, in Canada, the procurement process can take years, like two years, three years for a large system, even ten years. That's not going to work. You know, if we are moving towards great power competition, it can be in the Pacific, you need to have a job system and you need to incentivize your local producers, your startups. Canadian soldiers have trained around 400,000 Ukrainian soldiers, but they are also learning directly from the battlefield. It's a link where they can learn a little bit about the use of drones. (P29)

Innovation cycles remain rapid, typically operating on a 30- to 40-day rhythm. As soon as one side introduces a capability, the other develops a countermeasure. This creates a continuous evolutionary cycle rather than long-term stability in any single solution. The lesson here is clear: technological advantages in warfare are temporary. The side that can most quickly adapt and scale its innovations will have the upper hand. Ukraine's advantage has not been in the individual technologies it has deployed but in its ability to regularly outpace Russia in the innovation cycle. It is a model that other countries must study if they hope to maintain military readiness in the 21st century.¹⁵²

A key reason for Ukraine's success in defence innovation has been the role of its government in enabling, rather than controlling, the process. Instead of relying solely on traditional procurement systems, Ukraine has fostered a civil–military/public–private partnership that accelerates the deployment of new technologies. An innovation ecosystem has been formed around internal initiatives and joint manufacturing, research and development, and investments. Internally, Ukrainian defence companies are provided with proper technical requirements and state funding. There are around 800 companies involved—not only manufacturers but also suppliers, repair and maintenance facilities and logistics providers. Ukraine's war economy has been driven mainly by private industry, not the state. Various initiatives and defence clusters have been formed since 2022, including Brave1, the Ukrainian Council of Defence Industries (UCDI), Technological Forces of Ukraine, and the National Association of Ukrainian Defence Industries, to name a few, that accelerate innovation, industry and defence cooperation and international collaboration.

Brave1

When even the most advanced technologies have a lifespan of 3–6 month[s] in the current dynamics of the front line, it's hard to overestimate the importance of tight connection with the end-user. Rapid feedback loop is the cornerstone of the effective defence tech solutions today.

Artem Moroz, Head of Investor Relations, Brave1.¹⁵³

Brave1 is a Ukrainian defence technology platform accelerating innovation across all military domains. Founded by the Government of Ukraine in 2023, Brave1 covers the full cycle of military innovation—from analysing real frontline needs to developing, testing and rapidly deploying solutions in combat conditions (see Figure 38). In just two years, Brave1 has become the largest investor in Ukraine, awarding 750 grants to defence technology developers with a total value of approximately US \$86 million. More than 500 solutions have been codified in accordance with NATO standards.¹⁵⁴ Since 2023, Brave1 has launched grant programs for accelerating the development of cutting-edge defence solutions, as well as a number of initiatives. Two of these are 'Brave1 Market' and 'Test in Ukraine'.



Figure 38. Brave1 Demo Day. Photo credit: Brave1. Photo reproduced with the owner's permission.

Brave1 Market

In 2025, Ukraine launched the Brave1 Market, a new online marketplace for defence products, where military units can independently select and purchase equipment for combat operations. A defining feature is the 'Army of Drones' Bonus System, a 'points-for-kills' (ePoints) mechanism where units earn digital currency by submitting verified footage of strikes on enemy assets. These points are then reinvested into the marketplace to acquire more advanced technology, creating a self-sustaining tactical feedback loop. The marketplace is intended to simplify this process by allowing users to quickly compare different solutions, contact manufacturers, and sign contracts directly.¹⁵⁵ It works as follows:

- Troops earn points for destroying and hitting enemy targets.
- Troop units exchange these points for drones and equipment to fulfill combat tasks—on the Brave1 Market, via authorisation in DELTA.
- Supply is handled by the Defence Procurement Agency through DOT-Chain Defence.

Test in Ukraine

Many international manufacturers now attempt to test equipment in Ukraine, often providing it free for battlefield evaluation. But testing alone is insufficient. Ukraine's advantage, particularly for Ukrainian companies, is deep knowledge of frontline realities (tactics, frequencies, migration, protocols), experience operating in real combat conditions, rapid adaptation under pressure, continuous feedback loops, and signature databases (ability to recognise drone types and mission patterns from signal characteristics). Large Western primes have resources to replicate technologies, but they often lack the lived tactical context and the speed of iteration. The Test in Ukraine initiative has allowed Ukraine's frontline forces to provide real-time feedback to developers, ensuring that new technologies are battlefield tested and refined at record speed.¹⁵⁶

Ukrainian Council of Defence Industry

The Ukrainian Council of Defence Industry (UCDI) is Ukraine's largest independent association of private arms and military equipment manufacturers, uniting 280-plus member companies (see Figure 39). It consolidates industry associations, represents their shared position, and works with the state, the military and international partners to accelerate defence production and scale Ukraine's defence industry.¹⁵⁷

The UAS–counter-UAS contest is evolving week by week, and it's increasingly shaped by how fast industry can turn frontline feedback into reliable production. In 2026, UCDI's focus is to strengthen structured cooperation—inside Ukraine and with international partners—so proven solutions scale into predictable capability. Close defence–industry collaboration is becoming a baseline requirement for speed, resilience and quality.

Ihor Fedirko, CEO UCDI¹⁵⁸



Figure 39. Zbroya initiative by the Ukrainian Council of Defence Industry

Allyship and Strategic Partnership: the Global Sandbox

While domestic agility provides the tactical edge, international allyship provides the industrial scale and data architecture required to sustain a long-term campaign. Programs like the UNITE – Brave NATO competition initiative (launched in late 2025) focus on scaling tested technologies to meet NATO interoperability requirements, particularly in C-UAS and signals intelligence. UNITE – Brave NATO is the first joint NATO–Ukraine program for scaling prototyped and tested innovative technologies that help meet interoperability requirements. The focus of the first competition, where companies are invited to submit bids addressing specifically outlined problems, is on bringing to the front line innovative products aiming to counter UAS, strengthen air defence and secure frontline communications.¹⁵⁹

Recent industrial agreements between Ukraine and partner countries have shifted the focus from equipment donation to joint production lines. These initiatives will include cooperation in the production of aerial and ground drones, and preparation to scale up products on the European market.¹⁶⁰ Specifically, the ‘Drone Deal’ announcement in April 2026 by President Zelensky focused on providing a special cooperation format and weapons export arrangement with partners assisting Ukraine. This will include the production and supply of Ukrainian drones, equipment expertise, software, and integration with partners’ defence systems.¹⁶¹

Drone Capability Coalition

Beyond bilateral deals, the International Drone Capability Coalition—led by the UK and Latvia—is an initiative to supply Ukraine with advanced drones, enhancing its battlefield capabilities while also fostering collaboration among member nations. One of its goals is to standardise drone technology and establish long-term manufacturing resilience. It also aims to strengthen industrial capabilities via joint development and facilitate knowledge exchange and training among member countries.

Reflecting on a year of having the immense privilege of leading the Drone Coalition, we have had to evolve as an international organisation in line with the evolution of threat on the battlefield. Our initial approach of constant competition was—in hindsight—not quick enough to match the pace of adaptation we have witnessed in the operational theatre. We must learn from Ukraine’s experience—and they are sharing their knowledge—to ensure that if we too have to face an adversary in the same way, we are ready for the speed and agility required to remain credible. As such, we have shifted to a project approach; coherent lines of effort that seek to achieve a specific mission outcome on behalf of our Ukrainian partners. The first mission given was ‘defeat 500 SHAHEDS per night’ and has led to a collaborative approach that is already providing effective capabilities that are protecting Ukrainian citizens from that particular threat—an outcome we are all immensely proud to support.

Brigadier Stu Nassé OBE, Head Drone Capability Coalition¹⁶²

Ukraine and its allied partners demonstrate several pathways for industrial cooperation. The first is the direct financing model, or the Danish model, to strengthen the defence-industrial base, as direct financing to Ukrainian manufacturers gives flexibility to prioritise and respond to immediate operational needs of the military. The second is production and co-production inside Ukraine. Some of the initiatives in Ukraine have related to ammunition production and maintenance, and repair of European-donated equipment. The benefits

of this pathway are in building shared knowledge and expertise and bringing capabilities closer to the front line. The third is joint production or joint ventures on European/NATO countries and their partners' soil. Collaboration inside Europe provides safer operating conditions and the ability to scale (Ukraine–UK cooperation on interceptor drones, Ukraine–Denmark initiatives etc.). Hence, strengthening defence-industrial partnership with Ukraine is a European response with lasting strategic advantage.¹⁶³ Other allies can learn from these models.

Recommendations

Recommendations to the ADF and Military Leadership

1. Close the innovation-to-frontline loop through a Brave1-equivalent ecosystem.

The core strategic strength of Ukraine's innovation model is not any individual technology but the ecosystem that designs, tests, iterates and delivers capability to frontline units in weeks rather than years. The ADF must build an equivalent ecosystem. This requires bypassing traditional centralised procurement for small, expendable uncrewed systems and implementing direct, unit-level acquisition mechanisms—modelled on a credit-based or marketplace ordering platform—where units can trial and procure sovereign technology that meets operational performance benchmarks, with direct industry feedback enabling iteration every two to four weeks.

The ADF should establish 'sandbox' hubs—permanent testing and evaluation facilities on military ranges with embedded defence industry representatives—where prototypes can be tested under operationally realistic conditions, immediate feedback is provided, and solutions are refined to meet specific, operationally defined problems.

Bureaucratic compliance frameworks should be replaced with agile safety and performance benchmarks designed for expendable attritable systems rather than legacy crewed-aviation standards.

2. Substantially increase institutional risk tolerance for experimentation.

To compete in a drone-saturated battlespace, the ADF must significantly increase its institutional risk tolerance for experimentation, failure, and bottom-up innovation. Current training governance is over-regulated to the point of operational irrelevance: months of administrative process to authorise a single UAS flight fundamentally undermines the experimentation culture required to stay ahead of a rapidly adaptive adversary.

The ADF should remove administrative barriers that impede unit-level UxS experimentation, create formal pathways for soldiers to escalate bottom-up innovations to headquarters or research groups for rapid evaluation and scaling, and treat 'failing fast on the range' as a valued institutional outcome rather than an administrative risk to be avoided.

3. Implement wartime-equivalent regulations in peacetime.

The ADF's peacetime procurement procedures—often spanning decades—are fundamentally incompatible with the weeks-long innovation and adaptation cycles documented throughout this paper. Australia must develop 'wartime-equivalent' regulatory and certification frameworks that allow for the rapid deployment of systems that are operationally effective rather than fully compliant with legacy airworthiness or safety standards never designed for expendable attritable platforms.

The ADF should institutionalise the hard lessons of Afghanistan—where rigid procurement failed to counter the rapidly evolving IED threat despite significant resource advantages—and ensure that the same institutional failure is not repeated against the cheap, high-volume drone threat now defined by Ukraine. Procurement frameworks should be adjusted to treat small uncrewed systems as a category of consumable munitions rather than long-term capital assets, with modular, standards-based certification enabling rapid component-level upgrades on the 24-6-6 cycle (daily tactical adjustments, six-weekly hardware upgrades, six-monthly full capability updates).

4. Decentralise procurement for non-critical UxS and dual-use technologies.

Consistent with the Ukrainian model's demonstrated effectiveness, the ADF should empower local commanders to make independent procurement decisions for urgent tactical UxS needs within defined financial thresholds and performance standards. While this will result in some reduction in standardisation, it ensures the force remains at the cutting edge of rapid adaptation rather than waiting for centralised programs to deliver capability that is operationally current when designed but obsolete when fielded.

5. Foster bidirectional learning with Ukraine and allied partners.

The ADF should formalise and expand its learning exchange with the AFU—inviting AFU instructors and veterans to share operational knowledge and experience in UAS and C-UAS employment, specifically FPV training program development, drone interceptor employment, naval drone operations, and TTP development drawn directly from battlefield experience. The scope of ADF engagement in Operations Interflex, Kudu and Legio should be explicitly expanded to include lessons capture as a primary activity, not a secondary benefit.

