Federal Limits On Counter-Drone Options Need Updating

By **Carter Lee** (April 11, 2025)

Carter Lee

On March 18, Reps. John McGuire, R-Va., and Juan Ciscomani, R-Ariz., penned an interagency letter addressed to the U.S. Department of Defense, the U.S. Department of Homeland Security and the Federal Aviation Administration regarding unmanned aerial systems, or UAS, at the southern border.[1]

The letter's authors noted that, in a recent congressional delegation to the southern U.S. border, personnel on the ground — including U.S. Customs and Border Protection — stated their concern regarding their ability to conduct counter-UAS, or CUAS, operations should foreign drug cartels, for example, attempt a drone attack.

This concern is well founded, because, as cartels and other malicious actors worldwide swiftly and creatively adapt drone technology for nefarious ends, federal policies allowing CUAS options in the homeland have not evolved at the same pace.

As it turns out, a rather complex web of federal laws criminalizes efforts to damage, disable, or even detect and track UAS.[2] While Congress has carved out some ability to conduct CUAS, this limited authority only extends to select departments of the federal government.[3]

As it stands, state and local governments — not to mention private businesses and individuals — are currently stifled in their ability to protect against UAS threats. Legislative action is needed at the federal level to revamp policies and expand authority to prevent and deter dangerous drone activities.

CUAS Legal Constraints

Perhaps the best summary of the legal minefield associated with CUAS is found in a 2020 advisory from the FAA, the U.S. Department of Justice, the Federal Communications Commission and DHS to guide nonfederal public and private entities on the use of technology to detect and mitigate UAS.[4]

The advisory handily breaks down CUAS legal considerations into two main categories that penalize or limit the use of UAS detection and mitigation capabilities as follows: (1) federal criminal laws; and (2) federal laws and regulations administered by the FAA, the FCC and DHS.

While acknowledging that certain federal government departments have limited authority to conduct CUAS notwithstanding these laws, the advisory observes that state, local, tribal and territory governments and private sector entities have not been granted such authority.[5]

Currently, federal criminal laws that apply to protect traditional aircraft are also interpreted to apply to protect UAS.[6] In turn, the Aircraft Sabotage Act criminalizes destructive actions concerning aircraft, and thus prohibits damaging, destroying or disabling UAS. Taking CUAS action may also violate the Aircraft Piracy Act, which criminalizes seizing or exercising control of an aircraft with "wrongful intent."

With respect to legal limitations on UAS detection capabilities, the advisory notes that systems using radio-frequency capabilities to detect and track UAS by monitoring communications may implicate the Pen/Trap Statute and the Wiretap Act.

Generally, these statutes criminalize the interception of electronic communications and associated data, and they can apply to CUAS activities, since they can involve technologies that intercept data or electronic communications between a UAS and its remote control device.

The Pen/Trap Statute criminalizes "the use or installation of a device or process that records, decodes, or captures non-content dialing, routing, addressing, or signaling (DRAS) information."[7] This being the case, any CUAS technology that collects DRAS information, like device serial numbers, cell site information, media access control addresses, international mobile equipment identity or international mobile subscriber identity, may run afoul of the Pen/Trap Statute.

For its part, the Wiretap Act's Title III prohibits "intentionally intercept[ing] the content of any ... electronic communication" unless conducted under a court order or a statutory exception applies.

The Wiretap Act defines electronic communication as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce."[8]

The Wiretap Act also prohibits the manufacture, assembly, possession, sale, advertisement and distribution of devices that are "primarily useful for the surreptitious interception of wire, oral, or electronic communications."[9]

Other criminal prohibitions that CUAS activities may implicate can be found in Title 18 of the U.S. Code, Sections 1030 and 1367. The former statute, the Computer Fraud and Abuse Act, prohibits intentionally accessing a protected computer without authorization, obtaining information or intentionally damaging a protected computer without authorization.[10]

The latter statute, which concerns interference with the operation of a satellite, generally bars "obstruct[ing] or hinder[ing] any satellite transmission," and would thus prohibit jamming a drone's Global Positioning System.[11]

Limited Statutory Authorities Permitting CUAS Activities

The only entities statutorily permitted to conduct CUAS activities are the DOJ, the DOD, DHS and the U.S. Department of Energy.[12] Congress has authorized these entities by statute to engage in limited UAS detection and mitigation activities to contest UAS presenting a credible threat to covered facilities or assets, notwithstanding other potentially applicable laws such as those discussed above.

The term "covered facility or asset" is separately defined in each of the three statutes granting CUAS authority, and each statute requires the attorney general or respective department secretary to designate the specific "facility or asset" based on the criteria outlined in the statutes.

These statutes also attempt to mitigate the inherent risk of CUAS, by requiring coordination with the FAA and the secretary of transportation.

