The Ghost-X Unmanned Aircraft System awaits takeoff during experimentation at Project Convergence-Capstone 4, 11 March 2024 at Fort Irwin, California. Robots like the Small Multipurpose Equipment Transport ground robot (*in the background*) and the Ghost-X Unmanned Aircraft System are part of human-machine integration in simulated operations; this portion of the experimentation involved soldiers from across the U.S. Army including Fort Moore, Georgia, and Fort Liberty, North Carolina. (Photo by Sgt. Charlie Duke, U.S. Army)

Cunning Tools of War

Moving Beyond a Technology-Driven Understanding of sUAS Infiltration

Maj. Nathaniel Martins, U.S. Army

Small unmanned aircraft systems (sUAS) are shaping modern warfare. The capability of sUASs to bypass air defenses to provide targeting data, deliver munitions, and perform reconnaissance are their defining features in conflict across the world. Initially a convenient tool for situational awareness, sUASs now provide belligerents immense value through *infiltration*, which the U.S. Army's field manual on tactics (Field Manual 3-90, *Tactics*) defines as the "undetected movement through or into an area occupied by enemy forces."[1] Such infiltration by sUAS is an equalizer that has eroded the concept of air superiority by forcing all belligerents to defend against airborne threats even if one side of the conflict still controls the airspace above ten thousand feet. The area below this altitude, referred to as the *air littoral*, is now a contested space accessible to almost anyone.[2] Yet, sUASs do not fly with impunity—efforts to interdict or mitigate sUAS missions by the United States, Russia, Ukraine, and others have turned the air littoral into a back-and-forth struggle of adaptation to employ sUASs and their countermeasures.

The United States is investing in both sides of this struggle, and military leaders such as Lt. Gen. Sean Gainey, commander of U.S. Army Space and Missile Defense Command, have emphasized the need to generate advanced technical capabilities to maintain an edge in the battle between sUAS infiltration and counter-UAS (C-UAS).[3] Yet history shows us that success in warfare requires more than a technical edge, and C-UAS is more than a material problem. Success in the air littoral also requires an effective doctrine of employment. This idea echoes in the U.S. Department of Defense's strategy document for C-sUASs.[4] More fundamentally, success on both sides of this struggle requires a deep understanding of the causal logic of successful sUAS infiltration at the tactical level. Although technical mismatches play an important role in most sUAS infiltrations, close inspection of sUAS use in Ukraine, the Middle East, and the southern border of the United States reveals that these aircraft exploit other tactical means. Put simply, successful sUAS infiltration is far more than a technological battle—it is a *tactical art*. Moreover, if properly employed, this tactical art provides opportunities to produce effects in areas otherwise inaccessible or even denied to military operations. Likewise, C-sUAS efforts must acknowledge and respond to this tactical art.

Women's Auxiliary Air Force radar operator Denise Miley plots aircraft on the cathode ray tube of an RF7 receiver in the Receiver Room at Bawdsey Chain Home (CH) in England, circa 1945. Her right hand has selected the direction or height finding and her left hand is ready to register the goniometer setting to the calculator. RAF Bawdsey was originally an experimental system set up at Bawdsey Manor, home of Robert Watson-Watt's radar development team. When the team was moved away from Bawdsey, the radar station became a part of the operational CH network. (Photo courtesy of the Imperial War Museums)

Technology, Tactics, and Causal Logic

History indicates that technology requires an effective concept of employment to deliver success in battle. One particularly fitting example is the use of radar during World War II. Although both Germany and the Allies developed technically advanced radar systems, the British understood the "new logic of technological change" for air defense.[5] The speed of modern aircraft meant that defenders needed an early and accurate report of incoming air raids to enable effective preparation. This required linking radar systems together and fusing this information with other intelligence. To execute this concept, the British centralized all detection systems into a single station that could build a common intelligence picture and relay it to the fighter

Table. Tactical Logic of sUAS Infiltrations

Tactical Logic 1 (Physical): *Operate beyond the responsive capabilities of the adversary (physical and/or technical)*	Tactical Logic 2 (Cognitive): *Use uncertainty and dilemmas to impede an adversary's effective response*
Tactic 1.1: Use technical advantages to *create* gaps in the adversary's C-UAS cycle. Tactic 1.2: Use *intelligence* to find gaps in the adversary's C-UAS cycle. Tactic 1.3: Instead of precise intelligence, employ large numbers of expendable sUAS to locate gaps in the adversary's defenses.	Tactic 2.1: Make it difficult for the adversary to separate friend from foe. This includes manipulation of the adversary's rules of engagement. Tactic 2.2: Compress time available for the adversary to analyze the threat and respond. Tactic 2.3: Use mass to divide the adversary's resources and force decisions on which sUAS to interdict.

(Table by author)

command during the Battle of Britain. Simply put, the British understood that the tactical logic of air defense was combining sensors to enable advanced warning. In contrast, the Germans used their radar systems as extensions of preexisting human observer corps that remained relatively independent of each other. Ultimately, the German approach proved less effective despite leveraging highly advanced radar systems.[6]

So what is the tactical logic of sUAS infiltrations? This article presents evidence of two distinct but complementary logics that are summarized in the table. The first and most obvious logic is *operating beyond the responsive capabilities of the adversary* (Tactical Logic 1). The concept of infiltration does not rely on forcible entry. Instead, sUAS infiltration must frustrate or avoid altogether an opponent's ability to execute countermeasures. Avoiding detection is not a requirement per se, but the logic requires "the infiltrating force to *avoid* detection and engagement" or at least reduce exposure.[7] sUAS infiltration may succeed by taking advantage of gaps in any part of the C-UAS cycle that includes several steps: (1) detecting an airborne object, (2) identifying its relevant characteristics, (3) classifying it as a threat, (4) prioritizing a response, (5) deciding on an engagement method, (6) engaging the sUAS, and (7) exploiting information from the event to improve further efforts.[8]

Technical advantages provide just one option to operate outside of the capabilities inherent to this cycle (Tactic 1.1). Another way is to find gaps in C-sUAS system coverage that result from any variety of battlefield choices by the adversary. A technical advantage may permit an aircraft to fly through the expected coverage of a C-sUAS system undetected, but the latter approach might locate an area of dead space to fly around the coverage. Locating and exploiting these gaps is essentially a function of *intelligence* (Tactic 1.2). Additionally, sUAS infiltration can simply use mass in the form of large numbers of sUASs to find these vulnerabilities by attrition rather than precise intelligence (Tactic 1.3). Each case study of sUAS infiltration will show that although a technical edge provides one means to satisfy the first logic of sUAS infiltration, the other methods are very much in play.

