Soldier pushes RQ-7B Shadow unmanned aerial system on Joint Base McGuire-Dix-Lakehurst, New Jersey, February 2020 (U.S. Air National Guard/Matt Hecht)

The Imperative for the U.S. Military to Develop a Counter-UAS Strategy

By Edward A. Guelfi, Buddhika Jayamaha, and Travis Robison

Major Edward A. Guelfi, USA, is an Executive Officer at the 2nd Battalion, 11th Field Artillery Regiment. Dr. Buddhika Jayamaha is a Faculty Member at the United States Air Force Academy. Lieutenant Colonel Travis Robison, USA, is a Battalion Commander at the 2nd Battalion, 11th Field Artillery Regiment.

Military power often emerges at the nexus of technology, organizational processes of force employment, and training.[1] However, rapid technological change, the constantly evolving character of warfare, and the lingering effects of sustained combat on military readiness constrain the U.S. military's ability to respond to emerging global security challenges. The proliferation of unmanned aerial systems (UAS), more commonly referred to as drones, represents one of the largest emerging challenges to the joint community since the rise of improvised explosive devices during the onset of Operation *Iraqi Freedom*. Recent conflicts involving state and nonstate actors and the acquisition priorities of U.S. rivals like Russia and China demonstrate that Soldiers on future battlefields will see the widespread use of drones. For example, Russia and Russian-backed separatists have used various types of drones to achieve devastating effects during their ongoing conflict with Ukraine.[2] U.S. forces in Syria could not retain operational control of the airspace below 3,500 feet for an extended period of time where the so-called Islamic State (IS) conducted lethal and nonlethal drone operations.[3] Looking ahead, the

Department of Defense (DOD) anticipates that China will soon outspend the United States in drone investment, with more than $10 billion dedicated solely to research and development, and may become the world leader in this area by 2023.[4]

For the first time in more than six decades, U.S. ground forces have found themselves under aerial attack and are generally unable to counter the threat. Existing air defense systems have proved tragically unable to detect or engage slow, low-flying UAS.[5] Failure to mitigate this operational risk across the full spectrum of conflict will leave the U.S. Army vulnerable to the use of drones by state and nonstate adversaries. This risk results in an imperative for the Army to develop and implement a more comprehensive counter-UAS strategy than currently exists and that must include material, organizational, and Soldier solutions. Drones present a multidomain challenge, so improving the Army's counter-UAS strategy will provide a framework for developing and integrating counter-UAS capabilities into emerging warfighting concepts. This article explains the UAS threat in terms of technological diffusion and patterns of use and provides counter-UAS recommendations for consideration by senior military leaders.

The Threat

Technological Diffusion. The Cold War demand for persistent surveillance of the Soviet Union led the Air Force and U.S. intelligence agencies to pursue UAS development by the late 1950s, and these drone technologies materialized in the early 1960s.[6] During the latter part of the 1960s, the United States employed these new technologies to monitor China's development of nuclear and air defense capabilities, as well as to conduct battle damage assessments during the Vietnam War.[7] Following that conflict, the United States struggled to integrate UAS into its European operations against the Soviet Union due to technological and airspace restrictions.[8] Regardless, the United States continued to improve drone technologies and by the 1990s had successfully developed the Predator, which provided operationally viable persistent surveillance capabilities.[9]

The first operational deployment of a Predator squadron occurred in Bosnia in 1995, where it provided targeting information, monitored refugee flows, and provided battle damage assessments.[10] After seeing the operational benefits of 24-hour persistent surveillance in rough terrain and adverse weather conditions, Congress more than doubled the Predator budget and accelerated additional UAS programs, which subsequently became the foundation of current global drone fleets and tactics.[11] While the United States initiated the use of UAS, over the past two decades drones have proliferated throughout the world. Today, more than 90 state and nonstate actors possess drone capabilities ranging from small, commercial drones to more sophisticated military variants. Moreover, at least 16 countries have armed drone programs with another 20 countries attempting to develop them.[12] The evolution of electronics and software technologies and the changing character of warfare converged to influence the rapid and widespread proliferation of civilian and military drones. Today, there are more than 600 types of armed and unarmed drones used or being developed around the world.[13]

The accessibility, affordability, and capabilities of available UAS influence their proliferation. Small, affordable, and commercially available hobbyist drones are less capable overall, but they provide groups with an accessible intelligence, surveillance, and reconnaissance (ISR) capability that often rivals more sophisticated military variants. For example, the Chinese-made DJI Mavic is a commercially available quadcopter that costs less than $100 and is capable of autonomous takeoffs and landings, flying GPS-programmed routes, tracking and following moving objects, and sensing and avoiding obstacles.[14] The Mavic's degree of autonomous flight currently exceeds that of the U.S. Air Force's approximately $17 million MQ-9 Reaper UAS.[15]

