The Heritage Foundation

BACKGROUNDER

No. 3305 | APRIL 16, 2018

Establishing a Legal Framework for Counter-Drone Technologies

Jason Snead, John-Michael Seibler, and David Inserra

Abstract

As drones continue to proliferate, the counter-drone needs of American law enforcement and national security agencies will only grow. Congress has recognized the problem and, in the 2017 and 2018 National Defense Authorization Acts (NDAAs), afforded limited counter-Unmanned Aircraft System (CUAS) authority to the Departments of Defense and Energy—but more must be done. First, Congress should build on its approach in the 2018 NDAA by extending counter-drone authority to federal law enforcement agencies. Second, Congress should broaden this authority to ensure that all effective counter-drone technologies may be used, notwithstanding other provisions of law, to defend appropriate federal assets and facilities within these agencies' jurisdictions. Addressing federal CUAS needs is a critical first step, but these authorities should also be extended to state and local law enforcement agencies, as they will ultimately bear the brunt of defending the public from drone-related threats.

Introduction

Small Unmanned Aircraft Systems (UAS), commonly referred to as drones, continue to make headlines for their ability to engage in all manner of revolutionary and lifesaving activities.[1] Unfortunately, terrorists and criminals are proving as innovative as their industry counterparts in finding novel uses for UAS. The increasingly common use of drones by terrorists to launch strikes abroad has raised concerns that domestic malefactors may plan and execute similar attacks. Some criminal actors, meanwhile, are using drones to smuggle drugs across the border or into prisons, or otherwise to support their nefarious enterprises. These incidents, as well

This paper, in its entirety, can be found at **http://report.heritage.org/bg3305**

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

Key Points

- National security and law enforcement agencies must develop robust means of detecting, identifying, and countering hostile or threatening drones by disrupting, seizing control of, or even destroying them.
- Unfortunately, the legal authorities to develop and make use of this capability are ambiguous at best, and, in fact, a number of federal laws appear to frustrate efforts by federal, state, and local government officials to procure and use comprehensive counter-drone systems.
- To that end, Congress should continue the process it began with the National Defense Authorization Acts of 2017 and 2018 and expand the limited drone authority given therein.
- Congress should also establish a pilot program to allow DHS to deputize and train select state and local law enforcement officials in the operation of counter-drone platforms, given the integral role state and local agencies play in addressing all manner of threats to public safety.

as others, including unauthorized flights over sports stadiums and in controlled airspace near airports—and even a crash onto the White House lawn[2]—have exposed both the vulnerability of sensitive facilities and critical infrastructure to hostile or recklessly operated UAS, and serious shortcomings in the capabilities of law enforcement and national security agencies to address these threats.

Rectifying this will require national security and law enforcement agencies to develop robust means of detecting, identifying, and countering hostile or threatening UAS by disrupting, seizing control of, or even destroying them. Unfortunately, the legal authorities to develop and make use of this capability are ambiguous at best, and, in fact, a number of federal laws appear to frustrate efforts by federal, state, and local government officials to procure and use comprehensive counter-UAS (CUAS). If the public is to enjoy the many benefits drone technologies offer, this deficit must be overcome.

To that end, Congress should continue the process it began with the National Defense Authorization Acts (NDAAs) of 2017 and 2018 and expand the limited CUAS authority given therein to grant broad statutory exemptions to the Departments of Defense (DOD), Justice (DOJ), and Homeland Security (DHS), as well as other federal law enforcement agencies, to acquire CUAS technologies and develop departmental policies and "rules of engagement" to govern their use. Congress should also establish a pilot program to allow the DHS to deputize and train select state and local law enforcement officials in the operation of CUAS platforms, given the integral role state and local agencies play in addressing all manner of threats to public safety.

Threats

Terrorism. U.S. officials must consider the potential use of drones by terrorists. Hezbollah was using drones as early as 2004,[3] and a variety of other terrorist organizations have also made use of drones as weapons or for reconnaissance purposes. ISIS forces in Syria and Iraq began using off-the-shelf drones primarily for intelligence or propaganda purposes in 2014. As drones became cheaper and more powerful, however, ISIS began to seriously invest in UAS as implements of war. Facilities to produce crude bombers and scratch-built drone parts were discovered in territory recaptured from ISIS.[4] ISIS has released propaganda footage of its fighters learning how to weaponize drones and regularly posts videos of its bombing operations, as well as graphics claiming its drone strikes were causing significant damage and casualties.[5]

While ISIS propaganda overstates its efficacy, U.S. officials and analysts agree that ISIS's use of drones is growing more pronounced and deadly.[6] Lt. General Vincent Stewart, director of the Defense Intelligence Agency, testified in 2017: "In the past year, ISIS's use of UAS for surveillance and delivery of explosives has increased, posing a new threat to civilian infrastructure and military installations."[7] New concerns include the possibility of "swarms" of small weaponized UAS that overwhelm the ability to counter them.[8]

With the growth of drones as terrorist weapons of war in Syria and Iraq, U.S. policymakers and security officials are also becoming more concerned at the prospect of weaponized drones back home. In September 2017, FBI Director Christopher Wray testified: "I think that the expectation is that [terrorist use of drones] is coming here, imminently."[9]

UAS pose a unique threat in that they can avoid many traditional counterterrorism defenses. Events like the Super Bowl, a large concert, or critical infrastructure facilities such as a power plant or a chemical production plant feature multiple layers of security, such as screening of visitors to prevent the use of weapons or explosives inside the venue, hardened barriers to defeat vehicular attacks, and armed guards as an extra layer of defense to defeat any active threats. A drone-based attack avoids most of these defenses, making it attractive for would-be terrorists. As if to demonstrate the vulnerability of even the most hardened targets, in 2015 a drunken federal government employee crashed a drone onto the White House lawn.[10]

One important capability that remains is proactive intelligence gathering that seeks to detect would-be terrorists before they strike. Indeed, the U.S. has already relied on such intelligence in the case of Rezwan Ferdaus, whose 2011 plot to use remote control aircraft to attack the Pentagon and Capitol building was foiled by an FBI sting operation.[11] But the fact that drones can bypass so much of the traditional security apparatus and potentially strike high-value targets is disconcerting.

Indeed, given the widespread availability of drones today, it is easier than ever for terrorists to get their hands on these systems. The more difficult part of a drone-based attack is creating or acquiring the payload, such as explosives. Nevertheless, based on the uses of UAS in Iraq and Syria, it is relatively

easy to outfit a UAS with an explosive device and use the drone as a makeshift missile—or enable it to drop small explosive devices such as grenades. UAS attacks involving larger explosives or even chemical weapons are also possible, as detailed in a DHS National Terrorism Advisory Bulletin in November 2017.[12] In 2015, a protestor piloted a drone carrying a trace amount of radioactive material onto the roof of the Japanese Prime Minister's office.[13] Though the action was spurred by opposition to nuclear power rather than a desire to inflict terror, the incident could be a proof-of-concept for more nefarious individuals. Weaponized drones also pose a threat to European allies, as Europe faces a significant number of foreign fighters from Iraq or Syria returning to Europe with knowledge of explosives and weaponized drones.[14]

Criminal Activity

Recent history demonstrates that criminals are at least as inventive as mainstream entrepreneurs in concocting novel uses for UAS that further their existing illicit enterprises. One report in the U.K. pointed to the use of a small UAS by burglars to "case" private properties prior to initiating a break-in.[15] In similar, though more technologically sophisticated form, another report highlights the criminal use of drones equipped with infrared cameras to detect the heat signatures of marijuana grow-houses, so that the illegal cash crop could be stolen.[16] In Australia, a drug cartel used a UAS to spy on law enforcement authorities actively surveilling its illegal operations, forcing the authorities to "initiate procedures and methods to defeat it."[17]

Though none of these incidents involved weaponized drones, that threat is real and likely inevitable. One hobby flier in New Haven, Connecticut, modified two drones to carry a handgun and a flamethrower.[18] In videos posted to YouTube, the operator publicized his ability to remotely fire both weapons, raising the alarming prospect that nefarious actors could build and use similar platforms to launch remote attacks, whether for criminal or terrorist purposes.[19] Even unarmed, however, drones can pose a danger to the community. Malefactors could execute an assault or harass individuals simply by "buzzing" or charging them at high speed. An uninvited visit to another's property, by foot or by drone, may constitute a trespass. "Peeping Toms" could use drones to invade the privacy of others. Reckless operators can cause bodily harm simply by losing control of the drone. This was proven in Seattle when a hobby flier's drone collided with a building and fell onto a woman, who suffered a concussion.[20]

Another concern is the use of drones to smuggle contraband into state and federal prisons. The problem of contraband is perhaps as old as prisons themselves. Drones bring, literally, a new dimension to this problem, allowing individuals to easily transport banned items such as drugs and paraphernalia, cell phones, pornography, and weapons[21]—dropping them in prison yards or even ferrying them directly to a recipient's window.[22] Law enforcement officials are especially concerned that drones may be used to drop firearms into prisons. One plot was foiled in 2015 that involved a plan to ferry a gun, among other things, behind the walls of the Western Correctional Institution in Maryland.[23] The problem is widespread, with reports surfacing of drone-smuggling in more than a dozen states.[24] The rate of their detection is increasing at an alarming clip. In Georgia, one journalistic investigation revealed that prison officials detected 35 drones in the airspace above state prisons in the first half of 2017—compared with just three such incidents reported over the prior three years.[25]

The dangers these illicit package deliveries pose are real. A 75-inmate brawl broke out at the Mansfield Correctional Institution in Ohio when a drone dropped a package containing tobacco, marijuana, and heroin into the prison yard.[26] One inmate was recently able to escape a South Carolina maximum-security facility using a pair of wire cutters delivered by drone.[27] If a gun is successfully smuggled into a prison, officials fear it could spark a riot that would endanger the lives of inmates, prison guards, and other personnel.

