2019-05

The Legal, Technical, and Practical Challenges of Countering the Commercial Drone Threat to National Security

Ward, Allison

Monterey, California. Naval Postgraduate School

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
19-05-2019	Research Paper	

4. TITLE AND SUBTITLE

The Legal, Technical, and Practical Challenges of Countering the Commercial Drone Threat to National Security

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Ward, Allison, E, LCDR

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Civilian Institutions Office (Code 522)
Naval Postgraduate School
1 University Circle, Herrmann Hall Rm HE046
Monterey, CA 93943-5033

10. SPONSOR/MONITOR'S ACRONYM(S)

NPS CIVINS

11. SPONSORING/MONITORING AGENCY REPORT NUMBER

12. DISTRIBUTION AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Commercial-off-the-shelf (COTS) drones – also referred to as unmanned aircraft systems (UAS) or quadcopters – are nearly ubiquitous. In the U.S. alone, the Federal Aviation Administration (FAA) "projects the small model hobbyist UAS fleet to more than double from an estimated 1.1 million vehicles in 2017 to 2.4 million units by 2022." Given their range, photographic capability, and relatively low cost, they appeal to everyone from real estate agents to insurance claims adjusters to tech geeks to the Department of Defense (DoD) to terrorist actors. Their ubiquity and accessibility pose a growing concern to national security. Recognizing the potential impact to national security, as well as the tension between available counter-UAS (cUAS) systems and sections of title 18, U.S. Code, including the Aircraft Sabotage Act, Computer Fraud and Abuse Act, and the Wiretap Act, Congress has started passing legislation designed to assist Federal agencies with mitigating the threat posed by rogue UAS (e.g., 10 U.S.C. 130i; P.L. 115-302). There is no perfect cUAS interdiction solution, but hacking – including spoofing – may the most promising solution, with the least potential for collateral damage, thereby also likely making it the most compliant with the law enforcement principle of using non-lethal incapacitating weapons that minimize the risk of endangering uninvolved people.

15. SUBJECT TERMS

drone, UAV, UAS, cUAS, quadcopter, electromagnetic spectrum, jamming, hacking, spoofing, covered facility or asset

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPONE NUMBER (*Include area code)*
U	U	U	UU	30	

THIS PAGE INTENTIONALLY LEFT BLANK

Pro Seminar Allison Ward
December 21, 2018

The Legal, Technical, and Practical Challenges of Countering the Commercial Drone Threat to National Security

I. Background

It is well-established, common knowledge that commercial-off-the-shelf (COTS) drones – also referred to as unmanned aircraft systems (UAS) or quadcopters – are nearly ubiquitous. In the U.S. alone, the Federal Aviation Administration (FAA) "projects the small model hobbyist UAS fleet to more than double from an estimated 1.1 million vehicles in 2017 to 2.4 million units by 2022."[1] Given their range, photographic capability, and relatively low cost, they appeal to everyone from real estate agents to insurance claims adjusters to tech geeks to the Department of Defense (DoD) to terrorist actors. Their ubiquity and accessibility pose a growing concern to national security. Drones were used to smuggle drugs and phones to prisoners outside of London, at least one Mexican drug cartel has developed bomb drones, and "[m]ilitant groups such as the Islamic State have used drones to carry out attacks by dropping grenades or crashing into infrastructure."[2] In August 2018, two drones carrying explosives detonated in the vicinity of Venezuelan President Nicolas Maduro at a public event. The drones used in this attack "are available commercially for $5,000 each. They weigh less than 25 pounds and can be controlled from five kilometers away over a short-range radio link, essentially the computer equivalent of an old-fashioned walkie-talkie."[3] That these drones were able to get so close to a world leader speaks to how easy they are to acquire, and how difficult they are to detect and defend against.[4]

---

[1] Fed. Aviation Admin., *FAA Releases Aerospace Forecast*, https://www.faa.gov/news/updates/?newsId=89870 (last modified Mar. 16, 2018).
[2] Joseph Ax, *Apparent Attack in Venezuela Highlights Risk of Drone Strikes*, REUTERS (Aug. 5, 2018, 2:04 PM), https://www.reuters.com/article/us-venezuela-politics-drones/apparent-attack-in-venezuela-highlights-risk-of-drone-strikes-idUSKBN1KQ0MG; Nicholas Weaver, *The Necessary Authority to Counter Drone Threats*, LAWFARE (Oct. 4, 2018, 10:00 AM), https://www.lawfareblog.com/necessary-authority-counter-drone-threats.
[3] Weaver, *supra* note 2.
[4] Colin P. Clarke, Commentary, *Approaching a "New Normal": What the Drone Attack in Venezuela Portends*, THE RAND BLOG (Aug. 13, 2018), https://www.rand.org/blog/2018/08/approaching-a-new-normal-what-the-drone-attack-in-venezuela.html.

II. Challenges of Determining Intent and Countering UAS

a. Law Enforcement First Responders

Local, non-Federal law enforcement officials will most likely be the first responders to arrive on-scene in the event of reports of drone activity of unknown intent by unknown actors. Accordingly, law enforcement use of force standards will drive the initial response posture. The United Nations adopted 26 basic principles on the use of force and firearms (BPUFF) by law enforcement officials in 1990, and they have since become internationally accepted standards.[5] The BPUFF begin by recognizing that law enforcement officials provide an important social service and "have a vital role in the protection of the right to life, liberty and security of the person."[6] When conducting law enforcement operations, law enforcement officials have a range of options available to them depending on the circumstances they encounter, including use of force. Use of force "is generally understood as any physical constraint imposed on a person, ranging from physical restraint by hand or with a restraining device to use of firearms or other weapons."[7] Of note are principles 3, emphasizing that non-lethal incapacitating weapons should be deployed carefully to minimize the risk of endangering uninvolved people with the law enforcement incident, and 9, authorizing the use of firearms only in the following circumstances, and when lesser means of force are insufficient: "self-defence or defence of others against the imminent threat of death or serious injury, to prevent the perpetration of a particularly serious crime involving grave threat to life, to arrest a person presenting such a danger and resisting their authority, or to prevent his or her escape."[8]

---

[5] Eighth U.N. Cong. on the Prevention of Crime and the Treatment of Offenders, *Basic Principles on the Use of Force and Firearms by Law Enforcement Officials* (Aug. 27-Sept. 7, 1990), https://www.ohchr.org/Documents/ProfessionalInterest/firearms.pdf.
[6] *Id*.
[7] Int'l Comm. of the Red Cross, *The Use of Force in Law Enforcement Operations* (Sept. 3, 2015), https://www.icrc.org/en/download/file/24041/the_use_of_force_in_law_enforcement_06.20.2016.pdf.
[8] Eighth U.N. Cong. on the Prevention of Crime and the Treatment of Offenders, *supra* note 5.

Federal agencies, acknowledging that this is an emerging threat, and that local law enforcement agencies will be on the front lines of fighting this threat domestically, issued counter-UAS (cUAS) guidance and established liaisons for law enforcement officials to contact.