Israel is currently the largest exporter of military UAS, with over 60 percent of international transfers over the past 30 years.[16] But between 2010 and 2014, only approximately 2.5 percent of transferred drones were armed, so the majority of UAS transferred abroad have been unarmed systems primarily intended for reconnaissance.[17] The number of armed drone exports is increasing, however, given the number of countries actively developing UAS. In particular, China is quickly becoming a leader in exporting inexpensive, weapons-capable drones.[18]

Commercial UAS are proliferating more rapidly than military variants because of the latter's higher cost and greater support infrastructure requirements, as well as existing international arms trade agreements.[19] The availability and proliferation of commercial systems throughout the security environment complicate military responses because these drones often have comparable capabilities to small military UAS and can be easily modified for military uses.[20] Next-generation commercial drone technology is making these systems more like military ones, and they are exploiting new operational concepts such as swarming.[21] As a result, as UAS technology continues to advance and proliferate, the distinctions between commercial and military drones will become less clear, further enhancing operational risk.

As drone proliferation continues, military leaders must understand the capabilities and limitations of each type of drone to develop effective countermeasures. Currently, DOD classifies drones into one of five categories based on a system's size, speed, and operational range.[22] While helpful in distinguishing between a system's potential use in tactical or operational roles, these categories do not provide a roadmap for understanding two important UAS characteristics as they relate to likely battlefield use: a systems degree of accessibility or availability, and the technology and infrastructure required to support using a system. These two characteristics result in a taxonomy of UAS with four categories: hobbyist drones, midsize military and commercial drones, large military-specific drones, and stealth combat drones.[23] Each category of drones has distinct capabilities and limitations that provide a foundation for determining how to counter a system.

Hobbyist drones are widely available for purchase by the public and generally cost less than $3,000. These systems come preassembled or may require assembly; however, they do not require training to operate or any support infrastructure. Midsize military and commercial drones are generally unavailable because of their cost and infrastructure requirements. However, these systems are often sold or transferred by states to foreign militaries and nonstate actors. Large military-specific UAS include reconnaissance and armed variants and are rarely operated by actors other than major militaries because of the systems' costs and infrastructure requirements. Stealth combat drones contain highly sophisticated technologies such as jamming resistance and low observability and are only accessible to those states that produce the systems. Currently, the United States is the only known operator of stealth UAS; however, several countries are developing stealth combat drones.[24]

Patterns of Use. Drones are becoming more sophisticated and capable of conducting surveillance to lethal attacks, either as a delivery system or as an inexpensive precision-guided weapon. The ongoing pursuit and development of artificial intelligence and swarming ability suggest a future where numerous small and inexpensive systems might be used to achieve localized overmatch against a more capable force such as the U.S. Army.[25] The proliferation, sophistication, and weaponization of commercially available UAS mean that any state or nonstate actor will have access to this technology and will likely employ it in novel ways. Moreover, the use of drones may be strategically ambiguous because the international perception of the use of UAS in crises or conflicts is quite different than the use of traditionally piloted aircraft in similar circumstances.[26]

Wider use of drones may reshape military operational concepts and how states engage in conflict. The strategic ambiguity inherent in these systems increases the military options available to an actor, particularly in gray zone conflict or similar contested environments where multiple parties might claim control over airspace. Drones can lower the risks of certain actions such as violating another state's airspace because these systems operate without placing a human pilot at risk. But the lack of a human pilot also lowers the risk of a state using force against a drone during an incursion. Recent examples of this dynamic occurred in 2014 when Turkey shot down a suspected Russian UAS, and in 2015 when Syria reportedly shot down a U.S. Predator, neither of which resulted in escalation or retaliation.[27] For nonstate actors, drones may provide a military capability they otherwise would not have.[28] For instance, Russian-backed Ukrainian separatists have used drones to spot artillery strikes.[29] Another example occurred in 2016 and 2017, when IS launched air attacks against Iraqi troops using small armed drones.[30]

The level of tactical and operational risk to U.S. ground forces has increased dramatically, as more than 23 countries, including Russia, China, Iran, and North Korea, are known to possess or in the process of developing armed drone capabilities.[31] The list of hostile nonstate actors with drone capabilities is also rapidly growing and now includes terrorist organizations such as IS, Hizballah, and Hamas and insurgent groups such as Houthi rebels in Yemen.[32] In Africa, Boko Haram recently started employing armed drones in cross-border attacks on Nigeria and Cameroon.[33] Lastly, given al Shabaab's ties with Hizballah, it is likely only a matter of time before the group begins using drones in support of its terror operations.[34]

Russia, China, and Iran have armed drone capabilities, and these states have demonstrated operational innovation in the employment of small tactical drones. The behavior of these states in recent conflicts highlights how the use of drones increases the complexity of modern conflict, the effects of operational innovations and proliferation, and how a near-peer competitor might seek to exploit current U.S. military vulnerabilities. Together, Russia, China, and Iran's behaviors and capabilities highlight what the U.S. Army must expect from adversaries in every region of potential conflict.[35]

