International Journal of Aviation, Aeronautics, and Aerospace

Volume 7 | Issue 3 Article 11

2020

The Current State of Counter Unmanned Aerial System Policy in the U.S.

Travis L. Cline
Purdue University, cline40@purdue.edu
Damon Lercel
Purdue University, dlercel@purdue.edu
Umit Karabiyik
Purdue University, ukarabiy@purdue.edu
J. Eric Dietz
Purdue University, jedietz@purdue.edu

Small unmanned aerial systems (UAS), more commonly known as 'drones,' are an increasing security risk to fixed facilities due to their ease of use, high performance, and increasing prevalence. Prison systems have experienced incidents where drones were used to introduce contraband, such as cell phones, drugs, and weapons (Harvey, 2018; Otte, 2017). In December 2018, drones disrupted flights for an estimated 110,000 people over several days at London's Gatwick Airport ("Drones Ground Flights at Gatwick," 2018). Systems to counter UAS are rapidly being developed but are often unattainable by a majority of organizations due to high cost, liability concerns, and regulatory restrictions.

The FAA Reauthorization Act of 2018 defines counter unmanned aerial system (C-UAS) technology as "a system or device capable of lawfully and safely disabling, disrupting or seizing control of an unmanned aircraft or unmanned aircraft system" (p. 100). For this paper, C-UAS will include active measures to detect and interdict unwanted UAS traffic by a facility or entity. While geofencing has proven beneficial in deterring casual drone users from overflying restricted or otherwise sensitive areas, it is largely dependent on the drone manufacturer to implement and may be easily disabled by the user. Since the protected facilities have no active control over geofencing it will not be considered a C-UAS.

Industry regulatory standards for C-UAS are in the process of being developed but are not yet implemented. Several governing bodies have been identified to develop technical standards within this field. A multitude of legal issues exist that prevent public and private organizations from conducting C-UAS operations due, largely, to a broad application of the term "aircraft" and subsequent measures to protect manned aviation. Currently, few Federal agencies are legally permitted to use C-UAS technology within the United States within the constraints outlined in Public Law. This paper serves as a collective summary of the current state of C-UAS policy within the U.S. and highlights the current lack of industry standards and identifies major efforts to develop these standards.

Industry Regulatory Standards of C-UAS

As of December of 2019, the *Counter-Drone Systems* report highlighted that there are 537 C-UAS products and systems offered by over 277 different companies (Michel, 2019). It was noted that not a single manufacturer consulted in preparing the report was able or willing to provide operational or test data associated with their systems. This resultant C-UAS environment is one where manufacturers may publish performance specifications that are not established under a testing standard. From a consumer standpoint, this is concerning because manufacturer marketing claims may not match the operational performance of a system. In addition to this, many of the technical standards for drone technology are currently under development, making C-UAS more difficult to implement against the wide variety of methods being used by drone manufacturers (McCabe,

2020). Standardization of these technical aspects is one step toward the reliable performance that will help C-UAS become available outside of the Federal government.

Before a manufacturer sells a product within a market, the manufacturer must first determine if the product category is subject to any regulations or related industry standards. Regulations may require that a product adheres to certain technical specifications or testing standards (Standards Portal, 2020). Generally, these regulations are designed to protect the consumer. For example, a consumer purchasing gasoline that is not produced in accordance with approved specifications or standards could encounter costly vehicle repairs. Failing to adhere to the applicable laws and standards may result in manufacturers being subject to market denial, fines, imprisonment, or other penalties (Standards Portal, 2020). Governments rely on regulations and technical standards specifications generally established by professional bodies or standards organizations to ensure products follow industry best practices. Currently, no standards or regulations exist for C-UAS technology.

