

Doctrine in the Third Drone Age: how NATO should adapt to full spectrum drone warfare

JAMES PATTON ROGERS, DOMINIKA KUNERTOVA,
JAMES WESLEY HUTTO AND ELIZABETH H. REDMOND*

NATO faces a doctrinal reckoning. Allied members are investing heavily in uncrewed systems, but the alliance lacks a shared framework for integrating them into a coherent, cross-domain force. Full spectrum drone warfare (FSDW) will define the Third Drone Age,¹ and the central question for NATO is not whether to acquire drones but whether it can adapt fast enough to use them effectively. FSDW is not one single technology, but a systems revolution of autonomous air, ground and maritime machines that learn, adapt and fight as one. Going beyond simple acquisition and mass deployment, FSDW is about understanding the novel software layers of the battlefield—layers that are being built to allow next-generation uncrewed systems to operate in conjunction with each other and to integrate seamlessly.

While much of the current discussion centres around technological advancements, FSDW also requires a leap in doctrinal thought. In this policy paper we identify two major variables that will determine whether NATO members achieve FSDW: mature cross-domain uncrewed teaming and effective doctri-

* James Patton Rogers is Lecturer in the Department of War Studies at King's College London. He is a scholar of drone warfare and emerging military technologies who has worked with the United Nations, NATO and a range of nation-states on the challenges of AI, robotics and future war. Dominika Kunertova is a leading expert in drone warfare who has co-led projects with NATO. She is a research fellow with the International Security Program at Harvard Kennedy School's Belfer Center and a non-resident senior fellow at the Atlantic Council. James Wesley Hutto is Associate Professor of Military Strategy and Security Studies at the School of Advanced Air and Space Studies. Elizabeth Redmond is lead research associate at Cornell's Tech Policy Institute where she researches emerging technologies and security, including work on hybrid warfare, supply chain security, and critical infrastructure resilience. She is project lead on the Full Spectrum Drone Warfare project from which this article originates. The work was supported by NATO Science for Peace and Security under grant G6101. This article is part of the *International Affairs* policy paper series. These short papers bring new insights into policy debates on the most important problems of International Relations, and offer clear and concise guidance and 'real-world' recommendations for policy-makers and practitioners.

¹ The terms 'Third Drone Age' and 'full spectrum drone warfare' were first published in 2022 in James Rogers, 'The Third Drone Age: visions out to 2040', Centre for International Governance Innovation, 28 Nov. 2022, <https://www.cigionline.org/articles/the-third-drone-age-visions-out-to-2040>; and James Rogers and Dominika Kunertova, *The vulnerabilities of the drone age: established threats and emerging issues out to 2035, final report* (Zürich: Center for Security Studies, ETH Zürich, 2022), https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/NATO_VDA_Policy_Report.pdf. See also Zachary Kallenborn, 'Swarm clouds on the horizon? Exploring the future of drone swarm proliferation', Modern War Institute, 20 March 2024, <https://mwi.westpoint.edu/swarm-clouds-on-the-horizon-exploring-the-future-of-drone-swarm-proliferation>. (Unless otherwise noted at point of citation, all URLs cited in this article were accessible on 11 June 2026.)

nal adaptation. Simply put, NATO cannot focus solely on hardware and hope to succeed: it must also update the way it conceptualizes twenty-first century warfare.

Advancements in drone technology across domains are already evident in active conflicts. Ukraine's uncrewed surface vessels (USVs), such as the *Sea Baby*, have helped drive back Russia's Black Sea Fleet and have downed Russian military helicopters. Iran and its Houthi proxies have successfully deployed explosive-laden 'drone boats' against international shipping. Uncrewed underwater vessels (UUVs) have become the new 'must have' for NATO allies and partners. Maritime surveillance has only grown in importance in a new age of great power threats against subsea critical infrastructure and deterrence assets. In addition, military uncrewed ground vehicles (UGVs) are experiencing a renaissance with the advent of autonomous command and control systems that mitigate longstanding connectivity and navigation issues.

It is not yet known what the next generation of these systems will look like and how they will be deployed in conflict. However, certain emerging trends can help paint a picture: for example, bottom-up software development, tech encroachment and the prevalent threat of counter-autonomy. Combining the discussion of our major variables with these trends, we offer four possible drone futures, from pure FSDW to warnings of tech without tactics.

