Drones sit in takeoff position before drone swarm demonstration during NATO's Counter-Unmanned Aircraft Systems Technical Interoperability Exercise in Vredepeel, Netherlands, on November 10, 2021 (Courtesy NATOChannel)

Countering Swarms

Strategic Considerations and Opportunities in Drone Warfare

By Jonathan B. Bell

> *One of our most important duties as professionals is to think clearly about the problem of future armed conflict.*
>
> —General David Perkins[1]

The Department of Defense (DOD) and the U.S. Government face a significant national security challenge in adversarial use of small unmanned aircraft systems (sUAS). The available technology to create swarms of these capabilities results in multilayered and unmanageable threats. This article addresses ways to prepare for and respond to this looming challenge, colloquially known as "drone swarms." Driving this concern are underlying questions that challenge conventional thinking and practice. Some of the unanswered issues include the potential capability of sUAS swarms against U.S. interests and the reciprocal response.

Colonel Jonathan B. Bell, USA, is Director of Operations and Training (J3) for Joint Region Mariana, Guam.

No approach to date has adequately addressed America's potential responses to the strategic risk of drone swarms. Although DOD strategy includes some ways to counter the threat of enemy drones, it does not fully confront the challenges that it must to solve the strategic problem posed by future armed drone swarms.[2] To mitigate this emerging risk, the United States requires a coordinated approach to tackling the technical, legal, and doctrinal issues.

Strategic Links

Current U.S. strategy documents provide overarching requirements for securing and advancing national interests. However, the emerging threats and underlying drone swarm technology threaten U.S. posture. For example, the 2017 National Security Strategy states, "We will maintain a forward military presence capable of deterring and, if necessary, defeating any adversary."[3] With the extensive commitment of U.S. military forces worldwide, adversaries could employ drone swarms to challenge U.S. interests in many areas; if so, the U.S. military could not credibly project power to deter and defeat these same adversaries.

Additionally, the National Defense Strategy acknowledges the changing character of warfare, with actors more rapidly and easily accessing technology, including artificial intelligence (AI), autonomy, and robotics.[4] Then–Secretary of Defense James Mattis illustrated the concern domestically in 2018 by acknowledging that the homeland is no longer a sanctuary and that we must anticipate attacks against "our critical defense, government, and economic infrastructure."[5] Drone swarms pose a significant national security strategic risk, and countering this emerging threat presents the United States with challenges and opportunities in three key areas: technology, law, and doctrine.

Setting the Stage: Emerging Trends

The literature on adversarial sUAS employment reveals the potential for innovative ways to change the character of warfare. The technological revolution enables actors to employ drones to achieve national objectives. The recent war over the contested region of Nagorno-Karabakh in the South Caucasus region illustrates this reality. Azerbaijan's employment of sUAS significantly aided its victory by supporting its air and ground campaign against Armenia, which had more conventional air and ground forces, including fighter aircraft and tanks.[6] Moreover, the war illustrated the advantage of using sUAS to destroy air defense systems, ground forces, and armored vehicles with relatively inexpensive air capabilities.[7] The systems can avoid enemy air defense systems by virtue of their relatively small sizes and slower speeds, and they offer less prosperous states potential military advantages in conventional conflicts.[8] This rebalance of power suggests that states may employ sUAS in future conflicts more often to coerce their enemies, enable diplomatic concessions, and achieve national security objectives. Remotely piloted aircraft are instruments that have changed the character of warfare, and innovative uses of small drones illustrate the evolutionary next step, with a low cost and a high reward potential.

Beyond the current application of sUAS, future development of these air vehicle trends toward greater sophistication, with advances in *AI*, *autonomy*, and *machine learning*. These terms may cause some to think of fictional works, such as *Angel Has Fallen* (2019), a movie in which small propeller-driven drones launch from ground-based tubes to attack the U.S. President and his Secret Service detail.[9] However, major military powers currently pursue this capability.

The China Academy of Electronics and Information Technology tested the launch and employment of multiple sUAS in swarm formations from both ground-based and airborne launchers in September 2020.[10] Additionally, the U.S. Navy's Office of Naval Research and the Defense Advanced Research Projects Agency have conducted extensive testing in recent years, using large numbers of drones in coordination with each other to perform reconnaissance, fly in formation, or potentially drop munitions on targets.[11] A September 2020 exercise revealed that Russia also continues to pursue integrated teaming with three models of sUAS to strike ground targets.[12] Although that is not drone swarming per se, a Russia expert notes, "At this point there is lots of research in Russia on the UAV [unmanned aerial vehicle] swarm use, and there is testing and evaluation of such concepts."[13]

Civilian development of drone swarms shows that this is a dual-use technology. Demand for drone capabilities has increased over the past few years, as companies have programmed hundreds and sometimes thousands of sUAS for choreographed displays. For example, Intel set the world record for the largest number of drones in one display, with 2,066 in 2018. Intel's specific model of drones flew in numerous events, including the 2018 Winter Olympics and the halftime show at the 2017 Super Bowl.[14] Recently, a drone show displayed swarm-like capabilities for President-Elect Joe Biden's Delaware victory celebration.[15] A nefarious actor might conceivably seize control of these existing masses of drones and wreak havoc on events involving heads of state or large crowds. Iran demonstrated unusual sophistication with a drone attack against one of Saudi Arabia's largest crude oil stabilization plants in September 2019 and is also experimenting with employing masses of drones against 50 targets simultaneously.[16] These trends in both military and civilian applications of drone swarms portend a future in which U.S. power can be challenged. Although actors have not yet employed true small drone swarms against adversaries, such an application of the technology may not be far off.[17]