Allied innovation investment mechanisms should also be explored: the Danish model of combining national stockpile investment with direct funding of proven host-nation industrial capability should inform Australia's approach to Ukraine-linked industrial cooperation. Collaborative digital architecture standards—modelled on the Ukraine–NATO UNITE program—should be developed and adopted across AUKUS and Five Eyes partners, ensuring interoperability of systems and data from the component level upward. Non-governmental foundations with the agility to fund high-risk, high-

reward prototypes outside the state budget should be recognised and empowered as a legitimate component of the innovation ecosystem rather than treated as peripheral to the Defence enterprise.

Recommendations to Local Commanders

- Commanders should actively utilise available informal OSINT networks and direct peer connections with international counterparts to access tactical-level innovation and TTP updates in near-real time, rather than waiting for formal doctrine updates that will always lag the battlefield.
- Commanders should establish unit-level innovation forums—structured around specific, operationally defined problems—and create clear escalation pathways for promising solutions to reach industry and higher command rapidly.

Recommendations to Government

- Government must fund a Brave1-equivalent innovation hub in Australia as a permanent national capability infrastructure investment, with direct integration between military units, sovereign industry, and international partners.
- Government should invest in research and development partnerships between academia and defence industry, specifically targeting operationally defined UxS problems, and revise peacetime policies and regulations to enable the agile certification and deployment of systems at the pace the threat demands.
- Government should formalise and fund cooperation with Ukraine on joint production, testing, and technology transfer under the 'Build with Ukraine' initiative or an equivalent framework, treating this as both a strategic contribution to a partner nation and a direct investment in Australia's own capability development.

Lesson 11: Build Resilient Defence Industry and Supply Chains—Component Localisation Is Key

In a high-attrition environment where hundreds of thousands of uncrewed systems are lost monthly, the ability to maintain an operational tempo is dictated by the depth and resilience of the supply chains rather than the size of a pre-war stockpile (see Figure 40). As is evident from Ukraine's experience, little of what has been used in the war was developed or stockpiled before full-scale invasion. Ukraine's success in UAS holds a deeper lesson for Australia and its allies and partners: that technological sovereignty at the component level is essential to future battlefield dominance. Almost no military developments in recent history have matched the speed and scale of Ukraine's drone transformation. But behind this manufacturing success lies a critical strategic vulnerability: numerous drone components still originate from China. Hence, the main challenge remains critical—to produce components locally and reduce dependency on Chinese-made components.¹⁶⁴ Ukraine has demonstrated an agile integration model, where innovation is not the invention of a new platform but the optimisation of how components work together.

In the contemporary landscape of attrition warfare, the traditional metric of military success—the technical superiority of a single platform—is being superseded by the ability to sustain high-rate consumption. A tactical victory achieved by technology is irrelevant if the industrial base cannot replenish and sustain it within the next operational window. To maintain a competitive edge within the rapidly shifting parameters of modern multi-domain operations, NATO countries and partners should transition from viewing uncrewed systems as static, 'off-the-shelf' acquisitions towards treating them as evolving, open architectures to be mastered and refined in real time. This strategic shift requires the institutionalisation of agile qualification pathways for dual-use technologies, drastically compressed integration timelines, and the adoption of modular certification regimes that allow for iterative hardware and software updates without the friction of traditional multi-year procurement cycles. Central to this posture is the establishment of persistent data-driven battlefield feedback loops that connect frontline operational experience directly to the industrial base.¹⁶⁵

The primary threat to drone warfare is the 'single point of failure' inherent in global supply chains. Currently, a significant percentage of the sub-components for sUAS originate from a narrow cluster of countries in the Indo-Pacific (notably China and Taiwan). These sub-components include microelectronics (high-end chips for flight control), brushless direct current motors (rare earth magnet sourcing and precision winding capabilities), and energy density (lithium polymer cell production, which remains geographically concentrated). Without localisation, an adversary can achieve 'soft interdiction' simply by restricting the export of specialised components, grounding a fleet more effectively than any kinetic air defence system.¹⁶⁶

To achieve resilience against this threat, component localisation has emerged as a strategic necessity. Relying on global ‘just-in-time’ logistics for critical parts like flight controllers, GPS modules, and carbon-fibre frames creates a single point of failure that adversaries can exploit through sanctions, blockades or cyber-interdiction. By localising the production of these sub-components—often through advanced manufacturing techniques (e.g., 3D printing)—a nation can bypass international bottlenecks. For allied nations, the lesson is clear: building a resilient force requires moving beyond the acquisition of foreign systems towards a networked model of sovereign capability, where domestic component production is standardised and interoperable across the entire network. Australia should prepare for a scenario where there are no options to access foreign components. Hence, there is a strong need for domestic alternatives.

Before the full-scale invasion, I was teaching students and mentoring them on how to assemble drones while I was completing my PhD. When the invasion started, we organised those students and transformed our classroom into a laboratory. That lab became a place where we assembled drones for soldiers on the front line ... The biggest problem at that time was organising components—avionics, communication modules, all the parts needed to assemble drones.

What amazed me was how people helped. So many of my friends who had fled to Europe—to Germany, Australia, the Baltic states, the US—started sending parts by post. Our post office became full of packages with drone components. This is the key lesson: in wartime, if you do not have component stockpiles, you cannot produce drones. You cannot just go to a shop and buy parts. Markets stop working. In Ukraine, if we send a package from Kyiv to Sloviansk—a frontline city—a distance of 600 to 800 km, it arrives in less than 10 hours. Yesterday evening I sent a drone, and this morning it was already delivered to our soldiers, who immediately began combat operations. (P30)



Figure 40. Building an FPV drone from components in the workshop. Photo Credit: 12th Special Operations Forces Brigade Azov, First Corps Azov of the National Guard of Ukraine. Photo reproduced with the owner's permission.

The biggest threat area, which I think the United States has tried to address the most, has actually been handled completely wrong, by imposing a blanket ban of Chinese drones overnight. It destroyed a lot of innovative drone companies because there are no alternatives. For example, there are no magnets available to make motors in Australia that don't come from China. So, when we suddenly say, 'No Chinese products', we discover that our own products contain Chinese chips. That product is banned in the US and semi-banned in Australian Defence. We are trying to design a new version, but we cannot get support from either the US or Australian governments to help us transition to Western chip manufacturers. We have been trying to do this for four years—well before the bans—and it is extremely difficult. What is needed is a concerted government effort to support existing Western drone manufacturers. Governments need to actively use diplomacy and cooperation with allies to identify supply chain gaps and fill them. Instead, what I see is everyone focusing on autopilots—the 'sexy' part. Every man and his dog in the US is starting an autopilot company. But autopilots are already a solved problem. Where are the motors? (P22)

There is this massive push for sovereign manufacturing. If every allied country builds a sovereign drone industry, there is nowhere to sell our drones. That means everyone ends up with tiny industries—or one country crushes the rest and dominates anyway. There is a real risk in overdoing protectionist policies. Yes, I agree we need sovereign capability. We don't have Poland next door. We're geographically isolated. If sea lines of communication are cut, we must have stockpiles domestically. (P22)

Australia needs to stockpile the raw parts, because that allows continuous development and innovation. You do not want to stockpile outdated technology. You want the capability to rapidly build what you need when you need it. Hence, what's required—a resilient domestic supply chain, ready to activate. That means CNC [computer numerical control] equipment for motor manufacturing, rare earth processing capability, and full industrial depth. Australia already has rare earth resources. Australia can be a strategic supplier for the US and partner countries. But not just exporting raw materials—we need to process them here, produce magnets locally, and build true capability, but we will see what happens. (P22)

As outlined in the experts' quotes above, there is a belief in shifting the focus from full sovereign capability to supply chain security. However, developing an entirely sovereign supply chain would require substantial financial resources and prolonged time; hence it is important to strengthen collaboration between allies to sustain resilient supply chains, components production, and longer-term industrial cooperation.

Ultimately, a resilient supply chain serves as a form of non-kinetic deterrence. An adversary is less likely to engage in a war of attrition if they know their opponent possesses an 'infinite magazine' powered by a localised, high-capacity component pipeline. In the age of robotic and autonomous systems, the true 'front line' of the battlefield begins on the factory floor. The ability to localise the production of a \$500 flight controller is as strategically significant as the deployment of a \$100 million fighter jet.

Recommendations

Recommendations to the ADF and Military Leadership

1. Build a military-grade resilient sovereign industrial base.

The ADF must drive the development of a sovereign defence-industrial base capable of sustaining high-volume uncrewed systems production through a conflict of extended duration, independent of supply chains that are vulnerable to disruption, coercion or adversarial interdiction. This requires a fundamental shift in industrial strategy from

centralised, large-factory production models—which present single points of failure—towards distributed networks of ‘micro-factories’ utilising 3D printing, automated printed circuit board assembly and modular integration, ensuring that even if a major industrial hub is targeted or disrupted, production capacity is preserved across the network.

The ADF and the government should:

- map tier-two and tier-three supply chains comprehensively to identify which specific microchips, sensors, battery chemistries and sub-components are at highest risk of supply disruption
- shift from ‘just-in-time’ to ‘just-in-case’ stockpile logic for long-lead, high-risk items—particularly high-end optical sensors, encrypted radio modules and advanced semiconductors—that cannot be rapidly produced domestically
- avoid over-investing in static stockpiles of rapidly depreciating technology. Instead, prioritise industrial readiness—the documented ability to surge production from peacetime rates to conflict-level output within months
- establish a sovereign sub-component manufacturing base operating at low-rate production (tens of thousands of units annually) in peacetime, exercising the skills and processes required to surge to hundreds of thousands or millions within months if required
- introduce ‘subsystem sovereignty’ as a mandatory key performance indicator in all UAS capability program evaluations. A platform that is 90 per cent composed of imported sub-components is a strategic liability in a sustained war of attrition, regardless of its tactical capability.

2. Redefine ‘sovereign’ as control of materials, chemistry, and critical inputs.

Sovereignty in the uncrewed systems domain is not achieved by assembling imported components in Australian facilities; it requires control of the underlying materials, chemistry, and manufacturing processes that determine whether production can be sustained when global supply chains are disrupted. The ADF and Government must secure domestic or Five Eyes supply chains for aerospace-grade carbon fibre, aluminium-lithium alloys, and advanced semiconductors, and establish strategic stockpiles of non-renewable rare earth elements to ensure that production can surge even if global shipping is disrupted or deliberately interdicted.

De-risking Chinese-origin components in flight controllers, propulsion systems and electronic assemblies must be treated as an immediate and urgent priority—not a long-term aspiration—given both the strategic vulnerability this dependency represents and the operational evidence from Ukraine that dependence on a single foreign supplier of critical components can constrain drone production at decisive moments.

3. Develop collaborative standards with allies and partners.

Australia should develop shared component and interface standards within AUKUS, Five Eyes and NATO alliance structures to ensure that sub-components and assemblies produced in Australia are interoperable with airframes, ground systems and command architectures assembled by allied partners. The aspiration—consistent with the Ukraine–NATO UNITE digital architecture program—is a common digital and physical backbone across allied UxS ecosystems, ensuring that allied industrial capacity can surge and substitute for any single nation's production constraint during a conflict.

4. Implement rapid acquisition modelled on the Brave1 framework.

The ADF must move away from rigid, multi-year procurement cycles for UxS capability and adopt a Brave1-inspired framework in which technologies are tested, adapted and fielded in weeks. Procurement frameworks must be restructured around modular, standards-based certification—enabling component-level upgrades and platform modifications on the 24-6-6 cycle—and long-term sustainment contracts must give way to demand-certainty contracting that provides sovereign manufacturers with the production volume confidence required to invest in surge capacity without bearing commercial risk alone.

5. Build the dual-use industrial base as a national strategic asset.

The ADF should leverage the inherently dual-use nature of UxS sub-component technologies—lithium-ion batteries, electric motors, advanced electronics—to develop a broader national industrial base capable of pivoting to military production during a surge, drawing on the full range of Australian commercial manufacturing capacity rather than relying exclusively on a small number of dedicated defence manufacturers. Long-term government contracting should provide the demand certainty that enables domestic firms to scale and remain onshore, complemented by multi-year contracts with clear volume commitments that stabilise the investment environment for sovereign producers of critical sub-components.