Background: the rise of networked force

The 2000s and 2010s saw the platforming of optimized single drones for endurance and strike precision.² This trend produced isolated 'silver bullets' that now fail to scale, survive or coordinate within the contemporary security landscape. Legacy systems like Predator or Reaper are expensive and were built for asymmetric conflicts where command of the air was taken for granted.³ Interest in drone development grew slowly during the global 'war on terror' but surged after the effective use of drones by Islamic State from 2014 and by Azerbaijan in the Second Nagorno-Karabakh War of late 2020, and, in recent years, the use of maritime drones, first-person view quadcopters and long-range one-way attack drones in the Russia-Ukraine war (2022-) and the Iran war (2026-). As these instances attest, militaries are growing more comfortable with the integration into their operations of varying kinds of drone hardware and operating systems.

In contested spaces, high-cost drones are less appealing given the constant evolution of countermeasures, particularly between states with a high potential for development and large domestic defence-industrial bases. This was observed in the context of Russia's offensive war against Ukraine—in the early weeks

² James Patton Rogers, *Precision: a history of American warfare* (Manchester: Manchester University Press, 2023), pp. 1–6.

³ Sarah E. Kreps and James Patton Rogers, *Drones: what everyone needs to know* (Oxford: Oxford University Press, 2025), pp. 1–5.

of the Russian full-scale invasion, Ukraine deployed Bayraktar TB2 drones⁴ which soon disappeared from news reports as countermeasures against them were developed and deployed. Similarly, Russia has deployed its own combat-proven Orion drones sparingly because of their limited number and the threat posed to them by Ukraine's air defences. Even the United States has begun using one-way attack drones in its war against Iran. This is partly for reasons of experimentation, but also reflects the broader shift taking place in conflict where high-value airborne assets are increasingly vulnerable and command of the air is hard to obtain.⁵

High-cost drones are not attritable, which has popularized the new perception that investments in large numbers of small, disposable drones are the way to win modern wars. But mass alone does not constitute an effective strategy. FSDW depends on a networked force characterized by distributed collaboration, where systems exchange data and re-task one another autonomously and in real time. Ukraine's Magura V5 USV is a clear example. Designed to operate in rudimentary swarms and equipped with commercial connectivity that enables autonomous coordination without 'a human in the loop', the Magura V5 shows how enabling technologies are already converging in the field.⁶ For NATO, these developments should draw increased focus, analysis and funding; they will define the operational environment in which the alliance will operate and must now build a coherent, shared doctrine.

Major variables

We identify mature cross-domain uncrewed teaming and effective doctrinal adaptation as the two most important variables for the successful development of FSDW. States that want to maintain operational relevance in the coming decades must pay attention to both issues.

Technology: cross-domain uncrewed teaming

The technological core of FSDW is cross-domain uncrewed teaming, where air, land and sea drones can self-organize and adapt to environments and battlefields without a human in the loop. Backed by AI fusion, hardened connectivity and a common digital backbone, the software layer enables cross-domain uncrewed teaming as a central capability. This software layer is just as important as the physical hardware.

⁴ James Wesley Hutto and James Patton Rogers, 'The drone revolution: towards a synthesis in the drone debate', *European Journal of International Security* 11: 2, 2026, pp. 145–65, <https://doi.org/10.1017/eis.2025.10005>.

⁵ At the time of writing (April 2026), the US had lost between twelve and 24 medium altitude long endurance drones during its war against Iran, an unprecedented loss. Luis Martinez, 'More than a dozen \$16M Reaper drones have been destroyed in Iran operations, US officials say', ABC News, 17 March 2026, <https://abcnews.com/Politics/dozen-16m-reaper-drones-destroyed-iran-operations-us/story?id=131163787>.

⁶ Bryan Clark, 'Sea drones in the Russia–Ukraine war inspire new tactics', *IEEE Spectrum*, 10 July 2024, <https://spectrum.ieee.org/sea-drone>.