Strategic Risks and Implications

States should plan to employ drone swarms after careful consideration of their risks and implications. Some literature acknowledges the conceptual application of drone swarms in certain strategic military contexts. For example, one strategy expert theorizes that armed fully autonomous drone swarms (AFADS), a subset of drone swarms, could be considered a weapon of mass destruction (WMD).[18] A U.S. Army wargame applied methodology to demonstrate how drone swarm weapons might provide operational advantages in parallel attack.[19] One of the originators of the DOD directives on the employment of autonomous systems states:

> *Deploying fully autonomous weapons would be a weighty risk, but it might be one that militaries decide is worth taking. Doing so would be entering uncharted waters. . . . Hostile actors are actively trying to undermine safe operations* [in wartime]. *And no humans would be present at the time of operation to intervene or correct problems.*[20]

China may be willing to assume this risk; it is developing autonomous weapons capable of making decisions independent of a human operator. Former Secretary of Defense Mark Esper noted this distinction between U.S. and Chinese approaches to autonomous weapons development.[21] Several commentors have asserted that AFADS offer military advantages, including the freedom to strike traditional air defenses covering strategic assets or to conduct surveillance against nuclear and supporting capabilities.[22]

States must consider the strategic implications of autonomous weapons programs. An actor's employment of a drone swarm against an adversary could result in an unintended escalation, and an unexpected AI decision could inadvertently result in an enemy's counterattack or a diplomatic crisis. International discussions have not addressed the strategic considerations in terms of "crisis stability, escalation control, and war termination" with the use of fully autonomous weapons.[23] Many experts agree that autonomous weapons systems may provide operational advantages during crises or armed conflicts, particularly in gray zone or hybrid warfare, but the strategic risks require policymakers to consider these dangers now to avert catastrophic results later. Fully autonomous weapons systems increase the risk of miscalculation and/or misinterpretation, which may result in uncontrolled escalation among both state and nonstate competitors. This includes an increased threat of the use of WMDs.[24] Despite the inherent risks and consequences of employing autonomous drone swarms, these capabilities present actors with military and strategic options to achieve national objectives. Partial autonomous drone swarm weapons with a human in the loop could present risks, albeit to a lesser degree, to adversaries as well.

Important Terms

Key terms and the scope of analysis will clarify misconceptions. Irving Lachow, writing in the *Bulletin of the Atomic Scientists*, defines *swarming drones* as "distributed collaborative systems . . . flocks of small unmanned aerial vehicles that can move and act as a group with only limited human intervention."[25] Another definition of swarming specifies the military application: "large numbers of dispersed individuals or small groups coordinating together and fighting as a coherent whole."[26] According to DOD Directive 3000.09, autonomous weapons systems, "once activated, can select and engage targets without further intervention by a human operator."[27] The National Academies of Sciences, Engineering, and Medicine specify drone swarms as 40 or more sUAS where the group acts as a unit with individual behaviors, all members do not know the mission, members communicate with one other, and each sUAS "will position itself relative to other sUAS."[28] These innovations include applications of AI, autonomy, and machine learning, along with advancements in sUAS, designated by DOD as groups 1, 2, and 3, that behave as a whole for missions including intelligence, surveillance, and reconnaissance and offensive attacks.[29] This threat will be referred to as drone swarms for the rest of this article.

Technical Feasibility

Countering drone swarms involves three areas of both challenge and opportunity for DOD and national agencies tasked to defend the homeland. For the first, technology, DOD's efforts focus on material solutions. In fiscal year (FY) 2021, DOD initially planned "to spend at least $404 million on counter-UAS (C-UAS) research and development and at least $83 million on C-UAS procurement."[30] All military Services pursue a variety of cutting-edge technology solutions to detect, track, identify, and defeat targets. Material solutions for detection include radar as well as electro-optical, infrared, and acoustic sensors; all are limited in their effectiveness by the surface area characteristics and relative speeds of small drones.[31] Another technique involves the detection of radio command signals that an operator might require to control the drone.[32] Defeat mechanisms include methods such as jamming, spoofing, guns, nets, directed energy, and standard air defense systems.[33] However, current capabilities present operators with mixed results and primarily target smaller numbers of drones that do not exhibit swarm behaviors.[34] Other methods, including high-powered microwaves (HPM), which the U.S. Air Force and DOD are testing in operational settings, may offer more effective capabilities against drone swarms, but proprietary challenges could limit their effectiveness.[35] Admittedly, DOD may be pursuing more advanced HPM weapons with smaller infrastructure footprints, such as the Leonidas system, but the present research is limited to unclassified sources.[36]

The DOD counter-sUAS (C-sUAS) strategy rightly acknowledges the changing character of warfare that drone swarms present but does not specifically address the technology risk.[37] Significant limitations of the current technology considering the near-future requirement to counter drone swarms present a challenge to the industry. Moreover, DOD may not be focused on the emerging threats of drone swarms. Rather, development and acquisition efforts indicate an emphasis on sensors and weapons to defeat current sUAS. The DOD FY 2021 budget for C-UAS is an indicator of the near-term financial costs of developing current equipment and may not account for technology innovation required to meet the future demand. If so, this approach may prove inefficient and cause significant risk in an environment of declining budgets for DOD during and after the COVID-19 pandemic. The speed at which states are developing drone swarm technology indicates a more rapid rate of maturation than that of the equipment to counter such threats.

Observers note the need for rapid innovation to mitigate rising threats, but the current defense industrial base faces barriers to change, including military culture and new commercial technology testing.[38] One of the more common problems with rapid innovation originates in the acquisition of commercial products, in which intellectual property becomes an impediment to system employment. This problem becomes acute when companies' equipment or software cannot necessarily interoperate, leaving the C-sUAS operator without the fused, timely, and useful information necessary to defeat a target.[39] Military culture does not necessarily reward innovative thinkers and can be a barrier to rapid change. Although DOD's current C-sUAS strategy identifies the threat of drone swarms, it does not adequately address how DOD must overcome the technology risks of high cost and sluggish innovation to counter them.