Recommendations to Local Commanders

- Commanders should actively advocate for modular, field-maintainable UxS platforms within their units—platforms whose components can be locally repaired, replaced or upgraded by unit technicians rather than requiring return to centralised maintenance facilities, supporting the distributed resilience model at the tactical level.

Recommendations to Government

- Government must fund a comprehensive supply chain mapping exercise to identify single points of failure across the tier-two and tier-three supply chains underpinning Australia's UxS capability and immediately begin funding mitigation of the highest-risk dependencies.
- Government should establish strategic stockpiles of critical, non-expiring UxS sub-components—including advanced semiconductors, sensors and propulsion components—as a national security investment with the same strategic priority as fuel reserves or munitions stockpiles.
- Government should utilise long-term, demand-certainty contracting mechanisms to stabilise sovereign producers of critical drone sub-components, treating this as a foundational investment in national industrial resilience rather than a market intervention.

/ PART III. FUTURE FORCE LESSONS

Lesson 12: Future of Drone Warfare—Autonomy, AI and Swarming

Rise of Autonomy and AI

Autonomy, defined by the US military as ‘a system’s ability to accomplish goals independently or with minimal supervision in complex and unpredictable environments’,¹⁶⁷ is not yet present on the battlefield in Ukraine. The reason for this is that the necessary technology—AI in particular—has not reached the required level of development. Hence, the Ukrainian military uses the term ‘autonomous systems’ interchangeably with ‘uncrewed systems’ or in reference to platforms equipped with basic autonomous functions such as navigation or targeting.

The Ukrainian military’s objective is to remove warfighters from direct combat and replace them with autonomous uncrewed systems.¹⁶⁸ This goal reflects the need to conserve a limited human force and overcome vulnerabilities such as fatigue, stress, and the limited capacity to process and fuse large amounts of data from various sources and sensors. This vision unifies the Ukrainian military and defence industry around the adoption, acquisition and rapid deployment of advanced technologies—including AI-enabled capabilities.

In the military context, AI can be broadly characterised as an analytical enabler, a disruptor or a force multiplier.¹⁶⁹ As an analytical enabler, AI can help with the data-heavy aspects of warfare by collecting, fusing and analysing immense troves of data at scale and at great speeds. As a disruptor, generative AI techniques can both produce and help spread media—be it text, image or video—to be used in disinformation campaigns and cognitive warfare. As a force multiplier, AI is key to enabling the ever-increasing autonomy of various weapons systems. In Ukraine, AI has been present in all three of these functions.¹⁷⁰ For the purposes of this article, the focus is on the latter AI-enabled capabilities.

AI-enabled capabilities are often associated with a foundational technology for transitioning from automated to autonomous systems, or systems that can decide how to achieve a goal rather than merely execute human-programmed algorithms.¹⁷¹ The current deployment of AI is partial in scope, enhancing certain functions and addressing some operational challenges rather than enabling full system autonomy. AI significantly enhances specific functions such as drone footage analysis and target recognition, target tracking and autonomous navigation, including last-mile navigation and sound and text analysis for

intelligence extraction, where AI replaces 99 per cent of human labour. While such systems may operate without direct human control, they typically do not perform the entire process of finding, selecting and engaging targets independently.¹⁷²

Ukraine is developing standalone AI-driven software that can be integrated across various platforms to expand battlefield autonomy. This software enables key autonomous functions such as environmental perception, target recognition and navigation, including last-mile approach to the target. It comes with standalone modules, consisting of compact chips, with embedded software and sometimes cameras. These modules can be integrated into a range of platforms. Hence, companies are focusing on developing separate autonomous functions while ensuring their compatibility across multiple platforms and uncrewed systems.

Delegating target recognition to AI-enabled target recognition systems on board uncrewed platforms reduces human limitations and allows locking on targets up to 2 kilometres away. By automating equipment identification and object detection, drones ease the burden on frontline personnel affected by fatigue, stress, or skill variability. They have extended target recognition from 300 metres to an average of 1 kilometre in combat, up to 2 kilometres in optimal conditions. AI-powered software also counters decoys and camouflage, which can deceive the human eye.

Autonomous navigation makes drone strikes three or four times more likely to succeed. By removing the need for constant manual control and stable communications—both of which are vulnerable to EW and lack of operator skill—drones enabled with autonomous navigation raise the target engagement success rate from around 10 to 20 per cent to around 70 to 80 per cent.¹⁷³

Training to operate uncrewed systems equipped with autonomous features can now be completed in as little as 30 minutes to one day, substantially broadening access to these weapons systems. Drone training programs integrate autonomous targeting and navigation into their curricula, both manual and AI-assisted functionalities.

Ukrainian authorities are exploring the formal adoption and procurement of software and modules equipped with autonomous capabilities. Key initiatives include codifying modules in alignment with NATO standards and integrating them into official military service, which helps to scale acquisition. In 2024, Ukraine bought 10,000 AI-enabled drones. This was a fraction of the total number of drones (2 million), but it shows growing commitment to increasingly autonomous and capable platforms.

Two major challenges lie ahead for AI-enabled autonomy: extending these capabilities to ground, sea and undersea platforms; and enabling swarming. Achieving these capabilities will require sophisticated coordination protocols and real-time decision-making capabilities.

Human oversight remains pivotal, particularly for engagement decisions. Current human-in-the-loop practices allow operators to override autonomous functions, ensuring critical ethical and strategic judgements remain under human control. Human must make decisions.

If we are talking about launching drones, conducting missions, deploying munitions, evacuating personnel, or performing reconnaissance, yes—these missions can be partially autonomous when they are pre-planned. However, the key challenge is targeting certainty. If you do not know precisely where the target is, or whether the target will move, then full autonomy becomes extremely unreliable. In dynamic combat conditions, fully autonomous missions remain very difficult to execute successfully. At the moment, when we talk about fully autonomous systems, they are mostly limited to 'return home' functions if communications are lost, or basic pre-programmed flight paths. True autonomous strike missions without human oversight are not realistic in current battlefield conditions. (P30)

I think the autonomy levels used for cars make sense, because on the road you're trying to avoid hitting other vehicles, trees, pedestrians, animals, traffic lights, and so on. In the air, there's very little to hit, so we don't really care about obstacle avoidance in the same way. Because of that, I'd argue the actual level of autonomy is quite low—the system doesn't need to be particularly intelligent. You choose your flight path, tell it where to go, and it just executes the mission. It doesn't have to be as smart as people claim, because there's nothing to avoid. It's similar to flying a helicopter on a local flight. The pilot simply looks around and says, 'I want to go here, then here.' There isn't much intelligence involved in that flight planning, even with a human pilot. By contrast, when you drive to the shops, you have to avoid dogs, traffic lights—there's far more to think about on the ground. We don't have those problems in the air, which is why these autonomy levels are somewhat misleading. (P29)

We cannot talk about full autonomy. When we write about AI drones, everybody understands this as a drone that can already make decisions without a human being involved, that it can select its own target and attack autonomously. That is something we do not see yet. I think there are developments towards that, but we are not there. Something we recently saw is drone swarms in a testing mode. It was claimed that there have already been around 100 cases of the use of swarming technology by Ukrainian companies on the battlefield, involving between three to eight drones. (P29)

AI-Enabled Drone Warfare

Ukraine and Russia have been developing drones guided by AI in response to challenges posed by EW systems. AI-enabled drones have the potential to identify and lock onto their target without the need for communication with their pilot, making them impervious to signal jamming. These developments in Ukraine are broadly divided into visual systems helping identify targets and fly drones into them, and terrain mapping for navigation.

The potential for mature AI capabilities to dominate the global arena is becoming evident to military strategists and leaders. The decision-making power currently seen through the prism of the OODA loop will evolve with the integration of AI into the entire cycle. The machines and human teaming enabled with AI will act more quickly than an adversary to gain operational and tactical advantage on the battlefield.¹⁷⁴ In the context of UAS warfare, AI-enabled drones may allow for faster OODA loops and hence facilitate a faster decision-making process for UAS operators. Further technological advances in computing power that supports AI will allow more capability to be installed on smaller, cheaper drones. Using AI, drones may react autonomously to changing circumstances and communicate with each other to orchestrate a sortie.

AI-powered drones can do in seconds what would take a human several hours, simply because human performance is limited to a slow process of large volume of information; while the swarm is effective because one experienced drone pilot can work effectively with dozens of drones at the same time. (P11)

If your OODA loop is faster than mine, then you can act quicker than me, which means you will win because you can see that and act faster; with AI [its] speed of decision making is instantaneous ... (P6)

In Ukraine, AI is already assisting decision-makers to act and to better integrate warfighting systems on the battlefield. Specifically, AI's most widespread use in the war in Ukraine is in geospatial intelligence for object recognition to detect the identity of invading Russian troops (i.e., the digital platform by Clearview AI), real-time analysis of Russian unencrypted radio transmissions (i.e., AI-enabled voice transmission and translation services by Primer), and the imagery of Ukraine (i.e., AI for automated analysis of large datasets by Scale AI).¹⁷⁵ In fact, 12,000 enemy targets (units of enemy vehicles/equipment) are detected by the Ukrainian military weekly with the help of AI, via the Avengers platform. This platform enables operators to make decisions more quickly and more efficiently, reducing the risk of fatigue-related errors. Future work remains to enhance the platform's cloud capabilities and integrate AI solutions with drone systems.¹⁷⁶

An increasing number of Ukrainian UAS companies are developing AI technologies for UAS. For example, Ukraine's new Saker Scout drones, trained on machine learning, are able to independently identify up to 64 different types of Russian targets while also carrying explosives.¹⁷⁷ In addition, due to AI data analytics, the time from detection of a target to its destruction has, in some cases, been reduced to just over 30 seconds. However, the accelerated targeting and strike cycles are likely to come with inherent biases for speed—an action that may pose a challenge, since the battlefield is still human-centric.¹⁷⁸ AI has been used in some of Ukraine's long-range drone strikes that target military facilities and oil refineries hundreds of kilometres inside Russia. In these operations, a core drone flies to the target while others distract air defences along the way. AI with human oversight is used to assist in target or threat spotting and possible route planning.¹⁷⁹

The need for AI-enabled drones is becoming more pressing as both Ukraine and Russia roll out EW systems that disrupt signals between pilots and drones. According to Max Makarchuk, the AI lead for Brave1, some current projects are focusing on developing a defence technical accelerator to remove the connection between the pilot and UAS. As jamming increases, the hit rate by the FPV drones decreases. According to Makarchuk, the percentage of FPVs that hit their target is around 30 per cent to 50 per cent, while for novice pilots this could be as low as 10 per cent. AI-enabled drones can increase hit rates to around 80 per cent. The key enabler is the capacity to 'lock onto a target' to counter EW threats. In theory, an AI-enabled drone could fly itself around the designated area using preset instructions, use object recognition software to recognise potential targets, and send back brief, compressed and encrypted reports instead of live video. The challenge is to generate inexpensive, small AI-enabled systems that could be deployed en masse along the entire 1,000 kilometre front line, where thousands of FPV drones are used each week.

The estimate of a simple targeting system able to lock onto a shape visible to the drone's camera is around US\$150 per UAV.¹⁸⁰ Some of DJI's drones already can track designated targets, but high-end AI currently runs on large, powerful computers that are expensive and would not fit on a 'quadcopter-sized digital brain'. Hence, any sophisticated AI processing would require significant computational power that is not currently available on any small drone. In addition, AI computer vision models are not at a level of performance to operate without a constant link to an operator.¹⁸¹

A risk with AI-enabled drones is that they may be more vulnerable to EW-delivered malicious software than those that are remotely controlled. While all commercial-off-the-shelf drones are vulnerable to EW, platforms that rely on the EMS for their operation are especially vulnerable to EW. The risk exists that so-called 'self-learning' capabilities that are being explored by scientists would enable drones to quickly and effectively analyse large amounts of incoming information, while working out possible response scenarios. AI could enable drones to identify important data contained in intercepted signals,

conduct appropriate analysis, and distribute the results. Scientists are already working on creating a technology that will radically improve the ability to geolocate and assess the characteristics of devices that emit electromagnetic signals. It is expected that next-generation systems will be able to accurately identify signals with different approach angles and polarisation states, improve the signal-to-noise ratio, detect signals and source geolocation with multivariate adaptive signal processing, and provide accurate ionospheric state determination. Of course, the generation of effective counter-EW is technologically demanding and expensive. The question therefore remains whether the benefits outweigh the costs.¹⁸²

While debates remain about the current effectiveness and future potential of AI-enabled drones, there are several key areas where AI promises to make a significant impact. These include terminal guidance, visual navigation, target detection and swarming. Specifically, AI drone development is broadly split between visual systems helping to identify targets into which drones can be flown, terrain mapping for navigation, and more complex programs enabling UAVs to operate in interconnected ‘swarms’. Regardless of the purpose, it remains the case that AI drone control systems will always need a human in the loop to prevent the system making errors in target selection and to address the ethics of weapons use.