The Department of Transportation (DoT), through the FAA, has created a number of resources for local law enforcement officials to use, in anticipation of their interaction with UAS and UAS operators. The FAA recognizes that law enforcement agents "are often in the best position to deter, detect, immediately investigate, and, as appropriate, pursue enforcement actions in response to unauthorized or unsafe UAS operations."[9] The resource detailing recommendations for law enforcement officials who handle UAS sighting and reports recommends that law enforcement officers "focus on the underlying activity in drone complaints" by taking the drone out of the fact pattern and applying already-existing law to the infractions committed (e.g., reckless endangerment, voyeurism, harassment).[10] The recommended first step is to locate the drone operator, determine what they are doing (using the drone for hobby or recreational purposes, commercial purposes, etc.), and assess the situation and facts known to determine what level of law enforcement is required.[11] The FAA proffers the acronym DRONE:

> **Detect** all available elements of the situation; attempt to locate and identify individuals operating the drone. (Look at windows/balconies/roof tops).
>
> **Report** the incident to the FAA Regional Operations Center (ROC). Follow-up assistance can be obtained through FAA Law Enforcement Assistance Program special agents.

[9] Fed. Aviation Admin., *Law Enforcement Guidance for Suspected Unauthorized UAS Operations* (Aug. 14, 2018, Version 5), https://www.faa.gov/uas/public_safety_gov/media/faa_uas-po_lea_guidance.pdf.
[10] Fed. Aviation Admin., *Understanding Your Authority: Handling Sightings and Reports* (last modified Nov. 21, 2018) https://www.faa.gov/uas/public_safety_gov/sightings_reports/.
[11] *Id.*

> **Observe** the UAS and maintain visibility of the device; look for damage or injured individuals. Note: Battery life is typically 20 to 30 minutes.
>
> **Notice** features: Identify the type of device (fixed-wing/multi-rotor), its size, shape, color, payload (i.e., video equipment), and activity of device.
>
> **Execute** appropriate police action: Maintain a safe environment for general public and first responders. Conduct a field interview, request proof of UAS registration, and document ALL details of the event per the guidance provided by the FAA.[12]

The FAA is cognizant that they must not mix criminal law enforcement with their civil administrative safety enforcement function, but recognizes that "the public interest is best served by coordinating and fostering mutual understanding and cooperation between governmental entities with enforcement responsibilities."[13]

Department of Homeland Security (DHS) also published considerations for law enforcement officials who encounter UAS. It stresses that, while UAS in and of themselves are benign, the manner in which they are used, and by whom, "can seriously threaten the personal safety of emergency services personnel and the public, as well as obstruct law enforcement operations."[14] Law enforcement personnel who take action against UAS and UAS operators need to be aware of Federal statutes that may affect their engagement, as well as some of the technical aspects of UAS and UAS operations.[15] DHS recommends that law enforcement agencies develop plans and procedures detailing specific actions for when law enforcement officers interact with UAS and UAS operators, including working in close coordination with their agency's counsel to ensure their proposed actions do not run afoul of any applicable Federal statutes.[16]

---

[12] *Id.*
[13] Fed. Aviation Admin., *Law Enforcement Guidance*, *supra* note 9.
[14] Dep't. of Homeland Sec., *Unmanned Aircraft Systems, Considerations for Law Enforcement Action* (Jun. 2017), https://www.dhs.gov/sites/default/files/publications/uas-law-enforcement-considerations-508.pdf.
[15] *Id.*
[16] *Id.*

b. Federal Statutes Applicable to cUAS Operations

i. 18 U.S.C. § 32, Destruction of Aircraft or Aircraft Facilities

Title 18, U.S. Code, section 32 is colloquially referred to as the "Aircraft Sabotage Act." It criminalizes willfully setting fire to, damaging, destroying, disabling, or wrecking any aircraft in the special aircraft jurisdiction of the U.S.; or placing or causing to be placed a destructive device or substance in, upon, or in proximity to, or otherwise making or causing to be made unworkable or unusable or hazardous to work with, any such aircraft; or setting fire to, damaging, destroying, or disabling any air navigation facility; or communicating information, knowing the information to be false under the circumstances in which such information may reasonably be believed, thereby endangering the safety of any such aircraft of flight.[17] Title 49, U.S. Code, section 40102 defines "aircraft" as "any contrivance invented, used, or designed to navigate, or fly in, the air."[18] The "special aircraft jurisdiction" definition includes an aircraft in flight that is a civil aircraft of the U.S. or is another aircraft in the U.S..[19] A "civil aircraft" means any aircraft that is not a public aircraft.[20]

ii. 18 U.S.C. § 1030, Fraud and Related Activity in Connection with Computers

Title 18, U.S. Code, section 1030 is typically referred to as the "Computer Fraud and Abuse Act." Applicable subsections include (a)(2)(C), which criminalizes intentionally accessing a computer without authorization, and thereby obtaining information from any protected computer; (a)(4), which prohibits knowingly and with intent to defraud, accessing a protected computer without authorization and by means of such conduct furthering the intended fraud and obtaining

[17] 18 U.S.C. § 32.
[18] 49 U.S.C. § 40102.
[19] 49 U.S.C. § 46501(2).
[20] 49 U.S.C. § 40102(a)(16).

anything of value, unless the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000; and (a)(5)(A), which addresses knowingly causing the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causing damage without authorization, to a protected computer (or doing so recklessly (B) or negligently (C)).[21] Any computer that connects to the internet is considered a "protected computer."[22]

iii. 18 U.S.C. § 2511, Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited

Title 18, U.S. Code, section 2511 is commonly known as the "Wiretap Act." A person violates this statue when they intentionally intercept any wire, oral, or electronic communication; intentionally use any electronic, mechanical, or other device to intercept any oral communication when such device transmits communications by radio, or interferes with the transmission of such communication; or intentionally use the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this statute.[23]

iv. 18 U.S.C. § 3121, General Prohibition on Pen Register and Trap and Trace Device Use; Exception

Title 18, U.S. Code, section 3121 – the Pen Register/Trap and Trace Statute – directs that, except as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order.[24]

---

[21] 18 U.S.C. § 1030.
[22] Dep't. of Justice, Office of Legal Educ., *Prosecuting Computer Crimes* 4 (2015), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf ("it is enough that the computer is connected to the Internet; the statute does not require proof that the defendant also used the Internet to access the computer or used the computer to access the Internet. Several courts have held that using the Internet from a computer is sufficient to meet this element.").
[23] 18 U.S.C. § 2511.
[24] 18 U.S.C. § 3121.

v. 47 U.S.C. § 151, et seq., Purposes of this chapter; Federal Communications Commission Created

