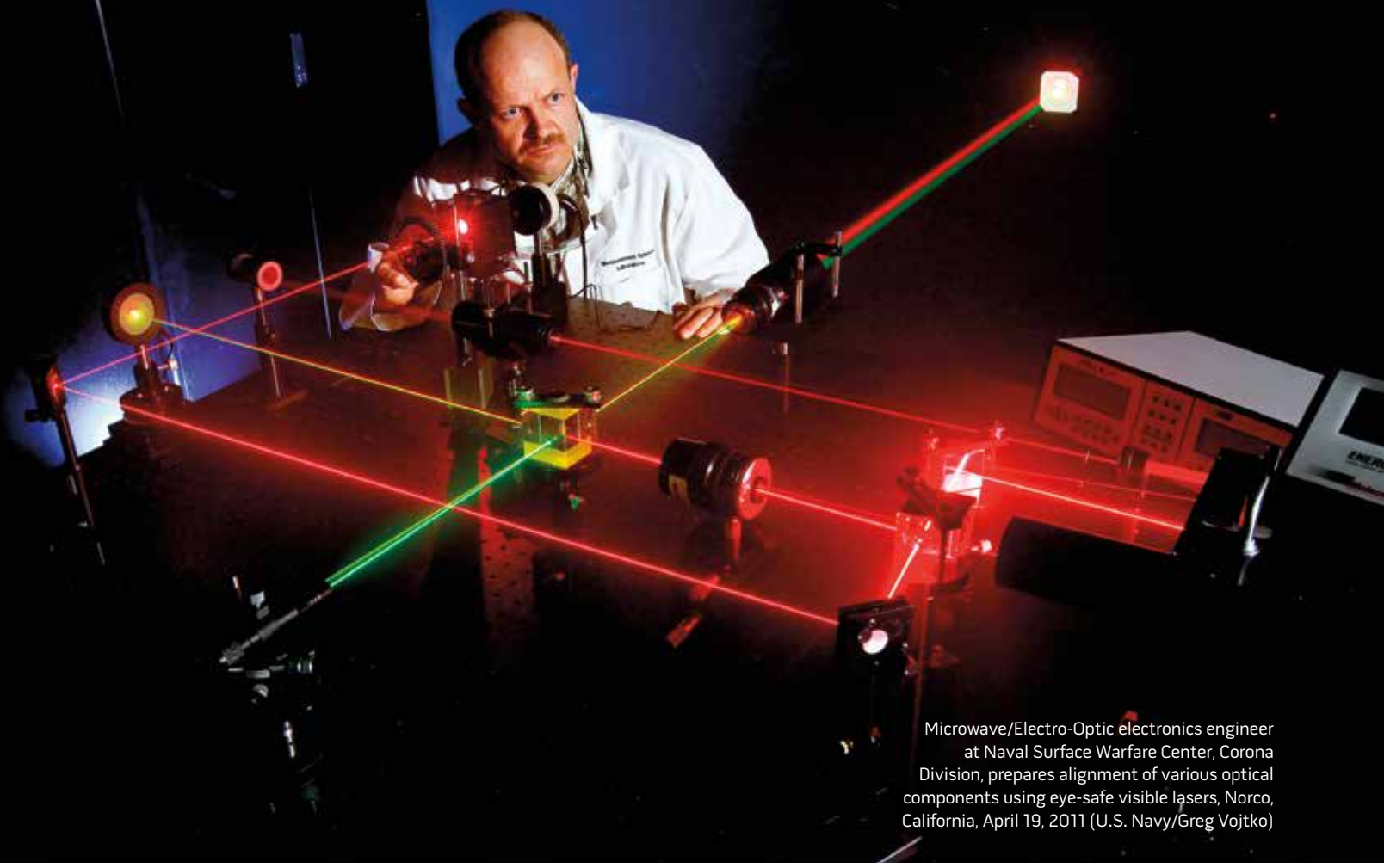

Microwave/Electro-Optic electronics engineer at Naval Surface Warfare Center, Corona Division, prepares alignment of various optical components using eye-safe visible lasers, Norco, California, April 19, 2011 (U.S. Navy/Greg Vojtko)