Lawful Acceptability

The second source of risk from the C-sUAS strategy originates in the seams found in the patchwork of legal constraints, particularly in the homeland.[40] The protections that current laws afford U.S. citizens in the homeland also inhibit DOD in its protective capabilities on military installations from drone threats. Drone swarms exacerbate the risk such constraints create, given the multiplying effects of their threat capabilities and the restrictions on detecting them. The C-sUAS strategy rightly asserts that key DOD stakeholders must collaborate with partners for success.[41] This imperative should drive legislative solutions to broaden authorities in the domestic environment in which this counter-drone equipment operates.

Staff Sergeant Noah Straman, assigned to Headquarters and Headquarters Company, 37th Infantry Brigade Combat Team, fires DroneDefender during Operation Northern Strike, at Camp Grayling, Michigan, August 14, 2022 (U.S. Army/Benhur Ayettey)

Marine Corps Corporal Chance Bellas, combat engineer with Littoral Engineer Reconnaissance Team, 9th Engineer Support Battalion, 3rd Marine Logistics Group, assembles small unmanned aircraft system VAPOR 55 during Balikatan 22, at Claveria, Philippines, March 30, 2022 (U.S. Marine Corps/Melanye Martinez)

The C-sUAS strategy correctly highlights the significant legal challenges of operating counter-drone capabilities in the homeland, asserting, "Many existing laws and federal regulations were not designed to address sUAS as threats, and the continued rate of technological change makes it difficult for the legal authorities to keep pace."[42] Current law does not allow for timely detection of potential drone threats, which may originate from outside a military installation. The Secretary of Defense and Armed Forces designees are authorized by 10 U.S. Code (USC) section 130i to take all kinetic or nonkinetic actions to "disable, damage, or destroy" an unmanned aircraft system that poses a threat to a "covered facility or asset."[43] This legal limitation prevents an operator from defeating a potential drone threat before it reaches the target.

Although 10 USC 130i authorizes DOD to "detect, identify, monitor, and track unmanned aircraft, without prior consent . . . by means of intercept or other access of a wire, oral, or electronic communication," it does not specify whether this authority extends beyond a base's boundary; if it did, it would provide a tactical advantage for the defender.[44] The new authorities are unclear also about whether DOD can collect the required information about drones outside its jurisdiction without violating intelligence oversight directives. Moreover, collecting such information against a potential drone swarm threat might amplify the liability. Detecting targets also requires distinguishing between hostile and friendly drones, and processing specific information related to legitimate civilian aircraft could be problematic given current authorities.

In accord with the C-sUAS strategy, DOD must act multilaterally and share threat information with law enforcement agencies, as permitted by 10 USC 130i.[45] One way in which this may be possible is during national security special events (NSSEs), when the Federal Bureau of Investigation (FBI) could have the temporary authority to counter drones without first obtaining warrants. The Preventing Emerging Threats Act of 2018 authorized both the Department of Homeland Security (DHS) and the Department of Justice (DOJ) "to mitigate the threat that unmanned aircraft . . . poses to the safety or security of facilities or assets, through a risk-based assessment."[46] In recent cases, the FBI worked with the Federal Aviation Administration (FAA) and successfully countered over 200 drones during FY 2020 at events including the 2020 Super

Bowl, the 2019 World Series, the 2020 Rose Bowl Game, Washington, DC's "A Capitol Fourth," and New York City's New Year's celebration.[47] The FBI also worked with DHS and state and local law enforcement in Georgia to confront 54 drone incursions during the 2019 Super Bowl; at least six were confiscated during the temporary flight restriction around the stadium.[48]

The language of the Preventing Emerging Threats Act of 2018 text closely resembles the authorities in 10 USC 130i, but it remains unclear how DHS, DOJ, and DOD could work together practically. First, the NSSEs are temporary, and the advantage of early warning of threats through coordination between the agencies would almost be negligible without permanent authorities. An adversary would likely not launch a drone swarm attack against DOD assets during a NSSE. Second, if DOD identified a threat outside its jurisdiction and warned DHS or DOJ, it is unlikely Federal, state, or local law enforcement would have the time and capabilities to interdict a drone swarm threat.

Local law enforcement and private entities have even fewer authorities to counter drones. According to a recent advisory from DHS, DOJ, the Department of Transportation, and the Federal Communications Commission, non-Federal public agencies and private persons who employ counter-drone technology could violate Federal laws. The law defines drones as aircraft, and any instrument to disrupt or destroy a drone could trigger liability involving the Aircraft Sabotage Act and the Aircraft Piracy Act.[49] Those who use radio frequency detection may be liable to lawsuits involving the Pen/Trap Statute (18 USC §§ 3121–3127) and the Wiretap Act (Title III, 18 USC §§ 2510 *et seq.*) depending on whether the capability records or intercepts electronic communications between the drone and controller.[50]

Finally, the collateral effects may cause local law enforcement or private entities to reconsider employing these capabilities. Jason Knight advanced an analysis of considerations for police agencies in urban areas and references examples in which counter-drone technology interferes with legitimate ground and air activities.[51] Current authorities do not provide the comprehensive legal foundation for the early warning capabilities that DOD requires to counter a drone swarm. Although multilateral coordination may provide defenders an advantage in certain situations with host nations or in contingency locations, the homeland provides adversaries with advantages in potential attempts to employ a drone swarm against critical infrastructure, given DOD's legal limitations.