Title 47, U.S. Code, section 151, et seq., is the Communications Act of 1934. The Act creates the Federal Communications Commission (FCC) for the purposes of: regulating interstate and foreign commerce in communication by wire and radio so as to make available, so far as possible, to all the people of the U.S., without discrimination on the basis of race, color, religion, national origin, or sex, a rapid, efficient, Nationwide, and world-wide wire and radio communication service with adequate facilities at reasonable charges; national defense; promoting safety of life and property through the use of wire and radio communication; and securing a more effective execution of this policy and centralizing authority, including enforcement authority, into a single agency.[25]

vi. 49 U.S.C. § 40103, Sovereignty and Use of Air Space

Title 49, U.S. Code, section 40103, states that the U.S. government has exclusive sovereignty of U.S. airspace, and that U.S. citizens have a public right of transit through navigable U.S. airspace.[26] It also directs the FAA to develop plans and policies for the use of navigable airspace and assign by regulation or order the use of the airspace necessary to ensure the safety of aircraft and the efficient use of airspace.[27] The FAA Administrator, in consultation with the Secretary of Defense (SECDEF), shall establish areas in the airspace where it is necessary in the interest of national defense, and by order or regulation, to restrict or prohibit civil aircraft flights.[28]

[25] 47 U.S.C. § 151.
[26] 49 U.S.C. § 40103.
[27] *Id.*
[28] *Id.*

vii. 49 U.S.C. § 46502, Aircraft Piracy

In title 49, U.S. Code, section 46502, "aircraft piracy" means seizing or exercising control of an aircraft in the special aircraft jurisdiction of the U.S. by force and with wrongful intent.[29] Outside special aircraft jurisdiction, the statute prohibits any individual from committing an offense (as defined in the Convention for the Suppression of Unlawful Seizure of Aircraft) on an aircraft in flight outside the special aircraft jurisdiction of the U.S.[30]

c. Public Law (PL) 112-95, FAA Modernization Act 2012

In addition to the robust statutory scheme that has potential to impact cUAS operations, additional legislative and regulatory measures must also be taken into consideration. The FAA Modernization Act of 2012 provides some clarifying definitions: an "unmanned aircraft" is "an aircraft that is operated without the possibility of direct human intervention from within or on the aircraft;" an "unmanned aircraft system" is "an unmanned aircraft and associated elements (including communication links and the components that control the unmanned aircraft) that are required for the pilot in command to operate safely and efficiently in the national airspace system;" and a "small unmanned aircraft" is "an unmanned aircraft weighing less than 55 pounds."[31]

It also, in section 336, provides special rules for model aircraft. It defines model aircraft as "an unmanned aircraft that is capable of sustained flight in the atmosphere; is flown within visual line of sight of the person operating the aircraft; and is flown for hobby or recreational purposes."[32] The FAA is prohibited from promulgating any rule or regulation regarding model aircraft, or an aircraft being developed as a model aircraft, subject to the following conditions:

---

[29] 49 U.S.C. § 46502.
[30] *Id*.
[31] FAA Modernization Act of 2012, Pub. L. No. 122-95, § 331, 126 Stat. 11, 72 (2012).
[32] *Id*. at § 336.

the aircraft is flown strictly for hobby or recreational use; the aircraft is operated in accordance with a community-based set of safety guidelines and within the programming of a nationwide community-based organization; the aircraft is limited to not more than 55 pounds; it is operated in a manner that does not interfere with and gives way to manned aircraft; and, when flown within five miles of an airport, the operator provides notice to the air traffic control tower.[33]

d. Advisory Circular (AC) Number 91-57A, Model Aircraft Operating Standards

AC Number 91-57A complements FAA Modernization Act of 2012 section 336 by providing guidance to model aircraft operators.[34] For example, model aircraft operators must comply with any Temporary Flight Restrictions (TFR) (TFR are issued for specific locations due to disasters, for reasons of national security, or when deemed necessary to manage air traffic); must not operate in Prohibited Areas, Special Flight Rule Areas, or the Washington National Capital Region Flight Restricted Zone, without specific authorization; should make themselves aware of other Notices to Airmen (NOTAMS) which address operations near locations such as military facilities, certain stadiums, power plants, electric substations, dams, oil refineries, national parks, etc. (permanent NOTAMS have been issued, for example, for Disney World Theme Park, Orlando, Florida, and Disneyland Theme Park, Anaheim, California);[35] and should follow best practices, including limiting operations to 400 feet above ground level.[36]

---

[33] *Id*.
[34] Fed. Aviation Admin., Advisory Circular No. 91-57A, *Model Aircraft Operating Standards* (Sept. 2, 2015), https://www.faa.gov/documentLibrary/media/Advisory_Circular/AC_91-57A.pdf.
[35] See, Fed. Aviation Admin., NOTAM No. FDC 4/3634 (Oct. 27, 2014), https://tfr.faa.gov/save_pages/detail_4_3634.html; Fed. Aviation Admin., NOTAM No. FDC 4/3635 (Oct. 27, 2014), https://tfr.faa.gov/save_pages/detail_4_3635.html.
[36] Fed. Aviation Admin., Advisory Circular No. 91-57A, *supra* note 34.

e. 14 C.F.R. § 107, Small Unmanned Aircraft System Rule

"Section 107" applies to all UAS weighing less than 55 pounds.[37] While it does not apply to model aircraft, as the definition is strictly interpreted, it does apply to commercial drone operations and recreational drone operations that fall outside the confines of the model aircraft definition.[38] Small UAS operators must hold a remote pilot certificate, and are subject to additional constraints, including: the small UAS must remain within visual line of sight of the operator; operations are limited to between daylight and civil twilight, with appropriate collision lighting; operate at a height of not more than 400 feet and a speed of not more than 100 miles per hour; and the UAS may not be operated over people who are not participating in the drone operations or are not protected from possible falling drones (by a structure or in a vehicle, for example).[39]

Given the extensive statutory and regulatory guidance that governs permissible UAS operations, it makes good sense that DHS encourages law enforcement officials to work closely with their agency's counsel.

f. Privacy Concerns

While largely beyond the scope of this paper, privacy concerns about UAS usage are routinely raised in secondary source materials on the topic. "Privacy law is defined as '[r]egulation[s] or statute[s] that protect a person's right to be left alone, and govern collection, storage, and release of his or her financial, medical, and other personal information.'"[40] With both government actors and regular citizens having access to UAS, the First, Third, Fourth, and

[37] 14 C.F.R. § 107.
[38] *Id.*
[39] *Id.*
[40] Jennifer Urban, *What is the Eye in the Sky Actually Looking at and Who is Controlling It? An International Comparative Analysis on How to Fill the Cybersecurity and Privacy Gaps to Strengthen Existing U.S. Drone Laws*, 70 FED. COMM. L. J. 1, 15 (2018).

