THE ARSENAL OF DEMOCRACY

TECHNOLOGY, INDUSTRY, AND DETERRENCE IN AN AGE OF HARD CHOICES

EYCK FREYMANN
HARRY HALEM

FOREWORD BY ADMIRAL JAMES O. ELLIS JR., USN (RET.), AND NIALL FERGUSON

7

UNMANNED AERIAL SYSTEMS

The war in Ukraine has shown how quickly the unmanned aerial system (UAS) ecosystem is moving forward. UAS are rapidly growing more capable in both reconnaissance and strike, and they are being deployed at a scale that is orders of magnitude greater than in any previous conflict. To be sure, there are many differences between a geographically bounded land war and a geographically expansive air-naval war. Ukraine struggles with Western-style combined-arms mechanized warfare and in particular lacks the airpower to establish localized air superiority for very long. Both factors have profoundly shaped its use of UAS. Even so, the speed of innovation in the development and use of UAS and counter-UAS (CUAS) on the battlefield in Ukraine serves as a warning to Washington. Current US and allied UAS platforms—large, expensive, fixed-wing UAS designed for counterterrorism in the Middle East—are ill-suited for a potential great-power war in the Indo-Pacific. They are currently unprepared for the way UAS would likely be used in a conflict with China, particularly a protracted conflict. And they are not fielded in great enough numbers to survive a major conflict's likely attrition rate.

The next five years will likely see the emergence of mission-specific UAS alongside more sophisticated CUAS technologies, including

directed energy weapons, EW, sensor spoofing, and adversarial AI (AAI). Swarm capabilities will mature, but they may continue to face significant scaling problems and will remain more vulnerable to CUAS than individual units. The enabling systems that UAS use—namely, power generation, data processing, and communications—will remain essential.

Given the critical role that UAS will likely play on the future battlefield, the United States and its allies must prioritize cutting-edge drone design *and* the development of a robust industrial base capable of large-scale production. Existing US and European producers lack the capacity to produce high-capability drones in the multiple thousands—let alone the tens of thousands—needed for sustained, high-intensity combat. By contrast, China's state-backed DJI drone maker dominates the global commercial market for small drones with 76 percent market share. This gives it economies of scale that Western companies struggle to match.[1] Restricting DJI's access to Western markets may be necessary but will not by itself suffice to cultivate a competitive industrial ecosystem. Allied democracies need a coordinated technological and industrial strategy to scale production capabilities across the supply chain.

In the long run, the West's ability to lead in cutting-edge semiconductor design and fabrication could be crucial to this strategy. Superior computational power will be a decisive factor in regaining technological and market advantage in the UAS sector. Advanced capabilities such as edge computing will enable drones to process data closer to the battlespace and provide Western producers with a potential competitive edge.[2] In the short to medium run, however, a robust industrial strategy that includes UAS componentry is more important than a project of chip dominance. China has domestic capacity for close-enough-to-leading-edge chips. Any differential will probably be significant enough only by 2030—and this assumes that China fails to even the gap in leading-edge capacity.[3]

UAS are not the only type of "drone" used in modern military operations, nor are they a single, uniform system. We have already dis-

cussed unmanned surface and undersea vehicles (USVs and UUVs) in chapter 5. There are two main reasons for discussing UAS separately. First, the development of UAS is closely tied to the maturation of the three-dimensional battlefield and the advancement of airborne technologies like precision strike and stealth, making it a distinct area of analysis. Second, operational trends that apply to very different types of UAS, from first-person view (FPV) copters to long-range fixed-wing strike drones, don't apply to either USVs or UUVs.[4]

The Origins of UAS

UAS should be understood as a relatively recent innovation in a much longer precision and reconnaissance revolution. In 1943, Nazi Germany fielded the first guided munition: the Fritz-X, an anti-ship glide bomb controlled by radio. A bomber crew would deploy the weapon and manually guide it into its target.[5] By the end of the war, the Allies had deployed a limited number of similar weapons. Precision-guided weapons were first used at scale during the 1972 Easter Offensive, when US heavy bombers dropped "camera bombs" on major bridges in Vietnam to halt the North Vietnamese assault.[6] Although the technology behind precision munitions is sophisticated, the core concept is simple: Any weapon capable of guiding itself to a specific target with a high degree of accuracy is extremely valuable. Weapons that can hit mobile targets such as ships are even more so.