The second logic of sUAS infiltration is *using uncertainty and dilemmas to impede an effective response by the adversary* (Tactical Logic 2). Whereas the first is essentially physical, this second logic occurs primarily in the cognitive domain. This is a far more subtle approach that relies on the fact that detection and identification technology rarely provide certainty, and effective use of the airspace by the adversary often requires C-sUAS concessions and trade-offs with other tactical interests. By leveraging these cognitive seams, sUAS infiltrations effectively burden the human

Maj. Nathaniel Martins, U.S. Army, is a Special Forces officer assigned to 5th Special Forces Group with operational experience in the U.S. Central Command area of responsibility. In addition to professional exposure to small unmanned aircraft systems as part of his current assignment, his thesis work at the Naval Postgraduate School included analysis on the tactical employment of low, slow, and small aircraft.

Small consumer drones have proved versatile tools for Ukraine. (Photo courtesy of the Dnipropetrovsk Territorial Defense Brigade)

decision-maker in war. Although this approach may not be deliberate in every case, it often plays a key role in success.

Subsequent examples from across the world show three general techniques for exploiting this tactical logic. The first method uses the tactical situation to make it difficult for the adversary to separate friend from foe (Tactic 2.1). sUAS infiltrations may accomplish this by either making their identity ambiguous or by flying in ways that make it difficult for the adversary to engage without damaging its own aircraft or resources. The second method is simply to compress reaction time. This creates cognitive stress during decision-making and physically limits the responses available (Tactic 2.2). The final method is using mass employment to force difficult decisions on how to prioritize assets (Tactic 2.3). Mass plays an important role in both the physical and cognitive logic of sUAS infiltration.

Short-Range sUAS Infiltration in Ukraine

The battles fought in Ukraine are undoubtably the most developed examples of sUAS infiltration to date. Since the invasion in 2022, sUASs have provided a critical means of locating and destroying critical targets beyond the forward line of troops. Even when these operations are conducted across just a kilometer or two, they still provide a critical sensor or munition in relatively inaccessible locations. The intensity of this kinetic conflict has prompted innovation on both sides, resulting in a diverse set of tactics and techniques to execute sUAS infiltration and prevent them.

The primary tension at the tactical level is the use of electronic warfare, especially jamming, global navigation satellite system (GNSS) spoofing, and cyber-enabled techniques.[9] Whereas kinetic C-sUAS methods require precise targeting data that can be difficult to obtain against small aircraft that are inherently difficult to detect, these methods exploit the radio frequency connection required by sUASs to control the aircraft, receive GNSS data, and provide a video feed. These techniques are also cost-effective and do not require munitions that may be exceedingly expensive.[10]

Technical advantages have played an important role in enabling Ukrainian sUASs to succeed in the face of substantial electronic warfare capabilities on both sides, especially jamming (Tactic 1.1).[11] Although recent Russian improvements in jamming have resulted in as many as ten thousand sUAS losses per month for Ukraine, technical advancements have allowed a small

number of Ukrainian sUASs to succeed. According to open-source reporting, these advances may be improvements in shielding methods, an automatic ability to detect and use unjammed frequencies, better filters that block out noise, or something else.[12] Another less sophisticated technical approach has been using the momentum of small first-person view drones to carry munitions to their target even after successful jamming and the loss of control by the operator. This works because Russian jammers such as the RP-377 reportedly only work at a short range (less than one hundred feet).[13] With the advent of more capable jammers such as the Volnorez and Saniya, the range of this type of jamming is increased, which will require more sophisticated sUAS navigation systems to maintain a favorable technical mismatch.[14] This fleeting advantage is an example of the inherent weakness of relying on technical advantages alone.