Fifth Constitutional Amendments may be implicated by drone technology, in particular the surveillance and data recording capabilities of nearly all COTS UAS. "The First Amendment gives persons the right to have their own personal, private beliefs. The Third Amendment protects a person's privacy within their home by not allowing soldiers to use a private person's home. The Fourth Amendment protects the privacy of a person in the United States against unlawful search and seizure. The Fifth Amendment protects the privacy of personal information by not requiring a person to commit self-incrimination."[41] Privacy concerns with respect to UAS proliferation arise in a number of contexts. Overflight of a third-party's private property is one example. "[I]f a drone operator was purposefully using his drone to hover over the fenced in pool of his neighbor to record her sunbathing, it is likely that a court would find his actions to be highly offensive to a reasonable person."[42] If, however, the drone operator intentionally flew his drone over his neighbor's backyard because he was attempting to record images of a bird, but accidentally also recorded images of his neighbor, the reasonable person standard becomes a more challenging analysis, and intent would have to be a factor in to take into consideration.[43] "Due to the lack of clarification on how to apply the reasonable person standard to drone operations, tort law does not provide an adequate solution to privacy issues raised by drones."[44] UAS assistance with law enforcement is another example. Louisville, Kentucky is piloting a program to "test the feasibility of using self-guided drones to investigate shootings: According to the proposal, the drones would be sent the GPS coordinates of a shooting location, then to take pictures and videos ahead of first responders, complementing location data with visuals."[45]

[41] *Id*. at 16.
[42] *Id*. at 17.
[43] *Id*.
[44] *Id*.
[45] Sidney Fussell, *Kentucky is Turning to Drones to Fix its Unsolved Murder Crisis*, THE ATLANTIC (Nov. 6, 2018), https://www.theatlantic.com/technology/archive/2018/11/police-drone-shotspotter-kentucky-gun-911-ai/574723/.

Privacy advocates are concerned with "the problem of mission creep: Technology brought in for one purpose eventually be used for another. Drone footage could be matched against criminal databases, mined for audiovisual data, or . . . used to justify further encroachment by police into vulnerable neighborhoods."[46] The Supreme Court has addressed concerns arising from law enforcement use of analogous technology to assist with investigative efforts in a few cases.

> In California v. Ciraolo, the U.S. Supreme Court held that local law enforcement officers did not engage in a search by flying a police plane at 1,000 feet in the air to see into the defendant's backyard full of marijuana plants because there could have been private and commercial planes at that altitude and, hence, any expectation of privacy from overhead surveillance was unreasonable. Florida v. Riley followed a few years later, upholding police discovery of marijuana plants in a mostly covered greenhouse spotted only through the use of a helicopter hovering at 400 feet. These cases would suggest strongly that high-altitude aerial surveillance by government drones would not violate any reasonable expectations of privacy.[47]

More recently, however, "the Court ruled that the use of devices to duplicate what police could have gleaned through human observation did not constitute a search so long as the human observations would have been valid."[48] In U.S. v. Jones, Federal Bureau of Investigations (FBI) agents placed a GPS device on the suspect's car, to track his movements.[49] All nine justices agreed that a search occurred, but disagreed on why it was a search; the five-to-four majority ruled that the FBI agents committed a physical trespass by placing the device on the suspect's car without consent and without a warrant, and that the "reasonable expectation of privacy test was an overlay on top of the prior understanding that any physical intrusion constituted a search. This trespass rationale enabled the majority to avoid deciding whether there was a reasonable

---

[46] *Id*.
[47] Tung Yin, *Game of Drones: Defending Against Drone Terrorism*, TEX. A&M L. REV. 635, 652-53 (2015) (referencing, California v. Ciraolo, 476 U.S. 207 (1967); Florida v. Riley, 488 U.S. 445 (1989)).
[48] *Id*. at 653.
[49] *Id*. (referencing, United States v. Jones, 132 S. Ct. 945 (2012)).

expectation of privacy in one's public locations and movements."[50] Privacy concerns also arise with cUAS technologies. As discussed in greater detail below, UAS interdiction methods include "intercepting signals between the controller and the drone (whether to identify or locate the controller, or to take control of the drone)."[51] Critics question whether any legislation that permits law enforcement to intercept such signals adequately protects the privacy of those communications, and whether a grant of authority to seize or destroy drones under specified circumstances adequately balances protections for private property.[52]

The FAA deliberately did not address privacy concerns in section 107.[53] The FAA's mission is to maintain a safe and efficient national airspace, and privacy is beyond its mission set and subject matter expertise.[54] Congress is the Federal entity best positioned to address private citizens' privacy concerns.[55] Justice Alito, in the Jones concurring opinion, noted, "[t]he availability and use of these and other new devices will continue to shape the average person's expectations about the privacy of his or her daily movements . . . A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."[56]

g. Detection Challenges

i. Effectiveness

Detecting a COTS drone is possibly the most challenging part of countering a UAS. "Consider that a drone capable of carrying a small package flying at an altitude of 400 feet with

[50] *Id*.
[51] Latham & Watkins, Client Alert Commentary No. 2364, *Congress Evaluates Regulatory Path Forward for Integrating Drones* 3 (Aug 15, 2018), https://www.lw.com/thoughtLeadership/congress-evaluates-regulatory-integrating-drones.
[52] *Id*.
[53] Urban, *supra* note 40, at 19.
[54] *Id*.
[55] *Id*. at 20.
[56] *Id*. at 18 (citing, Jones, 132 S. Ct. at 963-64 (Alito, J., concurring), referenced in Yin, *supra* note 47)).

an air speed of thirty to forty miles per hour will look 'like a tiny dot moving in the sky' and will be quiet enough that it cannot be heard."[57] "Detection, whether through radar, acoustic, optical or [infrared] surveillance is problematic given the small stealthy size of these devices."[58] Military air defense systems are generally ineffective against drones; their radars were designed to detect large, fast moving objects, not small, low-flying ones.[59] Drones can also be constructed with composite materials that absorb radar energy, to better evade radar detection.[60] "In civilian airspace, drones aren't required to carry transponders, so they cannot be detected and tracked with existing air traffic control systems."[61] Electro-optical, infrared, and certain radiofrequency detection systems must have a direct line of sight with the drone before they detect it.[62] The effectiveness of acoustic sensors is dependent on the intruding drone emitting a sound already saved in the sensor's library.[63] Radiofrequency detection is also dependent on the intruding drone to be operating on a frequency band contained in the sensor's library, and, as noted above, may be less effective overall if the intruding drone is not within the line of sight of the sensor.[64]

ii. False Negatives and False Positives

Drone detection systems also need to strike the right balance between being sensitive enough to detect all drones operating within the designated area, but not so sensitive that they "create an overwhelming number of false positives, rendering the system useless."[65] An effective cUAS system needs to be able to discriminate the UAS from other airborne objects like birds, other