UAS in the sense we know them today were first employed in combat in 1982, when the Israeli Defense Forces deployed them as decoys to suppress Syrian air defenses in Lebanon.[7] Over time, UAS have evolved to support precision strike weapons, providing accurate information on the enemy's location and sometimes launching precision strikes themselves. The US military fielded UAS during the 1991 Gulf War. Smaller UAS spotted for the *Iowa*-class battleship USS *Missouri* while larger UAS identified targets for B-52 bombers and conducted battle damage assessment after heavy strikes.[8]

UAS were employed extensively in the War on Terror, operating primarily in uncontested airspace—a stark contrast to the challenging environments they would face in an air-naval conflict with China. Western manufacturers developed specialized UAS for counterterrorism operations, focusing on large, fixed-wing platforms with sophisticated sensors and extended endurance capabilities.[9] The MQ-1 Predator and the MQ-9 Reaper emerged as prime examples of these medium-altitude, long-endurance (MALE) UAS, becoming the US military's workhorses throughout the Middle East.

These MALE UAS are equipped with extensive sensor packages and can maintain extended surveillance operations. The MQ-1 can survey a target for half a day, the MQ-9 for over a day. They're equipped with precision-guided weapons to engage targets while minimizing collateral damage. Though the Reaper is significantly slower than a typical fighter jet, cruising at maximum speed of 240 knots (around 450 kilometers per hour), it makes up for its modest speed with remarkable endurance—it can remain airborne for up to twenty-seven hours.[10] MALE UAS such as the Reaper have much larger wingspans than fighter jets but are smaller in all other dimensions.

These capabilities, however, come at a substantial cost. A single Reaper costs around $30 million, half the price of a fighter jet.[11] Although MALE UAS proved highly effective for long-range missions against al-Qaeda and other Islamist groups in the Middle East and Central Asia, their design emphasis on engaging low-tech nonstate adversaries makes them ill-suited for high-intensity conflicts with even countries of moderate-size. Their vulnerability to even basic anti-air defenses, particularly when combined with EW systems that can disrupt operator control, makes them poorly suited for great-power war.

To understand how the UAS ecosystem might evolve in the years ahead, the rise of airpower in the early to mid-twentieth century is a potentially helpful analogy.[12] In 1914 and 1915, near-continuous battle lines thousands of kilometers long emerged along the Western, Eastern, and Italian fronts. Going on the attack required massing an enor-

mous amount of machinery and ammunition. Defending against such a mass of men and matériel required effective reconnaissance. Both the Allies and the Central Powers turned to manned aircraft to scout enemy positions. Technological development soon opened up new possible applications, from long-range bombing to troop transport. Thus, aircraft designs soon became more specialized. Air wings began to develop into mutually supporting systems, with reconnaissance, targeting, strike, and damage assessment separated into differentiated roles.[13] Specialist systems, tactics, and personnel grew up for each.[14] These trends significantly affected the outcomes of key battles and campaigns. By World War II, airpower had become central to strike, as illustrated in the Battle of Britain, the D-Day landings, and the strategic bombing campaigns against Germany and Japan. The range of aircraft also increased significantly, allowing aircraft carriers to engage each other from great distances.

If UAS develops the way airpower did between the early 1910s and early 1940s, probably at a faster pace given the development and diffusion of technology, the long-term impact on the character of warfare could be enormous. Just as airpower diffused across all military organizations, each of the services might eventually operate its own networks of UAS for spotting, strike, and logistics. Just as early military aircraft transitioned from surveillance roles to integrated strike capacities, and air wings gained the capability to conduct complex operations, UAS might eventually operate as intelligent swarms more capable than the sum of their parts.

However, there are important limitations to the airpower analogy. World War I aviation initially operated with minimal coordination. The introduction of aerial radio—first using Morse code, then voice communications—made aircraft increasingly effective at guiding artillery and coordinating operations.[15] By World War II, advances in radar and communications had transformed airpower from merely a surveillance tool to an integrated strike force. Today's UAS face a fundamentally different challenge: If electronic warfare severely disrupts sensing, communications, and other critical functions, can UAS be

trusted to operate effectively? Can they make good decisions in contested environments without help from human operators?

The UAS Ecosystem in Ukraine and Beyond

The Russia-Ukraine war is the first conflict in which both sides have employed so many types of UAS—from highly sophisticated reconnaissance assets to hand-built FPV drones—to create large-scale reconnaissance and strike systems. As of early 2025, Ukrainian forces alone were receiving around 200,000 UAS per month.[16] Although this number will likely continue to fluctuate, it has been increasing exponentially since the war broke out in February 2022. Ukraine has become particularly dependent on FPV drones, which are designed to explode near the enemy.