Immature cross-domain teaming is marked by deconflicted but largely siloed operations, where uncrewed aerial vehicles (UAVs), UGVs, USVs and UUVs share data intermittently and require human coordination to translate sensor inputs into cross-domain effects. These systems may coexist within the same battlespace, but adaptation is slow and integration remains procedural rather than systemic. Mature cross-domain teaming, by contrast, is enabled by a common digital backbone, resilient communications and AI-driven autonomy that allows heterogeneous platforms to dynamically self-organize, share intent and fused sensor data in real time and re-task across air, land and maritime domains without human intervention. In this mature model, cross-domain effects emerge continuously through distributed sensing and action loops, supporting resilient kill chains, rapid adaptation under contested conditions and scalable cooperation across joint and allied forces.

NATO and allied partner militaries have already begun experimenting with cross-domain teaming. Exercises like the annual REPMUS⁷ and Arcane Thunder 25⁸ have trialled integrated UAV, UGV, USV and UUV operations across air, land and maritime domains, with Arcane Thunder 25 specifically focused on synchronizing effects across land, sea, air, cyber and space to enable joint freedom of action in contested environments.⁹ At the hardware level, systems like the ROBUST UGV, which can both deploy and recover UAVs via a built-in robotic arm,¹⁰ and the Defense Advanced Research Projects Agency's USX-1 Defiant, a 240-tonne uncrewed ship designed to integrate UUVs and UAVs into a single autonomous network, show that cross-domain teaming is being engineered into platforms from the outset rather than bolted on.¹¹ These developments confirm that cross-domain teaming is no longer theoretical, but they also expose how far current doctrine lags behind what the technology can already do.

The integration of AI by defence technology companies like Anduril, Rhombus Power and Helsing are key to this layered development. Anduril and Rhombus offer AI-assisted sensor and data fusion for command and control, ingesting and fusing data from multiple sources—drones, satellites, ground sensors, open-source intelligence and personnel—to create a real-time digital picture of the security environment. Recognizing that 'defence has become a software problem', Helsing helps connect existing defence hardware to a new AI network.¹²

⁷ REPMUS stands for robotic experimentation and prototyping with maritime uncrewed systems. See Domenico Frascà, Paola Fratantoni and Alessandro Zanasi, 'Maritime drones: role in the military doctrines of NATO and EU member states, market study and procurement needs', IEEE, 8 Jan. 2024, <https://ieeexplore.ieee.org/document/10380950>.

⁸ Courtney Benedetto, 'Arcane Thunder 25 tests live data-sharing across theaters', AFCEA, 30 May 2025, <https://www.afcea.org/signal-media/arcane-thunder-25-tests-live-data-sharing-across-theaters>.

⁹ Clinton Carroll, 'Exercise Arcane Thunder 25 press release', Defense Visual Information Distribution Service, 1 May 2025, <https://www.dvidshub.net/news/496977/exercise-arcane-thunder-25-press-release>.

¹⁰ Elbit Systems, 'The Israel Ministry of Defense will begin testing a robotic unmanned vehicle', press release, 13 June 2022, <https://www.elbitsystems.com/news/israel-ministry-defense-will-begin-testing-robotic-unmanned-vehicle>.

¹¹ Defense Advanced Research Projects Agency, 'NOMARS: no manning required ship', 2025, <https://www.darpa.mil/research/programs/no-manning-required-ship>.

¹² Helsing, 'About Helsing', <https://helsing.ai/company>.

Strategy: doctrinal adaptation

Adaptation of military doctrine to leverage new technologies will be vital to the achievement of FSDW. In its ideal form, doctrine encompasses organizational beliefs about how to fight; doctrinal updates are the products of intra- and inter-organizational contests over best practices. These contests can be long and drawn out or quick and decisive, depending on the various roles and missions any technology can perform. In the case of drones, doctrine is the difference between a force that simply owns large numbers of uncrewed systems and one that can choreograph them across air, land and sea as a coherent FSDW system.

Low doctrinal adaptation looks like continuity rather than change; uncrewed systems are added to existing concepts of operation, force structures and training pipelines without altering underlying assumptions about how wars are fought, resulting in fragmented employment and limited cross-domain effect. Drones may be procured at scale, but they are hemmed in by platform-centric thinking. On the other hand, high doctrinal adaptation looks like a deep institutional shift in which uncrewed systems shape force design itself. The reality of FSDW informs how missions are conceived, how personnel are trained and how effects are synchronized for offence and defence. In this model, doctrine prioritizes integration, adaptability and learning against a responsive adversary rather than prescribing fixed uses for individual platforms.