The Rise of the Commercial Threat

Countering the Small Unmanned Aircraft System

By Anthony Tingle and David Tyree

The Small Unmanned Aircraft System (sUAS) is a disruptive commercial technology that poses a unique and currently undefined threat to U.S. national security. Although, as with any new technology, the parameters of the capabilities regarding military use have yet to be fully discovered, recent events highlight the potential danger. In September 2013, an unarmed sUAS hovered near the face of German Chancellor Angela Merkel while she delivered a campaign speech.[1] In January of 2015, an sUAS defied restricted airspace and landed, initially undetected, on the White House lawn.[2] And more recently, in August of 2016, at least five sUASs disrupted wildfire fighting efforts near Los Angeles, grounding helicopters for fear of mid-air collisions.[3] Likewise, sUAS altercations with law enforcement are increasing, as the Federal Aviation Administration now receives over 100 adverse UAS reports per month.[4] These examples emphasize the intrusive, undetectable, and potentially lethal nature of this emerging technology.

The sUAS epitomizes the difficulties with rapidly advancing commercial technology.[5] The sUAS is as prolific as it is disruptive, and it will challenge our joint air-defense procedures and doctrine and redefine our perspective on the military uses of commercial technology. In this article, we examine the characteristics and capabilities of the sUAS, report on

Lieutenant Colonel Anthony Tingle, USA, is a Strategic Initiatives Analyst at the U.S. Army Space and Missile Defense Command. Second Lieutenant David Tyree, USAF, is a Flight Student Pilot at Vance Air Force Base, Oklahoma.

current counter-UAS initiatives within the Department of Defense (DOD), and present policy ideas to mitigate the future threat from militarized commercial technology.

Characteristics and Capabilities

The rapid rate of commercial technology's advance has directly contributed to the rise of sUASs. Improvements in communication equipment, cryptography, and lightweight materials have led to the current state of the multiple rotary-wing UASs, often referred to as "quadcopters," and extremely small fixed-wing UASs. For this article, we define aircraft that fall into the DOD UAS Category 1 (weighing less than 20 pounds) as an sUAS[6] because the interdiction of larger than Category 1 aircraft quickly approaches traditional defensive counterair operations.[7]

As technology advances, the sUAS will increase in lethality. If Moore's law continues to hold, we will see an increase in sUAS command and control distances, electro-optical sensor resolution, GPS guidance accuracy, and battlefield autonomy. With advances in material science, especially considering adaptive ("3D") printing techniques and carbon nanotubes, sUASs will become smaller, faster, and lighter, and will loiter longer and carry heavier payloads.

The basic physical structure of the sUAS (including the use of advanced materials) hinders radar technologies, the primary component of modern air defense. Radar works by bouncing energy off airborne objects and interpreting the return reflections. Although the carbon fiber and plastic components (of which the majority of most sUASs are comprised) naturally reduce radar return, size appears to contribute most to the shortcomings in sUAS radar identification and tracking.[8] While modern radar technology has the capability to engage smaller objects. Additionally, concerning radar, sUASs are often indistinguishable from other airborne objects (specifically birds).[9] While additional methods such as acoustic-phased arrays and electro-optical cameras show promise, a combination of these tracking and identification technologies may be necessary to defend against the growing sUAS threat.

It is hard to understate the current complexity and importance of positively identifying sUASs. As sUASs continue to be used for a variety of commercial and private purposes (including package delivery and photography), the sUAS operator's intent becomes difficult to discern. Unlike traditional aircraft, which require runways and thus provide longer lead times for tracking, the average sUAS is able to become airborne quickly and close on its target. Additionally, positive identification is a necessary component of engagement authority, especially when considering deployment of sUAS countermeasures on U.S. soil, including interdiction by law enforcement and the possibility of civilian casualties. To effectively counter sUASs, it will be necessary to refine and practice procedures and doctrine, while developing the capability to effectively detect, track, and positively identify the threat.