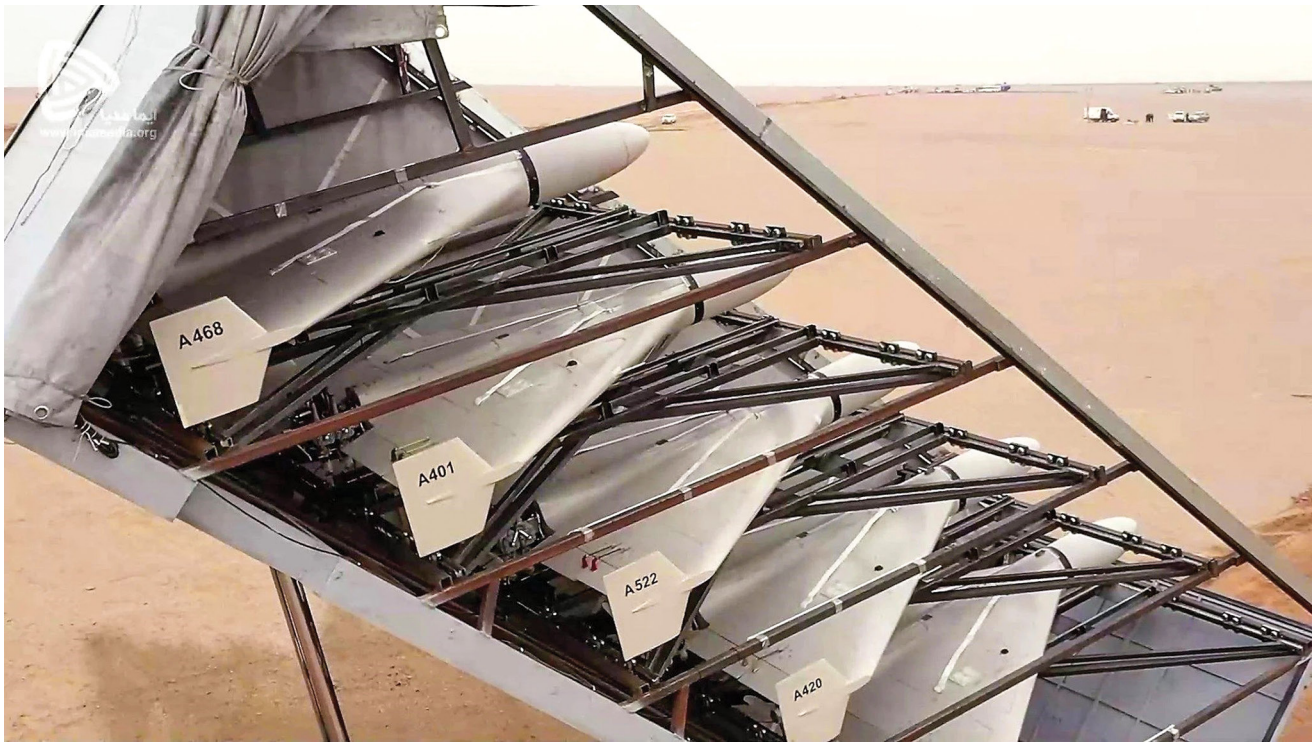
Instead of relying on an outright technical mismatch, Ukrainians use intelligence to locate gaps in jammer coverage and frequencies that Russians are not actively jamming (Tactic 1.2). These gaps result from several factors. One source of the gaps is the fact that Russians have been keeping their more valuable jammers far from the front lines.[15] This is likely due to their targetable electromagnetic signature. Another source of gaps may be the requirement for Russians to reduce electromagnetic fratricide with their communications, an issue that many analysts believe explains the impotency of Russian electronic warfare during the initial invasion.[16] U.S. Army doctrine acknowledges that these factors are inherent characteristics of electronic warfare, which means that gaps of some kind will be present for those cunning enough to use them.[17] Other gaps may be due to the movement of equipment during major troop movements or simply mistakes. Whatever the reason, successful Ukrainian sUAS infiltrations appear to leverage these opportunities through the use of intelligence, including maps of electromagnetic activity.[18]

Another central component of Ukraine's UAS strategy is to use mass to locate these gaps instead of precise intelligence (Tactic 1.3). This is possible because of two inherent qualities of sUAS. First, sUASs are unmanned. Although the controllers are always vulnerable to targeting, sUAS missions do not carry the same physical risk as manned infiltrations. Second, by keeping the manufacturing requirements low for sUASs, Ukrainians can afford attritive tactics in which only small numbers of aircraft survive infiltration. Some Ukrainian sUAS units report successful attacks for just 10 percent of their missions.[19] Yet, large numbers of sUASs can try different routes and different frequencies until weak points are discovered and exploited. This is a significant argument that some Ukrainian commanders have made against shifting to more expensive, technically advanced sUAS models.[20]

In addition to creating or finding gaps in electronic warfare defense, Ukrainian infiltrations impose dilemmas on Russian commanders (Tactic 2.1). Electromagnetic fratricide offers an obvious opportunity to do so. According to the commander of Ukraine's Aerorozvidka unit in 2022, one tactic involves executing sUAS missions when Russians are launching and employing their own sUASs to make it more difficult for the Russian commander to employ his own jamming capabilities.[21] The ability of Russians to coordinate electronic warfare with their own operations has improved since, but the same concept should still apply, albeit using more refined methods. If successful at flying at the same times, places, and frequencies as the adversary's aircraft, infiltrating sUASs put the Russian commander in a difficult position—begin jamming and lose his aircraft or attempt less effective protective measures and risk conceding a successful Ukrainian sUAS infiltration. This type of dilemma plays to the advantage of the infiltrating sUASs.

One-Way Unmanned Aerial Vehicles in the Middle East

Since the Islamic State first began using the tactic in 2016, U.S. forces, allies, and their partners in the Middle East have been grappling with sUAS infiltration.[22] The latest perpetrators have been Iranian-backed militias who employ "one-way UAV" (unmanned aerial vehicle) attacks in which explosive-laden sUASs fly into targets on American bases across the region. Between October and November 2023, American bases received over fifty attacks involving either sUASs or rockets.[23] Although most of these attacks have failed to inflict significant damage, a select number of sUAS infiltrations have inflicted serious casualties. An attack on 23 March 2023 killed a U.S. contractor, and another attack on 24 January



Iranian Shahed-136 loitering munitions in their launch container. (Photo courtesy of the Iran Ministry of Defense)

2024 killed three U.S. soldiers at the Tower 22 outpost in Jordan.[24] Other attacks have been close calls—attacks between October and November 2023 failed to cause significant damage but resulted in at least fifty-six injuries.[25] Given the grave consequences of sUAS infiltration into American bases, the Middle East is a critical case study to investigate.

Like Ukraine, successful one-way UAS attacks in the Middle East find ways to operate beyond our capability to detect and ultimately respond to these aerial threats (Tactical Logic 1). In some cases, this success likely benefits from technical mismatches between sUAS and the C-UAS used to defend U.S. bases in Iraq, Syria, and Jordan (Tactic 1.1). Class III UASs like the Iranian-made Shahed-136 are relatively small, can fly exceedingly low, and are made of lightweight material that further lowers its radar cross-section.[26] In some cases, these advantageous technical characteristics may be enough to avoid detection without any other tactical sophistication. Early attacks in 2021 appeared to avoid many of the technical detection and engagement options available.[27] However, the fact that many recent attacks are intercepted or otherwise unsuccessful suggests additional causal factors for the select cases that do strike their targets.