International drug cartels are employing drones to further their criminal conspiracies and trafficking activities across the border. In 2017, U.S. Border Patrol agents intercepted a drone carrying 13 pounds of methamphetamine, worth $46,000, at the San Diego border. Authorities arrested Jose Edwin Rivera, who said he had done this five or six times before.[28] In a 2016 article, John Sullivan and Robert Bunker noted that cartels have been using UAS with increasing frequency and effectiveness.[29] According to their research, an estimated 150 drones crossed the border from 2012 to 2014—a rate of about four drones per month. That rate may be accelerating: According to Border Patrol agents, 13 drones were spotted in November of 2017, though it is likely that many more

drones went unnoticed.[30] Sullivan and Bunker note that "narcodrones" are being used not only for smuggling but also reconnaissance and surveillance—to enhance their operations on the border. While they note that cartels have not yet used drones as weapons platforms, this will become more likely in the near future. Indeed, Mexican police seized a drone fitted with a bomb in 2017.[31]

Threats to Manned Aviation

In February 2018 a helicopter flying at low altitude near Charleston, South Carolina, struck a tree and crashed after its pilot reported sighting a small quadcopter approaching the aircraft, and attempted to evade it.[32] That incident, presently under investigation by the FAA, may be the first in which a manned U.S. aircraft has crashed after a close encounter with a drone.[33] Just a few months earlier, however, a U.S. Army Black Hawk helicopter detailed to provide security for a U.N. General Assembly meeting struck a drone 300 feet above sea level, sustaining damage to its rotor.[34] The drone was operating *despite* an FAA-imposed temporary flight restriction, and was flying well beyond the operator's visual line of site, two conditions barred by Federal Aviation Regulations (FARs) governing drone activity. Additionally, it is a federal crime to damage an aircraft, punishable by a fine and up to 20 years in prison.[35]

Nobody was injured in these incidents, but the specter of a mid-air collision resulting in the loss of life is a growing concern, particularly as the number of drones populating U.S. airspace grows.[36] Federal Aviation Administration (FAA) data reveal that pilots reported 1,698 drone sightings in the first nine months of 2017, a 24.49 percent increase in sightings compared to the same period in 2016.[37] Though critics correctly point out that only a tiny fraction of these cases were reported as "near misses" requiring any type of evasive action[38]—and that the FAA data does not distinguish unlawful flights from flights pursuant to FAA-issued airspace authorizations for operations near airports[39]—the fact remains that drones are illegally flying in airspace reserved for manned aviation, including in the densely packed airspace used for take-offs and landings.[40] Alarming videos shot from drones flying in close proximity to manned aircraft, in airspace and at altitudes clearly not permitted by FARs, confirm this.[41] Maintaining the integrity of the airspace is a critical consideration for aviation safety, particularly in light of recent simulation studies suggesting drones can cause more damage to airframes and jet engines than similarly sized birds.[42]

Capabilities

Ultimately, it is clear that drones, like so many technological innovations before them—firearms, automobiles, computers, and cell phones—can become tools for criminal and terrorist activity. Federal, state, and local officials involved in both law enforcement and national security activities are in need of comprehensive counter-UAS capabilities that will permit both the detection and interdiction of hostile or dangerous drones threatening public safety, critical infrastructure, and national security. Presently, few cost-effective solutions exist, and fewer still have been deployed by government agencies, owing to a combination of factors that include concerns about the legal authority to interdict drones, the cost and complexity of systems, and uncertainty regarding the best means of engaging drone threats in populated areas.

Further complicating matters, UAS and CUAS technologies are immature and rapidly evolving, making it difficult to predict which interdiction technologies will prove the most effective investment of public resources. Even once the technology matures, it is reasonable to assume that bad actors will work to overcome CUAS defenses, forcing defenders to continue innovating to remain ahead of the threat.

CUAS will be complemented by UAS traffic management (UTM) systems presently in development by the FAA, NASA, and private-sector partners.[43] UTM will give officials the ability to control low-altitude UAS traffic patterns, define restricted airspace, and selectively grant or deny access to controlled areas.[44] As described by NASA, UTM systems could come in two main variants: "portable" and "persistent."[45] The former could be transported to a particular location—a disaster area, for example—and manage UAS traffic in proximity to the site. The latter would provide continual coverage for a given area, such as the dense, low-altitude airspace above metropolitan areas.

UTM, in combination with the FAA's forthcoming rule on remote identification and tracking of UAS (remote ID),[46] will make it possible to remotely identify lawfully operated drones and define where and when they may fly—two capabilities that will be essential to providing security against hostile or dan-

gerous UAS.[47] Consequently, all drones flown in U.S. airspace, and which are capable of posing a substantial risk to people or property, should be fitted with equipment necessary for compliance with remote ID and UTM, including mandatory geo-fencing software designed to prevent drones from entering restricted airspace without proper authorization.[48]

Present Shortcomings

U.S. and foreign militaries have demonstrated an ability to interdict drone activities in combat conditions. In one incident described by the head of the U.S. Army Training and Doctrine Command, a U.S. ally used a Patriot missile to shoot down a small quadcopter.[49] Recently, a first-of-its-kind swarm attack of crude, fixed-wing drones was launched by Syrian rebels against Russian forces in western Syria.[50] The U.S. military is working to develop cost-effective means of engaging inexpensive, easily replaced UAS, and is experimenting with a variety of weapon systems that could provide U.S. forces with dedicated CUAS capabilities.[51]

Many of these systems were designed for the battlefield and are not viable options for use in domestic airspace above populated areas. To fill that gap, a multitude of private-sector solutions are emerging. Several federal agencies are actively involved in trials of drone detection and CUAS platforms. For example, the FAA is presently utilizing Cooperative Research and Development Agreements "to evaluate the small UAS detection and identification capabilities [offered by manufacturers], using different methodologies and systems on and near airports."[52] The goal of the program is to evaluate various technologies for effectiveness and ability to operate in an airport environment with a minimum of disruption to aviation traffic and communications systems.

In 2015, the Department of Homeland Security worked with Major League Baseball (MLB) officials to deploy a drone detection system during that year's All-Star Game.[53] The system succeeded in using radar to detect nearby UAS, but owing to its cost and lack of an interdiction component, MLB officials decided to forego a potential post-season deployment. At least one state, North Dakota, is actively pursuing CUAS and drone detection research. In 2017, Governor Doug Burgum formed a special task force seeking to build on the state's experience operating one of the seven FAA-authorized UAS Test Sites[54] by setting aside separate airspace to test CUAS technologies.[55]

At present, the principle tool available to most officials to intervene in the event a hostile or recklessly operated drone endangers public safety is most likely a sidearm, although other methods may be employed to avoid shooting at a drone, depending upon the situation. But the small size and high degree of maneuverability of drones makes hitting them difficult, while a successful hit—or even a round that misses the target—risks collateral damage from falling debris, or in more threatening scenarios, the inadvertent detonation of explosives or the spreading of chemical, biological, or radiological agents carried on board the drone.

Damaging or destroying a drone by any means, though, is considered a federal felony according to the FAA's designation of all drones as "aircraft." Even if it were lawful to shoot a drone, there are no established rules or best practices for distinguishing hostile from non-hostile drones, or for engaging them. Most federal, state, and local law enforcement officials have received no training in the CUAS space. Consequently, there is a risk of hesitation and confusion as to when and how to appropriately engage a UAS.

This lack of options, training, and, as will be discussed, authority represents a serious gap in CUAS capabilities that must be rectified.

What Does an Effective CUAS System Need to Do?

It is important to distinguish simple drone detection systems from a full CUAS platform.[56] The former offers only an ability to locate and identify drones, whether through reliance on remote ID and UTM, dedicated sensors, or both.[57] The latter adds a countermeasures function, allowing operators who detect an unauthorized or hostile drone to then interdict, deflect, seize control of, disable, or destroy it. There are likely a range of missions and purposes for which simple detection will be satisfactory.[58]

Missions related to law enforcement and national security, such as safeguarding the public or critical infrastructure, will require a CUAS capability, which should include the following:[59]

1. **Independently detect drones operating in the vicinity of the system.** Presently, the FAA is developing its remote ID requirement for small UAS that will, once established, require most drones in U.S. airspace to have a transponder-

like capability to permit accurate identification and location.[60] CUAS platforms should possess an ability to interface with remote ID and UTM systems to gather information about drones flying in close proximity to a protected venue or facility. However, CUAS should not be reliant on remote ID and UTM for detecting nearby drones, as bad actors could simply disable these systems (or build a homemade drone without them) and be rendered invisible. Rather, a CUAS platform should integrate a host of sensors—including radar, electro-optical, and infrared cameras, as well as acoustic sensors[61] and frequency-scanning equipment able to detect signals common to drone command links[62]—to maintain situational awareness.[63]

2. **Locate and identify hostile drones.** CUAS platforms should possess an ability to discern hostile and potentially hostile drone activity from background, nonthreatening flights. Using its sensors, the system should be able to: Pinpoint the location of a hostile drone; determine its operator's location by tracing command link signals, if possible; and identify the type or types of drones that pose the immediate threat, through data acquired through remote ID or UTM systems, by identifying the types of signals it is emitting, or other means.

3. **Provide notice to/warn off a drone operator.** In general, knowledge of the law is presumed, and UAS operators are obligated to understand relevant rules and restrictions. Therefore, in many circumstances, drones not complying with flight restrictions, FARs, or other applicable laws may be treated as presumptively threatening, allowing CUAS operators to dispense with a notice requirement. In the long run, UTM incorporating a robust, real-time, two-way communications capability will largely solve the question of notice, as it will afford law enforcement, aviation, and national security officials the ability to establish temporary or permanent zones of restricted airspace for UAS, immediately communicate this information to drone operators, and authorize or disallow particular drone operations. In the short term, policymakers will have to address the question of what constitutes satisfactory notice prior to taking action to damage, destroy, or seize a drone suspected of endangering public safety and determine when it is appropriate to use a CUAS platform to destroy or disable a drone without prior notice.

4. **Provide CUAS operators with a countermeasures ability.** Current countermeasures technologies fall broadly into two categories: kinetic and nonkinetic. Kinetic countermeasures use physical means to seize, disable, or destroy a drone. Examples include drone-capturing net guns and interceptor drones fitted with nets, birds of prey, and projectiles or firearms. Nonkinetic countermeasures feature a wide variety of technologies that include devices intended to jam a drone's control link or GPS signal;[64] hacking tools used to seize control of a drone from its operator or override autonomous programming;[65] high-power microwave or high-power electromagnetic weapons that "fry" a drone's electronics;[66] laser weapons;[67] and even sonic weapons.[68] There is no single method of interdicting drones that will be effective in every case or suitable for use in every operational environment.[69] As a result, an effective CUAS system will likely have to provide its operators with a range of countermeasures to address the likelihood that one or more may fail—or may be countered by malicious operators.[70]

Research and testing will have to be done to determine the appropriate and most effective combination of countermeasures for a specific site or category of sites, based on the surrounding environment and an assessment of the types of threats it is likely to face. Federal regulations establishing acceptable degrees of, and protocols for, interference to radio and wireless communications will be needed to allow CUAS operators to take appropriate actions in exigent circumstances. Federal agencies will need to develop, publicize, and train responsible CUAS operators on clear rules of engagement that define when it is reasonable and appropriate to use a CUAS platform's range of countermeasures functions, up to and including the possible use of firearms or other destructive means to stop a threatening drone. Such rules will be necessary to ensure that CUAS platforms are used to engage exigent threats properly, promptly, and consistently, and that risks of collateral damage are minimized.

Given the novel nature of CUAS technology, its many "unknown unknowns," the clear federal laws and interests such systems implicate, and the lack of expertise in drone interdiction among local and state law enforcement agencies, the initial deployment of CUAS systems would best be accomplished under federal direction and supervision. However, in the final analysis, federal agencies lack the manpower and resources to directly guard every critical facility or high-value target in the nation. Much of this responsibility will ultimately fall, as most routine law enforcement operations always have, to state and local officials who will eventually need independent authority to deploy and operate CUAS systems. Therefore, the goal of the early roll-out should be the development of core competencies and training programs in CUAS operations for both federal and state and local agency partners, to facilitate broader future deployments.

Authorities

Having addressed the question of how hostile drones might be countered, policymakers must confront the question of whether current law permits law enforcement agencies to engage in CUAS operations. A number of agencies have equities in the counter-drone space, but few have unquestionable authority to interdict drone operations, owing to a plethora of existing laws and regulations that restrict when and how hostile drones may be combatted.