Future advances in material and computational science will enable the sUAS to perform autonomously, increasing their efficacy as an offensive weapon. One of the characteristics of the sUAS is that it uniquely lends itself to advanced aerial tactics. As battlefield automation progresses, militaries are advancing toward the use of multitudes of sUASs in coordinated formations known as "swarming." This swarming tactic could make defense difficult, especially for large objects or fixed facilities. The use of swarm tactics increases the destructive power of the sUAS and presents adversaries with a defensive dilemma.[10] In this regard, militaries may have to reconsider the concept of *mass* on the battlefield.

Currently, the practical use of sUAS swarms suffers from a confluence of technological shortcomings seemingly resolved by relatively minor advances in technology. The lift capacity, speed, and agility of the sUAS is directly dependent on the amount of weight carried by the vehicle. Reductions in the weight of communications equipment, sensors, onboard processors, and kinetic payload (for example, "energetics")[11] will increase the range and maneuverability of these systems. Likewise, advances in small, lightweight power sources and materials such as carbon nanotubes (and corresponding manufacturing processes such as adaptive printing) will enable smaller and faster sUASs with longer loiter and greater operating distances.

While the size and maneuverability are defining characteristics of the sUAS, advances in automation algorithms are a necessary component of the swarming tactic. Simultaneous command and control of a large number of small objects necessitates autonomy technology that will undoubtedly be available in the near future.[12] In fact, a number of UASs currently deployed or in development operate with varying degrees of autonomy.[13] It is quite feasible that attacking sUAS swarms will be able to automatically sense and communicate weaknesses in the opposing defense, thus adapting their swarming tactics accordingly.

The development of sUAS swarm tactics and techniques in many ways mirrors the introduction of Multiple Independently Targetable Reentry Vehicle (MIRV) technology in the early 1970s. The MIRV concept included the use of multiple nuclear warheads included in a single ballistic missile, greatly increasing the probability of successfully striking the enemy with nuclear missiles.[14] Similar to the inability of the Soviets to counter a larger number of potential inbound nuclear warheads, the sUAS overwhelms those on the defense with possible multiple aggressors. Although similar in terms of using mass, sUAS differs from MIRV in terms of maneuverability and the ability to land and wait for more opportune times to attack. Not all the sUASs in the offensive swarm need to be deadly, as the parallels with MIRVs extend beyond a simple numerical advantage. Offensive sUAS tactics could co-opt the idea of decoys from MIRV technology. With the advent of MIRV decoys, or warheads that had the same physical characteristics as their nuclear counterparts, the economic efficiency of MIRV technology enabled asymmetric advantages.[15] Similarly, the use of decoys may reduce the overall cost of simultaneously attacking with large numbers of sUASs, presenting adversaries with multiple deadly dilemmas.

Current Counter-UAS Initiatives

The U.S. military currently has a multitude of ways to effectively destroy UASs. Starting in 2002, the military exercise Black Dart focused on countering the UAS threat. The exercise has tested a number of kinetic and nonkinetic methods ranging from 0.50-caliber guns to Hellfire missiles.[16] The ability to defend against this threat is, at its core, a problem of asymmetry and efficiency. How do we defeat swarms of $1,500 drones in a practical, cost-efficient manner? The following sections detail existing counter-UAS methods, including traditional kinetic and directed energy means, and examine their applicability to defending against sUASs.[17]

Traditional Kinetic Methods. Traditional kinetic means of air defense, while ostensibly effective in a single intruder scenario, are cost inefficient versus relatively cheap sUASs. Factoring in the possibility of multiple small, low, and fast targets, existing kinetic means of defense are tactically inadequate. Current kinetic defense systems lack the coverage, range, and accuracy to counter future sUAS swarms.[18] It is unlikely that these weapons systems could create a necessary "dome of steel" around stationary positions. Although reducing the caliber of these defensive weapons may ostensibly increase the *rate* of fire, one would expect a corresponding decrease in range. Disregarding possible Gaussian-type weapons (for example, railguns) currently under development, the most viable direct-fire kinetic defense from sUASs may be small-caliber precision-guided rounds.