Doctrinal Suitability

The final impediment to the C-sUAS strategy stems from an important but overlooked facet about effective employment of counter-drone equipment. The strategy correctly asserts the need for doctrine to be developed as technology matures, but simply acknowledging enterprise needs does not address the significant challenge of planning for *who* might operate the equipment.[52] Identifying doctrinal needs now will mitigate capability gaps in the future. The U.S. Army must assume a greater role in defending air bases from the drone swarm threats of the future.

One of the unique aspects of employing counter-drone capabilities is that it includes operating in all domains. Specifically, the immense challenge of targeting and mitigating adversaries in the air requires a clear-eyed assessment of division of labor among the three primary mission areas: air defense, force protection, and airspace control. Extracting principles of employment from these mission areas should be valuable for planning strategic uses of counter-drone capabilities. Joint doctrine is based on current force structures and responsibilities for helping solve complex problems.[53] Planning for ways to counter drone swarms requires a deeper assessment of the roles and responsibilities in joint doctrine.

Doctrine must account for training the operators of future equipment that will function in all domains. Operating in the air domain requires personnel who are fully knowledgeable and proficient in air defense, force protection, and airspace control. Designing and resourcing a force structure that evolves in tandem with technology and equipment will more efficiently deter and counter advanced threats. This development will then drive authoritative guidance for counter-drone-swarm doctrine and is part of the Joint C-sUAS Office (JCO)'s responsibility as DOD's executive agent.[54] Additionally, the JCO will "coordinate development of joint operational concepts and joint doctrine for C-sUAS" and leave to the individual Services responsibilities in the other domains.[55] However, this description of responsibilities fails to account for the current challenges of roles among DOD's Service departments in airspace control, force protection, and air defense against the drone swarm threat. A force protection military professional focused on countering ground threats does not have the requisite knowledge to counter air threats while avoiding friendly aircraft. Training these personnel in the relevant characteristics of the airspace environment, electromagnetic spectrum, space operations, and weather will yield more effective employment of capabilities against drone swarms. Overlapping shared responsibilities in air defense, particularly between the U.S. Army and U.S. Air Force, can solve this doctrinal challenge. However, the Services have relied on force protection specialists instead—which presents risks to the enterprise.

Doctrinal discussions also include debates on roles and missions, especially in the air defense of air bases. The wars in Vietnam and Iraq forced senior military commanders and the Services to allocate capabilities to traditional missions at the expense of defense of air bases supporting strategic and operational objectives.[56] The Army and Air Force especially have wrestled over specific roles in area and point air defense missions since the end of World War II. A 2020 RAND study highlighted the current debate:

> *Today, the U.S. Army is responsible for providing point AMD* [air and missile defense] *for Air Force bases and other fixed facilities, but years of neglect from both services have resulted in capability and capacity shortfalls. . . . Army leadership has*

understandably prioritized mobile short-range air defense for its maneuver units over fixed facility defenses.[57]

Until the Army adequately prioritizes resources for the air defense of main operating air bases both at overseas locations and in the homeland, strategic and operational objectives are susceptible to increased risk of exploitation by drone swarms. Additionally, the Air Force will likely continue to advocate and acquire C-sUAS capabilities absent doctrinal resolution. The Air Force may achieve its longstanding desire to assume a greater lead in tactical air defense—which would contradict the JCO's mandate to avoid duplication of effort and gain efficiency.[58] Similarly, the other Services will likely continue acquiring equipment and experimenting, which may not be optimal or effective without cross-domain and functional coordination.

The RAND report also details the misalignment of Army and Air Force roles in air defense. Of note, the table fails to show that commander, Navy Installations Command, employs master-at-arms personnel for shore-based C-sUAS capabilities, indicating misalignment of force structure and prioritization compared with air defense when afloat. A 2020 congressional research report poses an important question in the context of this debate: "Are planned SHORAD [short-range air defense] force structure and capabilities adequate to meet predicted future challenges?"[59] The report suggests that the Army's plans for 18 more battalions of air defense capabilities divided between Active and Reserve components may be inadequate for the needs of Army forces supporting both the European Deterrence Initiative and the Pacific Deterrence Initiative.[60] These capabilities include countering the sUAS threat but do not include the assumed mandate to defend critical Air Force assets and main operating bases. Although Joint Publication 3-0, *Operations*, calls for integrating offensive and defensive capabilities to achieve air superiority and force protection against enemy unmanned aircraft, it does not specify roles and missions to the Services.[61] This doctrinal ambiguity increases the danger of under-resourcing the SHORAD enterprise to counter the multiplying effects of future drone swarms.

The emerging development of technology and increased likelihood of actors employing drone swarms necessitates a reevaluation of doctrine and Service roles. In fact, the Air Force Chief of Staff has urged the Office of the Secretary of Defense to direct a review of roles and missions among the Services to determine lead organizations for joint warfighting concepts such as long-range precision fires and logistics under attack.[62] Both of these concepts are relevant to the protection of strategic assets from potential drone swarm attacks. Furthermore, DOD's lack of doctrinal guidance may also indicate a need to assess interagency concepts and methods to employ similar capabilities in civilian jurisdictions. The JCO and its DOD strategy will provide essential elements for continued doctrinal development, but more work must focus on aligning Services' roles and resources.