Russia rapidly implemented a drone development and acquisition program that entailed purchasing Israeli-made UAS while concurrently investing in domestic sourcing programs.[36] During its incursion into Crimea and Eastern Ukraine in 2014—the latter instance widely believed to be the first in which every belligerent used drones to produce decisive battlefield results—Russia and its proxies used tactical drones to provide ISR targeting information for supporting artillery units. The near real-time intelligence from these small platforms improved target location accuracy, counterfire response times, and fire mission lethality,[37] and in one instance in July 2014, Russia used this technique to destroy four Ukrainian army brigades preparing to conduct a cross-border attack against Russian-backed separatists' lines of supply.[38]

Whereas Russia demonstrates innovation in drone tactics, Iran displays an inclination toward technical innovation. Iran started its drone program decades ago during its conflict with Iraq, and it is now one of the most developed in the Middle East.[39] Iran has also demonstrated its willingness to share advanced drone technology with others throughout the region. It reportedly flew drones such as the Shahed-129 over Iraq and Syria, exported drone technology to Hizballah and Hamas, and may have provided an assortment of drones to Houthis in Yemen and shared advanced drone technology with Russia.[40] The U.S. military has also engaged and destroyed two Iranian-made drones in Syria that conducted an attack against U.S. ground forces. Incidents such as these highlight that Iran is continuing to expand its drone programs and is willing to employ drones as an asymmetric counter to U.S. military superiority. Iranian drones have been reported in locations from Pakistan to Syria and throughout the Persian Gulf region. They have also become the centerpiece of Iranian technology exhibits used to showcase their advanced security capabilities despite rigorous international sanctions.[41]

The extent of China's UAS development in support of its military remains unclear to Western military analysts and

Soldiers from 7th Air Defense Artillery Regiment engage targets with Patriot missile systems at NATO Missile Firing Installation at Chania, Greece, during German-led multinational air defense exercise Artemis Strike, November 2017 (U.S. Army/Jason Epperson)

senior leaders; however, there is evidence that China's efforts are a real cause for concern. Some experts believe that the Chinese military's drone efforts focus on swarming technology, increased payload and operational range, and the incorporation of artificial intelligence. In a congressionally mandated report, analysts noted that the number and types of China's domestically developed unmanned aerial vehicles continue to expand, with five new platforms displayed at the 2016 Zhuhai airshow.[42] China also appears to be betting that swarms of low-tech drones linked with high-tech artificial intelligence will become the weapon of choice in future conflicts and capable of countering any military force, including that of the United States. China's level of effort in developing UAS suggests the importance and relevance it perceives the technology holds for potential future conflict.[43]

Besides the activities of rival states, the recent employment of drones by nonstate actors reveals how quickly and relatively easily these groups can disrupt advanced industrial militaries. Drones are attractive to these groups because of "the way they carry [destructive] power and the distance from which they allow an adversary to control its delivery."[44] Small commercially available drones give groups such as IS the ability to field an air force capable of collecting ISR and providing limited close air support. The evolution of nonstate actors' use of small drones began in 2004 when Hizballah used drones to challenge the Israeli military.[45] Drone use by nonstate groups continues to evolve and demonstrates the ability to conduct complex attacks. For instance, during the year-long fight to recapture Mosul, Iraqi security forces faced persistent armed drone attacks that slowed their efforts to liberate IS-held neighborhoods.[46] Of concern is the increasingly complex and disruptive ways in which nonstate actors use tactical drones. Hizballah uses these systems for surveillance, manufacturing propaganda, armed strike missions, and kamikaze-type attacks.[47] The Russian ministry of defense recently reported that in January 2018, its forces in western Syria experienced an attack by a "swarm of home-made drones." According to the ministry, Russian forces at Khmeimim Air Base and Tartus naval facility faced a complex attack by 13 drones armed with small-diameter bombs that caused casualties and damaged facilities.[48] These types of swarm-like attacks are particularly threatening because existing kinetic defenses struggle to cope with the agility of small drones, and swarming would overwhelm most existing countermeasures.[49]

Recommendations for Countering the Threat

U.S. policy must not only respond to today's problems, but it should also be flexible enough to adapt to tomorrow's challenges. A comprehensive counter-UAS strategy must address the different nature of threats presented by the various types of UAS. It must also provide solutions for confronting the full scope of UAS challenges by potential state and nonstate adversaries. The U.S. Army's current counter-UAS strategy does not do this. The discussion herein shows that U.S. adversaries are learning and adapting, but the Army is failing to keep pace. Russia's operational employment of drones in Ukraine, Iran's proliferation of drone technologies, China's emphasis on developing full-spectrum drone capabilities, and the evolution of drone use by nonstate actors show that Army planners must anticipate extensive UAS employment in future conflicts. Changes in drone technologies and evolving adversary doctrines suggest that the Army must learn from recent conflicts, as the Russians did, and recognize that the changing character of warfare requires improved acquisition processes and training to effectively counter the UAS threat.