[57] Yin, *supra* note 47, at 650-51.
[58] David J. Praisler, *Counter-UAV Solutions for the Joint Force*, Air War College, Air University 10-11 (Apr. 6, 2017), https://apps.dtic.mil/dtic/tr/fulltext/u2/1037984.pdf.
[59] ARTHUR HOLLAND MICHAEL, CENTER FOR THE STUDY OF THE DRONE, COUNTER DRONE SYSTEMS 2 (Feb. 2018), http://dronecenter.bard.edu/files/2018/02/CSD-Counter-Drone-Systems-Report.pdf.
[60] Yin, *supra* note 47, at 651
[61] *Id.*
[62] MICHAEL, *supra* note 59, at 6.
[63] *Id.*
[64] *Id.*
[65] *Id.*

aircraft, or airborne debris, but a system that is not sensitive enough runs the risk of generating false negatives, leading to a potentially catastrophic situation.[66]

iii. Distinction

There currently does not exist a commercially available cUAS system able to distinguish between a legitimate and potentially threatening drone.[67] In the not-too-distant future, drones taking pictures or recording video may become so commonplace that it will be nearly impossible to distinguish a benign user from a terrorist conducting surveillance of potential targets.[68] "Rapid identification can mean rapid threat analysis. For example, if law enforcement officials rapidly identify a drone over a large crowd as a media newsgathering drone, they need not expend resources to counter it. Otherwise, they may be able to identify the drone as a potential threat before the crowd is vulnerable and contact the operator or take direct action against the drone."[69]

h. c-UAS Technology Challenges

i. Interdiction Hazards

Employing an effective cUAS system – if you can first detect the drone – brings additional sets of challenges. The first challenge is that they can present hazards to the very people they're designed to protect. Kinetic cUAS systems are dangerous, and generally result in a drone falling to the ground at considerable speed.[70] Even net-based systems designed with a parachute to bring the captured drone to the ground in a more controlled manner are risky over crowds and in metropolitan areas.[71] Non-kinetic cUAS systems present a different set of hazards.

---

[66] *Id.*
[67] *Id.*
[68] Clarke, *supra* note 4.
[69] Latham & Watkins, *supra* note 51.
[70] MICHAEL, *supra* note 59, at 6-7.
[71] *Id.*

Radiofrequency jamming systems disrupt the drone's communications link with the drone operator.[72] Because the drone, and the jammer, are operating on public frequencies, jamming a drone may disable other common electronic devices in the area, including Wi-Fi, baby monitors, and some personal electronic medical devices.[73] GPS jamming has potential to be even more dangerous, with the ability to interfere with emergency responders and air traffic management systems.[74] For example, a New Jersey truck driver installed GPS-jamming hardware in his truck to prevent his bosses from tracking his movements.[75] As a result, he was single-handedly responsible for disrupting a new piece of air traffic navigation equipment operating at Newark Airport when he drove to jobs.[76] The FCC fined him nearly $32,000.[77] The FAA has advised airports not to employ jammers.[78]

ii. Interdiction Effectiveness

The second challenge presented is that no cUAS system is 100% effective.[79] Despite employing at least eight cUAS systems during the 2016 Rio Olympics, several drones were still observed near and over many events.[80] In 2017, the DoD Joint Improvised-Threat Defeat Organization organized a five-day cUAS exercise; at the end, they found that drones were generally "very resilient against damage" and concluded that most cUAS systems require further development.[81] The limitations on effectiveness are compounded by how rapidly drone

[72] *Id*. at 7.
[73] Douglas Starr, *This Brilliant Plan Could Stop Drone Terrorism. Too Bad It's Illegal.*, WIRED (Feb. 28, 2017), https://www.wired.com/2017/02/sky-net-illegal-drone-plan/.
[74] *Id*.
[75] John Hegranes, *The Past, Present and Future of Anti-Drone Tech*, FORBES (Jan. 26, 2018), https://www.forbes.com/sites/forbestechcouncil/2018/01/26/the-past-present-and-future-of-anti-drone-tech/#19818ba952d6.
[76] *Id*.
[77] *Id*.
[78] MICHAEL, *supra* note 59, at 7.
[79] *Id*.
[80] *Id*.
[81] *Id*.

technology is evolving.[82] Drones are being developed to operate autonomously without a radiofrequency link and in GPS-denied environments, and those that have protected communications links may be resistant to hacking or spoofing.[83] Drone operators are also relatively easily able to get around manufacturer-installed software designed to enable the drone's compliance with Federal regulations.[84]

iii. Electronic Identification

Another challenge is lack of electronic identification. Electronic identification would allow for a drone's exact location, model type, operator name, and registration number to be remotely accessible.[85] The system could also provide the exact location of the drone's operator.[86] The benefit of such a system is, for example, if law enforcement or the FAA were able to tell by the drone's electronic identification that it belonged to and was being operated by a major news broadcasting network, then they would be able to quickly determine that it is unlikely a threat.[87] Industry groups like the Small UAV Coalition are proponents of these systems and urge the FAA to adopt the technology, with the idea that this technology would allow for expanded drone operations, including permissions to fly the drone beyond the visual line of sight and over people.[88]

iv. Legality

Additionally, cUAS systems may be illegal in the U.S. and elsewhere.[89] Radiofrequency (RF) jamming "[d]isrupts the radio frequency link between the drone and its operator by generating

[82] *Id*.
[83] *Id*.
[84] Starr, *supra* note 73.
[85] MICHAEL, *supra* note 59, at 7.
[86] *Id*.
[87] *Id*.
[88] *Id*.
[89] *Id*. at 8.

large volumes of RF output. Once the RF link, which can include WiFi links, is severed, a drone will either descend to the ground or initiate a 'return to home' maneuver."[90] GPS jamming disrupts the drone's navigation satellite link, causing it to hover in place, land, or return home.[91] In the U.S., both jamming systems and systems that detect and track a drone by downloading information about its location and telemetry may violate the Wiretap Act which, as noted above, forbids the interception of or interference with electronic communications.[92] Spoofing is also known as protocol manipulation and allows one to hack into a drone, taking control of the hijacked drone's communications link.[93] Researchers at the University of Texas employed spoofing to hack into a university-owned drone.[94] "The spoofing was done through a mechanism where the hackers were able to get the drone to mistake their signals for the ones sent by the owner's GPS satellites."[95] The research team's concerns that it was not very difficult to hack a drone were confirmed.[96] Spoofing systems may violate the Computer Fraud and Abuse Act, since the system's purpose is to intentionally access a computer without authorization; often also with intent to defraud and/or transmit information.[97] Both kinetic and non-kinetic systems may violate the Aircraft Sabotage Act.[98] "[D]rones are considered aircraft: It's just as illegal to shoot at one as it is to shoot at a Piper Cub, if for no other reason than you can't control where (or on what or whom) a falling drone will land."[99] As detailed above, many non-kinetic cUAS systems' purpose is to disable the drone. The Aircraft Sabotage Act "imposes heavy fines and even prison

[90] *Id*. at 4.
[91] *Id*.
[92] *Id*.
[93] *Id*.
[94] Urban, *supra* note 40, at 4.
[95] *Id*.
[96] *Id*.
[97] MICHAEL, *supra* note 59, at 8.
[98] *Id*.
[99] Starr, *supra* note 73.