Massive investment in uncrewed systems is already under way, but without doctrinal adaptation this funding risks becoming a money pit rather than a source of strategic advantage. The Trump administration's One Big Beautiful Bill Act (OBBBA) makes this clear; Section 20005 allocates US\$1.4 billion for the expansion of the small uncrewed aerial system industrial base, \$120 million for the development, procurement and integration of long-endurance uncrewed aerial systems for surveillance, \$500 million to prevent delays in delivery of attritable autonomous military capabilities, and \$145 million for the development of AI to enable one-way attack uncrewed aerial systems and naval systems.¹³ These and similar appropriations represent a strategic bet that drones will define victory in future war, even for advanced militaries. Yet, without concepts that explain what these drones are for, how they will be integrated across domains and services, and how they support a broader posture, such investments can generate fragmented capabilities, mismatched procurement procedures and escalating costs without decision advantage.

It is likely that taking one-to-one lessons from Ukraine will be ineffective for a global expeditionary power like the United States. Drones are not going away, but without doctrinal integration they remain disjointed novel technologies rather than an operational system. The U.S. Marine Corps' Force Design 2030 provides an early indication of what doctrinal adaptation for FSDW might look like: the establishment of the Small Unmanned Aircraft Systems (SUAS) School

¹³ 119th U.S. Congress, *H.R.1—An act to provide for reconciliation pursuant to title II of H. Con. Res. 14.*, 2025, <https://www.congress.gov/bill/119th-congress/house-bill/1/text>.

at the School of Infantry—East, the Small UAS and Counter-SUAS Integration Course at Camp Pendleton,¹⁴ and the publication of the First Marine Division School's Small UAS/Counter-small UAS integration handbook to support the course. These moves underlie a shift in how services see drones, not as a mere tool but a new reality of warfare; one commander stated that, through the instruction given, the students '... are not depending overly on any one piece of tech but are learning how to fight against an adaptive enemy'.¹⁵

Emerging trends

Bottom-up software development and implications for small-state and non-state actors

At one time, the data layer of warfare on which FSDW depends was only accessible to advanced militaries with developed defence-industrial bases. However, smaller states—like Ukraine, with its DELTA digital situational awareness ecosystem—have shown that bottom-up development of real-time digital command and control is possible. Ukraine has shown that digital warfare is no longer isolated to the largest, best-funded militaries using expensive platforms and cyberweapons, it is now developed by civilians responding to supreme emergency. DELTA, which now supports the efforts of nearly the entire Ukrainian army, was developed by a volunteer group called Aerorozvidka; the group was created in the wake of the Russian annexation of Crimea in 2014.¹⁶ This sort of citizen-led innovation, dependent on commercial rather than bespoke technology, underscores the growing ease of access to FSDW capabilities: put simply, interconnected cross-domain drone usage will proliferate widely by 2040.

Tech encroachment

The utility of commercial platforms on the battlefield—both augmenting and augmented by military hardware—has blurred the divide between the commercial and military sectors of the technology industry. There is a future in which militaries are entirely dependent on the tech sector, where technology companies are integrated into military organizations desperate to obtain, fuse and process data in ways that are operationally and tactically relevant. This practice is referred to as military–civil fusion, where private tech companies not only provide assets and/or services to the military but are involved on the 'ground floor' of the military technology development process.

Counter-autonomy as a dominant threat vector

¹⁴ Gidget Fuentes, 'Attack of the drones: : marines are learning to integrate drones for the ground fight', U.S. Naval Institute News, 25 June 2025, <https://news.usni.org/2025/06/25/attack-of-the-drones>.

¹⁵ Fuentes, 'Attack of the drones'.

¹⁶ Stefan Soesanto, *The Ukrainian way of digital warfighting: volunteers, applications, and intelligence sharing platforms* (Zürich: Center for Security Studies, ETH Zürich, 2024), <https://doi.org/10.3929/ethz-b-000685245>.