During the global war on terror, the Army made the deliberate decision based on budget priorities to emphasize long-range air defense systems by significantly reducing and eliminating short-range air defense systems. According to senior leaders, this decision was a calculated risk taken when leaders believed that the current and future capabilities of the Air Force would defeat any aerial threat and maintain air superiority.[50] As the assumptions underlying this decision have been proved invalid, the elimination of short-range air defense systems means the Army now relies on aging antiaircraft and missile intercept systems to counter every UAS threat.[51] Given the proliferation of tactical drones, the use of advanced air and missile defense systems is inappropriate due to cost, system availability, and an inability to defeat slow, low-flying drones.

Recently, the Israel Defense Forces employed their U.S.-made Patriot missiles against a single small drone from Syria that violated Israeli airspace. The Israelis used multiple $3 million PAC-2 missiles but failed to destroy the target.[52] This incident highlights the unsustainable cost and technical difficulty of employing limited theater-level air defense assets against tactical drones.[53] In 2017, then–commanding general of the U.S. Army Training and Doctrine Command, General David Perkins, told an audience, "If I'm the enemy, I'm thinking, 'Hey, I'm just going to get on eBay and buy as many of these $300 quadcopters as I can and expend all the Patriot missiles out there.'"[54] If the Patriot and Stinger missiles—which cost $3 million and $38,000 each, respectively—remain the primary defense means for countering drones, it may be possible for an adversary to employ tactics such as those IS used against Russia in Syria to deplete a theater-level air defense capacity that costs tens of millions of dollars. This low-cost act would make an entire area of operations vulnerable to subsequent air attack.

Though the U.S. Army has taken steps to improve its counter-UAS capabilities, these actions have been insufficient. The Army recently began the process of expanding the availability of short-range air defense systems in the Active force by having its Materiel Command overhaul legacy Avenger systems previously set to be destroyed. Though a step in the right direction, reintroducing short-range air defense systems will take time, during which maneuver forces will remain vulnerable. The Army took additional steps to mitigate this gap by training and assigning Stinger teams to its maneuver forces, along with developing Stinger upgrades to improve their effectiveness against tactical drones.[55] However, this is a solution that has already been proved ineffective. When the Army made a similar attempt to integrate Stinger teams in the 1990s, senior defense officials noted that the result "was not great, as we found that 80 percent, if not more, of all Stinger shots taken by maneuver Soldiers, were done in a revenge fashion, after the enemy had already destroyed most of the formation."[56] As the drone threat continues to evolve, so too must the solutions used to counter the threat.

The current drone threat is far too complex for a single solution to solve. A U.S. Army counter-UAS strategy must provide a framework for a persistent and comprehensive approach that links Soldier, materiel, and software solutions. The Army must creatively employ all means along these three lines of effort to regain operational initiative. Along the Soldier line of effort, the Army must retrain its troops to compete, fight, and win in a drone-saturated environment and to win in the counter-reconnaissance fight while restructuring its formations to meet the added demands of counter-drone requirements. Along the materiel solutions line, the Army must continue its reforms of an industrial age–acquisition process to promote rapid, creative, and independent technical solutions through public-private partnerships with corporate partners. Lastly, the Army must explore existing and emerging commercial technologies to identify counter-UAS measures it can rapidly field along with innovative software solutions compatible with existing systems. If no such technologies exist, the Army will have to spearhead the development of effective counter-UAS systems. The newly created U.S. Army Futures Command, whose mission is intended to result in a more rapid acquisition process, can spearhead these efforts. Early success in this command along these lines might provide an opportunity for the Army to leap ahead in drone technology and in ways to counter the drone threat.[57]

The Army must place its primary emphasis on the Soldier line of effort, since this is arguably the most important in terms of near-term counter-UAS effectiveness. This requires redeveloping atrophied air defense warfighting skills necessary in a contested drone environment. Capability and training in air defense skills declined during decades operating in uncontested airspace and counterinsurgency operations. The Army previously trained Soldiers in the fieldcraft necessary to conduct active and passive air defense. Active measures include tasks involving the detection and engagement of enemy aircraft; passive defense measures include skills related to camouflage, concealment, position hardening, dispersion, and mobility to guard against air attack.[58] To its credit, the Army is starting to reintroduce training related to these skillsets.[59]

Reintroducing and strictly enforcing standards of the passive defense is a low-cost and rapid solution to

Explosive ordnance disposal technician flies DJI Mavic Pro Drone while forward deployed in Middle East, May 2017 (U.S. Marine Corps/Shellie Hall)

immediately counter enemy drone threats. If Ukrainian forces at Zelenopillya in July 2014 had implemented passive air defense measures, the results of the Russian attack likely would have been much less severe. The Army should invest in home-station training kits of commercial drone systems like it did following the emergence of the improvised explosive device threat in the battlefields of Iraq and Afghanistan. Once the Army realized the magnitude of the threat posed by these devices, it quickly integrated methods designed to train deploying units in how to counter and defeat the threat. The Service also tested preparedness during culminating training events at its three combat centers. The same approach must be applied to counter-UAS training.