The miniaturization of precision-guided munitions may provide the capability to interdict a large number of sUASs at standoff distances. According to Deputy Secretary of Defense Robert Work, "We're not too far away from guided 0.50-caliber rounds. We're not too far away from a sensor-fused weapon that instead of going after tanks will go after the biometric signatures of human beings."[19] In the absence of a viable "brute force" or "shotgun" method of area defense (for example, massive amounts of "dumb" kinetic projectiles), these relatively cheap miniature guided munitions may hold the answer to countering swarms of sUASs. Another method to counter sUASs may be with the use of other sUASs.

One method to counteract swarms of attacking sUASs may be to use sUASs as "hunter-drones." Currently, there is a "drone war" occurring over the skies of Tokyo as the Japanese Yakuza (an organized crime syndicate) frequently use sUASs to courier drugs across the city. When the Tokyo police use sUASs with nets to capture these drones, the Yakuza retaliate by attacking the police drones.[20] Increases in battlefield automation might allow "hunting parties" of sUASs to degrade or destroy enemy sUASs with nets or other kinetic methods. Additionally, man-portable air-defense systems like anti-UAS weapons may prove effective against sUASs.[21] In the near term, though, solutions may lie in more natural means of sUAS interdiction.

There has been research into the use of birds of prey for countering the sUAS threat.[22] The U.S. Air Force Academy has recently conducted a year-long study involving gyr-saker falcons. Tests reveal the falcons were able to "detect, positively identify, track, and engage a specific sUAS already in flight."[23] Compared to soaring birds like hawks and eagles, falcons must actively flap their wings while in flight, limiting loiter time to around 20 minutes. Additionally, the training time per falcon is approximately 4 to 5 months.[24] While this study did not address the use of falcons to interdict different types of sUASs, the study lead, Lieutenant Colonel Donald Rhymer, believes that it is possible to "train falcons to generalize to different types of UASs."[25]

Directed Energy. If Army directed-energy systems are disadvantaged in terms of size and weight (compared with the Navy's), then Air Force systems are even more so. The Air Force is constrained by attempting to develop directed-energy systems carried by aircraft. The Air Force scientific advisory board is currently assessing the requirements for these missions on the modified AC-130H model,[26] with a projected demonstration date of 2020.[27] While this lofty endeavor recalls memories of the now defunct Airborne Laser System, the mission and domain of the Air Force forces the Service to pursue small, lightweight laser systems that can be mounted on aircraft.

Perhaps the most promising directed-energy technology in terms of defeating multiple sUASs is the use of high-powered microwaves. These microwave devices have the capability to render the electronic components of an sUAS useless, much like an electromagnetic pulse (EMP).[28] Although there may be practical considerations in the use of EMP devices in urban environments or on the battlefield (that is, necessitating controlled use of these weapons), microwave weapons are under development and, in the future, could be used simultaneously to destroy large numbers of sUASs.[29]

Addressing the Threat: Commercial Adaptive R&D

Since the early 2000s, DOD has acknowledged the necessity to increase the integration of commercial technology into military systems and procurement. But it is a recent phenomenon that commercial technology represents complete capabilities that circumvent the long lead times of traditional government research and development (R&D) and procurement. In other words, in many sectors commercial products are no longer simply contributing to military capabilities; they *are* the capabilities.[30]

While DOD has adapted to the commercial influence in defense procurement, it has failed to recognize the increasing rate of impact of technology on national security. The rising capabilities of commercial technologies, such as the sUAS, presage even greater future commercial threats. Similar to the impact of civilian malware across the spectrum of cyber operations (on both civilian and military concerns), future unforeseen commercial technologies will readily lend themselves to military applications, unnerving those most concerned with maintaining national security.

The challenge is to address this new and fast-moving commercial threat under the shadow of an antiquated and

Cadet-in-charge for Academy falconry team pulls lure as Ace, a black gyr-saker falcon, makes pass at it, September 10, 2010 (U.S. Air Force/Bennie J. Davis III)

inadequate defense procurement process. The existing DOD procurement paradigm relies on establishing requirements that are fulfilled, in part, by commercial-off-the-shelf (COTS) systems and components. Regarding DOD R&D, this requirements-based procurement happens either directly (from the national labs, for example) or indirectly through using COTS. As emerging COTS capabilities surpass the capacity of the government R&D establishment, the United States must develop policies to maintain its technical advantage over its adversaries.