Although not employed in the same numbers as observed in Ukraine, sUAS attacks on U.S. bases are frequent and provide multiple opportunities for Iranian-backed militias to breach air defenses (Tactic 1.3). Retired Gen. Kenneth McKenzie Jr., former commander of the U.S. Central Command, has articulated this logic differently: "If the opponent is allowed to continue these [sUAS] attacks on such a scope and scale, eventually they're going to get lucky with something."[28] However, because sUASs are inherently cheap, mass employment provides success not through luck but through statistical probability. If there is any gap in coverage for any reason, including maintenance needs, operator error, dead space, or some abnormal phenomena, high numbers of low-risk missions provide a tactical means of capitalizing on the smallest of vulnerabilities. This does not imply that this approach is haphazard either—there is a long insurgent tradition in the Middle East of probing U.S. positions systematically to find vulnerabilities.[29] Therefore, unless future technical prowess reduces these tactical seams to zero, mass employment of sUASs will retain a meaningful tactical logic.[30]

There is also potential for Iranian-backed militias to employ the cognitive logic of sUAS infiltrations in

A soldier with Company B, 2nd Battalion, 135th Infantry Regiment, looks through the optic device of the Drone Defender V2 during counter unmanned aircraft systems training at Camp Lemonnier, Djibouti, 19 August 2020. The Drone Defender V2 is an electronic warfare weapon that is capable of downing and disabling a small unmanned aircraft system. (Photo by Sgt. Sirrina Martinez, U.S. Army)

the Middle East (Tactical Logic 2) by mimicking other military or civilian aircraft to delay or prevent engagement by coalition forces (Tactic 2.1). Several factors make this an exploitable possibility against U.S. forces. First, the U.S. Army techniques publication (ATP) for C-UASs (ATP 3-0.1.81, *Counter-Unmanned Aircraft System*) notes, "the proliferation of friendly joint and multinational UASs, many of which do not have identify-friend-from-foe (IFF) capability."[31] This opens the door for technical difficulties to distinguish between friendly and adversarial aircraft. Second, although newer systems such as the Low, Slow, and Small UAV Integrated Defeat System (LIDS) can synchronize several detection and engagement options into one system, the large family of C-UASs employed by the Department of Defense still require some level of human coordination to reconcile information on aircraft detections.[32] These factors are featured in a report by the Center for Strategic and International Studies, concluding that "over the near term, identification will depend more on context or procedures than specific Identification Friend or Foe (IFF) systems."[33] These coordination mechanisms provide valuable tactical opportunities that a cunning adversary can exploit for their benefit. Finally, as with electronic warfare in Ukraine, even when U.S. forces can identify aircraft accurately, they may be unable to engage inbound sUASs due to fratricide concerns, especially if there are manned friendly aircraft in vicinity of the infiltrating adversary's sUASs.

Exacerbating this situation is that U.S. forces have very little time to make engagement decisions, a fact that is exploitable by adversaries in the Middle East (Tactic 2.2). Discussions with those involved in C-UAS operations in the region indicate that one of the most challenging factors is that engagement decisions must be made in a matter of minutes.[34] According to Raytheon, even a cutting-edge Ku-band Radar

Frequency System can only detect Class I UASs to a range of approximately sixteen kilometers.[35] For a small, commercial sUAS moving at maximum speed, this equates to a reaction time of less than thirteen minutes.[36] For the Iranian-built Shahed-136, this time shrinks to just six minutes.[37] If the situation is clear and unambiguous, this is plenty of time to make a decision and react, but with the introduction of just a little friction, this limitation in detection capability could have lethal consequences.

sUAS Smuggling on the Southern Border of the United States

The southern border provides yet another valuable example of sUAS infiltration. Although not a traditional military example, the use of both manned and unmanned varieties of low, slow, small aircraft by transnational criminal organizations for over a decade to smuggle contraband and people into the United States makes this case an exceptionally well-developed game of cat and mouse. Most of these aircraft cross the border to provide surveillance on U.S. Border Patrol (USBP) positions and guide illegal migrants across the border. A smaller number carry contraband such as fentanyl-based drugs.[38] Unlike the isolated bases in the Middle East, sUAS infiltrations on the southern border exemplify the challenges of protecting an extended region. Additionally, in contrast to the large-scale combat operations in Ukraine, this case shows how the nuances of a gray-zone environment provide additional opportunities for sUAS infiltrations. However, like belligerents in Ukraine and the Middle East, transnational criminal organizations still employ the same tactical logics.

From a technical perspective, transnational criminal organizations exploit that the USBP cannot employ cutting-edge C-UAS technology capable of apprehending sUASs. The USBP's Rio Grande Valley sector has detected thousands of sUAS along its 227-mile border. Yet, the USBP has only been able to mitigate a fraction of these aircraft.[39] It is a daunting problem. Conversations with USBP C-UAS personnel reveal that the majority of these aircraft are commercial sUASs manufactured by Da-Jiang Innovations, which broadens the options available to detect them, but engagement methods must adhere to restrictions designed to limit collateral damage that could impact the local civilian population.[40] As a result, methods such as jamming, GNSS spoofing, and kinetic means are seldom employed.[41] This provides criminal elements with considerably more flexibility. Although criminal organizations are exploiting a technical advantage in a strict sense (Tactic 1.1), they are actually benefiting from what the military would describe as stringent rules of engagement (ROE).