It is helpful to differentiate among seven types of UAS that have been widely deployed in Ukraine. These are small, medium, and large copters; small and large fixed-wing drones; and small and large loitering munitions (see table 7.1).[17] UAS have been used for both reconnaissance and strike, and combinations of them often work in tandem. Loitering munitions have been shown to be particularly useful for strategic bombardment and counter-battery suppression, but artillery remains paramount for these purposes—put otherwise, UAS amplify artillery rather than replacing it.[18]

Meanwhile, CUAS techniques are rapidly evolving.[19] A CUAS system may use any of four basic tracking techniques to assess targets: radar, radio frequency (RF) analyzers, acoustic sensors, and optical sensors.[20] Once a hostile UAS is detected and classified, CUAS systems can use a range of engagement mechanisms to respond. Today, the most common response is to employ frequency jammers.[21] These can be wide-area jammers or jamming guns with adjustable frequencies. Other response options include cyber takeover methods; directed energy weapons (DEWs); and kinetic weapons such as small missiles, guns, or interceptor UAS. The most effective way to neutralize enemy

Table 7.1 Seven types of UAS used with some success in Ukraine

Type	Control method	Range	Role	Ordinance	Example
Small copter	First-person VR goggles	2 km	Tactical reconnaissance	Light weapons	DJI Racing FPV
Medium copter	Small tablet	5–7 km	Tactical reconnaissance	Grenades, mortal shells	DJI Mavic
Large copter	Small tablet	More than 10 km	Deeper persistent reconnaissance	Generally unarmed	DJI Matrice
Small fixed-wing drone	Ground control station	More than 20 km (depends upon signal)	Operational reconnaissance against high-value targets	Unarmed	Russian Orlan-10, Ukrainian Shark
Large fixed-wing drone	Ground control station	More than 1,000 km	Operational and strategic reconnaissance	Can carry guided weapons	MQ-9 Reaper, Bayraktar TB-2
Small loitering munition	Ground control station	40 km	Counter-battery fire	Has a small warhead	Lancet, Ukrainian "Ukrolan-cet"
Large loitering munition	Ground control station	More than 1,000 km	Strategic bombardment and deep strike	Organic warhead outfitted	Shahed-136/ Geran 2

Sources: Author's interviews; Harry Halem, "Ukraine's Lessons for Future Combat: Unmanned Aerial Systems and Deep Strike," *Parameters* 53, no. 4 (2023).

UAS operations is often to target the control station or central data hub. Given the diverse threat landscape that modern adversaries present, effective CUAS systems must integrate multiple detection and response capabilities.

Zooming out beyond the tactical level, the Russia-Ukraine war has highlighted several lessons for the US and allied UAS ecosystem. First, any future US-China conflict will involve very high attrition rates for UAS. If neither side achieves a quick victory, industrial capacity will be crucial. In the Middle East, US forces are already countering cheap UAS launched by Iranian proxies with much more expensive interceptors. This defensive approach is unsustainable as unit costs of UAS fall and their capabilities improve. The solution in principle is to cultivate a large and competitive UAS industrial base in the West, but this will not appear organically. Although a number of UAS producers are in the United States, and several are in Europe, none of them can produce in the multiple thousands, let alone the tens of thousands of units needed for high-intensity combat. China by contrast has DJI, a dual-use producer with 76 percent market share in the global commercial drone market.[22] There is no historical precedent for Western firms recapturing market share once China dominates a sector.

One possible response is for the United States—ideally in tandem with key, trusted allies—to ban imports of commercial drones and parts from China to create space for domestic producers.[23] As of this writing, an active public debate is ongoing on the topic, and consensus is building for a near-comprehensive ban.[24] However, simply banning DJI is no panacea. Protecting the market will allow Western producers to achieve economies of scale, which will drive down unit prices, but limiting their exposure to competition from China will reduce incentives to innovate and adapt. Banning DJI will also accomplish little for deterrence if US UAS manufacturers remain dependent on China for components. In October 2024, China announced sanctions on Skydio, the largest US drone producer.[25] Facing a resulting shortage of batteries, the company immediately announced that it would have to ration batteries in the drones delivered to customers.[26]

This is an example of a supply chain dependency that must be addressed immediately and comprehensively, since China can actively leverage it to hamstring US and allied capacity. Not until January 2025 did the Commerce Department move decisively to restrict American UAS producers from relying on PRC components.[27]

Second, the technological competition around UAS covers enabling systems and CUAS, not just UAS hardware. Just as early air competition extended beyond aircraft design to encompass critical technologies such as interrupter gear, remote-release bomb racks, airborne radios, and radar, today's UAS competition spans multiple domains. Success for the United States and its allies will require mastery not only of the drone platforms themselves but of AI, EW and counter-EW, batteries and charging systems, sensors, communications, and collaborative systems—all supported by robust industrial capacity and manufacturing know-how for hardware. The United States will have to collaborate with allies to build out a robust industry of producers in this ecosystem—and ensure that their supply chains are resilient.