The arrival and detection of any enemy UAS can no longer be considered a mere inconvenience to the detected formation but immediately elevated to the commander's attention, as that origination must actively engage the threat while breaking contact to ensure its survival. The kinetic options to engage an enemy UAS once detected vary from the simple to the complex, but what has proved most effective to date often merges both the traditional kinetic and emerging nonkinetic options to achieve a layering of joint effect against the UAS platform. It is with this approach that all following suggestions should be considered. No single line of effort will be enough to defeat or even suppress this threat alone. It will require the layering of all of these efforts for the U.S. Army and the joint force to achieve a desirable outcome in this new counter-reconnaissance fight.

The blurred distinction between commercial and military drone production makes it necessary for the Army to study and understand the future potential of these systems by working with commercial industry partners. Given the current reliance of nonstate actors on the commercial development of this technology, collaborating with major manufacturers, including foreign manufacturers, will offer the Army insights on the direction of system change and potential threats. This early understanding will provide time for the Army to develop appropriate responses before adversaries employ the systems on the battlefield. As the Under Secretary of the Army recently announced regarding the creation of Army Futures Command, "We have to get more agile in how we work with both of those key constituencies or communities." He also noted that the "entire Department of Defense really divested a lot of its systems engineering talent back in the 1990s and it's been a challenge for the department for weapon systems development because of not having that organic capability inside the department."[60]

Army Futures Command is the ideal organization to implement the search for and development of materiel solutions to counter drones. The Army must ensure

Tim Giles pilots drone during ThunderDrone Tech Expo at SOFWERX in Tampa, Florida, September 2017 (U.S. Air Force/Barry Loo)

that the command is properly manned and given the necessary authorizations to become an institution that can reform an acquisition system that has become unable to keep pace with modern technological change. The U.S. Special Operations Command's relationship with SOFWERX provides a model for what larger scale Army materiel collaboration might look like. SOFWERX is a public-private technology incubator that has recently been preparing to host a series of drone competitions to explore how these systems and equipment might benefit the command.[61] This public-private model would benefit the larger conventional Army and provide a venue to not only discover how drones might benefit the Service but also devise ways to counter them.

While global reach on commercial drone systems is still an emerging technology, the areas that will have significant impacts on a commercial-to-military crossover remain steadily focused on improvements in autonomous flight, increased battery performance, and location technologies. Currently, there remain few commercial drones that can fly without the aid of a user-directed path, but this technology is quickly emerging along with the application of commercial artificial intelligence. Advances in location technologies will also present a significant challenge to the military. The stated goal of companies working in this area is to build systems that can identify their location without the aid of GPS.[62] Combining all the above technological advancements into a single commercial platform—and there is little reason to suspect that will not happen—will provide a potential adversary a commercial version of the most advanced military drones in the world. The Army must work with industry partners that could provide it with forewarning of when this may occur and perhaps influence the timing.

The final line of effort for developing a counter-UAS strategy is to link Soldier and materiel solutions with systems software within the existing structure of Army brigade combat team systems. The first step in formulating these solutions will require developing software for existing systems that enable detecting and tracking drones. Current air tracking systems are already capable of tracking larger operational drones, so the focus must be on smaller tactical UAS, which have smaller radar cross sections due to their small infrared and electromagnetic signatures. Therefore, the Army must invest in software for current and future sensors that can better detect tactical drones. The uncertain budget environment makes the acquisition of new radar systems unlikely, and previous acquisition failures suggest that the Army should not invest limited funds in a specialized counter-drone radar. Instead, it must develop better software for existing radars like the AN/MPQ-64 Sentinel and AN/TPQ-53 radar systems. The latter system was originally designed to track rocket, artillery, and mortar rounds, but the Army is testing its ability to track drones. One advantage that modern radars have is active electronically scanned arrays.[63] Radars with this feature have proved more versatile than older systems, so developing software for these systems to track tactical drones provides a solution short of developing a new radar system.

General Mark A. Milley believes, “One of our most important duties as [military] professionals is to think clearly about the problem of future armed conflict.” He also notes that fixed sites of any kind will be lethal magnets for destruction by enemies who will have a rich diet of targeting information.[64] This information will likely be provided in large part by hostile drones, some of which might conduct attacks. Recent conflicts involving state and nonstate actors and the drone acquisition priorities of U.S. rivals seem to confirm this reality. Despite these threats and the observable lessons from recent conflicts, the Army remains vulnerable to the long-term operational risks resulting from the proliferation and use of drones by state and nonstate adversaries. The reemergence of long-term geopolitical competition with rivals employing a variety of drones, rapid diffusion of drone technologies throughout every operational region, and adversary warfighting concepts that integrate drones into effective offensive operations result in a strategic imperative for the Army to develop and implement a counter-UAS strategy based on Soldier, materiel, and software solutions. This type of strategy will provide a framework for improving the Army’s acquisition process to better leverage emerging technologies and develop a comprehensive Soldier training program that integrates these technologies to regain the initiative through improved warfighting. The Army has spent trillions of dollars in the last decade building and generating a force that can fight, dominate, and win in the land domain, yet states and groups with far fewer resources are rising to challenge the United States in the new arena of drone warfare. The Army must take all necessary steps to mitigate this threat or risk losing the next war. JFQ

Notes

[1] Stephen Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle* (Princeton: Princeton University Press, 2006).