Standards Organizations

Several major standard-setting organizations within the U.S. oversee the development of standards within their respective areas of expertise. Examples of this include NSF International, which develops standards related to public health and safety, and the Society of Automotive Engineers International, who develop technical standards for self-propelled vehicles (Standards Developing Organizations, 2020). The American National Standards Institute (ANSI) is a non-profit standards organization that is made up of government, industry, and professional, technical, and trade societies. ANSI manages the establishment and implementation of thousands of standards across virtually all sectors of the economy (Grainger, 2020). ASTM International (formerly the American Society for Testing and Materials) serves similarly to ANSI and develops voluntary consensus standards for products, materials, systems, and services (Grainger, 2020).

Lack of C-UAS Technical Standards

In September 2017, ANSI stood up the Unmanned Aircraft Systems Standardization Collaborative (UASSC) in collaboration with the Federal Aviation Administration (FAA), the Department of Homeland Security (DHS), ASTM, and others, to help research and guide public policy and guidelines concerning the rapidly expanding UAS ecosystem (ANSI UASSC, 2020). The UASSC established a standardization roadmap to identify experts and stakeholders within facets of the UAS ecosystem and to guide efforts for standardization. The document acknowledges that "A comprehensive evaluation template for testing C-UAS systems is needed," and that "standards must be developed for user identification, design, performance, safety, and operations"(McCabe, 2020, p. 377). McCabe

further reports that there is a general lack of standards within the C-UAS industry, noting a significant variance of effectiveness and reliability of these systems. “Detection and mitigation of unmanned aerial threats” was listed as a high priority, and noted that standards in-development are not generally known to the public, due to the sensitive nature of C-UAS implementation for entities entitled to mitigate UAS threats (McCabe, 2020). The USAAC has a comprehensive list of UAS related standards that are currently in development to meet the rapidly growing presence of UAS within the U.S.

Legal Issues Preventing C-UAS Implementation

Federal law prevents organizations from using C-UAS other than a few select federal agencies, such as the Department of Defense (DoD), the Department of Energy (DOE), the Department of Homeland Security (DHS), and the Department of Justice (DOJ). These specific use cases will be discussed in a later section. To better understand these legal concerns, it is important for one to know some of the current detection and interdiction methods. Generally, C-UAS systems work by identifying and potentially tracking an intrusive UAS with sensors designed to detect some characteristic of the UAS. Methods for detecting and tracking include radar, acoustic, electro-optical, radio-frequency, and infrared. Often two or more of these detection methods are used. For example, a coarse bearing and location can be used from a network of acoustic sensors to cue a fine-detect electro-optical sensor on to the target for classification and processing (Siewert et al., 2019).

Interdiction methods involve means to subdue, divert, or destroy an intrusive UAS and can be accomplished through a myriad of means. Table 1 represents a summary of some of the more popular methods employed to interdict a UAS. To successfully mitigate an unwanted UAS threat, a drone must first be detected by sensors, then interdicted by one of the methods discussed in Table 1. Many laws are currently in place that would prevent individuals and organizations from using these methods and carry heavy fines and potential prison time (Michel, 2019).

Table 1
Types of Interdiction Methods Currently Employed

Sensor Type	Description
Radio Frequency (RF) Jamming	Interrupts the RF link between UAV and operator by generating large amounts of RF output. Once the RF link is disturbed, the UAV will land or return to the operator
GNSS Jamming	Interrupts the satellite link used for navigating. Once the satellite link is lost, UAV will hover or land
Spoof	Taking control of the UAV by hijacking the communications link
Kinetic	Destroys portions of the airframe with directed energy, causing a crash
Net	Entangles the UAV or its rotors
Projectile	Employs ammunition to destroy UAV
Combination	Several C-UAS methods employed – commonly tandem RF and GNSS jamming

Note. Descriptions are adapted from Michel (2018, p. 4)

The following represents several of the categories that carry legal implications for the use of C-UAS technology.