When these criminal elements use an opponent's ROE to their advantage, they impose an engagement dilemma (Tactic 2.1). Furthermore, this dilemma is not artificial. The legal requirements and use-of-force restrictions that underpin USBP engagement options exist for a reason. These rules must balance aircraft safety, commercial use of the electromagnetic spectrum, the public's right to safety, and other factors with the need to prevent illegal sUAS use. Criminals benefit from these restrictions by exploiting aircraft that are difficult to engage under our current standards for safety. They also do not exhibit obvious hostility that would trigger clear exceptions to use-of-force restrictions. This is not to say that these rules do not need serious adjustment—given the scope of the problem, the UBSP probably needs the authority to incorporate these technologies in a more flexible, case-by-case way. But even after the United States increases the countermeasures available, there will always be some exploitable margin inherent in the ROE. Therefore, the byproduct of any need to employ force selectively is a corresponding gap that spies, terrorists, and insurgents can exploit. This is true in wartime, but it is especially true in peaceful conditions in which the interests of commerce and public safety take on added weight.

Criminal groups conducting sUAS infiltrations across the U.S. border are also skilled at compressing USBP reaction times (Tactic 2.2) and using mass employment (Tactic 2.3) to divide limited U.S. government detection resources. During any given hour along the border of the Rio Grande Valley sector, agents may detect several different sUASs on the Mexican side of the border, often simultaneously. Although the detection coverage is quite good in this sector, C-UAS agents must choose exactly where to employ their limited engagement options that cannot cover the entire border. Because these detections can be miles apart, this creates a difficult resource allocation problem that provides opportunities for sUAS operators to take advantage

of displaced C-UAS capabilities. Additionally, many sUASs conduct surveillance from the Mexican side of the border without ever attempting infiltrations. This situation forces USBP personnel to decide which aircraft may attempt infiltration before committing C-UAS resources. Moreover, most sUAS flights start from concealed locations just meters from the border and often involve relatively short flights, further limiting the time available for C-UAS personnel to decide and react.[42]

Conclusion

Across Ukraine, the Middle East, and the southern border of the United States, sUASs use tactical art to bypass sophisticated defenses and access contested or denied areas. Although technology is a critical component of these tactics, it is not sufficient. Instead, sUAS infiltrations must also fly in ways that avoid the principal defensive measures of their adversaries (Tactical Logic 1). Less obviously, sUAS infiltrations must use the tactical situation and its inherent characteristics to impose uncertainty and dilemmas on their opponents (Tactical Logic 2). These basic tactical logics hold true in diverse conditions, including large-scale combat operations, base security in remote locations, and situations short of open military conflict. Training should acknowledge the psychological aspects of sUAS tactics as an inherent quality as important as the physical domain.

Further efforts to understand sUAS infiltrations should focus on understanding how the approaches in the table interact with the operational environment. Field Manual 3-90 acknowledges that tactics must be matched appropriately with the mission variables and operational conditions.[43] Just as doctrine may employ armor units differently in an open desert versus dense urban terrain, sUASs exhibit the same nuance, some of which can be gleaned from the different examples presented here. For one, sUAS infiltrations may benefit from situations with larger public safety or civilian infrastructure concerns because of opportunities to exploit dilemmas and uncertainty (Tactical Logic 2). This is far more likely in gray-zone conditions than in large-scale combat operations. Urban areas, in particular, may offer more dilemmas for commanders employing C-UASs because public services increasingly rely on the radio frequency spectrum and GNSS services.[44] Urban areas also play to the physical logic of sUAS infiltration by inhibiting the line of site necessary for most C-UAS equipment and generating higher levels of electromagnetic clutter, which complicates detection efforts.[45] Although areas with high population density make standard ground infiltration techniques difficult due to the threat of compromise by civilian bystanders, recent research on the locations of sUAS infiltrations across the southern border of the United States suggest the same rules do not apply in the air littoral.[46]

What does the tactical logic of sUAS infiltration mean for C-UAS efforts? There are several broad implications. First, C-UAS forces must use intelligence and act on it aggressively. The pressure placed on decision-making processes through uncertainty, dilemmas, and compressed reaction time requires commanders to place more emphasis on intelligence as a warfighting function. This effort requires thoughtful analysis and the constant fusion of all available sensors and collection platforms. Because sUASs can fly almost *anywhere*, commanders may be tempted to look *everywhere*. Given resource constraints, this strategy may not be feasible. Instead, intelligence efforts should focus collection and analysis on specific times and areas. Narrowing these efforts will require an understanding of the tactical art that is equal to or surpasses those attempting sUAS infiltration. By focusing efforts prior to launch or farther out along expected avenues of approach, commanders buy back valuable response time.[47]

Second, because sUAS infiltration benefits from intelligence, deception must be a critical component of C-UASs as well. Deception should include decoy targets such as those used by Ukrainians and the camouflage methods recommended in ATP 3-01.81, *Counter-Unmanned Aircraft System (C-UAS)*.[48] This effort might also include changing the configuration of C-UAS equipment to reduce predictable vulnerabilities in a manner similar to random antiterrorism measures. Changing the configuration of C-UAS equipment would inhibit mass employment of successive (but not necessarily simultaneous) sUASs by making it difficult for adversaries to systematically probe defenses.

Third, both sUAS and C-UAS technical development should focus on enhancing the military's ability to apply the tactical logic of sUAS infiltrations outlined in this article. The cheap, mass employment of sUASs means that engagement options must be even

U.S. Army soldiers practice assembling the Mobile Low, Slow, Small Unmanned Aerial Vehicle Integrated Defense System (M-LIDS) outside of Camp Buehring, Kuwait, 22 January 2022. (Photo by Spc. Damian Mioduszewski, U.S. Army)

cheaper. This is the promise of directed energy weapons. Engagement dilemmas, collateral damage, and fratricide means that this same technology must also be precise and reliable. Remote sensing efforts should focus on ways to correlate information from a variety of existing systems and manufacturers (including those not originally designed for C-UASs) to make the intelligence picture as clear as possible.[49] Investments in one-stop-shop sensor systems like the Low, Slow, and Small UAV Integrated Defeat System are useful, but the former approach may reap better rewards in the long run as technology changes and acquisitions shift focus to other products over time.