Agencies with Existing Authorities

Department of Defense. In addition to its whole range of military responsibilities outside the U.S., the DOD is responsible for defending its military installations and assets at home. The DOD and the Department of Energy (DOE) are the only federal agencies empowered by statute to counter hostile drones and are obligated to do so in consultation with the Secretary of Transportation. In the 2017 NDAA, Congress included two sections that allow the DOD and DOE to "[u]se reasonable force to disable, damage, or destroy the unmanned aircraft system or unmanned aircraft," as well as undertake other actions such as disrupting a drone's command link or taking control of the aircraft. Congress expanded this authority in the 2018 NDAA, "[n]otwithstanding section 46502 of title 49, or any provision of title 18"—code sections that deal with, among other things, aircraft piracy, the damaging or destruction of an aircraft, and interfering with certain types of communications.[71] The DOD can exercise this authority at any facility related to:

> (i) nuclear deterrence, including with respect to nuclear command and control, integrated tactical warning and attack assessment, and continuity of government;
>
> (ii) missile defense;
>
> (iii) national security space;
>
> (iv) assistance in protecting the President or the Vice President (or other officer immediately next in order of succession to the office of the President) pursuant to the Presidential Protection Assistance Act of 1976 (18 U.S. Code 3056 note);
>
> (v) air defense of the United States, including air sovereignty, ground-based air defense, and the National Capital Region integrated air defense system;
>
> (vi) combat support agencies (as defined in paragraphs (1) through (4) of section 193(f) of this title);
>
> (vii) special operations activities specified in paragraphs (1) through (9) of section 167(k) of this title;
>
> (viii) production, storage, transportation, or decommissioning of high-yield explosive munitions, by the Department; or
>
> (ix) a Major Range and Test Facility Base (as defined in section 196(i) of this title).[72]

Based on such authorization the DOD has issued classified guidance allowing the military to shoot down potentially hostile drones to protect "its installations, its aviation and its people."[73] This authority has limitations and does not cover all military installations, leaving some military facilities without authority to counter a hostile drone. Though some military officials might act in a moment of impending attack, the lack of clear authority and dedicated CUAS systems will leave parts of the DOD woefully unprotected.[74] The DOD needs the ability to protect its personnel, equipment, and facilities, and Congress should expand its authorities to allow this.

Department of Energy. The DOE's national security missions include defense of nuclear facilities, materials, and technologies,[75] as well as broader protection of the energy sector and electric grid. The DOE possesses identical authority as the DOD to "use reasonable force" against a UAV over any facility designed "to store or use special nuclear material,"[76] defined in law as grades of uranium or plutonium useable for fuel in nuclear reactors.[77] However, the Secretary of Energy lacks the authority required to protect its personnel and its full range of facilities, and Congress should expand its authorities to allow this.

Department of Homeland Security. DHS takes a leading role in various homeland security, immigration, and counterterrorism missions. It oversees the protection of U.S. critical infrastructure in conjunction with other departments and agencies such as the Departments of Energy, Defense, Transportation, Health and Human Services, Agriculture, and Treasury, as well as the Environmental Protection Agency and the General Service Administration.[78] Though charged with various security and immigration duties, nowhere in statute does DHS have the explicit authority to use force or electronic means to combat an unmanned aircraft.

While several DHS components, such as the Coast Guard or Customs and Border Protection, have authorities that could be construed as allowing them to use force against a drone, and DHS officers would likely act to defeat a hostile drone if necessary, even without explicit authority,[79] Elaine Duke testified before the Senate Homeland Security and Governance Affairs Committee that "we lack the authorities needed to counter threats from unmanned aerial systems (UAS). We know that terrorists are using drones to conduct aerial attacks in conflict zones, and already we have seen aspiring terrorists attempt to use them in external operations. Yet DHS and many other departments and agencies do not have the appropriate legal authorities to engage and mitigate these threats in the way we should."[80] Responding to a question from Senator John Hoeven (R–ND), Secretary Duke testified specifically that DHS lacked "the ability to interdict[,] if you will, the signals" of a potentially hostile drone and further stated that "because it's a new threat, the specific authorities to monitor these drones does not exist generally."[81]

Department of Justice. There are abundant federal statutes and regulations that may conceivably apply to drone operations, ranging from the federal criminal statutes and civil rights laws to anti-hacking and privacy laws. But none apparently grant the Bureau of Prisons or the other law enforcement agencies within the DOJ—the Federal Bureau of Investigations, the U.S. Marshals, the Drug Enforcement Administration, and the Bureau of Alcohol, Tobacco, Firearms, and Explosives—an exemption from otherwise applicable laws that restrict hostile drone interdiction. And it is unclear which, if any, technologies are most appropriate for implementation in law enforcement CUAS activities.[82]

Some hope that current Justice Department policies and U.S. Supreme Court case law would shield from liability any law enforcement officer who did have to act to protect himself and the public by interdicting a hostile drone, provided he did so in an objectively reasonable manner. But current law does not provide adequate certainty to ensure appropriate CUAS actions are taken if and when necessary. Congress must provide appropriate CUAS authorities for federal law enforcement agencies.[83]

Federal Communications Commission (FCC). The Federal Communications Commission is an independent agency that regulates the nation's interstate cable, radio, satellite, television, and wire communications infrastructure. Several federal laws and regulations prohibit operating, marketing, or selling signal "jamming" devices that have been recognized as potential CUAS tools because they interfere with cellular communications, radar, global positioning systems, and wireless networking services.[84]

Current law allows the U.S. government "or any agency thereof," to use such devices and systems which "shall be developed, procured, or otherwise acquired...under United States Government criteria, standards, or specifications designed to achieve the objectives of reducing interference to radio reception and to home electronic equipment and systems, taking into account the unique needs of national defense and security."[85] Federal law also authorizes the government to seize unlawful equipment.[86] The FCC should work with Congress to determine the scope of CUAS jamming regulations for law enforcement.

Federal Aviation Administration. The Federal Aviation Administration, part of the Department of Transportation, regulates aircraft operations in the National Airspace System (NAS), including drone

operations, to protect persons and property in the sky and on the ground, and to promote safe, efficient air commerce and national security.[87] The FAA is authorized to take civil enforcement action against persons who violate Part 107 rules that govern visual-line-of-sight drone operations; the federal rules for recreational operations; and against anyone operating drones in a reckless manner that endangers the integrity of the NAS or another person's life or property.[88] The FAA may also enforce, at times in conjunction with the DOJ, federal drone registration requirements.[89]

The FAA has taken a pragmatic approach to drone enforcement. It is responsible for enforcing FARs applicable to UAS. The FAA "recognizes though that State and local Law Enforcement Agencies (LEA) are often in the best position to deter, detect, immediately investigate, and, as appropriate, pursue enforcement actions to stop unauthorized or unsafe UAS operations."[90] Given that dynamic, many of the same authorities that will be granted to agencies at the federal level should also migrate to the state and local level.

Perhaps the most critical role played by the FAA in the CUAS context will be its responsibility to set and enforce flight restrictions designed to protect special events and sensitive operations such as the Super Bowl, certain law enforcement activities, and presidential movement.[91] These flight restrictions also apply to UAS, and in recent months the agency has established a series of "no drone zones" around national monuments and other sites. These restrictions may serve as the core of future CUAS activities, defining the regions within which only authorized drone traffic will be permitted.

State and Local Law Enforcement

Due to the dramatic growth in drone operations, state and local law enforcement will eventually bear the brunt of unlawful drone operations for the same reason that so many of society's other problems fall on state and local police: They are the front line of government. This is no different in the context of UAS. State and local law enforcement agencies are already responsible for enforcing state criminal laws that apply to drone operations.[92] They are typically the first government agencies to engage major threats to public safety.[93] A number of major police departments have developed counterterrorism units that work with federal agencies.[94] And every state has a clear interest in protecting its own critical infrastructure and residents.[95]

The FAA has issued guidelines to state and local police, both to aid them as well as to seek their help in the following key UAS-related areas: identifying and interviewing unlawful operators and witnesses of unlawful operations; observing and recording the facts of unlawful operations; collecting evidence of unlawful operations, including photo and video information; understanding the location and purpose of temporary flight restrictions; and notifying the nearest FAA Regional Operation Center of any suspected violation of federal law.[96] This list of requests reflects the fact that, when the average person observes what he suspects to be a hostile drone, his natural response is to call the local police rather than a federal regulatory or law enforcement agency.

Thus, while it is first necessary to develop CUAS authorities and capabilities for federal military, national security, and law enforcement agencies, the role of non-federal law enforcement in responding to terrorist and criminal threats must be addressed.[97] As the government increases federal agency authorities for countering hostile drones, it must recognize that much of the burden for enforcement will fall to the state and local levels, who also need CUAS authority, as well as access to equipment and training as resources become available.

Legal Barriers to CUAS Operations

As discussed above, there are several federal legal obstacles to CUAS operations. They include the following:

- 18 U.S. Code § 32: Prohibits damaging or destroying an aircraft.
- 18 U.S. Code § 1362: Prohibits willful or malicious interference with U.S. government communications.
- 18 U.S. Code § 1367(a): Prohibits intentional or malicious interference with satellite communications.
- Title 47: Requires radio transmitter operators to be licensed or authorized;[98] prohibits willful interference with radio communications of any station licensed, authorized, or operated by the U.S. government;[99] and prohibits using or generally dealing in (except by the U.S. government[100]) any signal "jamming" devices.[101]

- 49 U.S. Code § 46502: Prohibits "seizing or exercising control of an aircraft...by force, violence, threat of force or violence, or any form of intimidation, and with wrongful intent."[102]

- The Computer Fraud and Abuse Act:[103] Creates a long list of crimes prohibiting conduct that affects a computer that is "used in or affecting interstate or foreign commerce,"[104] including threatening to damage a computer with the intent to extort anything of value;[105] "knowingly caus[ing] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caus[ing] damage without authorization";[106] unauthorized access with intent to defraud[107] or in combination with destroying, damaging, or altering information;[108] and trafficking in "any password or similar information."[109]

- The Wiretap Act: Prohibits the use of "any electronic, mechanical, or other device" to intentionally intercept, attempt, or have someone else intercept the contents of an electronic, wire, or oral communication; disclosing (or attempting to disclose) the contents of any such communication obtained by unlawful interception; and intentionally using or attempting to use the contents of any such communication.[110] Additional federal privacy laws and regulations may relate to drone surveillance.[111]

- The Pen Register Act: Generally prohibits the installation or use, without a court order,[112] of pen registers—including any device that "records or decodes" signaling and other information transmitted by electronic communications—or a trap and trace device, including any device capable of identifying information that reveals the source of an electronic communication by capturing an incoming impulse.[113]

- Aviation regulations: For example, 14 CFR § 107.12 and § 107.19(a) require anyone controlling a drone to be the designated pilot in command with a remote pilot certificate, or a person under his or her immediate supervision, raising the possibility that a CUAS operator would also have to be licensed remote pilot.

To overcome these and other restrictions scattered throughout the United States Code and the Code of Federal Regulations, Congress should build upon and expand its prior, limited grants of CUAS authority to the DOD and DOE in the NDAAs of 2017 and 2018. As mentioned previously, the NDAA of 2018 afforded DOD officials limited CUAS authorities "[n]otwithstanding section 46502 of title 49, or any provision of title 18."[114] While this approach may serve as a model, as presently enacted it is inadequate for the task at hand and will need to be expanded in two ways.