Federal Communications Commission (FCC)

The FCC is an independent Federal regulatory agency that regulates domestic and international communications within the U.S. and is the primary authority for communication law and regulation. The FCC is responsible for Title 47 of the Combined Federal Regulations (CFR) and is granted authority through Title 47 of the United States Code (U.S.C.) (FCC, 2010). Title 47 (U.S.C.) Section (§) 301 requires licenses for entities to operate radio transmitters and compliance with FCC regulations. This would require entities to acquire authorization and licenses for the use of any radar UAS detectors, and RF and GPS jamming equipment. Title 47 U.S.C. § 302(a) prohibits the sale and use of devices that interfere with radio reception. Similarly, Title 47 U.S.C. § 333 prohibits maliciously or willfully interfering with any radio communications with a licensed station. This would directly preclude the sale and use of applicable RF and GPS jamming and spoofing operations. In 2016, a Chinese company was ordered to pay over $34 million to the FCC for the sale of signal jammers on their website (Rupprecht Law, 2020). The FCC related laws preclude several of the more popular interdiction methods commonly used by the federal government to include spoofing and jamming.

Criminal Code

Small unmanned aircraft are required to register with the Federal Aviation Administration (FAA) per Title 14 C.F.R. § 48.15 in which the definition of

"aircraft" is adopted from Title 49 U.S.C. § 40102 as "any contrivance invented, used, or designed to navigate, or fly in, the air." The application of this regulation to UAS inherently implies that small UAS are subject to many of the same laws that apply to larger manned aircraft. Therefore, any individual or organization that interdicts a small UAS may be subject to the same penalties imposed for larger manned aircraft.

Title 18 U.S.C. § 32 prohibits willful disablement, destruction, and damage to any aircraft within the jurisdiction of the United States, and carries a hefty fine and up to a 20-year prison sentence. This statute bans the use of kinetic, net, projectile, and other potentially destructive means of interdicting a small UAS. . Additionally, many Title 47 statutes that prevent C-UAS include a reference to Title 18 statutes, which carry fines or prison sentences as well. Title 18 U.S.C. § 1367 prohibits the interference with satellite transmissions and carries the penalty of a fine and a prison sentence of up to ten years.

Federal Aviation Administration (FAA)

The FAA established Title 14 C.F.R. § 107 to integrate UAS into the National Airspace System (NAS). Part 107 covers registration, certification, and operational regulations and procedures required to operate a civil small UAS within the U.S. From a legal perspective, an entity that successfully spoofs the UAS link and takes control of the aircraft is required to comply with Title 14 C.F.R. § 107. This requires a successful spoofer to have appropriate FAA certifications, airspace waivers (if applicable), and established a pilot in command for the flight. Additionally, the spoofer is responsible for the condition of the aircraft and the safety of the remaining flight (*Rupprecht Law*, 2020). In essence, the spoofer becomes completely liable for the aircraft and anything that happens for the remainder of the flight. Spoofing has possible additional penalties under Title 49 U.S.C. § 46308, in which a penalty of fines and up to 5 years imprisonment for a person with an intent to interfere with air navigation by interfering with a "true light or signal."

A 2019 FAA letter to airports reiterates some of the criminal penalties that could be leveraged from C-UAS implication and continues to cite some of the additional concerns with airport-specific implementation (FAA C-UAS letter to airports, 2019). This letter discusses the use of UAS sensors as a potential point of contention due to the emissive properties of many of the sensors. For example, while audio sensors are typically considered passive, they are typically required to be networked to other sensors and processing stations to locate and identify threats properly. This is typically through wireless networking between components of the system. The FAA letter cites Title 14 C.F.R. § 77 which requires airports to notify the FAA for any planned airport alterations and sets standards for determining if they cause obstructions to air navigation (FAA C-UAS Letter to Airports, 2019). Additionally, the FAA cautions the use of UAS detection systems due to potential

unknown effects on the navigational facilities and transmitters (NAVAIDs) used by pilots to navigate the national airspace. The letter also cites Title 14 C.F.R. § 139.333, requiring the protection of NAVAIDs as part of the airport certification process. While the FAA acknowledges the potential threat that UAS present, it certainly does not condone the casual use of even passive C-UAS technology for airports.