Third, force integration and training are crucial to successful UAS employment, demanding aggressive, comprehensive adoption of UAS throughout a military organization. Ukraine's case is particularly demonstrative. Ukrainian volunteer units developed UAS operational techniques from 2014 to 2022 and subsequently diffused these techniques across the regular army after Russia's full-scale invasion.[28] They benefited from a collaborative and open culture made up of small units in which new soldiers gained and refined insights from more experienced UAS operators. Without this baseline experience, the Ukrainian military probably could not have accelerated UAS deployment to its current scale. The US and Taiwanese militaries are not integrating UAS—or for that matter, any unmanned systems—into their force structures at anywhere near the same depth as prewar Ukraine.[29] The United States and its allies must help Taiwan revamp its training system so that its forces can assimilate cutting-edge UAS and CUAS technology and operational techniques. Taiwan and Ukraine should ideally foster a direct partnership in this area.

Fourth, rapid adaptive learning is critical for using drones effectively in combat. The US military has not been forced to adapt tactically at this speed since World War II. Ukraine and Russia are constantly switching to new frequencies, trialing new jamming and spoofing techniques, and fielding new UAS tactics, as well as fielding new UAS types. Many of the UAS that the United States has sent to Ukraine have become largely ineffective after only a few weeks of combat given the speed of Russian tactical adaptation.[30] Ukrainian adaptive learning occurs throughout the supply chain, with operators providing feedback that domestic producers use to modify designs month-to-month.[31] Russia has also essentially copied many Ukrainian procedures and has sought to expand and scale UAS production.[32] A war with China will require different and larger systems than the small FPV drones Ukraine employs at scale. The adaptation cycle may thus be slightly longer given the geographic distances involved in the Indo-Pacific, which necessitate larger and more expensive UAS than the ones used in Ukraine. Still US suppliers may need to modify designs and revamp production line changes on a monthly basis and design hardware that can remotely download software updates. US forces must also deepen knowledge exchanges and joint training to assimilate combat knowledge from Ukrainian UAS operators.

Economies of Scale in Small UAS Production

Small unmanned aerial system (SUAS) production and supply chains are pivotal to US military strategy and force structure, but scaling their production reveals systemic challenges within the American defense industrial base (DIB). Simply increasing funding cannot resolve these bottlenecks. Without structural reforms, additional resources risk being wasted or misallocated. SUAS epitomize broader difficulties in US military production: Despite advanced technology and vast budgets, the ability to quickly ramp up manufacturing remains elusive.

The production of SUAS hinges on two critical factors: power generation and airframe manufacturing. Most modern SUAS, including those deployed in Ukraine, are typically battery powered.[33] While fuel-powered variants offer longer endurance, greater range, and heavier payloads, battery-powered SUAS dominate frontline operations due to key tactical advantages.[34] Their quieter operation enhances stealth and surprise, especially in night missions, while their simpler maintenance requirements and logistical ease—charging batteries versus transporting fuel—make them ideal for mass production at lower costs.

China's dominance of the global battery supply chain poses a significant vulnerability for the United States.[35] The recent decision by US drone manufacturer Skydio to ration batteries due to Chinese sanctions starkly illustrates this dependency.[36] The issue extends beyond drone batteries to charging infrastructure, such as large lithium-ion batteries used as portable generators.[37] Although Ukraine has mitigated such constraints through informal procurement networks and donations, these ad hoc solutions are insufficient for the sustained demands of a major US conflict. Developing a robust domestic battery industry is a daunting task, given China's entrenched control over the supply chain from raw materials to finished products.

Beyond supply chain challenges, manufacturing techniques further constrain the ability to scale SUAS production. Injection molding, a cost-effective process where heated high-strength plastic is shaped in prefabricated molds, offers the most viable path to mass production.[38] This method reduces costs, improves performance, and supports rapid scalability. Chinese companies like DJI and Autel have achieved this level of efficiency by leveraging high civilian demand to justify the necessary investments. In contrast, the US military SUAS market lacks sufficient scale to incentivize comparable private-sector commitments, creating a production gap that would be acutely felt in wartime.

Ukraine's domestic SUAS production highlights these challenges. Unable to achieve the scale of injection molding, Ukrainian manufacturers rely on fiberglass molding, a labor-intensive process that meets

immediate tactical needs but falls short of the production volumes achieved by civilian-focused firms like DJI. For the United States, addressing these constraints will require preemptive investments in both supply chain resilience and scalable manufacturing capacity to ensure readiness before a crisis erupts.

Emerging Tech Trends

Several emerging drone-related technologies are not yet fully battle ready but are still worth tracking closely. Much of the aviation vehicle hardware exists, and software and system integration are progressing toward deployment.