First, the list of agencies with CUAS authority should grow beyond the DOD and DOE to include the DOJ and DHS, and other federal law enforcement agencies. Second, these agencies will require broader authority to acquire and use CUAS technologies to:

- Protect national security and public safety,

- Defend airspace above and around federal sites and facilities,

- Safeguard manned aviation,

- Police U.S. borders,

- Enforce flight restrictions,

- Support law enforcement activities, and

- Further other federal interests as may be necessary.

The authority to use CUAS should be granted notwithstanding all identified legal barriers to CUAS operations. In this way, Congress could, with a single legislative act, provide the necessary statutory exemptions for military and federal law enforcement agencies to begin employing the full range of CUAS technologies now being developed.

Simultaneously, Congress could also lay the groundwork for the eventual broadening of CUAS technologies to state and local law enforcement agencies—a necessary development—by establishing a program to pilot the deployment of CUAS platforms to select state and local agencies—after federal agencies develop the necessary rules and regulations. A potentially valuable model for accomplishing this may be drawn from the Department of Homeland Security's existing "287(g) program."[115] The 287(g) program authorizes the Director of Immigration and

Customs Enforcement to enter into agreements with state and local law enforcement organizations to deputize designated officers to permit them to aid in enforcement of federal immigration laws. Local law enforcement officers acting in a 287(g) capacity are "subject to the direction and supervision" of federal immigration officials and are "considered to be acting under color of Federal authority."[116]

To enter into a 287(g) agreement, state or local law enforcement organizations sign a memorandum of agreement with the DHS to define "the scope and limitations of the delegation of authority."[117] Officers that are selected to participate in the 287(g) program must attend a four-week training program and a one-week refresher course every two years. Delegated authority, subject to federal training and supervision, would allow for the early rollout of CUAS technologies beyond the federal government, balancing the need to expand CUAS capabilities with the need to provide expertise and supervision to ensure these capabilities are properly used.

Recommendations

To facilitate the broad adoption and use of beneficial UAS technology, policymakers must take steps to allow the development and deployment of effective CUAS platforms able to guard against the dangers posed by reckless or malicious drone users. To accomplish this goal, Congress should take the following steps:

- **Provide appropriate federal agencies with CUAS authority.** While some agencies have explicit CUAS authority, others do not, and in fact appear to be barred by law from engaging in some CUAS functions. While it is likely that some security personnel would act to neutralize a hostile drone without explicit authority, the status quo is confusing and could lead to inaction, inconsistent responses, unpreparedness, or harmful unintended consequences. To rectify this, Congress should build upon the approach already undertaken in the NDAAs of 2017 and 2018, and do the following:

  1. Grant authority to the heads of the DOD, DOE, DHS, DOJ, and DOT to identify appropriate federal assets and other facilities within their jurisdictions which are in need of CUAS capabilities, prioritizing the highest-value installations.
  2. Require the DOT to impose appropriate UAS flight restrictions around these protected assets and facilities, if no such restrictions have been imposed.[118]
  3. Authorize federal law enforcement and national security agencies, notwithstanding all identified legal barriers to CUAS activities,[119] to utilize CUAS platforms to enforce established flight restrictions. CUAS operators must have authority to engage in the following actions:
     - Detect, identify, monitor, and track UAS, including by intercepting communications or sensors designed to locate and identify drones;
     - Provide a warning to the UAS operator, whether by means of UTM or other methods; and
     - By kinetic or nonkinetic means, disrupt, disable, seize control of, or destroy UAS deemed a threat by the CUAS operator.
- **Provide appropriate exemptions to private firms developing CUAS technologies.** The development of effective CUAS capabilities will require substantial research and development by private-sector actors—activity that could be chilled by statutory and regulatory prohibitions on the manufacture, marketing, or sale of critical CUAS components, such as jamming technology, to non-U.S. government agencies.[120] Congress should provide CUAS developers with appropriate exemptions, so as to facilitate innovation and eventual adoption by state and local law enforcement agencies. To the extent necessary, specific DOD ranges and experimental facilities should be leveraged to accomplish this goal.
- **Develop and promulgate "rules of engagement" and other CUAS regulations.** Congress should condition the use of CUAS platforms on the prompt completion of preliminary departmental policies governing their use. These initial policies should be designed to facilitate testing of CUAS platforms and rules of engagement, to inform the development of final departmental policies and rules of engagement for federal

CUAS operators, as well as related regulations. Congress should provide a reasonable statutory deadline for the promulgation of these rules. After that deadline, the authority to use CUAS would expire unless and until final policies governing CUAS operations are promulgated. CUAS policies should be designed to ensure prompt, predictable, and consistent use of the technology while minimizing the risk of collateral damage and interference with spectrum used for navigation and communication. Given the diverse missions of federal national security and law enforcement agencies, each should be allowed to develop, in consultation with the others, its own set of CUAS rules and regulations, with an emphasis placed on developing rules that are compatible and consistent.

- **Codify safeguards for civil liberties.** The civil liberties enshrined in the U.S. Constitution and Bill of Rights, and expanded through statutes and case law, are another major factor for developing CUAS authority,[121] particularly with regards to seizing, commandeering, or destroying a UAS. Law enforcement agencies should establish departmental policies for those uses of CUAS tools.[122] Current NDAA language and police department drone use policies[123] provide useful starting points for developing CUAS policy that leverages the benefits of technology while protecting civil liberties. While law enforcement officers may interdict a UAS that they have probable cause to suspect is in violation of law, CUAS policies should emphasize that when public safety concerns require law enforcement officers to seize, commandeer, or destroy a drone, whenever possible they should notify the operator of an impending violation of law and provide some meaningful opportunity for the operator to respond appropriately (such as by changing course or lowering to the ground) prior to interdiction. Policymakers should address the question of notice requirements in the event that a UAS is not remote-ID-capable. [124]

- **Create a CUAS pilot program.** Many large public events and critical infrastructure facilities beyond federal installations will need protection from drone-based attacks. Congress should create a pilot program modelled after the 287(g) program, which would allow the DHS to enter into agreements with state and local law enforcement agencies to train and deputize particular officers to fulfill CUAS responsibilities under the direction of federal authorities. The pilot program should start after the completion and promulgation of CUAS regulations and rules by the Department of Homeland Security, and all program participants would be subject to these regulations. The pilot program should require the DHS to enter into agreements with a variety of different local partners, using an array of approved technologies at diverse venues and facilities.

- **Use best practices and lessons to broaden the pilot into a national program.** Upon the conclusion of this pilot program, the DHS, in consultation with the FAA and DOJ, should issue a report documenting the findings of the pilot and the best path forward for CUAS authorities and technologies to be made more widely available to law enforcement and critical infrastructure operators. This report must answer several critical questions regarding the future of CUAS authorities and use:

  1. Is the delegated-authority model the correct model for a nationwide expansion of the program?

  2. Using a risk-based analysis, what types of critical infrastructure and other facilities are most likely to need CUAS defenses? Should different types of facilities be limited to certain types of CUAS? And how should CUAS operators and platforms communicate with each other?

  3. Should non–law enforcement authorities, such as the operators of critical infrastructure, be allowed to operate CUAS? If so, what limitations and requirements should be placed on them? If not, how can CUAS capabilities be extended to such facilities?

- **Provide funds for CUAS deployment and training.** Federal agencies responsible for the security of government installations should acquire appropriate CUAS systems. A portion of the Homeland Security Grant Program should be redirected to provide moderate grants to local agencies participating in the pilot program to support the acquisition of CUAS technologies, though

Congress should limit the number and monetary value of such grants. Other grant programs, such as the Justice Department's Byrne JAG program,[125] should also be leveraged to support the CUAS pilot. Additionally, Congress should be prepared to allocate funds for the establishment of a law enforcement training program for state and local law enforcement to develop competencies in the use of CUAS systems upon the completion of the pilot program.

- **Require broad adoption of UTM capabilities for drones in the NAS.** A broad capability to remotely identify, track, and manage the flight paths of UAS operating in the NAS is required to effectively address safety and security concerns, as well as to aid CUAS operators in discerning hostile from non-hostile UAS. Congress should require the FAA to promptly promulgate a final rule on remote identification and tracking, as well as the development of industry standards to permit CUAS platforms to interface with remote ID and UTM networks to provide UAS pilots with notice prior to interdiction. The development and deployment of robust UTM systems should be prioritized and expedited. Congress should require all drones capable of posing a substantial risk to people or property to be remote-ID and UTM-compliant.[126]

- **Ensure model aircraft are covered by UTM regulations.** Section 336 of the 2012 FAA Modernization and Reform Act, the "Special Rule for Model Aircraft," shields many recreational UAS operators from additional FAA regulation. Congress should amend this section to allow the application of the FAA's forthcoming final rule on remote identification and tracking, as well as future UTM regulations, to be broadly and retroactively imposed on drone operators.

Conclusion: Drones and the Friendly Skies

Drones are increasingly providing significant benefits and services, ranging from lifesaving search-and-rescue functions to recreational sports videography to emerging commercial package delivery. Unfortunately, human creativity is not limited to legal or constructive purposes. While nation states were the first to use drones as tools of warfare, terrorists and criminals are now exploiting the growing capabilities of consumer-grade devices for their own nefarious purposes. The U.S. government must be prepared to counter hostile drones from these and other bad actors by unleashing the power of the private sector to develop a range of different CUAS technologies. Federal law enforcement and security officials must be trained in the use of CUAS, with these capabilities and training also spreading to state and local law enforcement.

Facing the threat posed by hostile UAS does not require extreme restrictions on lawful personal or commercial drone use, but instead requires dedication by all levels of government to encourage the development, acquisition, and proper use of CUAS. Such dedication will ensure the skies remain a vibrant and secure domain for recreation, travel, and commerce.

*—**Jason Snead** is Senior Policy Analyst in the Edwin Meese III Center for Legal and Judicial Studies, of the Institute for Constitutional Government, at The Heritage Foundation. **John-Michael Seibler** is Legal Fellow in the Meese Center. **David Inserra** is Policy Analyst for Homeland Security and Cyber Policy in the Douglas and Sarah Allison Center for Foreign Policy, of the Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy, at The Heritage Foundation.*

Endnotes

1 Jason Snead, "Drone Rescues Help Show It's Time to Let Revolutionary Aircraft Soar," Heritage Foundation *Commentary*, January 23, 2018, https://www.heritage.org/technology/commentary/drone-rescues-help-show-its-time-let-revolutionary-aircraft-soar. Drones have, among other things, been used for disaster relief and recovery; to deliver critical medical supplies (such as Zipline's use of drones to deliver medical supplies throughout Rwanda); and to rescue swimmers stranded offshore. Other uses and potential future uses include widespread package delivery systems, search-and-rescue operations, law enforcement functions, and infrastructure inspection. See William O. Ball, "Unmanned Aircraft Systems: Emerging Uses in a Changing National Airspace," testimony before the Subcommittee on Aviation, Committee on Transportation and Infrastructure, U.S. House of Representatives, November 29, 2017, https://transportation.house.gov/uploadedfiles/2017-11-29_-_ball_testimony.pdf (accessed March 30, 2018).