As states race to field autonomous drone systems, we are seeing that the future of war includes algorithms fighting algorithms for decision advantage. Under FSDW, where the kill chain is heavily dependent on real-time data collection and analysis, counter-autonomy will be a crucial area of study. Counter-autonomy includes jamming, spoofing, adversarial AI, supply-chain infiltration and other attacks that target how machines perceive and decide. In an FSDW environment, the contest between autonomous systems and counter-autonomy will directly shape the credibility of deterrence and the resilience of alliance operations. Many smaller, less expensive drones have no self-defences, partly because of cheap manufacturing material and low-resilience consumer electronics. Even though some first-person view (FPV) drone exemplars have been fitted with counter-jamming devices, this add-on substantially increases the cost per drone and can negatively affect payload effectiveness, capacity and battery life.¹⁷

Four possible futures for FSDW out to 2040

Drones will undoubtedly be a component of twenty-first-century warfare. The question is how they will be integrated and what ‘effective’ deployment will look like. Under FSDW, drones offer access to a form of warfare that moves at the speed of the machine and not the human. Uncrewed systems delivering real advantage, not just increased cost and complexity, are dependent on the maturity of cross-domain uncrewed teaming and effective doctrinal adaptation. Taken together, these dynamics produce four possible futures. For NATO specifically, the risk is that member states diverge across these scenarios, investing in incompatible systems and doctrines that undermine the interoperability on which the alliance depends.

Table 1: Matrix of four scenarios out to 2040 for doctrinal adaptation

	<i>Effective doctrinal adaptation</i>	<i>Ineffective doctrinal adaptation</i>
Mature cross-domain uncrewed teaming	Scenario A: full spectrum drone warfare	Scenario B: tech without strategy
Immature cross-domain uncrewed teaming	Scenario C: unoperation-alized doctrine	Scenario D: platform stagnation

¹⁷ Stacie Pettyjohn, *Evolution not revolution: drone warfare in Russia's 2022 invasion of Ukraine* (Washington DC: Center for a New American Security, 2024), <https://www.cnas.org/publications/reports/evolution-not-revolution>.

Scenario A: pure FSDW (likely)

In this scenario, the state develops AI capabilities to the extent that it can integrate autonomy into its drones, and its military readily adopts machine-teaming in its operations. The state's doctrine catches up with technology and the software layer becomes routine. AI-enabled fusion systems like DELTA, are scaled and federated; data from UAVs, UGVs, UUVs and USVs flow into a continuous command picture that can be acted upon with speed. Exercises such as REPMUS and Arcane Thunder 25 move from trials to practice. Field improvisations like Magura V5 supporting UAV launches are absorbed and standardized. Open, modular architectures and secure allied supply chains underpin this growth. The likely result is a living doctrine, updated as the field learns, that turns the software layer and cross-domain teaming into everyday advantage, while contributing to the maintaining of a credible alliance deterrence posture.

Scenario B: tech without strategy (likely)

In this scenario, the state develops AI capabilities to the extent that it can integrate autonomy into its drones, but its military organization remains sceptical and hesitant to fully adopt machine-teaming into its operations. The state possesses the capability, but bureaucratic politics slow the integration of the software into military doctrine. FPV inventories grow, but hand-offs fail, electronic warfare blunts effects and costs mount. Fleets of small, disconnected drones proliferate without common methods for sharing data or re-tasking across services and partners. Massive investments into drone technology (like those in the OBBBA) without equally substantial efforts being made to update doctrine will struggle to deliver advantages; the pace of drone and counter-drone technological development outpaces industry. The political takeaway that nations should simply buy more drones is misleading when the operational and strategic problem is a lack of shared software, links or updated practice.

Scenario C: unoperationalized doctrine (less likely)

In this future, doctrinal adaptation advances faster than technical integration. The state articulates sophisticated concepts for software-defined warfare and cross-domain machine-teaming, and services formally embrace these ideas in doctrine, training guidance and force design documents. However, this conceptual shift is not matched by investment in a resilient, shared digital backbone. As a result, cross-domain teaming remains shallow: data fusion is localized, connectivity is fragile and episodic and uncrewed systems cannot reliably self-organize across air, land and maritime domains. Exercises such as Arcane Thunder 25 demonstrate doctrinal alignment and joint intent, but these gains fail to translate into sustained battlefield advantage. Procurement continues to outpace integration, leaving services aligned in principle yet divided in

execution, with ambitious doctrine unfulfilled by the underlying technical and organizational infrastructure required to operationalize it.