Collaborative Combat Aircraft (CCA)

CCA are a kind of UAS imagined to work as "loyal wingmen" for next-generation manned aircraft, including sixth-generation fighters and bombers like the Northrop Grumman B-21 Raider.[39] Unlike conventional UAS, CCA incorporate a sophisticated AI-driven "autonomy package." This should make them more survivable and adaptable on the battlefield and capable of teaming up with pilots by expanding situational awareness and providing more and differentiated sensing, better analysis, and integrated recommendations. CCA are expected to cost significantly less than manned aircraft with comparable capabilities, and the goal is eventually to make them attritable. The Air Force is betting heavily on the technology and plans to invest more than $8.9 billion in CCA programs between fiscal years 2025 and 2029.[40]

The promise of CCA lies in their ability to integrate into formations, take on high-risk missions, enhance situational awareness, and reduce risks to human pilots by complementing manned platforms.[41] Equipped with modular payloads, CCA could perform a variety of tasks, from EW and scouting to offensive and defensive operations,

including precision strike.[42] By leveraging AI and state-of-the-art onboard compute, CCA could process vast amounts of data, make decisions autonomously, and execute missions with minimal human oversight. This is an essential capability since CCA will operate in contested environments where communications may be degraded or disrupted.

However, significant technical and operational challenges still need to be overcome. The Air Force and its contractors have not yet developed robust algorithms that could operate in unstructured or chaotic environments. Communication systems between CCA and manned aircraft remain vulnerable to EW. Rules of engagement for autonomous systems are still evolving, and clear boundaries between human and AI decision-making are essential to ensure predictable behavior and responsible deployment. The edge computing systems that CCA use to process data locally and operate autonomously are power and heat intensive. Running intense computing on board will require energy from either the propulsion system or the battery, which exacerbates perhaps the biggest challenge of all: limited range, especially when compared with a manned platform. Offboarding processing is possible, but it would still require some high–power consumption platform and would probably be susceptible to jamming. Protocols for handling situations such as communication loss or damage remain underdeveloped, and the complexity of assessing and repairing battle damage in autonomous systems has not been fully explored. These gaps all currently impact the developmental reliability of CCA and must be overcome before CCA could conceivably be paired with manned platforms in a combat environment.[43]

Production and logistics present another critical obstacle. Current prototypes, while promising, are expensive and rely on complex AI systems, sensors, and modular designs that are challenging to produce affordably and at scale. These components risk becoming outdated given the rapid pace of innovation in computation. Expanding the skilled workforce to build and maintain these systems will be a significant challenge.[44] Modular payloads offer mission flexibility, but

the Air Force must first invest in logistics and field maintenance infrastructure to support large-scale CCA deployments. Human factors also require attention. Training pipelines for operators and maintenance personnel must be expanded and updated to handle the complexities of CCA, particularly their reliance on advanced AI and autonomous systems. Integrating CCA into existing fighter squadrons will require cultural adjustments and additional resources to align manned and unmanned operations effectively. Pilots will take time to fully trust CCA and for good reason: Operating autonomous systems in proximity to manned aircraft will require high confidence in their reliability.

Despite these challenges, accelerating CCA programs will probably be crucial for maintaining US air combat capabilities into the 2030s. The US fighter fleet averages thirty years old.[45] Although these aging airframes remain effective thanks to technological updates and solid engineering, the older they become, the harder they will be to maintain and repair. A robust CCA fleet will be both cheaper than manned aircraft and, being more modern, easier to maintain.[46]

The Air Force has already begun developing CCA platforms to integrate into the fleet. Over the next five years, it plans to invest over $6 billion to acquire a fleet of more than one thousand CCA.[47] The FY 2025 budget request includes $8.9 billion for CCA over this period.[48] In collaboration with the Air Force Research Laboratory (AFRL), General Atomics Aeronautical Systems designed and tested the XQ-67A unmanned aircraft, which served as the foundation for its successful bid in the first round of CCA contracts.[49] The XQ-67A completed its maiden flight on February 28, 2024.[50] Similarly, Anduril Industries is developing a large, uncrewed aircraft named Fury, equipped with advanced command and control software.[51] Both companies will continue to receive funding from the Air Force to refine their prototypes, with full-scale production contracts expected in 2026.[52] Beyond these efforts, Congress has allocated substantial funding to DARPA's Air Combat Evolution (ACE) program. This initiative focuses on fostering trust in autonomous aircraft by showcasing the capabilities of human-machine collaboration in combat scenarios.[53]

In conclusion, while CCA represent a potentially transformative capability, their success depends on addressing significant technical, operational, and logistical challenges. A measured, realistic approach that includes clear testing milestones and incremental deployment will help ensure that the program delivers on its promise without overextending resources. Congressional support for research, testing, and supply chain resilience will be essential to making CCA a reliable and sustainable capability for the US military.