2 Michael D. Shear and Michael S. Schmidt, "House Drone Crash Described as a U.S. Worker's Drunken Lark," *The New York Times*, January 27, 2015, https://nyti.ms/2qdNjov (accessed March 29, 2018).

3 Steven Stalinsky and R. Sosnow, "A Decade of Jihadi Organizations' Use of Drones—From Early Experiments by Hizbullah, Hamas, and Al-Qaeda to Emerging National Security Crisis for the West as ISIS Launches First Attack Drones," The Middle East Media Research Institute *Inquiry & Analysis Series*, No. 1300, February 21, 2017, https://www.memri.org/reports/decade-jihadi-organizations-use-drones---early-experiments-hizbullah-hamas-and-al-qaeda (accessed March 29, 2018).

4 Ibid., and Joby Warrick, "Use of Weaponized Drones by ISIS Spurs Terrorism Fears," *The Washington Post*, February 21, 2017, https://wapo.st/2qdMYCf (accessed March 29, 2018).

5 Stalinsky and Sosnow, "A Decade of Jihadi Organizations' Use of Drones."

6 Don Rassler, Muhammad al-`Ubaydi, and Vera Mironova, "The Islamic State's Drone Documents: Management, Acquisitions, and DIY Tradecraft," Combating Terrorism Center at West Point, January 31, 2017, https://ctc.usma.edu/ctc-perspectives-the-islamic-states-drone-documents-management-acquisitions-and-diy-tradecraft (accessed March 29, 2018).

7 Robert Windrem, "U.S. Fears New Threat From ISIS Drones," NBC News, May 24, 2017, https://www.nbcnews.com/storyline/isis-terror/u-s-fears-new-threat-isis-drones-n764246 (accessed March 29, 2018).

8 Patrick Tucker, "Counter-Terror Chief: Expect Terrorist Drone Swarms 'Soon,'" *Defense One*, February 27, 2017, http://www.defenseone.com/technology/2017/02/counter-terror-chief-expect-terrorist-drone-swarms-soon/135736/ (accessed March 29, 2018).

9 "Homeland Security Threats," C-SPAN video, September 27, 2017, at (1:16:20), https://www.c-span.org/video/?434411-1/senior-officials-testify-homeland-security-threats&start=4705 (accessed March 30, 2018). Then-acting Secretary of Homeland Security Elaine Duke and National Counter Terrorism Center Director Nicholas Rasmussen also expressed similar concerns and stressed the need to work across government and with Congress to improve the U.S.'s ability to defend against terrorist attacks with UAS.

10 Shear and Schmidt, "House Drone Crash Described as a U.S. Worker's Drunken Lark."

11 Federal Bureau of Investigation, "Man Sentenced in Boston for Plotting Attack on Pentagon and U.S. Capitol and Attempting to Provide Detonation Devices to Terrorists," November 1, 2012, https://archives.fbi.gov/archives/boston/press-releases/2012/man-sentenced-in-boston-for-plotting-attack-on-pentagon-and-u.s.-capitol-and-attempting-to-provide-detonation-devices-to-terrorists (accessed March 29, 2018).

12 Don Rassler, "Remotely Piloted Innovation: Terrorism, Drones, and Supportive Technology," Combating Terrorism Center at West Point, October 2016, https://ctc.usma.edu/app/uploads/2016/10/Drones-Report.pdf (accessed March 29, 2018), and U.S. Department of Homeland Security, "National Terrorism Advisory System Bulletin," November 9, 2017, https://www.dhs.gov/sites/default/files/ntas/alerts/17_1109_NTAS_Bulletin.pdf (accessed March 29, 2018).

13 David Kravets, "Man Lands Drone Carrying Radioactive Sand on Japanese Prime Minister's Office," *Ars Technica*, April 25, 2015, https://arstechnica.com/tech-policy/2015/04/man-arrested-for-flying-drone-carrying-radioactive-sand-in-tokyo/ (accessed March 29, 2018).

14 Cahal Milmo, "Drone Terror Attack by Jihadists in Britain is 'Only a Matter of Time,' Security Sources Warn," *iNews*, September 8, 2017, https://inews.co.uk/news/uk/drone-terror-attack-jihadists-britain-matter-time-security-sources-warn/ (accessed March 29, 2018), and Lori Hinnant, "EU Threats: Drones, Frustrated Jihadis, Returning Fighters," Associated Press, June 5, 2017, https://www.apnews.com/a90f201a2b62497fa6469c36e99dafc3/EU-threats:-Drones,-frustrated-jihadis,-returning-fighters (accessed March 29, 2018).

15 David Barrett, "Burglars Use Drone Helicopters to Target Homes," *The Telegraph*, May 18, 2015, https://www.telegraph.co.uk/news/uknews/crime/11613568/Burglars-use-drone-helicopters-to-identify-targe-homes.html (accessed March 29, 2018).

16 Mario Aguilar, "Clever Crook Uses Heat Vision Drone to Hunt Down Weed and Steal It," *Gizmodo*, April 18, 2014, https://gizmodo.com/clever-crook-uses-a-drone-to-find-weed-so-he-can-steal-1564697853 (accessed March 29, 2018).

17 Marco Margaritoff, "Australian Drug Cartel Used Drone to Spy on Police," *The Drive*, June 30, 2017, http://www.thedrive.com/aerial/12050/australian-drug-cartel-used-drone-to-spy-on-police (accessed March 29, 2018).

18 Cyrus Farivar, "Man Who Built Gun Drone, Flamethrower Drone Argues FAA Can't Regulate Him," *Ars Technica*, June 9, 2016, https://arstechnica.com/tech-policy/2016/06/man-who-built-gun-drone-flamethrower-drone-argues-faa-cant-regulate-him/ (accessed March 29, 2018).

19 ISIS fighters abroad have demonstrated the effectiveness of commercially available UAS as platforms for aerial bombing missions.

20 John-Michael Seibler, "Seattle Case Shows Why Drone Regulation Should Be Local, Not Federal," The Daily Signal, March 9, 2017, http://dailysignal.com/2017/03/09/seattle-case-shows-why-drone-regulation-should-be-local-not-federal/ (accessed March 29, 2018). In that case, the UAS operator, Paul Skinner, was charged and convicted of reckless endangerment. DL Cade, "Man Facing Jail Time for Knocking Woman Unconscious with Drone," *PetaPix*, January 17, 2017, https://petapixel.com/2017/01/17/man-convicted-knocking-woman-unconscious-drone/ (accessed March 29, 2018). Skinner was sentenced to 30 days' imprisonment and given a $500 fine. Joseph Hincks, "A Man Who Accidentally Knocked Someone Out With His Drone Has Been Sent to Jail," *Fortune*, March 1, 2017, http://fortune.com/2017/03/01/seattle-drone-crash-jail-sentence/ (accessed March 29, 2018).

21 Michael S. Rosenwald, "Prisons Try to Stop Drones From Delivering Drugs, Porn, and Cellphones to Inmates," *The Washington Post*, October 13, 2016, https://www.washingtonpost.com/local/prisons-try-to-stop-drones-from-delivering-drugs-porn-and-cellphones-to-inmates/2016/10/12/645fb102-800c-11e6-8d0c-fb6c00c90481_story.html?utm_term=.c66cc724caea (accessed March 29, 2018); Lynh Bui and Matt Zapotosky, "Men Planned to Use Drone to Get Contraband Into Prison, Officials Say," *The Washington Post*, August 24, 2015, https://www.washingtonpost.com/local/crime/two-men-planned-to-use-a-drone-to-get-drugs-and-porn-into-a-prison-md-authorities-say/2015/08/24/c8e38fc2-4a75-11e5-8ab4-c73967a143d3_story.html?utm_term=.2b4f9d421606 (accessed March 29, 2018); and Michael Gerstein, "Drones with Weapons Are Latest Prison Threat," *Detroit News*, August 28, 2017, https://www.detroitnews.com/story/news/politics/2017/08/28/drones-weapons-threat-prisons/105044002/ (accessed March 29, 2018).

22 A British prison captured just such an incident on camera, revealing the ease with which a drone was able to penetrate prison airspace, locate the recipient, and deposit its payload without the inmate ever leaving his cell. "Footage Shows Drone Delivering Drugs to Prisoners," BBC video, May 16, 2016, http://www.bbc.com/news/av/uk-36302136/footage-shows-drone-delivering-drugs-to-prisoners (accessed March 30, 2018). It is ironic, but predictable, that bad actors are the first to enjoy the benefits of personalized drone delivery services.

23 Dominique Debucquoy-Dodley and Greg Botelho, "Authorities Foil Drone-Delivery of Porn, Drugs, and Gun to Maryland Prison," CNN, August 24, 2015, https://www.cnn.com/2015/08/24/us/maryland-prison-drone/index.html (accessed March 29, 2018).

24 Tracy Samilton, interview by Steve Inskeep, "Prisons Work To Keep Out Drug-Smuggling Drones," Morning Addition, National Public Radio, November 15, 2017, https://www.npr.org/2017/11/15/564272346/prisons-work-to-keep-out-drug-smuggling-drones (accessed March 30, 2018).

25 Randy Travis, "Threat From the Sky: 35 Drones Already Spotted at GA Prisons This Year," Fox 5 Atlanta, July 19, 2017, http://www.fox5atlanta.com/news/i-team/threat-from-the-sky-35-drones-already-spotted-at-ga-prisons-this-year (accessed March 29, 2018).

26 Lorenzo Ferrigno, "Ohio Prison Yard Free-For-All After Drone Drops Drugs," CNN, August 5, 2015, https://www.cnn.com/2015/08/04/us/prison-yard-drone-drugs-ohio/index.html (accessed March 29, 2018).

27 "Escaped South Carolina Inmate May Have Used Drone-Delivered Wire Cutters," *The Guardian*, July 8, 2017, https://www.theguardian.com/us-news/2017/jul/08/jimmy-causey-escaped-prisoner-south-carolina-drone (accessed March 30, 2018).

28 Pauline Repard, "In New Tactic, Smugglers Use Drone to Fly Meth over Mexican Border into San Diego, Officials Say," *Los Angeles Times*, August 19, 2017, http://www.latimes.com/local/lanow/la-me-drug-smuggle-drone-20170819-story.html (accessed March 30, 2018).

29 John P. Sullivan and Robert J. Bunker, "Mexican Cartel Strategic Note No. 18: Narcodrones on the Border and Beyond," *Small Wars Journal*, http://smallwarsjournal.com/jrnl/art/mexican-cartel-strategic-note-no-18-narcodrones-on-the-border-and-beyond (accessed March 30, 2018).

30 Stephen Dinan, "Thirteen Drones in Four Days: How Drug Smugglers Are Using Technology to Beat Border Patrol," *The Washington Times*, January 2, 2018, https://www.washingtontimes.com/news/2018/jan/2/drones-fly-drugs-us-no-border-patrol-detection-tec/ (accessed March 30, 2018).

31 Joshua Philipp, "Drug Cartels Are Building Assassin Drones," *The Epoch Times*, October 27, 2017, https://www.theepochtimes.com/drug-cartels-are-building-assassin-drones_2340727.html (accessed March 30, 2018).