Fourth, although the requirement to fuse capabilities from a variety of platforms may suggest the centralization of C-UAS efforts, local commanders must retain disciplined initiative. Hierarchal decision-making models will be too slow to address engagement decisions on compressed timelines. Current air defense doctrine already recognizes this reality by placing engagement decisions closer to the lower echelon executing element.[50] Yet lower-echelon commanders will also need the flexibility to cross-level ammunition and reposition systems dynamically. This requirement is more subtle and current doctrine does not recognize this level of agility.[51] Yet with the high cost of engagement options like the Coyote interceptor, sUAS infiltrations can overload defenses faster than traditional hierarchal approval processes.[52]

Finally, if sUAS infiltration is more than employing superior technology, C-UAS is also more than a scramble to get the best equipment—*it is also a race to develop the best tactics*. The C-UAS strategy acknowledges this fact through lines of effort directed at training and doctrine.[53] Of course, tactical art is far more than the concepts outlined in this article. Ultimately, tactical competence is a product of either (1) the back-and-forth struggle experienced in war or (2) realistic training conditions. This is the basic premise of the National Training Center. Opportunities to experiment with C-UAS methods of employment will benefit from difficult and realistic adversaries that employ the tactical logic outlined in this article. Given the role that the operational environment plays in the tactical art, force-on-force exercises and testing may need to abandon the sterile, desert environment of the National Training Center, White Sands Missile Range, or Yuma Proving Grounds in favor of more complicated urban environments.

The tactical art of sUAS infiltration and C-UAS remain just one part of warfare, and success in the air littoral will depend on a combination of internal and external factors. However, as the late strategist Colin Gray acknowledged, "strategic utility rests upon tactical feasibility," and sUASs show us that tactical feasibility cannot simply be bought with better technology.[54] With the right tactical application, sUASs provide a tool of strategic proportions to infiltrate areas that are otherwise denied or accessible only at great cost. Because this tool is available to everyone, whoever masters the tactical logic of sUAS infiltrations will reap offensive and defensive rewards. ■

Notes

1. Field Manual (FM) 3-90, *Tactics* (Washington, DC: U.S. Government Publishing Office [GPO], 2023), 2-24.

2. Maximilian K. Bremer and Kelly A. Grieco, "The Air Littoral: Another Look," *Parameters* 51, no. 4 (17 November 2021): 68, https://doi.org/10.55540/0031-1723.3092.

3. *Center for Strategic and International Studies: Countering Uncrewed Aerial Systems: A Conversation with General Sean Gainey*, YouTube video, posted by "Center for Strategic & International Studies, 14 November 2023, https://www.youtube.com/watch?v=szkb2MrhWzE. Lt. Gen. Sean Gainey, then commander of the Joint Counter sUAS Capability Office, stated that one of their goals was to "provide significant capability against the [sUAS] threat [by] leveraging future technology." Sarah Fortinsky, "Top Ukrainian Military Officer Says War with Russia at a 'Stalemate,'" The Hill, 2 November 2023, https://thehill.com/policy/international/4290701-ukrainian-general-war-russia-stalemate/. Ukraine's former commander in chief Valery Zaluzhny also stressed the importance of technological breakthroughs.

4. U.S. Department of Defense (DOD), *Counter-Small Unmanned Aircraft Systems Strategy* (Washington, DC: DOD, January 2021), 14, https://media.defense.gov/2021/Jan/07/2002561080/-1/-1/1/DEPARTMENT-OF-DEFENSE-COUNTER-SMALL-UNMANNED-AIRCRAFT-SYSTEMS-STRATEGY.PDF. The second line of effort in this strategy is "develop operational concepts and doctrine to improve the Joint Force's competitive edge."

5. Alan Beyerchen, "From Radio to Radar: Interwar Military Adaptation to Technological Change in Germany, United Kingdom, and the United States," in *Military Innovation in the Interwar Period*, ed. Williamson R. Murray and Allan R. Millett (New York: Cambridge University Press, 1996), 286–87.

6. Ibid., 274.

7. FM 3-90, *Tactics*, 2-24.

8. Army Techniques Publication (ATP) 3-01.81, *Counter-Unmanned Aircraft System (C-UAS)* (Washington, DC: U.S. GPO, 2023), 3-9–3-17. Although current C-UAS doctrine uses a less detailed topology, all of these elements are discussed in this ATP.

9. Paul Mozur and Aaron Krolik, "The Invisible War in Ukraine Being Fought Over Radio Waves," *New York Times* (website), 19 November 2023, https://www.nytimes.com/2023/11/19/technology/russia-ukraine-electronic-warfare-drone-signals.html; Sam Skove, "How Ukraine Learned to Cloak Its Drones from Russian Surveillance," C4ISRNet, 17 October 2022, https://www.c4isrnet.com/battlefield-tech/2022/10/17/how-ukraine-learned-to-cloak-its-drones-from-russian-surveillance/.

10. Jon Harper, "Army Buys 600 Additional Coyote Counter-Drone Weapons amid Attacks on US Troops," DefenseScoop, 9 February 2024, https://defensescoop.com/2024/02/09/army-600-coyote-counter-drone-rtx/. The unit price of a Coyote interceptor for this contract is $125,000, which is far more expensive than most Class I or II UAS.

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

12. David Hambling, "How Have Ukrainian Drones Beaten Russian Jammers: And Will It Last?," *Forbes* (website), 9 August 2023, https://www.forbes.com/sites/davidhambling/2023/08/09/how-did-ukraine-beat-russias-drone-jammers/; David Hambling, "Jam Buster: How Ukraine's 'Secret Weapon' Shrugs Off Russian Radio Interference," *Popular Mechanics* (website), 16 February 2023, https://www.popularmechanics.com/military/a42922481/tricopter-drone-atlaspro-resists-russian-jamming/.