[2] Phillip A. Karber, “‘Lessons Learned’ from the Russo-Ukrainian War: Personal Observations,” draft, Johns Hopkins Applied Physics Laboratory and U.S. Army Capabilities Center, July 2015, 12, available at <https://prodev2go.files.wordpress.com/2015/10/rus-ukr-lessons-draft.pdf>.

[3] Mark Pomerleau, “How $650 Drones Are Creating Problems in Iraq and Syria,” *C4ISRNET*, January 2018, available at <www.c4isrnet.com/unmanned/uas/2018/01/05/how-650-drones-are-creating-problems-in-iraq-and-syria/>.

[4] Ian McPhedran, “U.S. Predicts 42,000 Unmanned Chinese Military Planes by 2023,” News Corp Australia Network, July 8, 2015, available at <www.news.com.au/world/asia/us-predicts-42000-unmanned-chinese-military-planes-by-2023/news-story/b9b5bc52967c7347cb977f9b3460f98f>.

[5] Pomerleau, “How $650 Drones Are Creating Problems in Iraq and Syria.”

[6] Thomas P. Ehrhard, *Air Force UAVs: The Secret History* (Arlington, VA: Air Force Association, July 2010).

[7] Drones conducted 93 percent of damage assessments following Operation *Linebacker II*. See also Ehrhard, *Air Force UAVs*, 9, 28.

[8] Ehrhard, *Air Force UAVs*, 32–33.

[9] Frank Strickland, “An Insider’s Perspective on Innovation During Fiscal Austerity: The Early Evolution of the Predator Drone,” *Strategies in Intelligence* 57, no. 1 (March 2013), 6; Richard Whittle, *Predator: The Secret Origins of the Drone Revolution* (New York: Henry Holt & Co., 2014).

[10] Arthur Holland Michel, “Drones in Bosnia,” Center for the Study of the Drone, Bard College, New York, June 7, 2013, available at <http://dronecenter.bard.edu/drones-in-bosnia/>; Elizabeth Becker, “Crisis in the Balkans: The Drones; They’re Unmanned, They Fly Low, and They Get the Picture,” *New York Times*, June 3, 1999, available at <www.nytimes.com/1999/06/03/world/crisis-balkans-drones-they-re-unmanned-they-fly-low-they-get-picture.html>.

[11] Michel, “Drones in Bosnia”; Strickland, “An Insider’s Perspective on Innovation During Fiscal Austerity,” 3.

[12] Matt Fuhrmann and Michael C. Horowitz, “Droning On: Explaining the Proliferation of Unmanned Aerial Vehicles,” *International Organization* 71, no. 2 (Spring 2017), 397–418.

[13] Lynn E. Davis et al., *Armed and Dangerous? UAVs and U.S. Security* (Santa Monica, CA: RAND, 2014), 7–10; *United States Army Counter-Unmanned Aircraft System (C-UAS) Strategy Extract* (Washington, DC: Army Capabilities Integration Center, 2016), 5.

[14] More information on the DJI Mavic can be found at Web site of SZ DJI Technology Co., Ltd., available at <www.dji.com/mavic-air?site=brandsite&from=nav>.

[15] James Drew, “USAF to Automate MQ-9 Takeoffs and Landings,” *Flight Global*, May 4, 2016, available at <https://www.flightglobal.com/news/articles/usaf-to-automate-mq-9-takeofs-and-landings-424975/>.

[16] George Arnett, “The Numbers Behind the Worldwide Trade in Drones,” *The Guardian*, March 16, 2015, available at <www.theguardian.com/news/datablog/2015/mar/16/numbers-behind-worldwide-trade-in-drones-uk-israel>.

[17] Ibid.

[18] Kyle Mizokami, “For the First Time, Chinese UAVs Are Flying and Fighting in the Middle East,” *Popular Mechanics*, December 22, 2015, available at <www.popularmechanics.com/military/weapons/news/a18677/chinese-drones-are-flying-and-fighting-in-the-middle-east/>.

[19] Andrea Gilli and Mauro Gilli, “The Diffusion of Drone Warfare? Industrial, Organizational, and Infrastructural Constraints,” *Security Studies* 25, no. 1 (February 2016), 50–84.