Legal C-UAS Implementation

Several federal entities are allowed to legally conduct C-UAS per public law. The National Defense Authorization Act (NDAA) FY 2017 allows C-UAS implementation to the Department of Energy (DOE) and the Department of Defense (DoD). Division H of The FAA Reauthorization Act of 2018, also cited as the Preventing Emerging Threats Act of 2018, subsequently grants similar C-UAS implementation to the Department of Justice (DOJ) and the Department of Homeland Security (DHS).

Authorized C-UAS Actions

Both the NDAA 2017 and FAA Reauthorization Act of 2018 use similar verbiage to authorize C-UAS actions to the DoD, DOE, DOJ, and DHS. However, the context and justifications in which C-UAS actions may be employed differ between departments. In general, the DoD and DOE have slightly more freedom to execute actions to "mitigate the threat… to the safety or security of a covered facility or asset" (NDAA, 2017, pp. 641, 758) when compared with the DHS and DOJ actions being limited executing actions to "mitigate a credible threat…to the safety or security of a covered facility or asset" (FAA Reauthorization Act of 2018, p. 339). All four agencies' respective Secretaries are required to consult with the Secretary of Transportation for implementation of these C-UAS actions. This is primarily to mitigate and monitor negative impacts to the National Airspace System. The FAA Reauthorization Act of 2018 and the NDAA 2017 list the following broad actions permitted for UAS threat mitigation by the DoD, DOE, DHS, and DOJ:

- Detect, identify, monitor and track UAS
- Warn the UAS operator
- Disrupt control of the UAS
- Seize or exercise control of the UAS
- Use reasonable force to disable, damage, or destroy the UAS

Permitted DoD and DOE C-UAS Justifications

The primary difference between each of the respective agencies' ability to conduct C-UAS lies in how a 'covered facility or asset' is defined for each agency. Each of the respective agencies' secretary can define a covered asset or facility within the scope of the agency's responsibilities and under broad guidelines outlined in legislation. The NDAA 2017 (p. 759) defines a covered facility or asset

for the DOE as one which is owned by the United States and is used to store or use special nuclear material. Essentially, nuclear facilities are covered and the DOE can take the listed actions above to protect these facilities.

The DoD's 'covered facility or asset' is one that the Secretary of Defense identifies, is within the United States (or territories), and relates to the DoD's nuclear deterrence mission, missile defense mission, or national security space mission NDAA 2017 (p. 642). It is important to note that these restrictions apply only within the United States, and there are tactical guidelines to dispatch unwanted UAVs in combat situations. These provisions allow the DoD to continue strategic missions and deal with potential UAS threats appropriately.

Permitted DOJ and DHS C-UAS Justifications and Additional Restrictions

The DOJ and DHS have more restrictions and additional requirements placed upon them for C-UAS activities as outlined in the FAA Reauthorization Act of 2018 when compared to the DOE and DoD, likely due to the immediate gravity of possible consequences from unmitigated UAS threats from the 'covered facilities or assets' overseen by the DOE and DoD. Both the DOJ and DHS are authorized to take the common C-UAS actions for National Special Security Events and Special Event Assessment Rating events, at the request of the Governor for a specific time and specific event, and to protect active Federal law enforcement investigations, emergency response, or security functions that are also limited for a specific time and event (FAA Reauthorization Act of 2018, p. 344).

The DOJ is also permitted to take C-UAS action to protect the President of the United States and Attorney General, as well as federal detention centers, correctional facilities, and buildings, to include courts, that are owned or operated by the DOJ. The U.S. Marshals Service is somewhat unique in that it is specifically listed to protect certain persons instead of 'facilities or assets' and can take C-UAS action to protect "Federal jurists, court officers, witnesses and other threatened persons in the interest of justice" (FAA Reauthorization Act of 2018, p. 344). The U.S. Attorney General recently published department guidance on the implementation of this Act, describing the processes in which covered facilities will be identified, required risk-based assessments, and other measures designed to preserve First and Fourth Amendment rights (Barr, 2020).