sentences for anybody who willfully 'sets fire to, damages, destroys, disables, or wrecks any aircraft' in U.S. airspace."[100] Absent affirmative authority, government employees, including law enforcement officials, are not necessarily exempt from these provisions of title 18, U.S. Code.[101]

v. Lack of Standards

Finally, there are currently no standards for cUAS systems' design and use, raising safety concerns with their application.[102] In a crowded or urban environment, especially, a malfunctioning cUAS system might present a public safety threat (e.g., a jamming system that interferes with emergency response communications, or a kinetic system that misses its target).[103] Additionally, not all cUAS systems are as effective as advertised. In a 2017 report, DHS recommended only 13 cUAS products for use by emergency response agencies, and those recommendations were caveated by them not being based on any live testing.[104]

III. Partial Legislative Remedy for DoD

Recognizing the potential impact to national security, as well as the tension between available cUAS systems and title 18, U.S. Code, Congress has started passing legislation designed to assist Federal agencies with mitigating the threat posed by rogue UAS. DoD was the recipient of initial legislative relief from title 18, U.S. Code in the Fiscal Year (FY) 2017 and 2018 National Defense Authorization Acts (NDAA). DHS and DOJ then leveraged the FY17 and FY18 NDAA language to petition Congress and the public for similar authorities.

---

[100] MICHAEL, *supra* note 59, at 8.
[101] *Id*.
[102] *Id*. at 9.
[103] *Id*.
[104] *Id*.

The FY17 NDAA, in section 1697, added title 10, U.S. Code, section 130i. The FY18 NDAA, in section 1692, further refined title 10, U.S. Code, section 130i. The new section provides that notwithstanding the Aircraft Piracy Act, or any provision of title 18, U.S. Code, the SECDEF may take, and may authorize members of the armed forces and officers and civilian employees of the DoD with specifically assigned duties to take, specified actions necessary to mitigate the threat that a UAS poses to the safety or security of a covered facility or asset.

The actions that Congress specifically authorized include: detecting, identifying, monitoring, and tracking the UAS, without prior consent, including by means of intercept or other access to wire communication, oral communication, or electronic communication used to control the UAS; warning the UAS operator by passive or active, or direct or indirect, physical, electronic, radio, or electromagnetic means; disrupting control of the UAS, without prior consent, including by disabling the UAS by intercepting, interfering, or causing interference with wire, oral, electronic, or radio communications used to control the UAS; seizing or exercising control of the UAS; seizing or otherwise confiscating the UAS; using reasonable force to disable, damage, or destroy the UAS.

A "covered facility or asset" includes any facility or asset that: is identified by the SECDEF, in consultation with the Secretary of Transportation; is located in the U.S.; and directly relates to DoD's missions pertaining to: nuclear deterrence; missile defense; the national security of space; assistance in protecting the President or Vice President; air defense; combat support operations; special operations activities; production, storage, transportation, or decommissioning of high-yield explosive munitions; or a major range and test facility base. As of April 2017, the FAA prohibited UAS flights over 133 military facilities.[105] As of the end of FY18, there were

[105] Fed. Aviation Admin., *FAA Restricts Drone Operations Over Certain Military Bases*, (last modified Apr. 7, 2017), https://www.faa.gov/news/updates/?newsid=87865.

4,150 DoD sites in the U.S., and another 111 in U.S. territories.[106] The SECDEF addressed this delta in April 2018 testimony to the Senate Appropriations defense subcommittee.[107] He testified that UAS overflight of bases, ships, and airfields is being tracked closely, and his concern is for UAS overflight of "normal military bases" that do not fall within the definition of covered facility or asset.[108] He indicated DoD was "probably going to have to come in to the FAA and perhaps even to Congress and ask for additional authorities."[109]

IV. Federal Law Enforcement Legislative Solution

DHS made their case to Congress and the public for why DHS and DOJ needed the same legislative relief from title 18, U.S. Code, as DoD received.

On June 6, 2018, DHS Undersecretary for Intelligence and Analysis David Glawe and Deputy General Counsel Hayley Chang provided written testimony for a Senate Committee on Homeland Security and Governmental Affairs hearing titled, S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones.[110] Their testimony stressed that DHS and DOJ needed to "be provided the exact same relief from Title 18" as DoD, in order to effectively counter the threat that malicious drone operators pose to the public.[111] Their primary concerns with not having relief from title 18 fell into three areas: the challenges posed by the rapid technological advancement of UAS; concern for law enforcement personnel potentially subject

---

[106] DEP'T. OF DEF., BASE STRUCTURE REPORT – FISCAL YEAR 2018 BASELINE DoD – 7, https://www.acq.osd.mil/eie/Downloads/BSI/Base%20Structure%20Report%20FY18.pdf.
[107] Dan Parsons, *Mattis to Congress, FAA: Military Needs More Authority to Shoot Down Drones Over Bases*, DEF. DAILY (May 9, 2018), http://www.defensedaily.com/mattis-congress-faa-military-needs-authority-shoot-drones-bases/.
[108] *Id*.
[109] *Id*.
[110] Dep't. of Homeland Sec., *Written testimony of I&A Under Secretary David Glawe and OGC Deputy General Counsel Hayley Chang for a Senate Committee on Homeland Security and Government Affairs hearing titled "S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones"* (Jun. 6, 2018), https://www.dhs.gov/news/2018/06/06/written-testimony-ia-under-secretary-and-ogc-senate-committee-homeland-security-and.
[111] *Id*.

to criminal liability if they were to take action to mitigate a UAS threat; and the need to have comparable authority as DoD, to facilitate working together on domestic operations, including National Security Special Events and Special Event Assessment Rating events.[112] They note that, if enacted, S. 2836, the Preventing Emerging Threats Act of 2018, would authorize DHS and DOJ to conduct cUAS operations for the limited purposes of identifying, tracking, and mitigating drone threats, while also providing robust measures designed to protect privacy and civil liberties, including the limitation on the collection and retention of communications to and from the drone for purposes only related to mitigating the threat posed by the drone.[113]

On July 4, 2018, DHS Secretary Nielsen published an opinion editorial in the Washington Post, noting that without Congressional action on the Preventing Emerging Threats Act of 2018, "the U.S. government will remain unable to identify, track, and mitigate weaponized or dangerous drones in our skies" because of legal constraints on DHS' and DOJ's authority to develop, test, and deploy cUAS technology.[114] The Secretary closes the piece, in part, by noting that, "[t]he Defense Department already has similar authorities to protect U.S. forces overseas and certain domestic facilities. But it's time we had them to protect Americans here at home."[115] The language of the Preventing Emerging Threats Act of 2018 was incorporated into the FAA Reauthorization Act of 2018, which was signed into law on October 5, 2018 as Public Law 115-302.

The DHS Secretary and the Attorney General now have the authority, notwithstanding the Aircraft Piracy Act, as well as title 18, U.S. Code, sections 32, 1030, 1367, and chapters 119 and

---

[112] *Id*.
[113] *Id*.
[114] Kirstjen M. Nielsen, Opinion, *The U.S. Isn't Prepared for the Growing Threat of Drones*, WASH. POST (Jul. 4, 2018), https://www.washingtonpost.com/opinions/the-us-isnt-prepared-for-the-growing-threat-of-drones/2018/07/04/30cc2a76-7eef-11e8-b9f0-61b08cdd0ea1_story.html?utm_term=.38bfa3b85457
[115] *Id*.