In terms of contribution to national defense, the United States currently fails to take full advantage of its indigenous private industry. We recommend that DOD should work closer with private industry prior to the release of commercial technology, a policy that we call Commercial Adaptive R&D, or CARD.[31] The CARD concept promotes the use of DOD partnerships and relationships with commercial firms to enhance DOD visibility of impending commercial technological release. In contrast with simply using the results of commercial R&D in the form of COTS, under the CARD concept, DOD would seek to conduct research on technology at different stages of development. This pre-market R&D has a number of advantages for both DOD and the firm.

First, DOD gains knowledge on market-shaping technology that will inevitably find its way into the hands of our adversaries. With commercial technologies' rising level of capabilities, state and nonstate actors increasingly threaten U.S. ability to maintain technological overmatch. By conducting CARD, DOD gains vital knowledge on the possible uses of new technologies, and possible counters to these technologies, before our adversaries. Much like the development of the Defense Advanced Research Projects Agency after the launch of Sputnik in 1957, the use of the CARD strategy will help prevent the United States from being surprised by significant commercial technology.

Second, for both the firms and DOD, there exists a possible benefit from the discovery of additional uses for their technology. The dual-use nature of technology is rarely immediately apparent, especially if the government is not exposed to or knowledgeable of that technology.[32] By working closely with large firms, DOD is able to discover new national defense applications for commercial technology, helping both the firm and the government.

Third, DOD can revive the chances for possibly useful technologies that have fallen "below the cut line"—or, in other words, are deemed by the firm as not commercially viable. By signaling its interest in these technologies, DOD provides an opportunity for a "second life" to the firm's technology, resulting in possible commercialization.

Lastly, the CARD construct reduces government R&D risk. The government no longer directly vets new technology as the industry bears the brunt of maturation of the innovation. Utilizing these market-shaping firms in partnership roles with government R&D is disproportionately low given the amount of R&D

Sailors assigned to USS *Jason Dunham*, U.S. Air Force Academy Cadets, and engineers from Johns Hopkins University Applied Physics Lab test unmanned aerial systems aboard rigid hull inflatable boat during exercise Black Dart, September 20, 2016, Gulf of Mexico (U.S. Navy/Maddelin Angebrand)

that is conducted (for example, the Intel Corporation R&D budget for 2013 was roughly $10.6 billion).[33] A majority of the risk is placed on the commercial firm, whereas DOD begins to conduct R&D on the product in mid-to-late stream.

By adopting new policies toward government defense procurement and the degree to which they conduct research with private industry before the commercial release of COTS products, DOD will develop early defenses against threatening technologies, help shape the development of defense-related technologies, and prevent technological surprise. The greater integration of DOD into private R&D, or CARD, will help better ensure national defense in a period of increasing commercial threats.

Conclusion

Although current state-of-the-art sUAS capabilities are sufficiently threatening, we are on the cusp of technological advances that will make the sUAS exponentially more deadly. The asymmetric nature of the sUAS, especially when considering swarm tactics, makes the technology difficult to defend against. An sUAS is relatively inexpensive and ubiquitous (it is estimated that there are over one million sUASs in the United States alone).[34] Conversely, most defense systems are—at least at this stage of development—restrictively expensive. It may be fiscally restrictive and grossly inefficient to attempt to counter this commercial threat with large military programs. Additionally, as technologically state-of-the-art as current commercial sUASs appear, small advances in supporting technologies will yield huge leaps in sUAS capabilities, further compounding defensive problems such as detection and identification.

To protect against this threat, the United States must develop doctrines both for sUAS attack and defense. It is necessary to improve our capabilities in *both* offensive and defensive sUAS technologies. Additionally, this is inherently a joint fight, with the technology and techniques developed by each Service synergistically contributing to the development of anti-sUAS doctrine. Now may be the time to establish a joint organization specifically to address the sUAS threat, similar to the Joint Improvised-Threat Defense Organization (formerly known as the Joint Improvised Explosive Device Defeat Organization), originally established to counter improvised explosive devices.