The DHS has several other justifications for taking C-UAS action that are separate from the shared justifications with the DOJ. The DHS is authorized to use C-UAS actions for security and protection functions related to U.S. Customs and Border Protection, Secret Service protection operations, and to protect buildings and facilities occupied or secured by the Federal Government (FAA Reauthorization Act of 2018, p. 344).

The United States Coast Guard (USCG) falls under the purview of the DHS but has unique justifications for authorized use of C-UAS actions and is separately mentioned in the FAA Reauthorization Act of 2018. The 'covered facility' for the

USCG is one that is under the administrative control of the Commandant USCG or a vessel or aircraft that is involved in a USCG mission. The USCG may execute C-UAS actions involving a mission escorting or assisting a DoD vessel, other high value or high personnel vessels, to protect the POTUS and VPOTUS, as well as in search and rescue operations (FAA Reauthorization Act of 2018, p. 347).

A summary of the C-UAS implementation for Federal entities can be found in Table 2.

DOI: https://doi.org/10.15394/ijaaa.2020.1515

Table 2
Federal C-UAS Authorized Activity

	Department				
	DoD	DOE	DOJ	DHS	USCG*
Grounds	Facility or asset identified by the Secretary of Defense	Facility or asset identified by the Secretary of Energy	Facility, asset, or persons identified by the Attorney General (DOJ) or Secretary of Homeland Security (DHS) as high-risk and a potential target of unlawful unmanned aircraft activity		Facility under control of the Commandant or a vessel or aircraft operated by, assisted by, or otherwise involved in a mission with the USCG
Location	Located within the United States or one of its territories				Not explicitly bound by location
Justifications	1) Nuclear deterrence mission 2) Missile defense mission 3) National security space mission	1) Storage or use of nuclear material	1) National Security Special Event 2) Special Event Assessment Rating 3) At the request of a Governor 4) Protect active Federal investigation 5) FBI: protection of POTUS and AG 6) Marshals: protection of personnel involved in Federal trial 7) Protection of correctional facilities, courts, and other DOJ buildings	5) U.S. Customs and Border Protection 6) Secret Service protection operations 7) Protection of Federal buildings USCG	1) Assistance or escort mission for DoD 2) Assistance or escort mission for a vessel of national security significance, or a high interest, capacity, or value vessel 3) Protection of the POTUS and VPOTUS 4) National Security Special Event 5) Special Event Assessment Rating 6) Air Defense of US 7) Search and rescue mission

Note. United States Coast Guard (USCG) falls under DHS but has separate grounds and authorized C-UAS justifications

In addition to the necessary coordination with the Department of Transportation and the FAA for all C-UAS activities, both the DOJ and DHS have additional requirements and restrictions placed upon them. Both departments are required to "establish research, testing, training on, and evaluation of" equipment used for C-UAS before its implementation in the field (FAA Reauthorization Act

of 2018, p. 340). Other restrictions on the two departments include civil privacy protections to preserve First and Fourth Amendment rights. Both the DOJ and DHS are only allowed to keep electronic communications and data regarding C-UAS actions for up to 180 days and are prohibited from sharing such information outside of their respective departments unless the Secretary of Homeland Security or Attorney General determines that the information is necessary for prosecution or purposes of ongoing litigation (some exclusions apply to both of these rules). Additionally, semi-annual briefings are required to appropriate Congressional subcommittees regarding any previously mentioned exclusions and activities related to C-UAS policy and efforts (FAA Reauthorization Act of 2018, p. 341-342).

Conclusion

C-UAS implementation and policy are still in the early stages within the United States. As the UAS threat becomes more prevalent, reliable and accessible C-UAS options will need to be available to public agencies and private industry most at risk for drone threats. For this industry to mature, performance standards and testing metrics will need to be developed and adopted that pose minimal adverse effects to the National Airspace System. Once standards are set, new legal definitions can be applied to the equipment in use for manufacturer compliance, and implementation by non-federal entities. The required DHS and DOJ research and testing, coupled with the required semi-annual briefings to the appropriate Congressional committees, may serve as a responsible way to gather insights and data for wider C-UAS adoption. New legal definitions may be needed for UAS to prevent the hefty penalties that may be imposed for their interdiction.