13. David Axe, "More and More Russian Vehicles Have Drone-Jammers. Ukrainian Drones Blow Them Up Anyway," *Forbes* (website), 22 December 2023, https://www.forbes.com/sites/davidaxe/2023/12/22/more-and-more-russian-vehicles-have-drone-jammers-ukrainian-drones-blow-them-up-anyway/.

14. David Axe, "As the Ukrainians Fling 50,000 Drones a Month, the Russians Can't Get Their Drone-Jammers to Work," *Forbes* (website), 16 February 2024, https://www.forbes.com/sites/davidaxe/2024/02/16/as-the-ukrainians-fling-50000-drones-a-month-at-the-russians-the-russians-cant-get-their-drone-jammers-to-work/.

15. "The New Battle of the Beams," in *Economist* (website), special report, 3 July 2023, 6, https://www.economist.com/special-report/2023/07/03/the-latest-in-the-battle-of-jamming-with-electronic-beams.

16. Justin Bronk, Nick Reynolds, and Jack Watling, *The Russian Air War and Ukrainian Requirements for Air Defence* (London: Royal United Services Institute, 7 November 2022), 13, https://rusi.org/explore-our-research/publications/special-resources/russian-air-war-and-ukrainian-requirements-air-defence.

17. FM 3-12, *Cyberspace Operations and Electromagnetic Warfare* (Washington, DC: U.S. GPO, 2021), 2-9.

18. *Economist*, "The New Battle of the Beams," 6.

19. Joshi Shashank, "How Cheap Drones Are Transforming Warfare in Ukraine," *Economist* (website), 5 February 2024, https://www.economist.com/interactive/science-and-technology/2024/02/05/cheap-racing-drones-offer-precision-warfare-at-scale.

20. Andrew E. Kramer, "Budget Drones Prove Their Value in a Billion-Dollar War," *New York Times* (website), 22 September 2023, https://www.nytimes.com/2023/09/22/world/europe/ukraine-budget-drones-russia.html.

21. Julian Borger, "The Drone Operators Who Halted Russian Convoy Headed for Kyiv," *Guardian* (website), 28 March 2022, https://www.theguardian.com/world/2022/mar/28/the-drone-operators-who-halted-the-russian-armoured-vehicles-heading-for-kyiv.

22. Don Rassler, *The Islamic State and Drones: Supply, Scale, and Future Threats* (West Point, NY: Combating Terrorism Center at West Point, July 2018), 1, https://ctc.westpoint.edu/wp-content/uploads/2018/07/Islamic-State-and-Drones-Release-Version.pdf. Gen. Raymond Thomas III noted that in 2017 ISIS drones flew "right overhead and underneath our air superiority" during which the "Iraqi effort nearly came to a screeching halt."

23. Sabrina Singh, "Defense Department Briefing," C-SPAN video, 28:28, 14 November 2023, https://www.c-span.org/video/?531875-1/defense-department-briefing.

24. Jim Garamone, "U.S. Responds to Attack That Killed U.S. Contractor in Syria," DOD video, 18:36, 24 March 2023, https://www.defense.gov/News/News-Stories/Article/Article/3341127/us-responds-to-attack-that-killed-us-contractor-in-syria/; C. Todd Lopez, "3 U.S. Service Members Killed, Others Injured in Jordan Following Drone Attack," DOD video, 29:54, 29 January 2024, https://www.defense.gov/News/News-Stories/Article/Article/3659809/3-us-service-members-killed-others-injured-in-jordan-following-drone-attack/.

25. Meghann Myers, "Number of Troops Injured in Drone Attacks Jumps to 56," *Military Times* (website), 9 November 2023, https://www.militarytimes.com/news/your-military/2023/11/09/number-of-troops-injured-in-drone-attacks-jumps-to-56/. The DOD has not categorized casualty numbers by rocket or unmanned aerial vehicle (UAV).

26. Uzi Rubin, "Russia's Iranian-Made UAVs: A Technical Profile," Royal United Services Institute, 13 January 2023, https://www.rusi.org/explore-our-research/publications/commentary/russias-iranian-made-uavs-technical-profile.

27. Louisa Loveluck and John Hudson, "Iran-Backed Militias Turn to Drone Attacks, Alarming U.S. Forces in Iraq," *Washington Post* (website), 29 May 2021, https://www.washingtonpost.com/world/middle_east/iraq-militia-drones-threat/2021/05/28/864e44d0-bc8f-11eb-922a-c40c9774bc48_story.html.

28. Alex Horton et al., "U.S. Troops Killed, Wounded in Jordan Attack Blamed on Iranian Proxies," *Washington Post* (website), 28 January 2024, https://www.washingtonpost.com/politics/2024/01/28/americans-killed-drone-jordan/.

29. Jerry Meyerle and Carter Malkasian, *Insurgent Tactics in Southern Afghanistan, 2005–2008* (Alexandria, VA: Center for Naval Analysis Strategic Studies Division, August 2009), 6–8. This resource provides an excellent overview of insurgent tactics, many of which have a parallel logic to today's sUAS attacks including the use of probing attacks on fixed positions.

30. Similarly, although there is little readily available information on the use of specific intelligence to find these sUAS vulnerabilities (Tactic 1.2), insurgents have repeatedly shown the capability to collect on operations inside bases across the Middle East.

31. ATP 3-01.81, *Counter-Unmanned Aircraft System (C-UAS)*, 2-1.

32. Integrated Fires Rapid Capabilities Office, "LIDS [Low, Slow, Small UAS Integrated Defeat System] Family of Systems" (Huntsville, AL: Integrated Fires Rapid Capabilities Office, 2021), 5, https://www.srcinc.com/pdf/LIDS-Family-of-Systems-Brochure.pdf.