Recommendations

A new DOD approach to counter drone swarms must address the risks of rapid technology development, the legal seams adversaries could exploit between civilian and DOD protection of critical infrastructure, and the doctrinal challenges inherent in air defense, airspace control, and force protection. As the 2018 National Defense Strategy noted, the homeland is no longer a sanctuary and remains a target from enemy drone swarms, potentially with intercontinental range capabilities.[63]

Adversarial trends must drive the defense industrial base to relatively low-cost, rapid, and AI-enabled technical solutions. The Third Offset Strategy, which originally sought to incorporate future technologies, offers a particularly useful approach for mitigating this risk. This strategy explored ways in which swarming drones, hypersonic weapons, AI, and human-machine teaming could best combine to offer distinct advantages in combat, but it did not solely focus on material and equipment.[64] Rather, it considered how best to integrate human creativity with technological precision. When applied to countering drone swarms, human-machine teaming concepts can provide an advantage in the air defense enterprise. A solution should include a range of sensors fully integrated with AI software to identify potential targets more rapidly and with a greater confidence level. U.S. Army TRADOC Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028*, identifies these characteristics as desirable for AI and high-speed data processing

Table. Examples of Well-Aligned and Not Well-Aligned Service Responsibilities for Air Defense

	Example 1: Fleet Air Defense Afloat		Example 2: Ground-Based Air Defense of Air Force Bases	
	Navy	Marine Corps	Army	Air Force
Service assigned responsibility?	Yes	Shared with Navy when afloat	Yes	No
Service with greatest stakes?	Yes	Shared with Navy when afloat	No	Yes
Service priority?	Yes	No	No	Growing
Dedicated force structure?	Yes	When afloat	No	No
	Well-aligned		Not well-aligned	

Source: Alan J. Vick et al., *Air Base Defense: Rethinking Army and Air Force Roles and Functions* (Santa Monica, CA: RAND, 2020), 99, available at <https:doi.org/10.7249/rr4368>.

Marine Corps Lance Corporal Dmitri Shepherd launches drone while conducting infantry platoon battle course during Bougainville II, Pohakuloa Training Area, Hawaii, October 14, 2021 (U.S. Marine Corps/Brandon Aultman)

to improve "human decision making in both speed and accuracy."[65]

Worthy investments in this human-machine technology could include AI-enabled autonomous swarm drones to mitigate or destroy enemy swarms through dogfighting. Georgia Tech University conducted this kind of experiment in collaboration with the Naval Postgraduate School in 2017.[66] Additionally, DOD's low-cost-per-shot developmental capabilities include nonkinetic, direct energy weapons such as the tactical high-power microwave operational responder (THOR) and hybrid defense of restricted airspace (HyDRA) programs.[67] THOR presents a particularly effective capability to counter drone swarms because of its larger cone of influence compared with a HyDRA laser. However, when deployed in tandem and coordinated with an integrated command and control (C2) interface that teams AI with a human in the loop, the system could prove more effective at a lower cost than standard air defense capabilities.

C2 capabilities must enable faster targeting, connect sensors to defeat mechanisms, and allow the human operator to select more effective weapons rapidly. Recent reporting suggests the JCO is pursuing these capabilities and may require each of the Services to develop its own C2 systems for eventual integration into the U.S. Army's Forward Area Air Defense Command and Control system.[68] Other C2 systems include the U.S. Navy's CORIAN (Counter-Remote Control Model Aircraft Integrated Air Defense Network) capability and the U.S. Air Force's Multi-Environmental Domain Unmanned Systems Application Command and Control.[69] However, these specific systems do not appear to tie in to the Advanced Battle Management System or proposed Joint All-Domain Command and Control (JADC2) architecture at this time. Recent and nascent efforts demonstrate an initiative to tie sensors to shooters to counter drone swarms using the JADC2 concept in the North Atlantic Treaty Organization.[70] The future JADC2 architecture could conceptually enable a human operator to take command of an enemy drone swarm network for his or her own purpose.[71] Regardless of the innovation, the Third Offset Strategy offers a potentially valuable approach to the problem of countering future lethal autonomous drone swarms.

Pursuing disparate and Service-specific C2 capabilities without considering the future drone swarm threat or AI development activities would waste time and taxpayer funds. Instead, DOD should integrate the

Naval Aircrewman (Helicopter) 2nd Class Daniel Ayres, assigned to Helicopter Sea Combat Squadron 21, fires GAU-21 .50 caliber machine gun in MH-60S Seahawk at target drone during live-fire exercise with amphibious assault ship USS Essex, Pacific Ocean, April 18, 2021 (U.S. Navy/Sang Kim)

counter-drone-swarm C2 capabilities that it has already developed for FY 2021 into the JADC2 architecture more quickly.[72] Congress tasked the Secretary of Defense to assess integrated air and missile defense C2 systems, which include C-UAS capabilities, and to determine whether they are compatible with the emerging JADC2 architecture.[73] This framework meets the congressional preference for autonomous or semiautonomous capabilities with low operating and sustainment costs.[74] Although interoperability, intellectual property, data management, and information assurance remain challenges, integrating C-sUAS C2 systems into the JADC2 architecture will yield faster kill chains and potentially less costly programs. JCO director Major General Sean Gainey recently acknowledged this open architecture approach as one that might pay significant security dividends later.[75]

Second, working within the existing legal framework in the homeland, DOD must advocate for more authorities at fixed sites to defend critical infrastructure. Congress must grant increased powers to the Secretary of Defense both during contingencies and in peacetime. The proposal must include the authority for operators to identify potential targets outside a base's boundary. An operator should also have the legal support to warn local and Federal law enforcement agencies in near real time.

Fortunately, the FAA is pursuing several initiatives to counter enemy drones. These plans include incorporating drones into the national airspace system to distinguish between friendly and enemy drones.[76] DOD should actively encourage both the FAA and the National Aeronautics and Space Administration to continue their respective drone industry initiatives, including the Unmanned Aircraft System Traffic Management study, in order to "identify services, roles and responsibilities, information architecture, data exchange protocols, software functions, infrastructure, and performance requirements for enabling the management of low-altitude uncontrolled drone operations."[77] These increased authorities, combined with enhanced capabilities, could close the legal gap between civilian and military jurisdictions to protect both national infrastructure and critical DOD assets.