Scenario D: platform stagnation (not likely)

This scenario is a reversion to the prior drone age, characterized by a reliance on expensive platforms or sheer FPV mass with little coordination between them. This scenario already appears to be an unlikely future. It would assume that current countermeasures taken against FPV mass are indomitable, whereas we have already seen counter-countermeasures arise in Ukraine, taken by both sides' forces in iterative technological deployments. In our view, battlefield experience drives technological competition in such a way to make inevitable the layering of software onto drone platforms as it becomes available, as well as cross-domain machine-teaming.

Policy recommendations

FSDW is already emerging in practice, but its strategic consequences will depend on how states choose to pursue it. The four futures above show that technology alone does not guarantee advantage. What matters is how investments, institutions and doctrine interact. Against this, three policy recommendations stand out.

1. NATO members and partners should deliberately steer towards Scenario A (FSDW) and treat Scenario B (tech without strategy) as a strategic warning. The matrix displayed in table 1 shows that mature cross-domain uncrewed teaming without effective doctrinal adaptation produces exactly the 'mass without collaboration' problem. To avoid this, states should treat FSDW as a planning framework rather than a buzzword, using it to audit programmes, prioritize joint experimentation and update doctrine, training and command structures around cross-domain uncrewed teaming. Procurement, concept development and alliance interoperability standards should all be evaluated against a simple question: does this move us closer to a routine, software defined, multi-domain force, or are we just adding more drones to a force that cannot choreograph them?
2. Investments should be directed not just to platforms but into a defence-industrial base that enables FSDW, with particular emphasis on next-generation innovators and academic partners. FSDW depends on secure, modular and interoperable software and hardware stacks. This requires a defence-industrial base that is capable of producing open architectures, resilient supply chains and highly advanced AI-enabled fusion tools. Policy should prioritize funding streams, innovation challenges and public/private partnerships that connect start-ups, industry giants and

universities working on AI, autonomy, ethical and legal decision-making and human/machine teaming. Academia can provide the conceptual and analytical work that current practice lacks, mapping FSDW's regulatory and ethical frameworks and training the next generation of officers who can 'speak the language' of FSDW.

3. Policy-makers should recognize that FSDW is not an exclusive club for major powers; small states and non-state actors are already moving quickly, and proliferation of the drone technology and software that underlie FSDW will accelerate. Ukraine's bottom-up DELTA ecosystem demonstrates that sophisticated digital command and control can be built with commercial hardware and volunteer expertise. It is not a stretch for these trends to extend to regional powers and violent non-state actors who can combine cheap drones, open-source software and commercial AI products. Policy must pair FSDW adoption with proactive measures to monitor and constrain dangerous forms of diffusion, such as tight controls and better enforcement on critical components and dual-use technologies.

Conclusion

FSDW is not a prediction, but a description of current and quickly progressing trends in drone warfare, exemplified by Magura V5 teaming, joint hand-offs in Arcane Thunder 25 and fusion tools like DELTA. NATO members and partners should learn from these experiences by engaging in doctrine development around software-platform integration and deployment of cross-domain machine-teaming. Hardware acquisition without software development and testing is sure to leave critical shortfalls.

For states, the advent of FSDW presents both strategic opportunities and significant challenges. Ukraine's experience demonstrates that FSDW offers a path toward more agile, scalable and survivable military forces that can hold off large offensive military powers. Yet as FSDW is pursued, it is important to recognize the critical questions, key vulnerabilities and prominent threats its advent reveals. Traditional rules of war and methods of engagement are sure to be upended. Connected to this, FSDW does not shed the ethical problems of autonomous military weaponry, but its achievement is largely contingent on how states resolve these problems. FSDW is therefore both a military-technical and a political project: it will redistribute power among states, reshape alliance cooperation and interoperability and test emerging norms on autonomy and AI in war.