[20] Ben Watson, “The Drones of ISIS,” *Defense One*, January 12, 2017, available at <www.defenseone.com/technology/2017/01/drones-isis/134542/>; Michael C. Horowitz, Sarah E. Kreps, and Matthew Fuhrmann, “Separating Fact from Fiction in the Debate over Drone Proliferation,” *International Security* 41, no. 2 (Fall 2016), 7–42.

[21] Alexis C. Madrigal, “Drone Swarms Are Going to Be Terrifying and Hard to Stop,” *The Atlantic*, March 7, 2018, available at <www.theatlantic.com/technology/archive/2018/03/drone-swarms-are-going-to-be-terrifying/555005>/.

[22] Micro-tactical, small tactical, tactical, persistent, penetrating. See *Unmanned Systems Integrated Roadmap FY 2013–2038* (Washington, DC: Department of Defense, 2014), available at <https://apps.dtic.mil/dtic/tr/fulltext/u2/a592015.pdf>.

[23] Kelley Sayler, *A World of Proliferated Drones: A Technology Primer* (Washington, DC: Center for a New American Security, June 2015), 8, available at <http://drones.cnas.org/reports/what-are-drones/>.

[24] For details on the capabilities, limitations, and technological trends of these four categories of drones, see ibid.

[25] Ibid.

[26] Michael C. Horowitz, Paul Scharre, and Ben FitzGerald, *Drone Proliferation and the Use of Force: An Experimental Approach* (Washington, DC: Center for a New American Security, March 2017), available at <http://drones.cnas.org/reports/drone-proliferation-use force/>.

[27] Orhan Coskun, “Turkey Shoots Down Drone Near Syria, U.S. Suspects Russian Origin,” Reuters, October 16, 2015,

available at <www.reuters.com/article/us-mideast-crisis-turkey-warplane-idUSKCN0SA15K20151016>; Missy Ryan, "U.S. Drone Believed Shot Down in Syria Ventured into New Area, Official Says," *Washington Post*, March 19, 2015.

[28] Horowitz, Kreps, and Fuhrmann, "Separating Fact from Fiction in the Debate over Drone Proliferation," 7–42.

[29] Sydney Freedberg, Jr., "Russian Drone Threat: Army Seeks Ukraine Lessons," *Breaking Defense*, October 14, 2015, available at <http://breakingdefense.com/2015/10/russian-drone-threat-army-seeks-ukraine-lessons/>.

[30] Michael S. Schmidt and Eric Schmitt, "Pentagon Confronts a New Threat from ISIS: Exploding Drones," *New York Times*, October 11, 2016, available at <www.nytimes.com/2016/10/12/world/middleeast/iraq-drones-isis.html>; Watson, "The Drones of ISIS."

[31] Davis et al., *Armed and Dangerous?* 9.

[32] Peter Bergen, Melissa Salyk-Virk, and David Sterman, *World of Drones* (Washington, DC: New America Foundation, November 22, 2019), 4, available at <www.newamerica.org/in-depth/world-of-drones/3-who-has-what-countries-armed-drones/>.

[33] Simon Ateba, "Boko Haram Terrorists Now Using Drones in Nigeria and Cameroon," *The Nigerian Voice*, September 4, 2017, available at <www.thenigerianvoice.com/news/256790/boko-haram-terrorists-now-using-drones-in-nigeria-and-camero.html>.

[34] "Nigerian Army Links Boko Haram to Hezbollah," *Sahara Reporters*, May 30, 2013, available at <http://saharareporters.com/2013/05/30/nigerian-army-links-boko-haram-hezbollah>.

[35] Karber, "'Lessons Learned' from the Russo-Ukrainian War," 12.

[36] Nicholas Clayton, "How Russia and Georgia's Little War Started a Drone Arms Race," *PRI*, October 23, 2012, available at <www.pri.org/stories/2012-10-23/how-russia-and-georgias-little-war-started-drone-arms-race>.

[37] Karber, "'Lessons Learned' from the Russo-Ukrainian War," 12.

[38] Shawn Woodford, "The Russian Artillery Strike that Spooked the U.S. Army," Mystics & Statistics blog, March 29, 2017, available at <www.dupuyinstitute.org/blog/2017/03/29/the-russian-artillery-strike-that-spooked-the-u-s-army/>.

[39] Ariane Tabatabai, "Iranian Drone Program," *Bulletin of the Atomic Scientists*, October 12, 2017, available at <https://thebulletin.org/decades-making-iranian-drone-program11185>.

[40] Levi Maxey, "Next-Gen Drones: Making War Easier for Dictators and Terrorists," *The Cipher Brief*, December 12, 2017, available at <www.thecipherbrief.com/next-gen-drones-making-war-easier-dictators-terrorists>; John Kester, "Russian Drone Tech May Include Help from Iran," *Foreign Policy*, October 5, 2017, available at <http://foreignpolicy.com/2017/10/05/russian-drone-tech-may-include-help-from-iran/>.