Drone Swarming

A drone swarm is a group of drones that work together to achieve a common goal.¹⁸³ Instead of a single UAV operating alone, drone swarms could involve thousands of UAVs operating in the battlespace at any one time in a coherent, coordinated formation. In a swarm, the individual drones work in unison to complete tasks using distributed coordination, with each communication sent out by one drone providing the others with up-to-date information about their environment and roles in the mission.¹⁸⁴ As their commands are based on real-time data, these swarms react quickly and precisely to changes in their surroundings. Although defences might attempt countermeasures, such as physical barriers, swarms possess adaptive capabilities to overcome them. Companies and militaries around the world are racing to develop software that uses AI to link and manage groups of UAVs, leaving them to communicate and coordinate with each other after launch.

Swarming drones can perform multiple roles simultaneously, such as surveillance, reconnaissance and direct attack. This multi-role capability adds to the complexity of defending against them, as different defensive measures might be required for different drones. The sheer number of drones can saturate defence systems, making it difficult to target and neutralise each individual drone effectively. Even if several drones in the swarm are destroyed, the remaining drones can continue their mission, ensuring that the overall objective is still achievable. It becomes difficult to disrupt the entire swarm since there is no single point of failure.¹⁸⁵

People ask what a drone swarm actually is. Well, roughly speaking, this is a technology where drones can communicate and coordinate with each other, is the type of technology we do not really see yet. And when people say they see it in Russia, or that Russia and Ukraine already have drone swarms, I think that is also a little bit far from the truth. Yes, they use large waves of drones. They are kind of like flocks, so large groups of drones, but they are not necessarily communicating with each other. There are some AI-based technologies, yes, but that is not a swarm in the sense that we imagine it. So, yeah, the battlefield is still not there yet. (P29)

AI-powered drone swarms have now entered the battlefield in Ukraine. Swarmer's technology was first deployed by Ukrainian forces to lay mines around a year ago. It has since been used to target Russian soldiers, equipment and infrastructure (see Figure 41). The software has been successfully tested with groups of up to 25 drones, and testing is planned for over 100 drones. A standard operation involves the use of one reconnaissance drone and two strike drones armed with small bombs to hit a Russian trench. The operator sets the area to search for targets and gives the command to attack once they are found. The reconnaissance drone lays out a route for the strike vehicles, and the strike vehicles determine the time and order of the munitions drop.¹⁸⁶

In 2025, Ukrainian troops used a swarms of drones controlled by an AI system for a range of missions (i.e., mining, ISR, strike). The drones deployed in the attacks used technology that allows groups of drones to decide which one strikes first and adapt if, for instance, one runs out of battery.¹⁸⁷

Swarm technology represents the next frontier for drone warfare because of its potential to allow tens or even thousands of drones—or swarms—to be deployed at once to overwhelm the defences of a target, be that a city or an individual military asset. Hence, the pressing question arises of how to counter these coming threats.



Figure 41. Drone swarms in Ukraine. Photo credit: Swarmer Inc. Photo reproduced with the owner's permission.

Recommendations

Recommendations to the ADF and Military Leadership

1. Refine the human–machine authority framework—from ‘in the loop’ to ‘on the loop’.

The traditional human-in-the-loop model—in which a human operator authorises every individual engagement decision—is becoming operationally unsustainable in the face of machine-speed threats, particularly drone-on-drone interception, swarm saturation attacks, and EW-enabled multi-axis approaches that unfold more quickly than any human decision cycle can accommodate. The ADF must formally transition its doctrine and policy framework from human-in-the-loop towards a human-on-the-loop model for time-critical defensive engagements, in which humans retain oversight and veto authority, and the AI system executes within pre-authorised engagement parameters unless overridden.

For offensive and time-critical defensive missions, the ADF should implement a human-starts-the-loop model: a human operator defines mission parameters, ethical constraints, target profiles, and engagement rules before launch, allowing the system to operate with full autonomy within those guardrails during execution. This preserves meaningful human authorisation at the mission design stage while enabling machine-speed execution in the engagement phase.

Critically, the ADF must overhaul its terminology and classification framework for autonomous systems. Current labelling—in which entire platforms are described as ‘autonomous’—generates both false capability expectations and inaccurate legal and ethical assessments. The ADF should stop labelling hardware as ‘autonomous’ and instead classify the specific authority relationships and decision functions involved: a drone with AI-enabled pathfinding and target identification that still requires human intent validation and target confirmation prior to strike is not autonomous in any meaningful operational, legal or ethical sense. Classifications and frameworks should be revised to accurately describe the shared authority between human and machine at each mission phase.

2. Transition from manual control to algorithmic supervision of heterogeneous swarms.

The primary operational bottleneck in high-attrition drone warfare is the one-to-one operator-to-platform ratio that characterises current UxS employment. This model fails at scale. The ADF must transition from individual platform control towards algorithmic supervision of heterogeneous swarms, in which AI handles low-level tasks—collision avoidance, pathfinding, target prioritisation, formation management—enabling a single human operator to supervise and direct a substantial number of platforms simultaneously.

This requires investment in:

- software-defined attrition: prioritising platforms where the intelligence resides in the cloud or onboard chip rather than the airframe, enabling AI module updates in hours rather than years, and allowing counter-EW adaptations to be pushed to the fleet mid-operation
 - edge processing and computer vision: ensuring platforms can recognise targets and complete terminal attack legs autonomously after communications with the operator are severed—a capability that is operationally essential in GPS-denied and heavily jammed environments where remote control is unreliable
 - anti-automation bias training: ensuring operators are trained to recognise when AI probabilistic logic is failing due to spoofed sensor data or environmental camouflage and are empowered to override automated recommendations when human judgement identifies a failure mode the algorithm cannot detect.
3. Close the ‘imagination gap’—fund autonomous capability development now, not in the 2040s.

The ADF cannot and must not wait for AUKUS Tier-1 exquisite platforms to reach maturity before fielding meaningful autonomous capability. The 20-year gap between current capability and anticipated AUKUS deliverables represents an unacceptable strategic vulnerability in a threat environment that is evolving on a weekly basis. The government should reallocate a modest proportion (1 to 2 per cent) of the AUKUS and Hunter-class capital budget to rapid, sovereign AUKUS Pillar II autonomous systems projects, with a mandate to deliver operationally fielded capability within 12 to 24 months. This will create an immediate deterrent layer that complements long-term strategic investment rather than waiting for it.

4. Accelerate the shift to multi-domain swarming capability.

The ADF must accelerate the arming and swarming of uncrewed systems across air and maritime domains, transitioning from single-role ISR employment towards coordinated, multi-platform strike swarming—the ‘one-to-many’ operational concept—that has proven decisive in both the Ukrainian land and Black Sea maritime theatres. The Black Sea experience is particularly instructive: cheap, expendable naval drones costing a fraction of their targets achieved a level of sea denial that compelled the Russian Black Sea Fleet to abandon its primary operating base. The ADF should draw directly on this lesson to develop hundreds to thousands of autonomous underwater and surface systems for immediate sea denial and maritime domain management in the Indo-Pacific.

Concurrently, the ADF must invest in counter-autonomy capabilities—specifically the capacity to detect, disrupt and defeat adversary drone swarms in a cost-effective

manner—recognising that the adversary’s development of autonomous swarm attack capability will match, and may exceed, Australia’s own development trajectory if counter-autonomy investment is deferred.

5. Prioritise ‘zero-link’ edge autonomy as EW renders remote control increasingly unreliable.

As adversary EW capability evolves to render manual remote control of UxS increasingly unreliable across all frequency bands, the ADF must shift its development focus towards edge-processed autonomy—platforms capable of completing their mission without any communications link to the operator during the engagement phase. This requires investment in:

- edge AI and biologically inspired models (including BFBEL-P and equivalent architectures) that enable drone swarms to navigate, identify targets and coordinate without GPS or radio data links in a fully jammed environment
- data-driven model training: partnering with Ukraine to access and utilise the substantial volume of battlefield AI training data generated by millions of operational UxS sorties, enabling the training of superior target recognition, motion prediction and swarm coordination models before systems reach the production line
- tactical AI that can be updated on a daily basis in response to new adversary EW signatures, camouflage techniques or employment patterns—treating software adaptation as an operational activity requiring the same resourcing and command attention as logistics or fires planning.

Recommendations to Local Commanders

- Commanders should engage actively with current developments in autonomous systems doctrine, recognising that the human–machine authority relationships governing UxS employment are evolving rapidly and that commanders who understand these relationships will be better positioned to employ and defend against autonomous systems effectively.
- Commanders should train their operators to maintain meaningful human oversight of AI-assisted systems, including regular ‘de-biasing’ exercises that develop operators’ capacity to recognise and override AI recommendations that are failing due to spoofed data or unexpected environmental conditions.

Recommendations to Government

- Government must establish clear, legally robust and operationally workable frameworks governing lethal autonomy—distinguishing between human-in-the-loop, human-on-the-loop, and human-starts-the-loop authority models—and embed these frameworks in rules of engagement and acquisition policy before autonomous systems are fielded operationally rather than after.
- Government should fund AUKUS Pillar II autonomous systems projects with 12- to 24-month fielding mandates as an immediate priority, treating the gap between current capability and long-term AUKUS deliverables as a strategic vulnerability requiring an interim sovereign solution.
- Government should formalise a partnership with Ukraine for access to battlefield AI training data, recognising this as a unique and time-limited strategic intelligence resource of extraordinary value for Australian AI capability development.

/ CONCLUSION

This paper has examined the role of UAS/C-UAS in modern warfare in Russia's war against Ukraine. The evidence is unambiguous; uncrewed systems will shortly achieve persistent presence across every operational domain. The establishment of a dedicated USF within the AFU marks a crucial advancement in military organisational design, with implications extending well beyond the Ukrainian theatre.

Uncrewed systems have become embedded across the full spectrum of contemporary combat operations: reconnaissance UAVs, ground robots, surface and underwater vessels, loitering munitions and multirotor bombers, as well as middle- and deep-strike capabilities. These systems now constitute an integrated capability set rather than a collection of standalone tools. Approximately 80 to 90 per cent of enemy targets on the front line are now engaged by drones, while casualty evacuation is carried out almost exclusively by ground robotic systems. Battlefield isolation, disruption of logistics, and strikes on supply depots are achieved through middle strikes. In Ukraine, several hundred stable defence technology manufacturers have emerged, effectively covering almost the entire ecosystem—from communications, interceptors and guidance software to UGVs and naval drones. Among them are companies already working on solutions that may become operational within a few years—laser and electromagnetic weapons, AI-enabled autonomous systems, and software for rapid multi-sensor data processing.

During the first years of the full-scale invasion, the Western bureaucratic system observed the rapid development of Ukraine's defence technology industry from a distance. This conservative stance was driven by a combination of entrenched views among both senior officials and large legacy defence corporations. Neither group was willing to move away from the traditional model of warfare—one centred on systems costing tens of millions of dollars, contracts worth billions, and procurement cycles spanning decades. However, in recent years, representatives of European and American companies have begun arriving in Ukraine in large numbers. They understand that this war has produced innovations that will shape the future character of warfare. Consequently, there is a strong strategic imperative to rapidly adopt these developments and integrate them into their own defence markets; this is essential, not optional.