32 Patrick Phillips, "Charleston Helicopter Crash Blamed on Drone; FAA Investigating," KMOV, February 15, 2018, http://www.kmov.com/story/37518601/charleston-helicopter-crash-blamed-on-drone-faa-investigating (accessed March 30, 2018). The helicopter had two passengers, a student pilot, and an instructor. Both were unharmed in the incident. The instructor took control upon sighting the UAS—reportedly a "DJI Phantom Quad-Copter," one of the most popular consumer drones on the market—and crashed while attempting a landing.

33 Alan Levin, "Drone Suspected in Helicopter Crash Landing in South Carolina," *Insurance Journal*, February 16, 2018, https://www.insurancejournal.com/news/southeast/2018/02/16/480807.htm (accessed March 30, 2018).

34 The Black Hawk suffered a 1.5-inch dent in one rotor blade, and debris was lodged elsewhere in the helicopter, including a motor from the offending drone, a DJI Phantom 4. Nate Anderson, "Drone Collides With U.S. Army Helicopter, Puts 1.5-Inch Dent in Rotor," *ArsTechnica*, December 29, 2017, https://arstechnica.com/tech-policy/2017/12/drone-collides-with-us-army-helicopter-puts-1-5-dent-in-rotor/ (accessed March 30, 2018). A potential drone collision is also being investigated in Hawaii, involving a tourist helicopter. Rosemarie Bernardo, "Investigators Looking Into Report that Drone Struck Kauai Tour Helicopter," *Honolulu Star Advertiser*, February 13, 2018, http://www.staradvertiser.com/2018/02/13/breaking-news/investigators-looking-into-report-that-drone-struck-kauai-tour-helicopter/ (accessed March 30, 2018).

35 18 U.S. Code § 32.

36 As of this writing, the FAA reported receiving more than 1 million drone-related registrations, including approximately 878,000 hobbyists (who register as individuals and may operate multiple drones) and 122,000 commercial drone registrations, and issuing roughly 70,000 remote-pilot certificates under Part 107. See Dan Elwell, "Statement of Dan Elwell, Deputy Administrator," testimony before the Subcommittee on Aviation, Committee on Transportation and Infrastructure, U.S. House of Representatives, November 29, 2017, https://www.faa.gov/news/testimony/news_story.cfm?newsId=22354&omniRss=testimonyAoc&cid=105_Testimony (accessed April 6, 2018), and Jonathan Vanian, "Drone Registrations Have Soared to Sky-High Milestone," *Fortune*, January 11, 2018, http://fortune.com/2018/01/11/drone-registrations-million-faa/ (accessed April 6, 2018).

37 From January through September 2016, the FAA reported 1,364 drone sightings. UAS sighting data may be downloaded directly from the FAA and were available only through September 2017 as of this writing. U.S. Department of Transportation, Federal Aviation Administration, *UAS Sightings Report*, December 11, 2017, https://www.faa.gov/uas/resources/uas_sightings_report/ (accessed March 30, 2018).

38 The Academy of Model Aeronautics (AMA), the nation's largest recreational flying club, routinely analyzes FAA drone sighting data. Of 1,270 such sightings covering a period from February through September 2016, AMA researchers conclude that "the vast majority of reports are simply sightings of UAS sharing the airspace. Reported near misses and close calls remain very small—just 3.4 percent." "As Drone Sales Soar, Vast Majority of Reports Remain Simple Sightings," Academy of Model Aeronautics, https://www.modelaircraft.org/files/UASSightingsAnalysisbyAMA5-10-17.pdf (accessed March 30, 2018).

39 "Drone Sightings (2014–2017)," Rupprecht Law P.A., https://jrupprechtlaw.com/drone-sightings (accessed March 30, 2018).

40 According to the FAA, small UAS are generally not permitted to fly higher than 400 feet, unless within 400 feet of a structure or having otherwise received a waiver granting permission, nor are they permitted within "Class B, Class C, or Class D airspace or within the lateral boundaries of the surface area of Class E airspace designated for an airport unless that person has prior authorization from Air Traffic Control." 14 CFR § 107.41 (2016). These requirements were set to ensure separation between manned and unmanned aircraft, and to prevent UAS from entering the navigable airspace, which is reserved for manned aviation and begins at 500 feet above ground level in uncongested areas. 14 CFR § 91.119 (2010). The term "navigable airspace" is defined in statute as including all airspace "above the minimum altitudes of flight prescribed by regulations…including airspace needed to ensure safety in the takeoff and landing of aircraft." 49 U.S. Code § 40102 (2012).

41 One such video clearly shows an aircraft operated by Frontier Airlines on final approach to Las Vegas McCarran International Airport, passing directly beneath, and in close proximity to, the drone. Kurt Schlosser, "Drone Video Documents a Disturbingly Close Encounter with Passenger Plane," *GeekWire*, February 2, 2018, https://www.geekwire.com/2018/watch-drone-video-shows-close-call-unmanned-aircraft-passenger-plane/ (accessed March 30, 2018).

42 For the study, the Alliance for System Safety of UAS through Research Excellence (ASSURE) conducted computer simulations of impacts by both quadcopter and fixed-wing drones on aircraft models representing the Boeing 737, Airbus A320, and a smaller Learjet. The study concluded that drones' rigid components are likely to cause more damage to an airframe than a bird strike; that their onboard batteries may survive low-speed collisions, creating a fire hazard; and that mid-size jet engines may suffer significant damage if a drone is ingested. " FAA and ASSURE Announce Results of Air-to-Air Collision Study," Alliance for System Safety of UAS through Research Excellence, November 27, 2017, https://pr.cirlot.com/faa-and-assure-announce-results-of-air-to-air-collision-study/ (accessed March 30, 2018); U.S. Department of Transportation, Federal Aviation Administration, "Researchers Release Report on Drone Airborne Collisions," November 28, 2017, https://www.faa.gov/news/updates/?newsId=89246&omniRss=news_updatesAoc&cid=101_N_U (accessed March 30, 2018); and Matt Schutte, "Study Finds Drones More Damaging Than Bird Strikes to Planes," The Ohio State University, December 6, 2017, https://news.osu.edu/news/2017/12/06/study-finds-drones-more-damaging-than-bird-strikes-to-planes/ (accessed March 30, 2018).

43 U.S. Department of Transportation, Federal Aviation Administration, "Unmanned Aircraft System Traffic Management (UTM)," May 16, 2017, https://www.faa.gov/uas/research/utm/ (accessed April 6, 2018), and National Aeronautics and Space Administration, "Unmanned Aircraft System (UAS) Traffic Management (UTM)," March 5, 2018, https://utm.arc.nasa.gov/index.shtml (accessed April 6, 2018).

44 UTM provides operators with an ability to identify nearby drones and selectively grant or deny access to fly within restricted airspace. For example, airspace above and surrounding an active crime scene could be closed to non–law enforcement drones, allowing authorized UAS and, if necessary, manned aircraft, to operate safely and without intervention.

45 National Aeronautics and Space Administration, "Unmanned Aircraft System (UAS) Traffic Management (UTM)."

46 The FAA is presently developing a rule for remote identification and tracking of drones. U.S. Department of Transportation, Federal Aviation Administration, "FAA Releases UAS Remote Tracking and ID ARC Report," December 19, 2017, https://www.faa.gov/news/updates/?newsId=89404 (accessed April 6, 2018).

47 The first phase of UTM deployment is already underway. Through the Low Altitude Authorization and Notification Capability (LAANC), UAS operators can request and receive automated approval to fly in airspace near some of the nation's major airports. To accomplish this, the FAA has designated select controlled airspace, up to certain altitudes, within which drone flights can be pre-approved. Through LAANC, UAS operators provide specifics regarding their flight, and then generally receive nearly instantaneous permission to fly within the approved airspace. The FAA is presently developing a rule for remote identification and tracking of drones. U.S. Department of Transportation, Federal Aviation Administration, "FAA Facilities Participating in LAANC Initial Prototype Evaluation," December 21, 2017, https://www.faa.gov/uas/programs_partnerships/uas_data_exchange/airports_participating_in_laanc/ (accessed April 6, 2018), and Gregory S. McNeal, "Automated ATC Authorization for Drone Flights Will Occur at These 50 Airports This Fall," *Forbes*, July 19, 2017, https://www.forbes.com/sites/gregorymcneal/2017/07/19/automated-atc-authorization-for-drone-flights-will-occur-at-these-50-airports-this-fall/#1e7fbd0bfb77 (accessed April 6, 2018).

48 As the remote-ID Aviation Rulemaking Committee reported, not all drones will be physically capable of supporting remote-ID equipment owing to size, weight, and power requirements. Most drones that fall into this category will likely be relatively small devices with limited ranges and insignificant payload capacities. Prior FAA work surrounding the recreational drone-owners' registration requirement determined that drones weighing less than 0.55 pounds posed a low risk to people or property on the ground. U.S. Department of Transportation, Federal Aviation Administration, "Unmanned Aircraft Systems (UAS) Registration Task Force (RTF) Aviation Rulemaking Committee (ARC) Task Force Recommendations Final Report," November 21, 2015, https://www.faa.gov/regulations_policies/rulemaking/committees/documents/media/UASRTFARC-102015.pdf (accessed April 6, 2018).

49 Though the missile succeeded in finding and destroying its target, the solution can hardly be considered cost-effective given the price disparities between quadcopters and anti-aircraft missiles. Derek Hawkins, "A U.S. 'Ally' Fired a $3 Million Patriot Missile at a $200 drone. Spoiler: The Missile Won," *The Washington Post*, March 17, 2017, https://www.washingtonpost.com/news/morning-mix/wp/2017/03/17/a-u-s-ally-fired-a-3-million-patriot-missile-at-a-200-drone-spoiler-the-missile-won/?utm_term=.0e7c3412ed22 (accessed March 30, 2018).

50 David Reid, "A Swarm of Armed Drones Attacked a Russian Military Base in Syria," CNBC, January 11, 2018, https://www.cnbc.com/2018/01/11/swarm-of-armed-diy-drones-attacks-russian-military-base-in-syria.html (accessed March 30, 2018). Following the assault, the Russian Ministry of Defense claimed the base's Pantsir-S anti-aircraft missile systems had successfully destroyed seven of the attacking UAS, while electronic warfare units seized remote control of six others. Tyler Rogoway, "Russia Says January 5th Attack on its Syrian Air Base Was by a Swarm of Drones," *The Drive*, January 8, 2018, http://www.thedrive.com/the-war-zone/17493/russia-says-january-5th-attack-on-its-syrian-air-base-was-by-a-swarm-of-drones (accessed March 30, 2018).

51 Lt. Col. Thomas Palmer, "Defeating Small Civilian Unmanned Aerial Systems to Maintain Air Superiority," *Air and Space Power Journal*, Vol. 31, No. 2 (2017), p. 102. One such project, the Mobile Low, Slow Unmanned Aerial Vehicle Integrated Defense Systems (MLIDS), developed by Leonardo DRS, uses two Mine Resistant Ambush Protected vehicles (MATVs) to mount two halves of the MLIDS counter-drone system. The first vehicle mounts an electro-optical/infrared camera to track incoming targets and uses an electronic warfare system to jam the drone. The second uses radar tracking systems and offers kinetic countermeasures that include mounted weapons and drones designed to fly out and engage targets at a distance. Valerie Insinna, "Army to Test Counter-Drone MATV Upgrade in Combat Next Year," C4ISRNET, October 9, 2017, https://www.c4isrnet.com/digital-show-dailies/ausa/2017/10/09/army-to-test-counter-drone-mat-v-upgrade-in-combat-next-year/ (accessed March 30, 2018).