[41] "U.S. Shoots Down Second Iran-Made Armed Drone Over Syria in 12 Days," *The Guardian*, June 20, 2017, available at <www.theguardian.com/us-news/2017/jun/20/us-iran-drone-shot-down-syria>.

[42] According to the *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2017* (Washington, DC: Department of Defense, May 15, 2017), 29, "China displayed five airframes: the Wing Loong I, Wing Loong II, WJ-600A/D, Yunying Cloud Shadow, and the CH-5 (Rainbow 5)."

[43] Emily Feng and Charles Clove, "Drone Swarms vs. Conventional Arms: China's Military Debate," *Financial Times*, August 2017, available at <www.ft.com/content/302fc14a-66ef-11e7-8526-7b38dcaef614>.

[44] Brian A. Jackson, *Evaluating Novel Threats to the Homeland: Unmanned Aerial Vehicles and Cruise Missiles* (Santa Monica, CA: RAND, 2008), xv.

[45] Avery Plaw and Elizabeth Santoro, "Hezbollah's Drone Program Sets Precedents for Non-State Actors," *Terrorism Monitor* 15, no. 21 (November 10, 2017).

[46] Jamie Crawford, "Report Warns of ISIS Developing Drones for Chemical Attacks," CNN, October 20, 2016, available at <www.cnn.com/2016/10/20/politics/terrorist-groups-and-drones/index.html>.

[47] Plaw and Santoro, "Hezbollah's Drone Program Sets Precedents for Non-State Actors."

[48] David Reid, "A Swarm of Armed Drones Attacked a Russian Military Base in Syria," CNBC, January 11, 2018, available at <www.cnbc.com/2018/01/11/swarm-of-armed-diy-drones-attacks-russian-military-base-in-syria.html>.

[49] Madrigal, "Drone Swarms Are Going to Be Terrifying and Hard to Stop."

[50] Randall McIntire, "The Return of Army Short-Range Air Defense in a Changing Environment," *Fires Bulletin* (November–December 2017), 5.

[51] Barry Pike, Program Executive Officer, Missiles and Space, statement, *On Fiscal Year 2018 Priorities and Posture of Missile Defeat Programs and Activities: Hearing Before the Subcommittee on Strategic Forces, Committee on Armed Services, United States House of Representatives*, 115th Cong., 8 (2017).

[52] Callum Paton, "Iran Drone No Match for U.S. Patriot Missile as Israel Blows Hezbollah Aircraft Out of the Sky," *Newsweek*, September 2017, available at <www.newsweek.com/iran-drone-no-match-us-patriot-missile-israel-blows-hezbollah-aircraft-out-sky-667570>.

[53] "IDF Fails 3 Times to Bring Down Drone over Golan," *Times of Israel*, July 17, 2016, available at <www.timesofisrael.com/idf-we-tried-and-failed-3-times-to-bring-down-drone-over-golan/>.

[54] Alexandra Larkin, "How Do You Shoot Down a $200 Drone? With a $3 Million Patriot Missile," CNN, March 16, 2017, available at <www.cnn.com/2017/03/16/americas/drone-shot-by-patriot-missile-trnd/index.html>.

[55] McIntire, "The Return of Army Short-Range Air Defense in a Changing Environment," 5–6.

[56] Interview with senior Defense official, February 2017.

[57] Jen Judson, "Army Futures Command Taking Charge of Conjuring Up New Capability," *Defense News*, March 24, 2018, available at <www.defensenews.com/digital-show-dailies/global-force-symposium/2018/03/24/army-futures-command-taking-charge-of-conjuring-up-new-capability/>.

[58] Christopher L. Spillman and Glenn A. Henke, "The New Threat: Air and Missile Defense for Brigade Combat Teams," *AUSA Magazine*, February 17, 2017.

[59] Anne Chapman, *The National Training Center Matures, 1985–1993* (Fort Eustis, VA: U.S. Army Training and Doctrine Command, 1997), 26.

[60] Judson, "Army Futures Command Taking Charge of Conjuring Up New Capability."

[61] Michael Bottoms, "SOFWERX: A Smart Factory of Innovation Helping the Warfighter," U.S. Special Operations Command Office of Communication, February 2, 2018, available at <www.socom.mil/pages/SOFWERX—A-smart-factory-of-innovation-helping-the-warfighter.aspx>.

[62] Judson, "Army Futures Command Taking Charge of Conjuring Up New Capability."

[63] Sydney J. Freedberg, Jr., "Drone Defense: Army Anti-Artillery Radar Tracks UAVs," *Breaking Defense*, June 27, 2016, available at <https://breakingdefense.com/2016/06/drone-defense-army-anti-artillery-radar-tracks-uavs/>.

[64] David Barno and Nora Bensahel, "Three Things the Army Chief of Staff Wants You to Know," *War on the Rocks*, May 23, 2017, available at <https://warontherocks.com/2017/05/three-things-the-army-chief-of-staff-wants-you-to-know/>.