33. Shaan Shaikh, Tom Karako, and Michelle McLoughlin, *Countering Small Uncrewed Aerial Systems: Air Defense by and for the Joint Force* (Washington, DC: Center for Strategic and International Studies, November 2023), 22, https://www.csis.org/analysis/countering-small-uncrewed-aerial-systems.

34. U.S. Army senior noncommissioned officer (NCO), interview with author, 22 January 2024.

35. Paolo Valpolini, "Raytheon: C-UAS Capabilities Move to The Next Level," *European Defense Review* (website), 17 September 2019, https://www.edrmagazine.eu/raytheon-c-uas-capabilities-move-to-the-next-level.

36. "Specs: DJI Mavic 3 Classic," Da-Jiang Innovations (DJI), accessed 16 August 2024, https://www.dji.com/mavic-3-classic/specs: calculations performed by author.

37. "Shahed-136 Iranian Loitering Munition Unmanned Aerial Vehicle (UAV)," Operational Environment Data Integration Network (ODIN), accessed 19 August 2024, https://odin.tradoc.army.mil/Search/WEG/shahed-136. Calculation performed by author.

38. "Human Smugglers Now Using Drones to Surveil USBP," U.S. Customs and Border Protection (USBP) media release, 1 March 2023, https://www.cbp.gov/newsroom/local-media-release/human-smugglers-now-using-drones-surveil-usbp; Tim Wright, "How Many Drones Are Smuggling Drugs across the U.S. Southern Border?," *Smithsonian Magazine* (website), June 2020, https://www.smithsonianmag.com/air-space-magazine/narcodrones-180974934/. Additionally, personal communication with Border Patrol agents and Air and Marine Operations personnel indicate that the primary purpose of sUAS is surveillance to help move illegal migrants across the border.

39. *On the Front Lines of the Border Crisis: A Hearing with Chief Patrol Agents Before the Committee on Oversight and Accountability*, 118th Cong. (7 February 2023) (statements of John Modlin, Chief Patrol Agent, U.S. Border Patrol Tucson Sector; and Gloria Chavez, Chief Patrol Agent, U.S. Border Patrol Rio Grande Valley Sector), https://www.congress.gov/event/118th-congress/house-event/115281/text; U.S. Department of Homeland Security (DHS), *Fiscal Year 2024 Congressional Budget* (Washington, DC: DHS, 13 March 2023), 43, https://www.dhs.gov/sites/default/files/2023-03/DEPARTMENT%20OF%20HOMELAND%20SECURITY%20OVERVIEW_Remediated.pdf. As of March 2023, the Rio Grande Valley sector reported eleven mitigations in 2023 and twenty-two mitigations in 2022 using aerial armor systems. The systems focus on DJI products.

40. USBP C-UAS agents, interview with author, 11 May 2023.

41. *The Preventing Emerging Threats Act of 2018: Countering Malicious Drones: Hearing on S. 2836 Before the Committee on Homeland Security and Governmental Affairs*, 115th Cong. (6 June 2018) (statements of David J. Glawe, Under Secretary for Intelligence and Analysis, DHS; and Hayley Chang, Deputy General Counsel, DHS), 103, https://www.govinfo.gov/content/pkg/CHRG-115shrg34314/pdf/CHRG-115shrg34314.pdf. This testimony outlines the collateral damage concerns of these technologies.

42. USBP C-UAS agents, interview with author, 12 May 2023. The author also personally observed C-UAS operations in this sector for one day.

43. FM 3-90, *Tactics*, 1-1.

44. David Kilcullen and Gordon Pendelton, "Future Urban Conflict, Technology, and the Protection of Civilians: Real-World Challenges for NATO and Coalition Missions" (Washington, DC: Stimson Center, 10 June 2021), 8, 16, https://www.stimson.org/2021/future-urban-conflict-technology-and-the-protection-of-civilians/.

45. J. B. Billingsley, *Low-Angle X-Band Radar Ground Clutter Spatial Amplitude Statistics*, Technical Report 958 (Lexington,

MA: Lincoln Laboratory, Massachusetts Institute of Technology, 20 December 2002), 65, 113, https://apps.dtic.mil/sti/pdfs/ADA410042.pdf. Among other findings, this report showed that urban terrain produces significantly stronger clutter than other terrain types.

46. Nathaniel Martins and Joel Vinson, "Low, Slow, and in the Clutter: Applying Lessons Learned from the U.S. Southern Border to SOF Aerial Infiltration" (Monterey, CA: Naval Postgraduate School, 2023), 120.

47. Senior NCO, interview.

48. ATP 3-01.81, *Counter-Unmanned Aircraft System (C-UAS)*, 3-1.

49. Dan Gouré, "Defeating Small Drones: The U.S. Army's Next Big Challenge," RealClearDefense, 18 March 2021, https://www.realcleardefense.com/articles/2021/03/18/defeating_small_drones_the_us_armys_next_big_challenge_768769.html. This article lays out the argument for why "deploying dedicated counter-small UAS systems is not the answer in the long term."

50. FM 3-01, *U.S. Army Air and Missile Defense Operations* (Washington, DC: U.S. GPO, 2020), 2-2.

51. Ibid., 1-6.

52. Harper, "Army Buys 600 Additional Coyote Counter-Drone Weapons."

53. DOD, *Counter-Small Unmanned Aircraft Systems Strategy*. Lines of effort 2.2 and 2.3 address doctrine and training.

54. Colin S. Gray, "Handfuls of Heroes on Desperate Ventures: When Do Special Operations Succeed?," *Parameters* 29, no. 1 (Spring 1999): 2–24, https://press.armywarcollege.edu/parameters/vol29/iss1/4/.