52 U.S. Department of Transportation, Federal Aviation Administration, "Letter to Airport Sponsors," October 26, 2016, https://www.faa.gov/airports/airport_safety/media/UAS-Counter-Measure-Testing-letter.pdf (accessed March 30, 2018).

53 Michael S. Schmidt and Michael D. Shear, "Drones Spotted, But Not Halted, Raise Concerns," *The New York Times*, January 29, 2015, https://www.nytimes.com/2015/01/30/us/for-super-bowl-and-big-games-drone-flyovers-are-rising-concern.html (accessed March 30, 2018).

54 Seven UAS Test Sites are operated nationwide and were initially set up to facilitate the FAA's mandate to integrate UAS into the NAS by offering operators a place to test their drone designs. U.S. Department of Transportation, Federal Aviation Administration, "UAS Test Sites," September 29, 2017, https://www.faa.gov/uas/research/test_sites/ (accessed March 30, 2018).

55 "Grand Sky to Anchor Counter UAS Task Force," Grand Sky, May 31, 2017, http://grandskynd.com/news/grand-sky-anchor-counter-uas-task-force/ (accessed March 30, 2018).

56 John Knowles, "A Sampling of Counter-UAS Systems," *Journal of Electronic Defense*, Vol. 40, No. 9 (2017), p. 37.

57 The FAA is presently developing a rule for remote identification and tracking of drones. Federal Aviation Administration, "FAA Releases UAS Remote Tracking and ID ARC Report." Because this rule is still in development, drone detection systems presently in development all rely on their own sensors. However, in the future it is unquestionable that Internet-based systems similar to today's flight tracking services will emerge, which will offer users an ability to see all remote-ID-compliant drones in their vicinity. Such a system could be sufficient for addressing most property owners' concerns surrounding drone trespass or invasion of privacy by facilitating easy identification of the responsible parties.

58 For example, detecting a drone operating in airspace above a sensitive corporate facility, possibly for the purposes of industrial espionage. Once detected, the property owners may then contact law enforcement officials, who would be responsible for seizing or using force against a drone. Similarly, law enforcement agencies may be able to use remote-ID data to identify aerial trespassers reported by private-property owners, or operators who intrude upon people's' privacy.

59 Innovators have developed both fixed and mobile CUAS systems which provide comprehensive coverage for a given area. Man-portable devices, such as a portable drone jammer, have also been designed that would permit individual agents or officers to take action against a drone in an area where a more comprehensive CUAS system may be unavailable.

60 Federal Aviation Administration, "FAA Releases UAS Remote Tracking and ID ARC Report." The FAA's UAS Identification and Tracking ARC recommends the consideration of two distinct methods for accomplishing remote identification of a drone: "direct broadcast," whereby drone location and identifying information are transmitted and available to be "received by anyone within broadcast range," or "network publishing," which calls for drones to send this information to "an internet service or federation of services." U.S. Department of Transportation, Federal Aviation Administration, *UAS Identification and Tracking (UAS ID) Aviation Rulemaking Committee (ARC): ARC Recommendations Final Report*, September 30, 2017, http://www.faa.gov/regulations_policies/rulemaking/committees/documents/media/UAS%20ID%20ARC%20Final%20Report%20with%20Appendices.pdf (accessed March 30, 2018).

61 Rosenwald, "Prisons Try to Stop Drones from Delivering Drugs," and "Company's Mobile Acoustic Sensing and Electronic Attack Innovations Detect and Defeat Emerging Threats in Complex Scenarios," Northrop Grumman, October 4, 2016, https://news.northropgrumman.com/news/releases/northrop-grumman-demonstrates-counter-uas-technologies-at-black-dart-exercise (accessed March 30, 2018).

62 Rosenwald, "Prisons Try to Stop Drones from Delivering Drugs."

63 Asif Anwar, "Countering the UAS Challenge," *Microwave Journal*, Vol. 60, No. 11 (2017). A number of private-sector developers are working to bring CUAS capabilities to market. "The Counter UAS Directory," Unmanned Airspace, April 2018, http://www.unmannedairspace.info/wp-content/uploads/2018/04/Counter-UAS-directory.-April-2018.-v1.pdf (accessed April 6, 2018).

64 Many consumer models of drones feature a "return-to-home" failsafe that triggers when a control signal is disrupted, and automatically flies a drone back to a preprogrammed point—theoretically a drone's launching pilot. GPS jamming may be necessary in the event the drone is flying autonomously along a preprogrammed course rather than under the direct control of a remote pilot. "FAA Selects British Counter-UAV Technology for U.S. Airport Trials," UAS Vision, June 3, 2016, http://www.uasvision.com/2016/06/03/faa-selects-british-counter-uav-technology-for-us-airport-trials/ (accessed March 30, 2018).

65 Caroline Rees, "Lockheed Martin Develops Counter-UAS Laser Weapon," Unmanned Systems Technology, September 21, 2017, http://www.unmannedsystemstechnology.com/2017/09/lockheed-martin-develops-counter-uas-laser-weapon/ (accessed March 30, 2018).

66 Palmer, "Defeating Small Civilian Unmanned Aerial Systems."

67 Rees, "Lockheed Martin Develops Counter-UAS Laser Weapon."

68 One such device disrupts the accelerometers and gyroscopes used by drones to maintain stable flight, essentially making a drone dizzy. Paul Wagenseil, "Sonic Weapon Knocks Drones Right Out of the Sky," *Fox News*, July 31, 2017, http://www.foxnews.com/tech/2017/07/31/sonic-weapon-knocks-drones-right-out-sky.html (accessed March 30, 2018).

69 Knowles, "A Sampling of Counter-UAS Systems." Each of the proposed technologies has its own set of trade-offs and risks. Shooting down a drone, for example, creates a danger from falling debris. The use of jamming equipment in populated areas risks disrupting nearby wireless communications. For example, one truck driver who installed an illicit GPS jamming device on his truck inadvertently disrupted operations at the Newark airport simply by driving by the facility. Chris Matyszczyk, "Truck Driver Has GPS Jammer, Accidentally Jams Newark Airport," CNET, August 11, 2013, https://www.cnet.com/news/truck-driver-has-gps-jammer-accidentally-jams-newark-airport/ (accessed April 10, 2018).

70 For example, using a jammer to disrupt a control signal will not stop a drone operating autonomously; disrupting a GPS signal might accomplish this, unless the drone uses an inertial navigation system; nefarious actors may set the "return to home" feature to carry a drone to its *target* as a safeguard against jamming; drones may feature software protections against hacking; interceptors or net guns may be overwhelmed in the event of a swarm attack; etc.

71 Sec. 1692. 49 U.S. Code § 46502 deals with aircraft piracy, while Title 18 includes a number of statutes criminalizing, among other things relevant to this discussion, damaging or destroying an aircraft, or interfering with certain types of communications.

72 National Defense Authorization Act for Fiscal Year 2018, Public Law 115–91, § 1692.

73 Terri Moon Cronk, "DOD Cracks Down on Use of Drones Over Installations," U.S. Department of Defense, August 7, 2017, https://www.defense.gov/News/Article/Article/1270758/dod-cracks-down-on-use-of-drones-over-installations/ (accessed March 30, 2018).

74 The authority to shoot down a UAS could also be derived from the authority to shoot down a hostile manned aircraft, although this shoot-down authority is limited to the President and a select few DOD officials, which might not be timely in the case of a UAS. Chris Mellow, "Would a Fighter Pilot Shoot Down a Private Airplane?," *Air and Space Magazine*, March 2010, https://www.airspacemag.com/flight-today/dont-cross-that-line-5841988/?page=2 (accessed March 30, 2018).

75 U.S. Department of Energy, "Security," https://www.energy.gov/ehss/services/security (accessed March 30, 2018).

76 National Defense Authorization Act for Fiscal Year 2017, Public Law 114–328 § 3112, https://www.congress.gov/bill/114th-congress/senate-bill/2943/text (accessed April 12, 2018).

77 U.S. Nuclear Regulatory Commission, "Special Nuclear Material," March 28, 2017, https://www.nrc.gov/materials/sp-nucmaterials.html (accessed March 30, 2018).

78 U.S. Department of Homeland Security, "Critical Infrastructure Sectors," July 11, 2017, https://www.dhs.gov/critical-infrastructure-sectors (accessed March 30, 2018).

79 For example, the Coast Guard has the authority to fire on a vessel that is subject to search or seizure if a vessel refuses to obey a Coast Guard order to stop. 14 U.S. Code § 638 (2010).

80 Elaine C. Duke, Christopher A. Wray, and Nicholas J. Rasmussen, "Threats to the Homeland," testimony before the Committee on Homeland Security and Governmental Affairs, U.S. Senate, September 27, 2017, https://www.hsgac.senate.gov/hearings/09/18/2017/threats-to-the-homeland (accessed March 30, 2018).

81 "Homeland Security Threats," C-SPAN video, September 27, 2017, at (1:17:00), https://www.c-span.org/video/?434411-1/senior-officials-testify-homeland-security-threats&start=4705 (accessed March 30, 2018), and Bill Carey, "DHS, Other Agencies Seek Law Changes to Intercept Drones," AINOnline, September 7, 2017, https://www.ainonline.com/aviation-news/defense/2017-09-07/dhs-other-agencies-seek-law-changes-intercept-drones (accessed April 6, 2017).

82 U.S. Department of Justice, Bureau of Prisons, Acquisitions Branch, "RFI for Protection from Unmanned Air Vehicles," November 4, 2015, https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=c1c13ff92dde7d9575ad0bc67716cb81&_cview=0 (accessed March 30, 2018).

83 Representative Vicky Hartzler (R–MO) introduced H.R. 5366, the Safeguarding America's Skies Act, to amend Title 18 to allow Justice Department and Homeland Security personnel "to detect, track, and engage with drones that pose a security risk to agency facilities and assets"; to require those agencies "to coordinate with the Department of Transportation, the Federal Communications Commission, and the National Telecommunications and Information Administration in developing the rules and guidance to carry out this new authority"; calling on the Secretary of Transportation "to issue a final regulation requiring remote identification and tracking of drones within one year"; and for the Justice Department and Department of Homeland Security "to submit an annual report to Congress outlining actions taken to implement and carry out this new authority." News release, "Hartzler Introduces Bill to Safeguard America's Skies," Representative Vicky Hartzler, March 22, 2018, https://hartzler.house.gov/media-center/press-releases/hartzler-introduces-bill-safeguard-america-s-skies (accessed March 30, 2018).

84 The Communications Act of 1934, 47 U.S. Code Part I, § 302(b) (prohibiting manufacture, dealing, or operating jamming devices); § 333 (prohibiting willful interference with any radio communications of any station licensed or authorized by, or operated by, the United States); 47 CFR § 2.803 (2008).

85 47 U.S. Code § 302a (2010).