Swarms

The evolution of UAS has enabled increasingly sophisticated swarming technologies. As these systems develop autonomous navigation and decision-making capabilities and can exchange data with each other more effectively, they can increasingly coordinate attacks without the need for human intervention. A key advantage of swarming lies in its inherent redundancy. All military organizations have a few key nodes through which orders flow and coordination occurs.[54] Unlike traditional units, a swarm lacks a single control point and can therefore continue operating even if some drones are disabled. Using "mesh networks," each drone can function as both a node and a relay, extending range and maintaining connectivity even if others go offline.[55]

Future swarm architectures will likely combine numerous low-cost, expendable UAS with specialized, high-capability UAS for surveillance and strikes.[56] Some designs incorporate "mother ship" drones as power banks, though this approach risks creating a single point of failure if the mother ship is targeted and incapacitated. Swarms with autonomous capabilities offer additional benefits, such as low latency (the ability to respond very quickly to commands) and specialized task execution.

Swarming technologies are generally not yet robust enough to use in complex combat missions. Most UAS used in Ukraine are still manually operated.[57] Swarm scaling is hindered by intensive computing

requirements for autonomous decision-making. Edge computing and distributed processing have reduced these requirements but have not yet solved the problem.[58] Swarms are also more vulnerable to electronic warfare than UAS operating individually. Techniques such as frequency hopping provide some protection against EW, and advances in inertial systems and vision-based navigation have reduced reliance on GPS, but data transmission between units in a swarm remains susceptible to interference.[59]

Progress in computing will be a key long-term driver of swarms' combat effectiveness. The Biden administration's export controls on advanced semiconductors to China aimed to exploit US and allied advantages in chipmaking to give the US forces access to cheaper and more abundant compute than the PLA. If the price of computation keeps falling exponentially, as it has been doing since the 1950s, and China cannot keep up through indigenous innovation and black-market chip purchases, US combat systems could gain nonlinear advantages over their PRC competitors over a five- to fifteen-year horizon. Limiting access to cutting-edge graphics processing unit (GPU) compute in the cloud also impedes China from training new UAS computer vision and decision models. Efficiency improvements for model inference will also be important, since power supply is a major constraint for all UAS. Wireless power transfer could be transformative, but it faces technical obstacles, particularly in adversarial settings.[60] Advances in high-density batteries, including solid-state designs, are also worth watching as potential game changers that improve the amount of compute that both sides can deliver to the combat "edge."

Spoofing and Adversarial AI (AAI)

UAS are vulnerable to spoofing, a technique that involves feeding false information to UAS sensors and navigation systems and leading them to break from formation flying, waste munitions on phantom targets, or crash. GPS spoofing is commonly used in Ukraine, which

explains the race to develop non-GPS navigation systems.[61] Spoofing threats are particularly acute for CCA, since errors can potentially result in the loss of the fighter aircraft as well as any CCA that accompany it.

Adversarial AI (AAI) poses an additional threat in the same vein as spoofing. AAI targets a UAS's decision-making systems rather than its traditional communication links. AAI techniques like evasion attacks can mislead UAS into misidentifying threats or use "data poisoning" to degrade system performance over time.[62] AAI can also extract information on adversaries' AI algorithms.[63]

Military UAS are adopting layered defenses in response. Multimodal sensors can reduce reliance on any single data stream, while anomaly detection algorithms identify potential attacks in real time.[64] However, sophisticated spoofing attacks are coordinated across multiple data streams. Encrypted communications provide some protection from spoofing, but they require frequent updates as adversaries are constantly trying to bypass security protocols. Anomaly detection systems can be compromised by the very data poisoning they aim to prevent. All these approaches are compute-intensive and thus reduce compute and power available for other operations. Most critically, defensive systems make UAS more expensive to design and build.

For the foreseeable future, the threat from AAI and spoofing will continue to shape the design and deployment of UAS and CCA at a fundamental level. Commanders will face a critical trade-off: Overreliance on autonomy increases vulnerability to AAI attacks, while heavy dependence on human input could slow decision-making in high-threat scenarios. Adversaries are likely to target the weakest links in CCA formations, which include human pilots, potentially compromising individual units or entire operations. Production challenges amplify these risks. On top of short supplies for standard chips, specialized manufacturing processes inflate costs for the hardened processors and efficient chips required for inference, optimization, and AAI resilience. These delays create opportunities for adversaries to develop and test new attack methods on commercial platforms,

potentially keeping their offensive capabilities ahead of US defensive measures.