The broader global security environment has reinforced this imperative. Concurrent conflicts involving Iran and its proxies have accelerated the international technological competition, while also highlighting convergent patterns across modern conflicts. Most notable is the employment of massed missile-and-drone strike packages to target infrastructure (energy systems, ports, industrial facilities, command centres) and maritime assets, with cruise missiles and drones combined deliberately to saturate and overwhelm

air defence architectures The persistent combination of cruise missiles and drones is used to overwhelm air defence systems. Low-cost, mass drone attacks against expensive and limited air defence assets have demonstrated that it is no longer feasible to protect all critical infrastructure using traditional approaches. The cost imbalance is prohibitive—even for the United States and oil-rich states.

The 2024–2026 drone war over Ukraine has advanced military thinking into new conceptual territory. For the ADF and NATO member countries, this conflict offers an unobstructed view into the future operating environment—one in which ubiquitous uncrewed systems, persistent multi-domain sensing, and AI-enabled decision support will constitute the operational norm rather than the exception. The central lessons are clear and actionable: procure with speed and flexibility; devolve capability to the lowest tactical echelon; restructure command architectures at the tempo technology demands; reshape force structure to sustain and exploit uncrewed systems at scale; and field layered defences capable of countering massed swarm attacks.

As former Commander-in-Chief of the AFU General Valerii Zaluzhnyi stated:

*The Russian-Ukrainian war completely changed the nature of warfare. It is obvious that victory on the battlefield now depends entirely on the ability to outpace the enemy in technological development. Changes occur in the chain ‘science (development)—production—application’. Innovative development will depend on the effective interconnection between them.*¹⁸⁸

According to General Zaluzhnyi, uncrewed systems and digital technologies are outpacing the traditional types of weapons. Armoured vehicles have become defenceless against cheap drones. High-precision weapons that use GPS positioning have lost their effectiveness due to the development of EW. Air defence is undergoing perhaps the biggest transformation, with drones making expensive missiles impractical. Airspace above the battlefield has become inaccessible to crewed aircraft, necessitating the ability to conduct reconnaissance and strike from different distances. Sea space has been occupied by naval drones, and powerful ships are hiding in ports. These conditions all require the revision of military doctrines, principles of organising armed forces, and defence planning.¹⁸⁹

Ukraine’s experience—paid for at extraordinary human cost and relentless ingenuity—now stands as the principal reference point for allied militaries preparing for the uncrewed and autonomous era of conflict. Ukraine has demonstrated a more rapid and more effective institutional capacity than Russia, despite operating with a fraction of its adversary’s industrial and economic base—a fact that should itself inform allied assumptions about the relationship between resource scale and innovation at hypersonic speed.¹⁹⁰

Finally, an important lesson of analytical humility: despite the revolutionary tactical impact of drones, Ukraine's war underscores that drones alone do not win wars. They have not delivered unilateral strategic victory (as yet); rather, they have become an indispensable element within a combined arms framework. The enduring determinants of operational outcome—terrain control, logistics endurance, troop morale and command resilience—remain decisive, though uncrewed systems now exert profound influence over each of these factors. Military strategists should resist the temptation to view uncrewed systems as a panacea; instead they are force multipliers that must be integrated with doctrine, training and force development.

The war in Ukraine has shown the promise of smaller, low-cost, mass-producible and expendable uncrewed systems. Small expendable systems, deployed en masse, have a tactical advantage on the battlefield—identifying, disrupting and even destroying large armoured columns; interdicting resupply convoys; and destroying critical or high-value targets. Massed uncrewed formations will present an increasingly difficult defensive problem for any force, requiring sophisticated EW capability, substantial expenditure of high-value air-to-air and surface-to-air interceptors, directed-energy and HPM systems, or—more likely—an integrated combination of all three. Future contests for air superiority may ultimately be decided not by platform performance alone but by which combatant most effectively and efficiently allocates finite resources to the counter-UAS mission under conditions of sustained, high-volume threat.

The continuous evolution of uncrewed systems technology necessitates an equally organised and disciplined institutional response. This includes establishing robust certification, testing, and operational documentation standards to ensure platforms entering service are reliable and fit for purpose. As the proportion of battalion-level formations equipped with organic strike UAV capability continues to grow, the institutional importance of training establishments and qualification pipelines will grow commensurately. While strategies and tactics inevitably evolve, the cost of conflict is measured in human lives. It is therefore of paramount importance to ensure that systems that support the use of drones in warfare are robust, reliable and effectively integrated into military operations in order to safeguard forces while enhancing operational effectiveness.

Every conflict is unique, characterised by different participants, military capabilities, organisations and strategic objectives. This paper does not claim that Ukraine's experience translates uniformly to every future contingency. What is clear is that rapid technological adaptation and sustained innovation in uncrewed systems will be a decisive determinant of military effectiveness in future warfare. By sustaining an accelerated cycle of innovation and systematically incorporating the lessons generated in Ukraine, nations including Australia and its allied partners will retain a genuine opportunity to maintain advantage over potential adversaries and ensure readiness for the contemporary and future strategic challenges that uncrewed systems warfare now presents.

The proliferation of drones in modern warfare signals, above all, that the character of conflict has changed at a velocity that has outpaced the institutions, policies and assumptions built to govern it. It signals that mass, speed and adaptability now outweigh legacy assumptions of military dominance—and, critically, that the human dimension of warfare—judgement under pressure, endurance, and moral courage—remains the decisive variable, even as the instruments of war become increasingly autonomous. Uncrewed systems are frequently discussed in technical terms—platforms, payloads, autonomy architectures, cost curves—yet beneath this vocabulary lies a more fundamental contest: the confrontation between human will and the fragility of existence under sustained threat.

A Final Reflection

For Ukrainians, the rising sun—so constant, so taken for granted—has acquired a meaning beyond symbolic. For those living under its light in war, each dawn is survival, continuity against sustained pressure, proof that a nation under existential threat endures. Across Ukraine, the sun rises over shattered infrastructure, contested airspace, and disrupted civilian lives – but it also rises over demonstrated resilience, continuous adaptation, and an unbroken human spirit. The bravery of the Ukrainians – soldiers, engineers, volunteers, civilians – lies not only in resisting aggression but in redefining how resilience is built under constant threat. They remind us that courage is operational, daily, and often invisible.

That same sun rises, too, over those still waiting – the families of soldiers and civilians held in captivity, who measure each day not in operational tempo but in the absence of a husband, a wife, a son, a daughter, a parent. For them, the sunrise carries a different and harder kind of hope: that captivity will end, that exchange will come, and that every family separated by this war will one day reunite. No paper on technology or doctrine can capture what that reunion means—but it remains, quietly, the truest measure of why this war must end, and end justly on Ukrainian terms.

For those observing this war from a distance, there is a critical lesson that extends beyond doctrine, capability development or procurement cycles: tomorrow is not guaranteed—not for nations, not for institutions, not for individuals. The illusion of stability can no longer underpin defence planning. Preparedness must be continuous, and complacency must be treated as a strategic risk. As we look forward, the lessons from the current conflict will continue shaping the future character of warfare. The question for allied military leadership is whether the institutional capacity exists to absorb and operationalise these lessons within the window available. This is because in modern conflict, as Ukraine has shown, survival is earned—every day, under conditions of sustained pressure, and under the same rising sun (see Figure 42).



Figure 42. Ukrainian sunrise. Photo credit: Volyn Falcons. Photo reproduced with the owner's permission.

ABOUT THE AUTHOR

Dr Oleksandra Molloy – A two time ‘Academic of the Year’ and one of the leading experts in uncrewed and autonomous systems in modern conflicts. Dr Molloy is a Senior Lecturer in Aviation, and the Lead of the Human Factors Research Lab, at the University of New South Wales. Dr Molloy is a research trailblazer who conducts multi-disciplinary research in human factors, transport safety, uncrewed and autonomous systems, and AI. Her work contributes valuable insights into the evolving role of uncrewed systems with contemporary operations, and specifically in the war in Ukraine.

Dr Molloy has a PhD in Aviation (UNSW, Australia); a MSc in Human Factors (University of Nottingham, UK); a Master of Education (Central Ukrainian State Pedagogical University, Ukraine); a Graduate Research Certificate (Kirovograd Flight Academy of National Aviation University, Ukraine); and a Diploma in Aviation Safety (International Air Transport Association, Canada). Dr Molloy is serving as a Chair of the Council of Technical Groups of the Human Factors & Ergonomics Society (USA).

DISCLAIMER

The Australian Army Research Centre acknowledges that the author's preference is for all references to Russia, Russian, and associated regions and entities to appear in lowercase as a conscious choice in response to Russia's illegal invasion of Ukraine. However, in accordance with AARC editorial standards and Australian Defence Force style conventions, these terms have been capitalised throughout the article. This editorial decision does not affect the content of the author's analysis and should not be understood as diminishing or altering the author's stated position.

/ ENDNOTES

- 1 Reuters, “Russian drone attacks on Ukraine kill four, including mother and child,” (Reuters), February 9, 2026 2026, <https://www.reuters.com/world/europe/russian-drone-attack-ukraines-odesa-kills-one-governor-says-2026-02-09/>.
- 2 Oleksandra Molloy, “Drones in Modern Warfare: Lessons Learnt from the War in Ukraine,” Australian Army Research Centre (2024).
- 3 Worldstats, Military Drone Fleets by Country 2026 (Worldstats, 2026), https://worldstats.com/country-stats/military-drones-by-country/#google_vignette.
- 4 Harper Ellis, “Ukraine Ramps Up FPV Drone Production to 4.5 Million in 2025,” (2025). https://defensefeeds.com/news/army-news/ukraine-ramps-up-fpv-drone/#google_vignette.
- 5 Julia Struck, “Ukraine’s Drone Output Soars 900%, Producing 200K UAVs a Month,” (July 8, 2025 2025). <https://www.kyivpost.com/post/55897>.
- 6 Alexander Kozatskyi, “В Україні понад 500 компаній виробляють дрони – Федоров,” (February 26, 2025 2025). https://militaryni.com/uk/news/v-ukrayini-ponad-500-kompanij-vyrobyayut-drony-fedorov/?utm_source=chatgpt.com.
- 7 David Kirichenko, “Drone superpower: Ukrainian wartime innovation offers lessons for NATO,” May 13, 2025 (2025). <https://www.atlanticcouncil.org/blogs/ukrainealert/drone-superpower-ukrainian-wartime-innovation-offers-lessons-for-nato/#:~:text=Ukrainian%20production%20of%20FPV%20drones%20has%20mushroomed%20in,was%20reportedly%20producing%20200%2C000%20FPV%20drones%20per%20month>.
- 8 Ministry of Defence of Ukraine, “Unmanned Systems Forces,” accessed August 1, 2026, <https://mod.gov.ua/en/about-us/unmanned-systems-forces>
- 9 Mick Ryan, “Translating Ukraine Lessons for the Pacific Theatre,” Australian Army Occasional Paper 33 (2025), <https://doi.org/DOI: 10.61451/267533>, <https://researchcentre.army.gov.au/sites/default/files/Occasional-Paper-33-Translating-Ukraine-Lessons-for-the-Pacific-Theatre.pdf>.
- 10 Oleksandra Molloy, “Drones in modern warfare: lessons learnt from the war in Ukraine,” Australian Army Occasional Paper 29 (2024).
- 11 Virginia Braun and Victoria Clarke, “Using thematic analysis in psychology,” *Qualitative research in psychology* 3, no. 2 (2006).
- 12 Oleksandra Molloy, “Drone-on-drone War: The Rise of Drone Interceptors During the War in Ukraine,” (May 5, 2026 2026). <https://mickryan.substack.com/p/drone-on-drone-war-the-rise-of-drone>.
- 13 Serhii Kuzan, “Ukraine’s growing military strength is an underrated factor in peace talks,” (March 25, 2025 2025). <https://www.atlanticcouncil.org/blogs/ukrainealert/ukraines-growing-military-strength-is-an-underrated-factor-in-peace-talks/>.
- 14 Zafra, Mariano, Max Hunder, Anurag Rao, and Sudev Kiyada, “How drone combat in Ukraine is changing warfare,” (26 March 2024 2024). <https://www.reuters.com/graphics/UKRAINE-CRISIS/DRONES/dwpkeyjwkpml/>.
- 15 Tsiporah Fried, The Impact of Drones on the Battlefield: Lessons of the Russia-Ukraine War from a French Perspective (Hudson Institute, November 13, 2025 2025), <https://www.hudson.org/missile-defense/impact-drones-battlefield-lessons-russian-ukraine-war-french-perspective-tsiporah-fried#:~:text=Finally%2C%20from%202023%20onward%2C%20FPV,6>.
- 16 Tia Fiber Optic Tech Consortium, “Optical Fiber Technology,” (2025), <https://www.tiafotc.org/optical-fiber-technology/>.
- 17 Jamie Mortensen, “New Stealth Fiber-Optic Guided Drones (FOG-D) & How to Detect Them,” (April 26, 2024 2024). <https://www.spotterglobal.com/blog/spotter-blog-3/new-stealth-fiber-optic-guided-drones-fog-d-how-to-detect-them-12>.