Finally, DOD must aggressively hone doctrine through wargaming and exercises to determine the most appropriate roles and functions in the air base air defense enterprise. As drone technology matures and presents friendly forces with more complex problems, establishing the right force structure early will more effectively meet the challenge. This will allow the required training and appropriate resourcing to meet congressional demand for effective and low-cost equipment. As the RAND study noted, no single course of action but, rather, a combination provides the solution. A realignment of roles and functions, however, is essential to success.[78] The pursuit of appropriate joint doctrine will provide the foundation for a strong and risk-based model to counter drone swarms in the future and avoid the strategic mistakes of the past. JFQ

Notes

[1] U.S. Army Training and Doctrine Command (TRADOC) Pamphlet 525-3-1, *The U.S. Army Operating Concept: Win in a Complex World* (Fort Eustis, VA: TRADOC, October 31, 2014), iii, available at <https://info.publicintelligence.net/USArmy-WinComplexWorld.pdf>.

[2] "Pentagon's Counter Small Drone Strategy," *USNI News*, January 8, 2021, available at <https://news.usni.org/2021/01/08/pentagons-counter-small-drone-strategy>.

[3] *National Security Strategy of the United States of America* (Washington, DC: The White House, December 2017), 47, available at <https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>.

[4] *Summary of the National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Washington, DC: Department of Defense, 2018), 3, available at <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.

[5] Ibid., 3.

[6] Peter Vincent Pry, "Armenia's 'Pearl Harbor' Will Be a Case Study in Technological Surprise," *Washington Times*, November 18, 2020, available at <https://www.washingtontimes.com/news/2020/nov/18/armenias-pearl-harbor-will-be-a-case-study-in-tech/?utm_source=RSS_Feed&utm_medium=RSS>.

[7] Robyn Dixon, "Azerbaijan's Drones Owned the Battlefield in Nagorno-Karabakh—and Showed Future of Warfare," *Washington Post*, November 11, 2020, available at <https://www-washingtonpost-com.cdn.ampproject.org/c/s/www.washingtonpost.com/world/europe/nagorno-karabkah-drones-azerbaijan-aremenia/2020/11/11/441bcbd2-193d-11eb-8bda-814ca56e138b_story.html?outputType=amp>.

[8] Ibid.

[9] *Angel Has Fallen*, directed by Ric Roman Waugh (Santa Monica, CA: Lionsgate, August 23, 2019).

[10] Joseph Trevithick, "China Conducts Test of Massive Suicide Drone Swarm Launched from a Box on a Truck," *The Warzone*, October 14, 2020, available at <https://www.thedrive.com/the-war-zone/37062/china-conducts-test-of-massive-suicide-drone-swarm-launched-from-a-box-on-a-truck>.

[11] Michael Safi, "Are Drone Swarms the Future of Aerial Warfare?" *The Guardian*, December 4, 2019, available at <https://www.theguardian.com/news/2019/dec/04/are-drone-swarms-the-future-of-aerial-warfare>; Thomas McMullan, "How Swarming Drones Will Change Warfare," BBC News, March 16, 2019, available at <https://www.bbc.com/news/technology-47555588>; Trevithick, "China Conducts Test of Massive Suicide Drone Swarm."

[12] "Swarms of Drones Used in Kavkaz-2020 Exercise First Time Against Enemy Forces," TASS, September 24, 2020, available at <https://tass.com/defense/1204513>.

[13] David Hambling, "Russia Uses 'Swarm of Drones' in Military Exercise for the First Time," *Forbes*, September 24, 2020, available at <https://www.forbes.com/sites/davidhambling/2020/09/24/russia-uses-swarm-of-drones-in-military-exercise-for-the-first-time/?sh=2b5364f47712>.

[14] Andrew Tarantola, "The Drones That Announced Joe Biden as the 46th President-Elect," *Engadget*, available at <https://www.engadget.com/the-drones-that-announced-joe-biden-as-the-46th-president-elect-150014496.html>.

[15] Ibid.

[16] Michael Rubin, *A Short History of the Iranian Drone Program* (Washington, DC: American Enterprise Institute, August 26, 2020), 9, available at <https://www.aei.org/research-products/report/a-short-history-of-the-iranian-drone-program/>.

[17] Masses of drones are different from drone swarms. This project focuses on the definition of drone swarms in the important terms sections of the *Bulletin of the Atomic Scientists* (2017) and in Travis Kneen, *Defining Unmanned Aerial Systems (UAS) Swarms*, DSIAC-2020-1208 (Belcamp, MD: Defense Systems Information Analysis Center, August 2019), available at <https://www.dsiac.org/wp-content/uploads/2020/05/dsiac-2191004.pdf>, to account for the distinguishing characteristics. Generally, trends in drone swarm technology suggest that state actors will more likely employ drone swarms against their adversaries on the basis of more technically advanced algorithms.

[18] Zachary Kallenborn, *Are Drone Swarms Weapons of Mass Destruction?* Future Warfare Series No. 60 (Maxwell Air Force Base, AL: U.S. Air Force Center for Strategic Deterrence Studies, May 6, 2020), 27, available at <https://permanent.fdlp.gov/gpo139494/MONO60%20Drone%20Swarms%20as%20WMD.pdf>.

[19] Sean M. Williams, *Swarm Weapons: Demonstrating a Swarm Intelligent Algorithm for Parallel Attack* (Fort Leavenworth, KS: School of Advanced Military Studies, 2018), 22–23, available at <https://apps.dtic.mil/sti/citations/AD1071535>.

[20] Paul Scharre, *Army of None: Autonomous Weapons and the Future of War* (New York: W.W. Norton and Co., 2018), 194–195.