The US military should take several steps to stay on top of the AAI and spoofing challenge. First, it should invest in scalable defensive technologies, focusing on affordable sensor fusion and advanced edge computing. Second, it should create training scenarios that prepare operators to handle compromised systems and develop clear contingency plans. CCA should be built with combat losses in mind, making redundancy a key feature in both individual platforms and the overall fleet. In the short term, efforts should focus on fallback navigation systems, secure software updates, and kill switches for compromised drones. Finally, CCA acquisition strategies must prioritize flexible designs that can quickly integrate new defenses as threats continue to evolve.

UAS in the Indo-Pacific

In a potential war over Taiwan, UAS would be essential for combat in the First Island Chain. In any conflict scenario over Taiwan, the US Marine Corps (USMC) would probably fight out of low-profile, austere bases in Japan's Ryukyu archipelago and other small islands. Under Force Design 2030, the USMC is preparing to deploy small, distributed teams across the First Island Chain. Equipped with antiship missiles, mobile launchers, and UAS, these teams would compel the PLA to shift combat power and scouting assets away from Taiwan. Organized in a new force structure called Marine Littoral Regiments (MLRs), they would be fighting within the Chinese anti-access bubble and would need to minimize the signature of their movements and communications.[65]

MLRs would need UAS to help spot and attack PLA targets. If US space-based communications are jammed, they might also use UAS to transmit information to headquarters and receive orders in return. MLRs would also require sustainment and resupply in remote loca-

tions. Over time, the USMC would need to purchase hundreds—and, in time, thousands—of large copters and small- and medium-size fixed-wing UAS for logistics and reconnaissance. The USMC has signed an initial-rate contract with SURVICE Engineering to deliver twenty-one large uncrewed resupply copters.[66] More programs along these lines are probably coming. However, unless there is a drastic improvement in battery technology, it is hard to imagine rotary wing drones will be relevant in the Pacific outside of near-littoral or terrestrial operations. Gas-powered drones are an option, but they are not efficient for long distances.

US allies and partners in the Indo-Pacific are moving swiftly to adopt UAS, though they too are struggling to produce affordable drones at scale (see table 7.2). The Japanese Self-Defense Forces, in the process of a broader reorganization, are emerging as a potential buyer. Although Japanese manufacturers like Kawasaki and Yamaha have UAS production experience, they have yet to achieve meaningful scale.[67] South Korea, too, is expanding its UAS capabilities. It now produces an entire indigenous truck-launched, fixed-wing UAS system.[68] The Australian military has prioritized larger UAS, but it is too geographically distant from Taiwan to field its own UAS usefully in a conflict unless Australian forces are forward-deployed.[69] The United States, United Kingdom, and Australia could deepen cooperation on UAS production through the AUKUS framework. India has contracted with General Atomics to buy MQ-9B Reapers, some components of which will be locally produced. India might eventually become a major US partner for UAS component manufacturing.[70]

Taiwan's UAS program deserves particular attention. The indigenous Teng Yun system is sophisticated and similar to the Reaper. However, Taiwan currently lacks the ability to produce larger UAS in quantity. Taiwanese small UAS, in particular the Cardinal series and loitering munitions such as the Chien Hsiang, which seek out enemy radars, are more promising.[71] Taiwan needs to make heavy investments to build a domestic UAS supply chain and stockpile relevant parts. In a conflict scenario, Taiwan would probably be blockaded. It

Table 7.2 Major UAS programs in regional democracies

Program name	Country	Function	Stage of development
Elbit Hermes 900	Philippines	Tactical reconnaissance	In use
ScanEagle	Philippines	Low-altitude reconnaissance	In use
KAI RQ-101	South Korea	Collect military intelligence	In use (fielded in late 2010s)
MQ-28 Ghost Bat	Australia	"Loyal wingman" alongside manned fighters	Prototype
BAE Strix	Australia	Intelligence, surveillance, and reconnaissance (ISR)	Prototype
MQ-9B	India	ISR and precision strikes	Contracted, some components to be locally produced
NCSIST Teng Yun	Taiwan	Reconnaissance and strikes	In development
NCSIST Albatross I/II	Taiwan	Reconnaissance, target acquisition missions, and strikes	Under evaluation
NCSIST Cardinal series	Taiwan	ISR	In development
NCSIST Chien Hsiang	Taiwan	Loitering munition targeting enemy radars	In development

Sources: Publicly available national defense documents

would have to rely on components and supplies already positioned on the island.