References

7 big problems with counter drone technology (drone jammer, anti drone gun, etc.). (2020, March). https://jrupprechtlaw.com/drone-jammer-gun-defender-legal-problems

ANSI unmanned aircraft systems standardization collaborative (UASSC). (2020, March). https://www.ansi.org/standards_activities/standards_boards_panels/uassc/overview?menuid=3

Barr, W. (2020). *Department activities to protect certain facilities or assets from unmanned aircraft and unmanned aircraft systems*. Retreived from https://www.justice.gov/ag/page/file/1268401/download

Drones ground flights at Gatwick. (2018, December 20). *BBC News*. https://www.bbc.com/news/uk-england-sussex-46623754

Electronic Code of Federal Regulations (eCFR). (2020). [Text]. Electronic Code of Federal Regulations (ECFR). https://www.ecfr.gov/

FAA Reauthorization Act of 2018, Pub. L. No. 115–254, 463 (2018).

Harvey, K. (2018, May 18). *State invests $35k on pilot program to keep unwanted drones out of prisons | KBAK*. https://bakersfieldnow.com/news/investigations/state-invests-35k-on-pilot-program-to-keep-unwanted-drones-out-of-prisons

McCabe, J. (2020). *ANSI UASSC standardization roadmap for unmanned aircraft systems*. 412.

Michel, A. H. (2019). *Counter-drone systems* (2nd ed.). Bard College. https://dronecenter.bard.edu/publications/

National Defense Authorization Act for Fiscal Year 2017, Pub. L. No. 114–328, 970 (2016).

Non-governmental agencies in the safety industry—Quick tips #100—Grainger industrial supply. (2020, March). Understanding ANSI, ASTM International, FM Global, NFPA, SEI, UL and CSA Group. https://www.grainger.com/content/qt-safety-ansi-astm-international-100

OLRC USC. (2020, March). Office of the law revision counsel United States Code. http://uscode.house.gov/browse/&edition=prelim

Otte, J. (2017, November 7). *Drones dropping drugs into prisons; Ohio fights back.* Dayton Daily News. https://www.daytondailynews.com/news/drones-dropping-drugs-into-prisons-ohio-fights-back/GSB3jLP3sy9VMVWiaO31KM/

Siewert, S. B., Andalibi, M., Bruder, S., & Rizor, S. (2019, January 7). Slew-to-cue electro-optical and infrared sensor network for small UAS detection, tracking and identification. *AIAA Scitech 2019 Forum*. AIAA Scitech 2019 Forum, San Diego, California. https://doi.org/10.2514/6.2019-2264

Standards Developing Organizations (SDOs). (2020). https://www.standardsportal.org/usa_en/resources/sdo.aspx

Steps to determine technical requirements for market access. (2020, March). https://www.standardsportal.org/usa_en/key_information/technical_requirements.aspx

UAS detection and countermeasures technology at airports. (2019, May 7). https://www.faa.gov/airports/airport_safety/media/Updated-Information-UAS-Detection-Countermeasures-Technology-Airports-20190507.pdf

What we do. (2010, November 22). Federal Communications Commission. https://www.fcc.gov/about-fcc/what-we-do

Definitions

§	Section (generally used in reference to regulations and statutes)
C-UAS	Counter Unmanned Aerial System(s)
CFR	Code of Federal Regulations
DHS	Department of Homeland Security
DoD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
FAA	Federal Aviation Administration
NAVAID	Aerospace Navigational Aid
POTUS	President of the United States
UAS	Unmanned Aerial System
UAV	Unmanned Aerial Vehicle
SECDEF	Secretary of Defense
VPOTUS	Vice President of the United States