[21] Joe Gould, "AI's Dogfight Triumph a Step Toward Human-Machine Teaming," *Defense News*, September 10, 2020, available at <https://www.defensenews.com/congress/2020/09/10/ais-dogfight-triumph-a-step-toward-human-machine-teaming/>.

[22] James Johnson, "Artificial Intelligence, Drone Swarming and Escalation Risks in Future Warfare," *The RUSI Journal* 165, no. 2 (2020), 1, 5, available at <https://doi.org/10.1080/03071847.2020.1752026>.

[23] Scharre, *Army of None*, 351.

[24] Burgess Laird, "The Risks of Autonomous Weapons Systems for Crisis Stability and Conflict Escalation in Future U.S.-Russia Confrontations," *The RAND Blog*, June 3, 2020, available at <https://www.rand.org/blog/2020/06/the-risks-of-autonomous-weapons-systems-for-crisis.html>.

[25] Irving Lachow, "The Upside and Downside of Swarming Drones," *Bulletin of the Atomic Scientists* 73, no. 2 (2017), 96, available at <https://doi.org/10.1080/00963402.2017.1290879>.

[26] Paul Scharre, *Robotics on the Battlefield Part II: The Coming Swarm* (Washington, DC: Center for a New American Security, 2014), 26, available at <https://www.cnas.org/publications/reports/robotics-on-the-battlefield-part-ii-the-coming-swarm>.

[27] Department of Defense (DOD) Directive 3000.09, *Autonomy in Weapon Systems* (Washington, DC: DOD, November 21, 2012, Incorporating Change 1, May 8, 2017), 13, available at <https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf>.

[28] Kneen, *Defining Unmanned Aerial Systems (UAS) Swarms.*

[29] *Counter–Small Unmanned Aircraft Systems Strategy* (Washington, DC: DOD, January 2021), 26, 29, available at <https://media.defense.gov/2021/jan/07/2002561080/-1/-1/1/department-of-defense-counter-small-unmanned-aircraft-systems-strategy.pdf>.

[30] John R. Hoehn and Kelley M. Sayler, "Department of Defense Counter-Unmanned Aircraft Systems," IF11426, Congressional Research Service, Updated January 11, 2021, 1, available at <https://crsreports.congress.gov/product/pdf/IF/IF11426/9>.

[31] Ibid.

[32] Ibid.

[33] Ibid.

[34] Author experience as Division Chief of Air Operations at Security Forces Center and Commander of Security Forces Squadron, January 2017–June 2020; Jason Knight, "Countering Unmanned Aircraft Systems" (master's thesis, Naval Postgraduate School, 2019), 54–59, available at <https://calhoun.nps.edu/handle/10945/63997>.

[35] Jared Keller, "The Air Force Has Deployed Its Drone-Killing Microwave Weapon to Africa," *Task and Purpose*, December 18,

2020, available at <https://taskandpurpose.com/military-tech/air-force-microwave-weapon-africa/>.

[36] "Counter Electronics: Swarm Defeat," *Epirus*, available at <https://www.epirusinc.com/solutions/counter-uas>.

[37] *Counter–Small Unmanned Aircraft Systems Strategy*, 6.

[38] David McCormick and James Cunningham, "America's Military Needs an Innovation Overhaul," *Fast Company*, December 8, 2020, available at <https://www.fastcompany.com/90580251/americas-military-needs-an-innovation-overhaul?fbclid=IwAR1Clu2FFDthFUlnP4Kbv4T34Y4gi0SUnxGaF67cTFPoezrhU2F1MdagXNg>; Elizabeth Vaughan Moyer, "Wanted: Innovation Tools for Air Force Leaders," *War Room*, December 3, 2020, available at <https://warroom.armywarcollege.edu/articles/innovation-tools/>.

[39] Author, personal experience; Eric Lofgren, "Contract Challenges for Modular Open Systems," *Acquisition Talk*, May 16, 2020, available at <https://acquisitiontalk.com/2020/05/contract-challenges-for-modular-open-systems/>.

[40] *Counter–Small Unmanned Aircraft Systems Strategy*, 8–9.

[41] Ibid., 4–5.

[42] Ibid., 8–9.

[43] "Protection of Certain Facilities and Assets from Unmanned Aircraft," 10 U.S. Code § 130i (2016).

[44] Ibid.

[45] *Counter–Small Unmanned Aircraft Systems Strategy*, 16.

[46] *Preventing Emerging Threats Act of 2018*, S. 2836, 115th Cong., 2nd sess. (2018), available at <https://www.congress.gov/bill/115th-congress/senate-bill/2836>.

[47] "Department of Justice Forecasts an Increase in Counter Unmanned Aerial Systems (C-UAS) Protection Activities and Criminal Enforcement Actions," Department of Justice, October 13, 2020, available at <https://www.justice.gov/opa/pr/department-justice-forecasts-increase-counter-unmanned-aerial-systems-c-uas-protection>.

[48] Anna Giaritelli, "Super Bowl Saw 54 Drone Incursions: Homeland Security," *Washington Examiner*, April 10, 2019, available at <https://www.washingtonexaminer.com/news/super-bowl-saw-54-drone-incursions-homeland-security>; Sean O'Kane, "Drones Are Already Being Confiscated Near the Super Bowl," *The Verge*, February 1, 2019, available at <https://www.theverge.com/2019/2/1/18207081/super-bowl-2019-drones-atlanta-fbi>.

[49] "Advisory on the Application of Federal Laws to the Acquisition and Use of Technology to Detect and Mitigate Unmanned Aircraft Systems," Department of Homeland Security, Department of Justice, Department of Transportation, Federal Communications Commission, August 2020, 6, available at <https://www.dhs.gov/publication/interagency-legal-advisory-uas-detection-and-mitigation-technologies>.