Additionally, since the early 2000s, it has been widely accepted that DOD needs to integrate COTS requirements solutions. In this "linear model" of innovation, private industry conducts R&D to develop the COTS product, and the government applies COTS to existing requirements. Most important, DOD needs to conduct R&D on the pre-COTS product to discover new requirements based on new capabilities.

This form of R&D should supersede the old model of simply fulfilling government requirements. DOD can accomplish this through close interaction with private industry to discover uses for emerging COTS products before they are simultaneously released to the public and our potential adversaries.

In the history of modern warfare, there have been few purely commercial technologies that so readily lend themselves to immediate weaponization as the sUAS. The threat lies not only in the technology itself, but also in the degree to which that technology is sufficiently capable and available to all potential nefarious actors. In this sense, the potential threat from sUASs should catalyze new thinking in DOD about the uses of commercial technology. Moving forward, it is this commercial availability of advanced technology that is the true threat, and it is this new technological frontier that may pose the greatest future challenge to our national security. **JFQ**

Notes

[1] Wallace Ryan and Loffi Jon, "Examining Unmanned Aerial System Threats and Defenses: A Conceptual Analysis," *International Journal of Aviation, Aeronautics, and Aerospace*, no. 4 (January 10, 2015).

[2] Faine Greenwood, "Man Who Crashed Drone on White House Lawn Won't Be Charged," *Slate.com*, March 18, 2015, available at <www.slate.com/blogs/future_tense/2015/03/18/white_house_lawn_drone_the_man_who_crashed_it_there_won_t_be_charged.html>.

[3] Michael Martinez, Paul Vercammen, and Ben Brumfield, "Above Spectacular Wildfire on Freeway Rises New Scourge: Drones," *CNN.com*, July 19, 2015, available at <www.cnn.com/2015/07/18/us/california-freeway-fire>.

[4] The latest Federal Aviation Administration (FAA) reports are available at <www.faa.gov/uas/law_enforcement/uas_sighting_reports/>.

[5] While the militarization of the Small Unmanned Aerial System (sUAS) would ostensibly increase its lethality, this article focuses on the possible capabilities of commercial sUASs (including the addition of an explosive payload).

[6] Practically, the discussion of sUASs should not be limited to this weight. The FAA categorizes aircraft under 55 pounds as an sUAS.

[7] UAS Task Force Airspace Integration Integrated Product Team, *Unmanned Aircraft System Airspace Integration Plan* (Washington, DC: Department of Defense, March 2011), available at <www.acq.osd.mil/sts/docs/DoD_UAS_Airspace_Integ_Plan_v2_(signed).pdf>.

[8] William Camp, Joseph Mayhan, and Robert O'Donnell, "Wideband Radar for Ballistic Missile Defense and Range-Doppler Imaging of Satellites," *Lincoln Laboratory Journal* 12, no. 2 (2000), 267–280.

[9] In the same vein as radar, infrared systems have a similarly difficult time in detecting small heat signatures of an sUAS.

[10] John Arquilla and David Ronfeldt, *Swarming and the Future of Conflict* (Santa Monica, CA: RAND, 2000), available at <www.rand.org/pubs/documented_briefings/DB311.html>.

[11] *Energetics* refers to the reduction of explosive size while increasing explosive power. See John Gartner, "Military Reloads with Nanotech," *MIT Technology Review*, January 21, 2005, available at <www.technologyreview.com/s/403624/military-reloads-with-nanotech>.

[12] Daniel Gonzales and Sarah Harting, *Designing Unmanned Systems with Greater Autonomy* (Santa Monica, CA: RAND, 2014), available at <www.rand.org/pubs/research_reports/RR626.html>.

[13] One example of autonomous UAS operations is the use of the Israeli Harpy 2 for suppression of enemy air defense operations. See T.X. Hammes, "Cheap Technology Will Challenge U.S. Tactical Dominance," *Joint Force Quarterly* 81 (2nd Quarter 2016).

[14] Lynn Etheridge Davis and Warner R. Schilling, "All You Ever Wanted to Know About MIRV and ICBM Calculations but Were Not Cleared to Ask," *The Journal of Conflict Resolution* 17, no. 2 (1973), 207–242.