86 47 U.S. Code §§ 503, 510 (2012). Chief of the FCC Enforcement Bureau, P. Michele Ellison, has said that "[j]amming devices create serious safety risks" and that the agency will "be intensifying our efforts through partnerships with law enforcement agencies to crack down on those who continue to violate the law. Through education, outreach, and aggressive enforcement, we're tackling this problem head on." The FCC has issued several enforcement advisories on the issue and asks any member of the public to file a complaint if they know of someone operating or dealing in jamming devices. See Federal Communications Commission, "Jammer Enforcement," https://www.fcc.gov/general/jammer-enforcement (accessed March 30, 2018). The FCC also works with the Justice Department to enforce criminal laws prohibiting willful interference with U.S. government communications (18 U.S. Code § 1362 [2011]) and intentional interference with satellite communications (18 U.S. Code § 1367(a) [2011]).

87 49 U.S. Code § 40103 (2011), and 49 U.S. Code § 44701(a) (2011).

88 FAA Modernization and Reform Act of 2012, Public Law 112–95, § 336(b).

89 Federal Aviation Administration, "FAA Drone Zone," https://faadronezone.faa.gov/#/ (accessed March 30, 2018), and FAA Modernization and Reform Act of 2012, Public Law 112–95.

90 Federal Aviation Administration, "Law Enforcement Guidance for Suspected Unauthorized UAS Operations," June 5, 2017, https://www.faa.gov/uas/resources/law_enforcement/media/FAA_UAS-PO_LEA_Guidance.pdf (accessed March 30, 2018).

91 For a list of current Temporary Flight Restrictions, see Federal Aviation Administration, "TFR List," http://tfr.faa.gov/tfr2/list.html (accessed March 30, 2018).

92 That includes pre-existing, technology-agnostic laws that may be violated; for example, "reckless endangerment, criminal mischief, voyeurism, inciting violence, trespassing, obstruction of police emergency services duties, and nuisance/noise laws." Michele Coppola, "Law Enforcement Encounters with Suspicious UAS Operations," TechBeat, November 28, 2017, https://techbeat.justnet.org/law-enforcement-encounters-suspicious-uas-operations/ (accessed March 30, 2018).

93 See, for example, "'Hero' NYPD Cop Who Shot Terror Suspect Sayfullo Saipov Identified," Fox News, October 31, 2017, http://www.foxnews.com/us/2017/10/31/hero-nypd-cop-who-shot-terror-suspect-sayfullo-saipov-identified.html (accessed April 6, 2018); news release, "Sayfullo Saipov Indicted on Terrorism and Murder in Aid of Racketeering Charges in Connection with Lower Manhattan Truck Attack," Department of Justice, November 21, 2017, https://www.justice.gov/usao-sdny/pr/sayfullo-saipov-indicted-terrorism-and-murder-aid-racketeering-charges-connection-lower (accessed April 6, 2018); Abigail Hauslohner and Stephanie McCrummen, "Orlando Shooting: A Quick Response and Then a Long Wait," *The Washington Post*, June 21, 2016, http://www.nola.com/politics/index.ssf/2016/06/orlando_shooting_a_quick_respo.html (accessed April 6, 2018); and Las Vegas Metropolitan Police, "LVMPD Preliminary Investigative Report," January 18, 2018, https://www.lvmpd.com/en-us/Documents/1_October_FIT_Report_01-18-2018_Footnoted.pdf (accessed April 6, 2018).

94 Los Angeles Police Department, "Counter-Terrorism and Special Operations Bureau (CTSOB)," http://www.lapdonline.org/inside_the_lapd/content_basic_view/6502 (accessed March 30, 2018).

95 For a recent discussion of a controversy between state and federal police authority, see *Arizona v. United States*, 567 U.S. 387 (2012).

96 FAA, "Law Enforcement Guidance for Suspected Unauthorized UAS Operations."

97 As with their federal counterparts, state and local law enforcement agencies are bound by federal laws, including statutes that prohibit the use of signal-jamming equipment and the damaging or destruction of an aircraft, which render some counter-UAS activities unlawful, unless, perhaps, exigent circumstances present an objectively reasonable perception of imminent threat of serious injury or death to the officer or other persons. *Tennessee v. Garner*, 471 U.S. 1 (1985), and *Graham v. Connor*, 490 U.S. 386 (1989).

98 47 U.S.C § 301 (2011).

99 Ibid., at § 333.

100 Ibid., at § 302a(c).

101 The Communications Act of 1934, 47 U.S. Code Part I, § 302(b), (prohibiting manufacture, dealing, or operating jamming devices); § 333 (prohibits willful interference with any radio communications of any station licensed or authorized by, or operated by, the United States); 47 CFR § 2.803 (2008); and The Cable Communications Policy Act of 1984 (codified at 47 U.S. Code Chapter 5, subchapter V–A).

102 It is unclear whether the "wrongful intent" requirement would apply to law enforcement–related interdictions, but Congress nevertheless exempted the DOD from this section in the 2018 NDAA.

103 18 U.S. Code § 1030 (2010). See also Paul J. Larkin Jr., "Reasonably Construing the Computer Fraud and Abuse Act to Avoid Overcriminalization," Heritage Foundation *Legal Memorandum* No. 95, June 19, 2013, http://thf_media.s3.amazonaws.com/2013/pdf/lm95.pdf, and National Association of Criminal Defense Lawyers, "CFAA Background," https://www.nacdl.org/criminaldefense.aspx?id=34244 (accessed March 22, 2018).

104 18 U.S. Code § 1030(e)(2)(B) (2010).

105 Ibid., at § 1030(a)(7).

106 Ibid., at § 1030(a)(5)(A).

107 Ibid., at § 1030(a)(4).

108 Ibid., at § 1030(a)(5).

109 Ibid., at § 1030(a)(6).

110 18 U.S. Code § 2511 (2011).

111 Including the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104–191 (1996); The Stored Communications Act (18 U.S. Code §§ 2701–2710 [1986]); and The Privacy Act (5 U.S. Code § 552a [2012]).

112 Under the Foreign Intelligence Surveillance Act of 1978 or 18 U.S. Code § 3123.

113 18 U.S. Code §§ 3121–3126 (2015).

114 National Defense Authorization Act for Fiscal Year 2018, § 1692.

115 U.S. Department of Homeland Security, U.S. Immigration and Customs Enforcement, "Delegation of Immigration Authority Section 287(g) Immigration and Nationality Act," March 26, 2018, https://www.ice.gov/287g (accessed March 30, 2018).

116 Ibid.

117 Ibid.

118 The FAA Extension, Safety, and Security Act of 2016 (Public Law 114–190) authorizes the FAA to impose UAS flight restrictions around critical infrastructure and related fixed sites. The FAA has also exercised its authority under 14 CFR § 99.7 to issue "special security instructions" to impose UAS flight restrictions over military bases. See News release, "FAA Restricts Drone Operations Over Certain Military Bases," Federal Aviation Administration, April 7, 2017, https://www.faa.gov/news/updates/?newsId=87865 (accessed April 11, 2018).

119 For more detail on which provisions of law currently restrict the use of CUAS, see the "Legal Barriers to Counter-UAS Operations" section, supra.

120 Greater clarity must be provided to private-sector developers of CUAS jamming technologies, as current law subjects them to potentially stiff liability for marketing such equipment. In 2014, the FCC levied a $34.9 million fine on the Chinese firm CTS Technology for illegally marketing and selling jamming devices in the United States. The fine was the largest ever against a company unlawfully marketing jammers. The FCC cited its authority under 47 U.S. Code § 302a(b), which states that "[n]o person shall manufacture, import, sell, offer for sale, or ship devices or home electronic equipment and systems, or use devices, which fail to comply" with FCC regulations promulgated to prevent interference with lawful transmissions. In *re C.T.S. Technology Co., et al.*, 14 FCC 92 (June 2014), https://apps.fcc.gov/edocs_public/attachmatch/FCC-14-92A1.pdf (accessed April 11, 2018), and Jacob Kastrenakes, "FCC Issues Largest Fine in History to Company Selling Signal Jammers," The Verge, June 19, 2014, https://bit.ly/2GGfXK4 (accessed April 6, 2014).

121 Those include the following: the Privileges and Immunities Clause safeguards the right to acquire and possess property and the freedom of movement (U.S. Constitution, Article IV, Section 2, Clause 1; *Corfield v. Coryell*, 6 Fed. Cas. 546 (1823)); the Fourth Amendment secures freedom from unreasonable searches and seizures (U.S. Constitution, amendment IV); the U.S. Supreme Court maintains a "right to privacy" (*Griswold v. Connecticut*, 381 U.S. 479 (1965)) (while privacy interests are important, those are addressed elsewhere and beyond the scope of this article); and the First Amendment protects the freedom of expression (U.S. Constitution, amendment I). Some state action may chill protected First Amendment activity involving journalism, photography, and videography, such as overbroad legislative proposals to criminalize photography of "critical infrastructure." See, for example, Ari Rosmarin, "Drone Rules Are Already Colliding with the First Amendment," American Civil Liberties Union, July 16, 2015, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/drone-rules-are-already-colliding-first-amendment (accessed April 11, 2018); and Paul Larkin and Evan Bernick, "Filming the Watchmen: Why the First Amendment Protects Your Right to Film the Police in Public Places," Heritage Foundation *Legal Memorandum* No. 127, June 12, 2014, https://www.heritage.org/the-constitution/report/filming-the-watchmen-why-the-first-amendment-protects-your-right-film-the.

122 "A 'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property." *United States v. Jacobsen*, 466 U.S. 109, 113 (1984).

123 See, for example, Los Angeles Police Department, "Los Angeles Police Department Small Unmanned Aerial System Pilot Program Deployment Guidelines and Procedures," http://assets.lapdonline.org/assets/pdf/2017.10.17%20-%20APPROVED%20FINAL%20-%20sUAS%20Guidelines.pdf (accessed April 6, 2018); *Los Angeles Times*, "LAPD Takes Time to Perfect Law Enforcement Drone Regulations," August 11, 2017, http://www.govtech.com/opinion/LAPD-Takes-Time-to-Perfect-Law-Enforcement-Drone-Regulations.html (accessed April 11, 2018); and Kent, Washington Police Department, "Kent Police Department Drone Policy," https://www.kentwa.gov/residents/public-safety/police-department/kent-police-department-drone-policy (accessed Apr. 6, 2017).

124 These, too, must respect special privacy concerns, such as any involved in delivering medical supplies or treatment may trigger the HIPAA of 1996, providing for data privacy and security to protect medical information.

125 Office of Justice Programs, "Edward Byrne Memorial Justice Assistance Grant Program," https://www.bja.gov/jag/ (accessed April 12, 2018).

126 The assessment of what class or classes of drone pose a substantial risk should go beyond the FAA's present weight threshold for registration and include other considerations, such as the drone's performance capabilities and whether the UAS is flying solely within airspace determined to be private property. This analysis would require the question of property rights in low-altitude airspace to be resolved. For a full discussion, see Jason Snead and John-Michael Seibler, "Seizing the Sky: Federal Regulators Use Drones to Justify Controlling the Airspace Over Your Backyard," Heritage Foundation *Issue Brief* No. 4565, May 19, 2016, https://www.heritage.org/crime-and-justice/report/seizing-the-sky-federal-regulators-use-drones-justify-controlling-the.