- 18 Kateryna Stepanenko, Russian Force Generation & Technological Adaptations Update (Institute for the Study of War, 2025), <https://understandingwar.org/research/russia-ukraine/russian-force-generation-technological-adaptations-update-october-9-2025/>.
- 19 Sania Kozatskyi, “FPV drones: weapons that changed the modern war,” (October 12, 2023 2023). <https://militarnyi.com/en/articles/fpv-drones-weapons-that-changed-the-modern-war/>.
- 20 Oleksandra Yan, “Ukraine’s new loitering munition will hit ground and air targets,” (2024), <https://militarnyi.com/en/articles/ukraine-s-new-loitering-munition-will-hit-ground-and-air-targets/>.
- 21 Vikram Mittal, “Ukraine Increases Deep Drone Strikes Gaining Leverage For Peace Talks,” (December 4, 2025 2025). <https://www.forbes.com/sites/vikrammittal/2025/12/04/ukraine-increases-deep-drone-strikes-gaining-leverage-for-peace-talks/>.
- 22 Kirichenko, “Drone superpower: Ukrainian wartime innovation offers lessons for NATO.”
- 23 Dmytro Shumlianskyi, “In 2025, the Ukrainian Defense Forces started receiving about 200 thousand drones per month,” (February 9, 2025 2025). <https://militarnyi.com/en/news/in-2025-the-ukrainian-defense-forces-started-receiving-about-200-thousand-drones-per-month/>.
- 24 Ministry of Defence, Ukrainian air defense intercepted nearly 92% of drones amid intensified aerial attacks in May, (Ministry of Defence of Ukraine 2026). <https://mod.gov.ua/en/news/ukrainian-air-defense-intercepted-nearly-92-of-drones-amid-intensified-aerial-attacks-in-may>.
- 25 Kateryna Hodunova, “Ukrainian long-range drone successfully completes 3,000-kilometer test, Zelensky says,” (March 17, 2025). <https://kyivindependent.com/ukrainian-drone-with-3-000-kilometer-range-has-passed-tests-zelensky-says/>.
- 26 Ukraine War Analytics, “Ukraine’s Military Strategy Under General Syrskyi, 2024–2025,” (February 25, 2026). <https://ukraine-war-analytics.com/analysis/ukraine-military-strategy-syrskyi-2025.html>.
- 27 Shumlianskyi, “In 2025, the Ukrainian Defense Forces started receiving about 200 thousand drones per month.”
- 28 David Brennan, “Ukraine scales up drone attacks in Moscow, across Russia to record highs, data shows,” (June 4, 2026). <https://abcnews.com/International/ukraine-scales-drone-attacks-moscow-russia-record-highs/story?id=133511283>.
- 29 Ivan Khomneko, “Ukraine’s Long-Range Drones Cut Russian Artillery Use in Half, Forcing Warplanes Deeper into Russia,” (Apr 9 2025 2025). <https://united24media.com/latest-news/ukraines-long-range-drones-cut-russian-artillery-use-in-half-forcing-warplanes-deeper-into-russia-7463>.
- 30 “Ukraine war briefing: Zelenskyy ridicules Russian military drive, saying Putin keeps postponing goal deadlines,” (June 30 2026). <https://www.theguardian.com/world/ukraine>; “Ukraine war briefing: Zelenskyy ridicules Russian military drive, saying Putin keeps postponing goal deadlines.”
- 31 Oleksandra Molloy, “No safe distance: the war Russia started has come home to moscow,” (June 20, 2026 2026). <https://www.linkedin.com/pulse/safe-distance-war-russia-started-has-come-home-moscow-molloy-pa5fc/>.
- 32 Taras Safronov, “VAMPIRE Bomber Drone Becomes the Most Effective Weapon on the Front Line in 2025,” (January 30, 2026 2026). <https://militarnyi.com/en/news/vampire-bomber-drone-becomes-the-most-effective-weapon-on-the-front-line-in-2025/#:~:text=The%20VAMPIRE%20bomber%20drone%2C%20also%20known%20as%20%E2%80%9CBaba,according%20to%20information%20provided%20to%20Militarnyi%20by%20SkyFall>.
- 33 Safronov, “VAMPIRE Bomber Drone Becomes the Most Effective Weapon on the Front Line in 2025.”
- 34 Ukraine War Analytics, “Drone Cargo Delivery to the Ukraine Frontline 2026: Logistics Revolution Under Fire,” (February 28 2026 2026). <https://ukraine-war-analytics.com/drones/drone-cargo-delivery-frontline.html>.

- 35 Taras Safronov, “Drone from Rubizh Brigade Airlifts E-Bike to Evacuate Wounded Soldier,” *Militarnyi*, July 31, 2025, <https://militarnyi.com/en/news/drone-from-rubizh-brigade-airlifts-e-bike-to-evacuate-wounded-soldier/>
- 36 Meaththew Loh and Jake Epstein, “Ukraine’s cheap interceptor drones are rewriting the air war playbook,” (Oct 18). <https://www.businessinsider.com/ukraine-interceptor-drones-air-defense-2025-10>.
- 37 Ibid.
- 38 Ministry of Defence of Ukraine, Defence City launch, record interceptor drone deliveries, and procurement reform: the Ministry of Defence’s highlights of the week, (Ministry of Defence of Ukraine 2026).
- 39 Katie Livingstone, “Novel interceptor drones bend air-defense economics in Ukraine’s favor,” (2026). <https://www.defensenews.com/global/europe/2026/03/05/novel-interceptor-drones-bend-air-defense-economics-in-ukraines-favor/>.
- 40 423rd Unmanned Systems Battalion, “The Evolution of Drone Interception Technologies in 2025–2026,” (2026). <https://423grifony.com/en/the-evolution-of-drone-interception-technologies-in-2025-2026/>.
- 41 Sofia Syngaivska, “Ukraine Claims First Remote Interception as Litavr Downs Shahed Drone During Mass Attack (Video),” (March 25, 2026). https://en.defence-ua.com/news/ukraine_claims_first_remote_interception_as_litavr_downs_shahed_drone_during_mass_attack_video-17943.html.
- 42 Daryna Vialko, “Ukraine launches new level of air defense to hit targets thousands of miles away,” (April 23, 2026). <https://newsukraine.rbc.ua/news/ukraine-launches-new-level-of-air-defense-1776970256.html>.
- 43 The Global Statistics, “What is the Sting Drone by Wild Hornets?,” (2026). <https://www.theglobalstatistics.com/sting-drone-statistics/>.
- 44 Jacob Gronholt-Pedersen and Gwladys Fouche, “‘We’re all having to catch up’: NATO scrambles for drones that can survive the Arctic,” (January 30, 2025 2025). https://www.reuters.com/world/nato-scrambles-drones-that-can-survive-arctic-2025-01-30/?utm_source=chatgpt.com.
- 45 Abduljalil Abdurasulov, “Fog helps Russian forces push deeper into key Ukrainian city of Pokrovsk,” BBC (12 November 2025 2025). <https://www.bbc.com/news/articles/cx276px3280o>.
- 46 Oleksandra Molloy, “Drone Warfare in Ukraine: From Myths to Operational Reality – Part 1,” (March 11, 2026 2026). <https://researchcentre.army.gov.au/library/land-power-forum/drone-warfare-ukraine-myths-operational-reality-part-1>.
- 47 Allison, David M., Stephen Herzog, Brendan Rittenhouse Green, and Austin Long., “Correspondence: Clandestine Capabilities and Technological Diffusion Risks,” *International Security* 45, no. 2 (2020).
- 48 Tech Ukraine, “Vyriy Drone Ignites Ukraine’s DefenceTech Scene with a \$4M+ M&A Onslaught,” (October 7, 2025 2025). <https://techukraine.org/2025/10/07/vyriy-drone-ignites-ukraines-defencetech-scene-with-a-4m-ma-onslaught/>.
- 49 Eric Milzarski, “How Vietnam-era commo guys talked through the jungles,” *We are the Mighty* (March 29, 2021 2021). <https://www.wearethemighty.com/popular/how-vietnam-era-commo-guys-talked/>.
- 50 Ryan, “Translating Ukraine Lessons for the Pacific Theatre.”
- 51 Molloy, “Drone Warfare in Ukraine: From Myths to Operational Reality – Part 1.”
- 52 Ryan, “Translating Ukraine Lessons for the Pacific Theatre.”
- 53 Ibid.
- 54 ⁵⁴ Kirichenko, David. “Ukraine’s Robot Army Will Be Crucial in 2026 but Drones Can’t Replace Infantry.” *Atlantic Council*, January 8, 2026. <https://www.atlanticcouncil.org/blogs/ukrainealert/ukraines-robot-army-will-be-crucial-in-2026-but-drones-cant-replace-infantry/>
- 55 Kirichenko, “Drone superpower: Ukrainian wartime innovation offers lessons for NATO.”
- 56 Ibid.

- 57 Peter Dickinson, "Ukraine is shaping the future of drone warfare at sea as well as on land," (June 12, 2025 2026). <https://www.atlanticcouncil.org/blogs/ukrainealert/ukraine-is-shaping-the-future-of-drone-warfare-at-sea-as-well-as-on-land/>.
- 58 Taras Safronov, "SSU Presents New Generation of Sea Baby Naval Drones: Range Exceeds 1,500 km," (October 22, 2025). <https://militarnyi.com/en/news/ssu-presents-new-generation-of-sea-baby-naval-drones-range-exceeds-1-500-km/>.
- 59 Oleksandr Yan, "Defence Intelligence of Ukraine Reveals Capabilities of Magura v7 Marine Drones," (May 15, 2025 2025). <https://militarnyi.com/en/news/defence-intelligence-of-ukraine-reveals-capabilities-of-magura-v7-marine-drones/>.
- 60 Safronov, "SSU Presents New Generation of Sea Baby Naval Drones: Range Exceeds 1,500 km."
- 61 Safronov, "SSU Presents New Generation of Sea Baby Naval Drones: Range Exceeds 1,500 km."
- 62 Taras Safronov, "Ukrainian Underwater Drones Blow Up Russian Submarine," (December 15, 2025 2025). <https://militarnyi.com/en/news/ukrainian-underwater-drones-blow-up-russian-submarine/>.
- 63 Ibid.
- 64 Sebastien Roblin, "Black Sea Drone War: How a Country with No Warships Has Russia's Navy on the Run," (October 19, 2023 2023). <https://insideunmannedsystems.com/black-sea-drone-war-how-a-country-with-no-warships-has-russias-navy-on-the-run/>.
- 65 Safronov, Taras. "Ukrainian Underwater Drones Blow Up Russian Submarine." Militarnyi, December 15, 2025. <https://militarnyi.com/en/news/ukrainian-underwater-drones-blow-up-russian-submarine/>
- 66 David Kirichenko, "Ukraine's robot army will be crucial in 2026 but drones can't replace infantry," (January 8, 2026). <https://www.atlanticcouncil.org/blogs/ukrainealert/ukraines-robot-army-will-be-crucial-in-2026-but-drones-cant-replace-infantry/>.
- 67 Abdujalil Abdurasulov, "In Ukraine's 'kill-zone,' robots are a lifeline to troops trapped on perilous eastern front," (November 23, 2025 2025). <https://www.bbc.com/news/articles/cvgkg4zr33lo>.
- 68 Katie Livingstone, "Ukraine to field 25,000 ground robots in push to replace soldiers for frontline logistics," (April 25, 2026). <https://www.defensenews.com/unmanned/2026/04/24/ukraine-to-field-25000-ground-robots-in-push-to-replace-soldiers-for-frontline-logistics/>. 25 April 2026.
- 69 Roman Sudolsky, "'100% of frontline logistics should be handled by robotic systems': Mykhailo Fedorov meets UGV manufacturers," (April 19, 2026 2026). <https://thedefender.media/en/2026/04/fedorov-ugv/>.
- 70 Simon Lacroix and Guy Le Besnerais, "Issues in cooperative air/ground robotic systems" (paper presented at the Robotics Research: The 13th International Symposium ISRR, 2010).
- 71 David Axe, "The Ukrainian Navy's Robotic Aircraft Carriers Are Raiding Russian Coastal Defenses," *Forbes, Aerospace & Defence*, March 9, 2025 (2025). <https://www.forbes.com/sites/davidaxe/2025/03/09/the-ukrainian-navys-robotic-aircraft-carriers-are-raiding-russian-coastal-defenses/>.
- 72 Ibid.
- 73 Noah Schmidt, "Ukraine's Magura Naval Drones May Have Been Used as an FPV Mothership to Strike Deep Behind Enemy Lines," (2025). <https://www.sofx.com/ukraines-magura-naval-drones-may-have-been-used-as-an-fpv-mothership-to-strike-deep-behind-enemy-lines/>.
- 74 Ibid.
- 75 Anna Fratsyvir, "Ukrainian sea drone downs Russian fighter jet in 'world-first' strike, intelligence says," (May 3, 2025 2025). <https://kyivindependent.com/ukrainian-intelligence-says-sea-drone-downs-russian-fighter-jet-in-world-first-strike/>.
- 76 Army Recognition Group, "Exclusive: World's First Ukrainian naval drone launching Air-to-Air Missile to shoot down Russian Su-30 fighter jet.," *The Global Defense News* (Army Recognition Group), May 4, 2025, <https://www.armyrecognition.com/focus-analysis-conflicts/army/conflicts-in-the-world/russia-ukraine-war-2022/exclusive-world-first-ukrainian-naval-drone-launches-air-to-air-missile-to-shoot-down-russian-su-30-fighter-jet>.