Taiwan has adopted two strategies to address this risk. First is a program to indigenize production of UAS components. Taiwanese firms eye both growing domestic demand and global export of dual-use drones as an alternative to PRC vendors. More local capacity across those supply chains could improve industrial resilience in a conflict. Second is to buy from abroad. Taiwan's growing defense budget is a market opportunity, and the United States is ramping up sales of defensive drones in response.[72] The US Department of Commerce in 2024 led a trade mission of two dozen firms seeking to sell UAS to the island's military or first responders; US export controls nonetheless impede direct commercial sales. Taiwan is also interested in non-US UAS vendors; this commercial-adjacent sector could be an avenue for friendly countries to reconsider existing prohibitions on defense business with Taiwan.

Taiwan also needs better CUAS to defend both military assets and critical infrastructure. The Taiwanese government recently announced the creation of a ground-based but satellite-enabled CUAS detection and tracking network, using a low-earth orbit (LEO) satellite constellation for communications resilience.[73] Taiwan's planned LEO "constellation," however, has only two satellites. US-based SpaceX is now the world's largest launch provider, satellite manufacturer, and constellation operator and would seem a natural partner.[74] Taiwan has explored cooperation since 2018, and it has used SpaceX commercial launch services.[75] But there have been frictions on satellite manufacturing supply chains and on business terms for access to the SpaceX Starlink network.[76]

Recognizing the centrality of UAS capabilities in a potential conflict, the DOD has announced special programs and initiatives to put drone warfare at the forefront of development. The most prominent is Replicator, a $1 billion effort based on the concept of "All-Domain Attritable Autonomy."[77] The DOD intends to buy tens of thousands of unmanned UAS and underwater and surface drones for rapid deployment to the Indo-Pacific, at low-enough unit prices that they can be treated as disposable. The US government has made few details public,

and the timeline is uncertain. Replicator is also an attempt to test the productized-sales model discussed in chapter 6, in which vendors fund most of the research and development costs and in return enjoy much higher margins.

In June 2024, INDOPACOM Commander Admiral Samuel Paparo publicly acknowledged a related program, called Hellscape. If China attacks one of its neighbors, "I want to turn the Taiwan Strait into an unmanned hellscape using a number of classified capabilities," Paparo said. "I can make their lives utterly miserable for a month, which buys me the time for the rest of everything." Paparo declined to elaborate but promised that the program "is real and it's deliverable."[78] Hellscape might involve UUVs, unmanned surface vehicles (USVs), and naval mines, as well as UAS. The DOD has disclosed no details.

These threats will make for more credible deterrents if allied industrial capacity can fully back them up. Currently, no single company can provide large-scale UAS, or any type of unmanned systems, to meet the mission that Hellscape envisions or to meet the requirements that Replicator articulates. Moreover, Replicator is neither a formal program of record nor a defined set of programs. In the medium term, the DOD will have to clarify Replicator's mission and enable US allies to participate and potentially help accelerate the program.[79] Israel's existing MALE drones, for example, could potentially prove useful if the United States can build off the momentum of joint air defense development programs.[80] The DOD will also need to provide clearer guidance to potential vendors about its precise tactical, operational, and force design concepts, particularly for advanced technologies like swarming and counter-drone systems. Changing this guidance process will require a cultural change in the DOD.

Conclusion

Over the medium term, each service will require large numbers of UAS capable of deploying from austere environments across the Indo-

Pacific, fulfilling diverse roles in scouting, strike, communications, and logistics. These assets will be vital for sustaining operational tempo and ensuring the cohesion and effectiveness of distributed forces in contested environments. Although the United States is likely to remain at or near the cutting edge of UAS technology, the primary challenge lies in industrial capacity: how to produce enough of the right UAS and components affordably, at scale, and in competition with China's dual-use producers, while ensuring continuous adaptation and innovation.

To meet this challenge, the United States and allied militaries must urgently establish a secure industrial base to mass-produce cheap, expendable UAS along with the necessary components and sensors. As a first step, the US should consider banning imports of UAS and critical componentry from the PRC. Such a move would create room for domestic and allied providers to scale up and innovate while reducing dependency on foreign systems that could pose security risks. However, banning PRC drones is no silver bullet. The US and its allies must collaborate with the private sector to incentivize scalable production and drive ongoing investment in software, modular parts, and CUAS tools.

To integrate UAS effectively into future military operations, the US must embed organic UAS capabilities at every level of the armed forces, including down to the squad level for the Marine Corps and the Army. This aggressive integration is critical not only for combat effectiveness but also for future force development. The US cannot wait to adopt UAS at scale once a major war begins; the operational differences between fighting with and without UAS demand deep experience in their use beforehand. This requires extensive exposure—in every service and every domain—through peacetime exercises, war games with allies, and day-to-day training. Only by embedding UAS in routine operations and refining tactics through combat data can the US and its allies adapt effectively as new systems come online.