206, to authorize personnel whose assigned duties include the security or protection of people, facilities, or assets, to take actions necessary to mitigate a credible threat that a UAS poses to the safety or security of a covered facility or asset.[116] Congress authorized the same actions for DHS and DOJ, as it did for DoD, and the robust privacy and civil liberties measures referred to by Undersecretary Glawe and Deputy General Counsel Chang are also incorporated, including: that communications to and from a UAS will be intercepted, acquired, accessed, or maintained consistent with the First and Fourth Amendments and applicable Federal law; those communications will be intercepted or acquired only to the extent necessary to execute an enumerated, authorized action; absent an ongoing investigation or legal proceeding, records of such communications will only be maintained for as long as necessary and for not more than 180 days; such records of communications will not be shared outside of DHS or DOJ unless necessary to support a Federal investigation into or prosecution of a violation of law; and DHS and DOJ are authorized to share threat information, but not communications, with local law enforcement.[117]

The "covered facility or asset" definition gives far more latitude to DHS and DOJ than to DoD, and includes: a facility or asset identified by the Secretary or Attorney General, in consultation with the Secretary of Transportation; located in the U.S.; and directly relates to one or more missions: authorized to be performed by DHS, pertaining to U.S. Customs and Border Protection functions, U.S. Secret Service protection operations, or protection of facilities pursuant to 40 U.S.C. § 1315(a); authorized to be performed by DOJ, pertaining to FBI and U.S. Marshals Service protection operations, Federal Bureau of Prisons' protection of penal, detention, and correctional facilities, and protection of the buildings and grounds leased, owned,

[116] FAA Reauthorization Act of 2018, Pub. L. No. 115-302, § 1601, 132 Stat. 3186 (2018).
[117] *Id*. at § 1602 (note, 10 U.S.C. § 130i(e) also contains similar privacy safeguards).

or operated by or for the DOJ, and the provision of Federal court house security; by DHS and/or DOJ pertaining to National Special Security Event and Special Event Assessment Rating events, support to state and local law enforcement, and protection of an active Federal law enforcement investigation, emergency response, or security function; and authorized to be performed by the U.S. Coast Guard.[118] The authority to employ cUAS measures to protect the buildings and grounds leased, owned, or operated by or for the DOJ, and as part of missions authorized to be performed by the U.S. Coast Guard, for example, is far more expansive than that currently granted to DoD.

Notably, this relief from title 18, U.S. Code, to conduct cUAS operations does not extend to local law enforcement officials, even though they "are often in the best position to deter, detect, immediately investigate, and, as appropriate, pursue enforcement actions in response to unauthorized or unsafe UAS operations."[119]

V. Future Challenges

a. Managing the Electromagnetic Spectrum

With jamming as the most commonly-available cUAS technology, and the reprieve from title 18, U.S. Code, that DoD, DHS, and DOJ have been granted, there is more competition than ever for space on the publicly-available portions of the electromagnetic spectrum.

Management of the electromagnetic spectrum in the U.S. is bifurcated between the National Telecommunications and Information Administration (NTIA) and the FCC.[120] NTIA manages the Federal Government's use of the spectrum; the FCC manages all other use.[121] The

[118] *Id*.
[119] Fed. Aviation Admin., *Law Enforcement Guidance*, *supra* note 9.
[120] Nat'l Telecomm. & Info. Admin., *Who Regulates the Spectrum*, https://www.ntia.doc.gov/book-page/who-regulates-spectrum.
[121] *Id*.

Communications Act of 1934 played a crucial role in allocating radiofrequency bands and authorizing frequency use, but it does not provide for specific band allocations for Federal or non-Federal use; allocations that exist are a result of agreement between NTIA and FCC.[122] While NTIA and FCC have separate constituencies, the agencies' close coordination is required since 93.1% of the spectrum below 30GHz is shared use (5.5% is allocated exclusively to the public sector, 1.4% is allocated exclusively to the Federal government).[123]

COTS drones "are controlled through the public part of the radio spectrum (either 2.4 or 5.8GHz)."[124] Each band of the spectrum has its advantages and disadvantages; 2.4GHz is the lower frequency but has a farther reach, while the 5GHz band has the capacity to carry more transmissions over a shorter distance.[125] DJI brand products account for approximately 70% of the COTS drone market, and generally both operate and transmit at the 2.4, 5.2, and 5.8GHz frequencies.[126] Jamming works by blasting radio waves at those specific frequencies to make a drone deaf to its controller, causing the drone to return to its operator or land.[127] A similar result occurs by jamming at the GPS frequency.[128]

While UAS and cUAS jamming systems operate at the 2.4GHz frequency, so do many other products members of the public have come to rely on. Put another way, "[y]ou live your life at 2.4GHz. Your router, your cordless phone, your Bluetooth ear piece, your baby monitor and your garage opener all love and live on this radio frequency and no others."[129] Personal medical

---

[122] *Id*.
[123] *Id*.
[124] Starr, *supra* note 73.
[125] John Patrick Pullen, *Here's How Wi-Fi Actually Works*, TIME (Apr. 24, 2015), http://time.com/3834259/wifi-how-works/.
[126] DJI, *Mavic Pro Specs*, https://www.dji.com/mavic/info#specs (last accessed Dec. 20, 2018); DJI, *Phantom 4 Specs*, https://www.dji.com/phantom-4/info (last accessed Dec. 20, 2018).
[127] Starr, *supra* note 73.
[128] *Id*.
[129] John Herman, *Why Everything Wireless is 2.4GHz*, WIRED (Sept. 7, 2010), https://www.wired.com/2010/09/wireless-explainer.

devices are also not exempt from this love of 2.4GHz, and rely on radiofrequency wireless technology for purposes such as controlling and programming a device, monitoring patients remotely, and transferring patient data.[130] The Food and Drug Administration cautions patients that, because the airwaves are shared, wireless medical devices may be impacted by other wireless devices in the user's vicinity and may result in data loss or disruption.[131] "Interference is a cost of doing business in wireless."[132] Microwave ovens are to blame for this. When the FCC began establishing which frequencies unlicensed products could broadcast on, they first excluded the ones already in use by radio and TV, then, of the "remaining, usable, unallocated frequencies, they sought out ones that were already being used by existing equipment."[133] Microwaves were very popular, had been commercially available since 1947, and operated at 2.4GHz.[134] While unlicensed, free-for-all frequency overcrowding is a possibility, the FCC is primarily concerned with the frequencies it licenses.[135] The system as it exists now "is administratively manageable, and it affords great opportunities for incumbent service providers to truncate entry (automatically limited by the blocks and channels allocated)."[136]