- 77 Ivan Khomenko, “Ukraine Shoots Down Shahed With Sea-Launched Drone For The First Time,” (April 25, 2026). <https://united24media.com/latest-news/ukraine-shoots-down-shahed-with-sea-launched-drone-for-the-first-time-18042>.
- 78 Ukrinform, “SSU releases new footage of “Spider Web” operation to destroy Russian strategic aircraft,” June 11, 2025, <https://www.ukrinform.net/rubric-ato/4002993-ssu-releases-new-footage-of-spider-web-operation-to-destroy-russian-strategic-aircraft.html>.
- 79 Global Security, “‘Spider Web’ is the result of a unique symbiosis between human intelligence and technical components of the Service’s work - SSU Head Vasyl Maliuk,” AUGUST 12, 2025 2025, <https://www.globalsecurity.org/wmd/library/news/ukraine/2025/08/ukraine-250812-ukraine-ssu04.htm>.
- 80 Volodymyr B., “Russia Lost 34% of Strategic Aviation in Spiderweb Operation — NATO,” (June 4, 2025). <https://militaryni.com/en/news/russia-lost-34-of-strategic-aviation-in-spiderweb-operation-nato/>.
- 81 Carl von Clausewitz, “On War, ed. and trans,” Michael Howard and Peter Paret (1976).
- 82 Taras Safronov, “Spiderweb Operation: Drone Strikes Destroyed Russian Bombers in \$7 Billion,” (June 8, 2025 2025). <https://militaryni.com/en/news/drone-strikes-destroyed-russian-bombers-in-7-billion-spiderweb-operation/>.
- 83 Kateryna Bondar, How Ukraine’s Operation “Spider’s Web” Redefines Asymmetric Warfare (Centre for Strategic and International Studies, 2025), <https://www.csis.org/analysis/how-ukraines-spider-web-operation-redefines-asymmetric-warfare>.
- 84 Jack Watling and Noah Sylvia, Competitive Electronic Warfare in Modern Land Operation (Royal United Services Institute, 2025), https://static.rusi.org/competitive-electronic-warfare-in-land-operations_1.pdf?utm_source=chatgpt.com.
- 85 Consortium for Defence Information, “War in the Spectrum,” (2025). <https://www.newgeopolitics.org/2025/07/23/war-in-the-spectrum/>.
- 86 Consortium for Defence Information, “War in the Spectrum.”
- 87 ChiTown Darren, “Ukraine’s cheap interceptor drones are rewriting the rules of war,” B17 News, October 18, 2025, <https://b17news.com/ukraines-cheap-interceptor-drones-are-rewriting-the-rules-of-war/>.
- 88 Ministry of Defence of Ukraine, Ukraine’s air defense intercepted over 90% of drones in March, (2026). <https://mod.gov.ua/en/news/ukraine-s-air-defense-intercepted-over-90-of-drones-in-march>.
- 89 Ministry of Defence of Ukraine, War Plan: our steps to force russia into peace, (Ministry of Defence of Ukraine, 2026).<https://mod.gov.ua/en/news/war-plan-our-steps-to-force-russia-into-peace>.
- 90 Livingstone, “Novel interceptor drones bend air-defense economics in Ukraine’s favor.”
- 91 Alya Shandra, “Can Ukraine’s \$ 1,000 drones really beat Russia’s \$ 35,000 Shaheds?,” (July 16, 2025). <https://euromaidanpress.com/2025/07/16/the-math-of-survival-ukraine-bets-1000-drones-can-stop-35000-shahed-killers/>.
- 92 Olgor Anokhin, Monthly Analysis of Russian Shahed 136 Deployment Against Ukraine (Institute for Science and International Security, 2026), https://isis-online.org/isis-reports/monthly-analysis-of-russian-shahed-136-deployment-against-ukraine?utm_source=chatgpt.com.
- 93 Watling and Reynolds, Tactical Developments During the Third Year of the Russo–Ukrainian War.
- 94 Indigo Monsser-Kernosh, “The Thread of War: How Fiber Optic Drones Are Making Electronic Warfare Obsolete,” Frontline Insights (2025). <https://www.linkedin.com/pulse/thread-war-how-fiber-optic-drones-making-electronic-monsser-kernosh-nuube/>.
- 95 Ethan Encarnacion, “Ukraine Introduces ‘Sunray’: A Silent Laser Weapon Against Aerial Drones,” (2026). <https://thedefensepost.com/2026/02/12/ukraine-sunray-laser-weapon/>.
- 96 Yuliia Zavadzka, ‘Ukraine Develops Low-Cost Laser Air Defense System to Counter Russian Drones,’ Kyiv Post, 11 February 2026.
- 97 ; Olha Pokotylo, “General Lebedenko: Ukraine to receive domestic laser air defence systems within quarter,” (July 23, 2026 2026). <https://thedefender.media/en/2026/07/lebedenko-laser-weapon/>.

- 98 Vicky Maggiani, “The £103M project to build Ukraine’s anti-drone ‘wall’ “ (2025). <https://www.defenceonline.co.uk/2025/02/17/the-103m-project-to-build-ukraines-anti-drone-wall/>.
- 99 “Setup and Innovation of Atlas, the EW System Now in Service With Ukraine’s National Guard,” (July 6, 2025 2025). https://en.defence-ua.com/weapon_and_tech/setup_and_innovation_of_atlas_the_ew_system_now_in_service_with_ukraines_national_guard-15054.html.
- 100 Annika Burgess, “US and Arab states turn to Ukraine for help against Iranian drone attacks,” (10 March 2026 2026). <https://www.abc.net.au/news/2026-03-10/us-gulf-states-call-on-ukraine-for-iran-shahed-drone-defence/106431514>.
- 101 Aditya Kumar, “Ten Ukrainian Soldiers Neutralizes Two NATO Battalions in Single-Day During Exercise Hedgehog 2025,” (February 14, 2026 2026). <https://www.thedefensenews.com/Ten-Ukrainian-Soldiers-Neutralizes-Two-NATO-Battalions-in-Single-Day-During-Exercise-Hedgehog-2025/>.
- 102 Ibid.
- 103 Alistair MacDonald, “AI-Powered Drone Swarms Have Now Entered the Battlefield,” (September 2, 2025 2025). <https://www.wsj.com/world/ai-powered-drone-swarms-have-now-entered-the-battlefield-2cab0f05?msockid=3f98c9d76298614c3501dfb663ee60fc>.
- 104 Oleksandra Yan, “Robert Brovdi Tells European Generals Their Countries Are Unprepared for Modern Warfare,” (July 21, 2025). <https://militaryni.com/en/news/robert-brovdi-tells-european-generals-their-countries-are-unprepared-for-modern-warfare/>.
- 105 Ministry of Defence of Ukraine, «Контракт 18-24»: визначено перелік підрозділів ЗСУ та штатних посад для операторів БПС, (Ministry of Defence of Ukraine 2025). <https://mod.gov.ua/en/news/contract-18-24-the-ministry-of-defence-introduces-a-new-model-of-voluntary-military-service>.
- 106 Paul Cornish, *Machine-guns and the Great War* (Casemate Publishers, 2009).
- 107 Vadim Kushnikov, “Ukraine Launches Unmanned Systems Force as New Military Branch,” (June 11, 2024 2024). <https://militaryni.com/en/news/ukraine-launches-unmanned-systems-force-as-new-military-branch/>.
- 108 Olena Kryzhanivska, “(Un)Manned Warfare: 80% of Drone Success Depends on Pilot Skill,” (October 25, 2025 2025). <https://ukrainearmsmonitor.substack.com/p/unmanned-warfare-80-of-drone-success>.
- 109 Howard Altman, “Russia Creates New Military Branch Dedicated To Drone Warfare,” (November 13, 2025 2025). <https://www.twz.com/news-features/russia-creates-new-military-branch-dedicated-to-drone-warfare>.
- 110 Anna Kovalenko, “Number of women in Armed Forces of Ukraine rose during 2025,” (8 March 2026 2026). <https://www.pravda.com.ua/eng/news/2026/03/08/8024458/>.
- 111 David Hambling, “A Woman’s Place Is In The Drone War: How Technology Changes Attitudes,” (March 25, 2026). <https://www.forbes.com/sites/davidhambling/2026/03/25/a-womans-place-is-in-the-drone-war/>.
- 112 Hambling, “A Woman’s Place Is In The Drone War: How Technology Changes Attitudes.”
- 113 Christine Casimiro, “Ukraine Recruits Female ‘Harpies’ for Drone Warfare,” (April 4, 2025 2025). <https://thedefensepost.com/2025/04/04/ukraine-female-harpies-drone-unit/>.
- 114 Mirko Niederkofler, *Drones Win Battles, Components Win Wars* (Royal United Services Institute, 2025), *Drones Win Battles, Components Win Wars*.
- 115 Tetiana Frolova Cyril Barabaltchouk, “Ukraine Forms World’s First Battalion of Ground-Based Unmanned Systems,” (August 4, 2025 2025). <https://united24media.com/latest-news/ukraine-forms-worlds-first-battalion-of-ground-based-unmanned-systems-10424.4> August 2025.
- 116 Wesley Wark, “Canadian Army to “Flood the Zone” with Drones, Commander Says,” (November 5, 2025 2026). <https://thewalrus.ca/canadian-army-to-flood-the-zone-with-drones-commander-says/>.
- 117 Matthew Slusher, *Lessons from the Ukraine Conflict: Modern Warfare in the Age of Autonomy, Information, and Resilience* (CSIS, 2025), <https://www.csis.org/analysis/lessons-ukraine-conflict-modern-warfare-age-autonomy-information-and-resilience>.
- 118 John Hardie, ‘Ukraine’s New Unmanned Systems Forces Takes Shape,’ *Long War Journal*, at: <https://www.longwarjournal.org/archives/2024/06/ukraines-new-unmanned-systems-forces-takes-shape.php>.