[15] John Wilson Lewis and Hua Di, "China's Ballistic Missile Programs: Technologies, Strategies, Goals," *International Security* 17, no. 2 (1992), 5–40.

[16] Richard Whittle, "Military Exercise Black Dart to Tackle Nightmare Drone Scenario," *NewYorkPost.com*, July 25, 2015, available at <http://nypost.com/2015/07/25/military-operation-black-dart-to-tackle-nightmare-drone-scenario/>.

[17] While possible sUAS countermeasures exist, this article does not discuss technologies and techniques associated with cyber effects, such as GPS spoofing and command link capture.

[18] The 20-mm Phalanx (Close-In Weapon System) has a left-to-right limit of 300 degrees. For more information, see "USA 20 Mm Phalanx Close-in Weapon System (CIWS)," *NavWeaps.com*, June 16, 2010, available at <www.navweaps.com/Weapons/WNUS_Phalanx.htm>.

[19] Cheryl Pellerin, "Work Details the Future of War at Army Defense College," *Defense News*, April 8, 2015, available at <www.defense.gov/News-Article-View/Article/604420>.

[20] James Vincent, "Tokyo Police Unveil Net-wielding Interceptor Drone," *TheVerge.com*, December 11, 2015, available at <www.theverge.com/2015/12/11/9891128/tokyo-interceptor-net-drone>.

[21] Andrew Tarantola, "The SkyWall 100 Is a Net-launching Anti-Drone Bazooka," *Engadget.com*, March 3, 2016, available at <www.engadget.com/2016/03/03/the-skywall-100-is-a-net-launching-anti-drone-bazooka/>.

[22] See Peter Holley, "Watch This Trained Eagle Destroy a Drone in a Dutch Police Video," *Washington Post*, February 2, 2016, available at <www.washingtonpost.com/news/worldviews/wp/2016/02/01/trained-eagle-destroys-drone-in-dutch-police-video/>.

[23] Don Rhymer et al., "Falconry: Alternate Lure Training (FALT)," Report nos. 56250 and 63300.

[24] Don Rhymer, telephone interview by authors, November 11, 2015.

[25] Ibid.

[26] William P. Head, *Night Hunters: The AC-130s and Their Role in U.S. Airpower* (College Station: Texas A&M University Press, 2014).

[27] Thomas Masiello and Sydney Freedberg, Jr., "Air Force Moves Aggressively on Lasers," *BreakingDefense.com*, August 7, 2015, available at <http://breakingdefense.com/2015/08/air-force-moves-aggressively-on-lasers/>.

[28] For both microwaves and lasers, there exist the possibility of countermeasures. In terms of microwaves, electronic hardening of the sUAS could provide protection. Against laser attack, countermeasures such as smoke might provide a level of survivability.

[29] Jason D. Ellis, *Directed-Energy Weapons: Promise and Prospects* (Washington, DC: Center for a New American Security, April 2015), available at <www.cnas.org/sites/default/files/publications-pdf/CNAS_Directed_Energy_Weapons_April-2015.pdf>.

[30] Additionally, we especially see this commerciality phenomenon in the cyber domain.

[31] The authors want to thank Dr. Terry Pierce for providing the opportunity to observe the Department of Homeland Security's Center of Innovation, the operations on which the Commercial Adaptive R&D (CARD) concept is based. Dr. Pierce also provided valuable input into developing the CARD theory itself.

[32] John A. Alic, *Beyond Spinoff: Military and Commercial Technologies in a Changing World* (Cambridge: Harvard Business Press, 1992).

[33] Michael Casey and Robert Hackett, "The Top 10 Biggest R&D Spenders Worldwide," *Fortune*, November 17, 2014, available at <http://fortune.com/2014/11/17/top-10-research-development/>.

[34] Andrew Amato, "Drone Sales Numbers: Nobody Knows, So We Venture a Guess," *Dronelife.com*, April 16, 2015, available at <http://dronelife.com/2015/04/16/drone-sales-numbers-nobody-knows-so-we-venture-a-guess/>.