A proposed solution to potential interference and overcrowding is to treat the electromagnetic spectrum as a natural resource, to be protected and regulated like any other natural resource.[137] Nearly everyone, including the Supreme Court, agrees that the electromagnetic spectrum is a

---

[130] Food & Drug Admin., *Radio Frequency Wireless Technology in Medical Devices* (Aug. 14, 2013), https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077272.pdf.
[131] *Id*.
[132] Thomas W. Hazlett, *The Wireless Craze, the Unlimited Bandwidth Myth, the Spectrum Action Faux Pas, and the Punchline to Ronald Coase's "Big Joke": An Essay on Airwave Allocation Policy*, 14 HARV. J. L. & TECH. 335, 374 (Spring 2001).
[133] Herman, *supra* note 128.
[134] *Id*.
[135] *Id*.
[136] Hazlett, *supra* note 131, at 373.
[137] Patrick S. Ryan, *Treating the Wireless Spectrum as a Natural Resource*, 35 ENVTL. L. REP. 10620 (Sept. 2005).

scare natural (and national) resource.[138] However, the Federal government does not treat the spectrum as a natural resource.[139] The agencies that routinely deal with natural resources have little or nothing to do with the electromagnetic spectrum; as noted above, it is managed by NITA and FCC.[140] If the spectrum is considered as a commons – a resource available to all – some spectrum advocates fear that a "grazing" tragedy will occur if too many broadcasters are allowed unfettered access to the same electromagnetic spectrum "pasture," resulting in harmful interference.[141] By preventing the public from using large swaths of frequencies, "overexploitation" of certain limited frequency bands may be the natural consequence.[142] According to biologist Garrett Hardin, "[f]reedom in a commons brings ruin to all."[143] Underexploitation may also lead to the "tragedy of the uncommons" severely restricting the public's access to untappable, viable portions of the spectrum.[144] "Services that could be efficiently provided to consumers are prevented, therefore lowering social welfare."[145] A complementary proposal is to treat the spectrum as property and assign property rights to frequency band owners, either public or private entities.[146] It is an idea that has been discussed for nearly 70 years.[147] Like land, the electromagnetic spectrum is a scare and finite resource, and "a system of property rights for real estate is generally accepted as a sensible way for our economy to encourage [its] efficient use."[148] "The property right to the use of the spectrum

[138] *Id*. at 10620-21.
[139] *Id*. at 10621.
[140] *Id*.
[141] *Id*. at 10625.
[142] *Id*. at 10628.
[143] Hazlett, *supra* note 131, at 381.
[144] Ryan, *supra* note 136, at 10628.
[145] Hazlett, *supra* note 131, at 382.
[146] Lawrence J. White, *"Propertyzing" the Electromagnetic Spectrum: Why it's Important, and How to Begin*, 9 MEDIA L. & POL'Y 19, 20 (Fall 2000)
[147] *Id*.
[148] *Id*. at 21.

should be defined in terms of specified spectrum frequency band, a specified geographic area, a specified permitted maximum strength of the signal beyond the boundaries of the geographical area, and a specified time period."[149] Even after the spectrum has been allocated, there would still be a role for the NTIA and FCC to play with, for example, maintaining a national registry, administering national enforcement efforts to address large-scale interference problems "(similar to the role of the Environmental Protection Agency in limiting pollution, albeit with a limiting benefit-cost mandate)," coordinating the Federal government's spectrum holdings, representing the U.S.'s spectrum interests in the international forum, and encouraging coordination on technical standards.[150]

Given the millions of COTS drones already in the U.S., moving COTS drones, and cUAS jammers, to another publicly-available frequency may be too little too late, but further refining where, exactly, in the 2.4, 5.2, or 5.8GHz range they operate may be a more viable step to minimizing the potential collateral consequences employing jamming as a cUAS technology implicates. A frequency can be set to broadcast on a certain channel (the 5GHz frequency has more channels than the 2.4GHz frequency), and wireless routers are already good at automatically detecting the best channel to use.[151] There is, of course, risk that drone operators with malintent will find a work-around.

b. Hacking

Given the potential for collateral damage associated with jamming as an interdiction method, the Federal government may be well-served by focusing future cUAS development efforts on hacking technology. Hacking a drone "could give law enforcement a way to take control of

[149] *Id*. at 29.
[150] *Id*. at 32.
[151] Pullen, *supra* note 124.

dangerous drones from a safe distance" and "offers more flexibility than signal jamming or shooting drones out of the sky."[152] In fact, DHS officials have publicly expressed interest in the technology. In Undersecretary Glawe and Deputy General Counsel Chang's testimony, they noted that "a highly effective technology is the ability to access signals being transmitted between a nefarious UAS and its ground controller to accurately geolocate and track both without false alarms, and potentially take over the control of the UAS and/or stop its ground operator without the use of kinetic measures."[153] Echoing this idea, in the DHS Secretary's opinion editorial in the Washington Post, she noted "DHS should be able to access signals being transmitted between a nefarious drone and its ground controller to accurately geolocate both quickly. This would allow authorities to take control of the device or stop its operator on the ground to prevent a potential attack."[154]

Drones are susceptible to hacking because of their exposed technical systems, including configurations such as an open state of all sensors at all times, wireless network, and serially safety structure.[155] In addition to the University of Texas spoofing research detailed above, in October 2016, the Federal Trade Commission (FTC) spent less than $200 to successfully hack into three types of COTS drones.[156] The FTC identified four main points demonstrated by the hacks: (1) because the data was sent unencrypted, researchers were able to take over the video feed on all three drones; (2) with two of the three drones, researchers were able to take control of the flight path and turn off the UAS, resulting in them falling from the sky; (3) the drones'

[152] Hegranes, *supra* note 75.
[153] Dep't. of Homeland Sec., *Written testimony*, *supra* note 110.
[154] Nielsen, *supra* note 114.
[155] Urban, *supra* note 40, at 11.
[156] *Id*. at 12-13.

corresponding smartphone apps gave no indication that a third party had connected to the drone; and (4) each drone acted as a WiFi access point that was not password protected.[157]

If drone operators encrypt or otherwise protect their data, hacking may become a more technically challenging solution to implement. Additionally, Massachusetts Institute of Technology researchers developed an algorithm to protect drone swarms from being hacked.[158] The algorithm "makes the wireless signal controlling a group of robots a unique identifier in and of itself," so any deviations from this unique signal "would be read as false by the drone swarm" and ignored.[159] There is no perfect cUAS interdiction solution, but hacking – including spoofing – may the most promising solution, with the least potential for collateral damage, thereby also likely making it the most compliant with the law enforcement principle of using non-lethal incapacitating weapons that minimize the risk of endangering uninvolved people.

[157] *Id*.
[158] Dvani Sabin, *MIT Just Made Drone Swarms Way Harder to Hack*, INVERSE (Mar. 20, 2017), https://www.inverse.com/article/29297-mit-drone-swarms-hacking-algorithm-wireless-signals.
[159] *Id*.