- 119 Sinead Baker, “Ukrainian drone schools say there’s little the West can teach them about fighting a drone war,” (January 28, 2026 2026). https://www.businessinsider.com/ukrainian-drone-schools-say-west-cant-teach-them-drone-war-2026-1?utm_source=chatgpt.com.
- 120 “Dronarium Academy,” <https://www.dronarium.academy/en>.
- 121 Daniel Tilles, “Ukraine and Poland sign agreement to cooperate on drone warfare,” (2025). https://notesfrompoland.com/2025/09/18/ukraine-and-poland-sign-agreement-to-cooperate-on-drone-warfare/?utm_source=chatgpt.com.<https://notesfrompoland.com/2025/09/18/ukraine-and-poland-sign-agreement-to-cooperate-on-drone-warfare>.
- 122 Baker, “Ukrainian drone schools say there’s little the West can teach them about fighting a drone war.”
- 123 Sarah Vesey, ADF drone racers top international field, (Australian Government. Defence., 2025). <https://www.defence.gov.au/news-events/news/2025-06-23/adf-drone-racers-top-international-field>.
- 124 Australian Government. Department of Defence., Army accelerates drone training, (Australian Government., 2026). <https://www.defence.gov.au/news-events/news/2026-03-27/army-accelerates-drone-training>.
- 125 Department of Defence. Army Accelerates Drone Training [photograph]. March 27, 2026. Department of Defence
- 126 Mick Ryan, Combat Adaptations. A USAREUR-AF Ukraine Lessons Learned Publication (2025).
- 127 Major General (Dr) Mick Ryan, ““Choosing not to learn”: How Western militaries are failing to adapt to modern war,” Lowy Institute (2026), <https://www.lowyinstitute.org/publications/modern-war-and-the-systemic-learning-deficit-in-western-military-institutions>.
- 128 Mick Ryan, Combat Adaptations. A USAREUR-AF Ukraine Lessons Learned Publication.
- 129 Ryan, Mick. War Transformed: The Future of Twenty-First-Century Great Power Competition and Conflict. Annapolis, MD: Naval Institute Press, 2022
- 130 Scott Douglas Jacobsen, “How Ukraine Became the World’s Most Recorded War—and a Laboratory for AI-Driven Combat,” (December 4, 2025). <https://intpolicydigest.org/how-ukraine-became-the-world-s-most-recorded-war-and-a-laboratory-for-ai-driven-combat/#:~:text=In%20this%20interview%2C%20he%20outlines,but%20they%20adapt%20poorly%20to>.
- 131 Molloy, “Drones in Modern Warfare: Lessons Learnt from the War in Ukraine.”
- 132 Mick Ryan, “Australia’s new National Defence Strategy must embrace adaptation as warfare evolves,” (February 11, 2026). <https://www.lowyinstitute.org/the-interpreter/australia-s-new-national-defence-strategy-must-embrace-adaptation-warfare-evolves#:~:text=The%20slow%2C%20zero%2Drisk%20management,survivable%20in%20a%20future%20war>.
- 133 Slusher, Lessons from the Ukraine Conflict: Modern Warfare in the Age of Autonomy, Information, and Resilience.
- 134 Yannick Veilleux-Lepage, “On the horizon: The Ukraine war and the evolving threat of drone terrorism,” CTC Sentinel (2025).
- 135 Ryan, “Translating Ukraine Lessons for the Pacific Theatre.”
- 136 Dr Lee Willett, “Ukraine lessons include technology arms race and mass production, says NATO official,” (September 22, 2025). <https://www.janes.com/osint-insights/defence-news/sea/ukraine-lessons-include-technology-arms-race-and-mass-production-says-nato-official#:~:text=%E2%80%9CThis%20war%20has%20seen%20remote,%E2%80%9D>.
- 137 Niederkofler, Drones Win Battles, Components Win Wars.
- 138 Rheinmetall, “Work smarter, not harder: Rheinmetall’s proven capabilities to deliver rapid munitions industrial base expansion in the U.S.,” (December 11, 2025).
- 139 Eric Johnson, “Guns and Ammo: The Ukraine War and NATO’s Ammunition Interoperability Problem,” (July 11, 2025). <https://mwi.westpoint.edu/guns-and-ammo-the-ukraine-war-and-natos-ammunition-interoperability-problem/#:~:text=If%20the%20war%20in%20Ukraine,there%20remains%20a%20separate-%20issue>.

- 140 TSN, “Shmyhal announced the number of drones to be produced in Ukraine by the end of the year,” (TSN), 02.10.2024, <https://tsn.ua/en/ato/shmyhal-announced-the-number-of-drones-to-be-produced-in-ukraine-by-the-end-of-the-year-2671659.html>.
- 141 Ann Marie Dailey Franklin D.Kramer, Josley Brodfuehrer, NATO multidomain operations: Near- and medium-term priority initiatives (Atlantic Council, February 21, 2024), <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/nato-multidomain-operations/#:~:text=bring%20NATO%20even%20closer%20to,industrial%20base>.
- 142 News Pravda, “Ukraine mobilizes approximately 30–34 thousand people per month, and Russia mobilizes about 10 thousand more,” News Pravda, February 28, 2026 2026, <https://news-pravda.com/img/20260228/80d46709843e30acc7b1016ae74f1fa8.jpg>; Pravda, “Ukraine mobilizes approximately 30–34 thousand people per month, and Russia mobilizes about 10 thousand more.”
- 143 Ryan, “Translating Ukraine Lessons for the Pacific Theatre.”
- 144 North Atlantic Treaty Organisation - NATO, Defence Expenditure of NATO Countries (2014-2025) (2025), <https://www.nato.int/content/dam/nato/webready/documents/finance/def-exp-2025-en.pdf>.
- 145 Niederkofler, Drones Win Battles, Components Win Wars.
- 146 Defence., Short Budget 2025-2026.
- 147 Stockholm International Peace Research Institute (SIPRI), SIPRI Fact Sheet (2026), https://media.licdn.com/dms/document/media/v2/D4E1FAQGjFHue7rP_aw/feedshare-document-pdf-analyzed/B4EZ3PRLg.KwAY-/0/1777298882573?e=1778112000&v=beta&t=-fnXX3xh4B3gPUIXQyYUSiEQP7PqBIDQEtCbTHFb8lo.
- 148 (SIPRI), SIPRI Fact Sheet.
- 149 Ibid.
- 150 Ibid.
- 151 Joyce Hakmeh, “What Ukraine can teach Europe and the world about innovation in modern warfare,” (March 5, 2025). <https://www.chathamhouse.org/2025/03/what-ukraine-can-teach-europe-and-world-about-innovation-modern-warfare>.
- 152 MacDonald, “AI-Powered Drone Swarms Have Now Entered the Battlefield.”
- 153 Artem Moroz, the written statement provided to the author for this research, February 2, 2026.
- 154 “Brave1. Ukrainian Defense Innovations,” 2024, 2024, <https://brave1.gov.ua/>.
- 155 Volodymyr B., “Ukraine Launches Drone Marketplace for Military Units,” (April 28, 2025). <https://militaryni.com/en/news/ukraine-launches-drone-marketplace-for-military-units/>.
- 156 Brave1, “Brave1. Ukrainian Defense Innovations.”
- 157 “The Ukrainian Council of Defence Industry —is a consolidated voice of the Ukrainian defence industry,” 2025, <https://ucdi.org.ua/en/>.
- 158 Ihor Fedirko, the written statement provided to the author for this research, March 10, 2026.
- 159 NATO., NATO and Ukraine announce new joint-initiative to accelerate defence innovation: UNITE – Brave NATO, (2026).
- 160 Asami Terajima, “4 Ukrainian defense companies sign partnership deals with European allies valued at nearly \$950 million,” (February 25, 2026). <https://kyivindependent.com/4-ukrainian-defense-companies-sign-partnership-deals-with-european-allies-valued-at-nearly-950-million/>.
- 161 Oleksii Tucha, “Zelensky announces automatic business permits for weapons exports. Here’s what is known.” <https://thedefender.media/en/2026/04/zelensky-drone-deals/>.
- 162 Stu Nassé, the written statement provided to the author for this research, February 9, 2026.
- 163 Sophia Besch, “From Production to Procurement: How Europe and Ukraine Are Transforming Defense Supply Chains,” (December 10, 2025). <https://carnegieendowment.org/posts/2026/01/from-production-to-procurement-how-europe-and-ukraine-are-transforming-defense-supply-chains>.

- 164 Niederkofler, Drones Win Battles, Components Win Wars.
- 165 Ibid.
- 166 Ibid.
- 167 U.S. Department of Defense, DoD Directive 3000.09. AUtonomy in Weapons Systems, (2023).
- 168 Kateryna Bondar, Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare (CSIS, March 6, 2025 2025), <https://www.csis.org/analysis/ukraines-future-vision-and-current-capabilities-waging-ai-enabled-autonomous-warfare>.
- 169 Jean-Marc Rickli, Peace of Mind: Cognitive Warfare and the Governance of Subversion in the 21st Century (Geneva Centre for Security Policy, 2023), <https://dam.gcsp.ch/files/misc/pb-9-rickli-mantellassi?>
- 170 Jean-Marc Rickli and Federico Mantellassi, The War in Ukraine: Reality Check for Emerging Technologies and the Future of Warfare (Geneva Centre for Security Policy, 2024), <https://www.gcsp.ch/sites/default/files/2024-12/geneva-paper-34-24.pdf>.
- 171 Bondar, Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare.
- 172 Ibid.
- 173 Ibid.
- 174 Varun Sehgal, "Artificial Intelligence and Military Decision Making: Revisiting OODA Loop Framework," International Journal for Multidisciplinary Research 6, no. 4 (2024), <https://www.ijfmr.com/papers/2024/4/26389.pdf>.
- 175 Dominika Kunertova, Learning from the Ukrainian Battlefield: Tomorrow's Drone Warfare, Today's Innovation Challenge, ETH Zurich (2024).
- 176 'Kateryna Chernohorenko: "AI helps to detect and destroy enemy's targets," Ministry of Defence of Ukraine, 2024, <https://www.mil.gov.ua/en/news/2024/09/23/12-000-enemy-targets-are-detected-by-the-ukrainian-military-weekly/>.
- 177 David Hambling, "Ukraine's AI Drones Seek And Attack Russian Forces Without Human Oversight," Forbes, Aerospace & Defence 17 (2023).
- 178 Kunertova, Learning from the Ukrainian Battlefield.
- 179 Max Hunder, "Ukraine rushes to create AI-enabled war drones," (July 18 2024 2024). <https://www.reuters.com/technology/artificial-intelligence/ukraine-rushes-create-ai-enabled-war-drones-2024-07-18/>.
- 180 Ibid.
- 181 Sydney J Freedberg Jr, "Dumb and cheap: When facing electronic warfare in Ukraine, small drones' quantity is quality," Breaking Defence 13 (2023).<https://breakingdefense.com/2023/06/dumb-and-cheap-when-facing-electronic-warfare-in-ukraine-small-drones-quantity-is-quality>.
- 182 Ibid.
- 183 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>.
- 184 Polat Cevik et al., "The small and silent force multiplier: a swarm UAV—electronic attack," Journal of Intelligent & Robotic Systems 70, no. 1 (2013).
- 185 Defensebridge, "What is a Drone Swarm? An Overview of the Technology " (January 31, 2023 2023). <https://defensebridge.com/article/what-is-a-drone-swarm-an-overview-of-the-technology.html>.
- 186 Vladislav V., "Ukraine Uses Autonomous Drone Swarm Against Russian Forces," (September 2 2025). <https://militaryni.com/en/news/ukraine-uses-self-deciding-drone-swarm-against-russian-forces/>.
- 187 MacDonald, "AI-Powered Drone Swarms Have Now Entered the Battlefield."
- 188 Valerii Zaluzhnyi, "The evolving nature of warfare has redefined the fundamental principles of global security: the Ukrainian experience and the emerging world order.," (April 25, 2025). https://www.pravda.com.ua/eng/columns/2025/04/25/7509135/?utm_source=chatgpt.com.

- 189 Rickli, *Peace of Mind: Cognitive Warfare and the Governance of Subversion in the 21st Century*.
- 190 Jean-Marc Rickli and Federico Mantellassi, “The War in Ukraine: Reality Check for Emerging Technologies and the Future of Warfare,” (2024).



RESEARCHCENTRE.ARMY.GOV.AU