[50] Ibid., 2–3.

[51] Knight, "Countering Unmanned Aircraft Systems," 60–61.

[52] *Counter–Small Unmanned Aircraft Systems Strategy*, 4.

[53] Joint Publication (JP) 1, *Doctrine for the Armed Forces of the United States* (Washington, DC: The Joint Staff, March 25, 2013, Incorporating Change 1, July 12, 2017), VI-3, available at <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1_ch1.pdf>.

[54] *Counter–Small Unmanned Aircraft Systems Strategy*; DOD Directive 3800.01, *DOD Executive Agent for Counter Small Unmanned Aircraft Systems for Unmanned Aircraft Groups 1, 2, and 3* (Washington, DC: DOD, February 21, 2020), 10.

[55] *Counter–Small Unmanned Aircraft Systems Strategy*, 28.

[56] Alan J. Vick et al., *Air Base Defense: Rethinking Army and Air Force Roles and Functions* (Santa Monica, CA: RAND, 2020), 65, 91, available at <https:doi.org/10.7249/rr4368>.

[57] Ibid., 97.

[58] *Counter–Small Unmanned Aircraft Systems Strategy.*

[59] Andrew Feickert, *U.S. Army Short-Range Air Defense Force Structure and Selected Programs: Background and Issues for Congress*, R46463 (Washington, DC: Congressional Research Service, July 23, 2020), 24, available at <https://fas.org/sgp/crs/weapons/R46463.pdf>.

[60] Ibid., 25.

[61] JP 3-0, *Operations* (Washington, DC: The Joint Staff, January 17, 2017, Incorporating Change 1, October 22, 2018), III-30.

[62] Theresa Hitchens, "Roles & Missions Scrub Needed for All Domain Ops: CSAF Brown," *Breaking Defense*, February 23, 2021, available at <https://breakingdefense.com/2021/02/roles-missions-scrub-needed-for-all-domain-ops-csaf-brown/amp/>.

[63] T.X. Hammes, "The Future of Warfare: Small, Many, Smart vs. Few and Exquisite?" *War on the Rocks*, July 16, 2014, available at <https://warontherocks.com/2014/07/the-future-of-warfare-small-many-smart-vs-few-exquisite/>.

[64] Theodore R. Johnson, "Will the Department of Defense Invest in People or Technology?" *The Atlantic*, November 29, 2016, available at <https://www.theatlantic.com/politics/archive/2016/11/trump-military-third-offset-strategy/508964/>.

[65] TRADOC Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028* (Fort Eustis, VA: TRADOC, December 6, 2018), 20, available at <https://adminpubs.tradoc.army.mil/pamphlets/TP525-3-1.pdf>.

[66] John Toon, "A Swarm First: Dogfighting," *Georgia Tech Research Horizons*, no. 1 (2017), available at <https://rh.gatech.edu/front-office/swarm-first-dogfighting>; See also Paul Scharre, "Counter-Swarm: A Guide to Defeating Robotic Swarms," *War on the Rocks*, March 31, 2015, available at <https://warontherocks.com/2015/03/counter-swarm-a-guide-to-defeating-robotic-swarms/>.

[67] Leslie F. Hauck III and John P. Geis II, "Air Mines: Countering the Drone Threat to Aircraft," *Air & Space Power Journal* (Spring 2017), 32, available at <www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-31_Issue-1/V-Hauck_Geis.pdf>; Keller, "The Air Force Has Deployed Its Drone-Killing Microwave Weapon to Africa."

[68] Sean A. Gainey, Nicole M. Thomas, and Tom Karako, "A New Strategy for Countering Small Unmanned Aerial Systems," transcript, Center for Strategic and International Studies, January 8, 2021, 7–8, available at <https://www.csis.org/analysis/online-event-new-strategy-countering-small-unmanned-aerial-systems>.

[69] Thomas Brading, "Army Selects Countermeasures Against Drones," Army News Service, June 29, 2020, available at <https://www.army.mil/article/236839/army_selects_countermeasures_against_drones>.

[70] Kris Osborn, "JADC2: NATO's Answer to the Threat of Drone Swarm Attacks," *The National Interest*, November 29, 2021, available at <https://nationalinterest.org/blog/reboot/jadc2-natos-answer-threat-drone-swarm-attacks-197128>.

[71] Scharre, "Counter-Swarm."

[72] John R. Hoehn, "Joint All-Domain Command and Control (JADC2)," IF11493, Congressional Research Service, December 9, 2020, 2, available at <https://crsreports.congress.gov/product/pdf/IF/IF11493/12>.

[73] *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021*, HR 6395 (2020), 116th Cong., 2nd sess. (2020), 58, available at <https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf>.

[74] Jen Judson, "Congress Hits Fast-Forward to Field New Capability to Counter Drones," *Defense News*, December 4, 2020, available at <https://www.defensenews.com/pentagon/2020/12/04/congress-hits-fast-forward-to-field-new-capability-to-counter-drone-threats/>.

[75] Gainey, Thomas, and Karako, "A New Strategy for Countering Small Unmanned Aerial Systems," 7.

[76] "U.S. Department of Transportation Issues Two Much-Anticipated Drone Rules to Advance Safety and Innovation in the United States," Federal Aviation Administration, December 28, 2020, available at <https://www.faa.gov/news/press_releases/news_story.cfm?newsId=25541>.

[77] "Unmanned Aircraft System Traffic Management (UTM)," Federal Aviation Administration, available at <https://www.faa.gov/uas/research_development/traffic_management/>.

[78] Vick et al., *Air Base Defense*, 108.