CUAS Activities and the Risk of Violating Federal Law

State, local, tribal and territorial leadership and law enforcement have not been granted authority to conduct CUAS operations — despite the fact that such entities have general police power.[13]

Thus, even though these entities have the sacred charge of ensuring their people are secure in person and property, they currently risk running afoul of federal law if they engage in CUAS while fulfilling their duty to safeguard the common good. Individuals and private organizations are similarly hamstrung from engaging in CUAS self-help.

But nonfederal entities cannot rely solely on the federal departments currently permitted to conduct CUAS activities to counter the threat from drones. As UAS technology becomes more widespread, the DOJ, the DOD, the DOE and DHS do not have adequate bandwidth to cover the expansive area of the 55 states and territories of the U.S.

So what does a nonfederal government agency or private sector company do? The good news is that citizens do not lose their inherent right to self-defense even if the federal government has imposed strict "rules of engagement" on CUAS activities.[14]

Included in this is the right to defend others,[15] and also to defend against unlawful interference with property rights.[16] The right to protect oneself and others from harm also applies to law enforcement, and officers may use force to carry out their duties to ensure public safety, as long as such use of force is objectively reasonable.[17]

As in any case, multiple factors must fall into place before self-defense, collective self-defense or defense of property could be a plausible affirmative defense to a charge under the Aircraft Sabotage Act or a related offense.

However, if nonfederal entities carefully follow specific procedures and protocols before responding to dangerous drones, their otherwise unauthorized CUAS activities may be defensible.

Such guidelines would need to be designed to help decision-makers positively identify a UAS threat, evaluate the severity of the threat, estimate the potential for collateral damage or other risks of engaging in CUAS, and choose a reasonable use of force or nonkinetic option that is proportional to counter the threat.

Recent Attempts at Legislation

During the last congressional session, lawmakers struggled to pass significant CUAS legislation. The only success was the Counter-UAS Authority Extension Act, which temporarily extended DHS and Federal Bureau of Investigation authorities.

This year, additional short-term extensions were included in the American Relief Act and the Continuing Appropriations and Extensions Act, pushing the sunset date to Sept. 30. Efforts to expand CUAS powers faced opposition, including a bill blocked by Sen. Rand Paul, R-Ky., over Fourth Amendment concerns.

In the current session, new bipartisan efforts include federal grants for drone operations, training standards for CUAS use, and a bill by Sens. Tom Cotton, R-Ark., and Jacky Rosen, D-Nev., to bolster aerial security at major events.

The most expansive proposal seeks to create a U.S. Department of State domestic protection mission for UAS, granting the secretary of state limited CUAS authority similar to that of the DOJ, the DOD and DHS.

The Path Ahead

The increasing proliferation of UAS presents both opportunities and challenges. While drones offer significant benefits across various sectors, the potential for nefarious activities necessitates a robust CUAS framework.

To address UAS threats comprehensively, it is imperative to empower nonfederal entities to partner with federal agencies and law enforcement in a mutually supportive effort. This requires a holistic approach to CUAS, encompassing policy, capacity building, domain awareness and cooperation between multiple governmental entities.

A cornerstone of effective CUAS operations lies in empowering appropriately trained private sector and law enforcement entities with advanced detection and mitigation technologies. Current legal restrictions often hinder the ability of these entities to address drone threats proactively.

For example, there is currently no authority to permit federally requested assistance to protect critical infrastructure operated by utility companies and transportation businesses. Laws must be modified to allow nonfederal law enforcement or critical infrastructure owners and operators to submit requests for CUAS support to an appropriate federal sponsor — e.g., DHS or the DOJ.

Another helpful legislative update would be to modify the Aircraft Sabotage Act and the Aircraft Piracy Act to specify that these statutes do not apply to unmanned aircraft.

In addition to changing the laws to make CUAS protection of critical infrastructure an authorized mission for DHS and the DOJ upon request of nonfederal authorities or the infrastructure's owners or operators, the DOD could be allowed to empower the nonfederalized National Guard to support such requests.

Another option would be to pass legislation to explicitly authorize National Guard support to law enforcement under Title 6 of the U.S. Code, Section 124n, providing a solid legal foundation for their involvement in CUAS activities during domestic emergencies.

Finally, alongside legislative and policy changes, it is essential to educate all potential stakeholders in the process to conduct CUAS operations in collaboration with the appropriate governmental entities.

This education should cover legal considerations, operational procedures, technology utilization, potentially adverse secondary effects of CUAS devices and activities, and communication protocols.

Ultimately, addressing the evolving threat of nefarious drone activity requires new federal legislation to broaden the authority to conduct CUAS activities. This will allow a more comprehensive and practical CUAS framework — and enhance domestic security.

C. Carter Lee is a principal at Woods Rogers Vandeventer Black PLC. He is also a colonel in the Virginia National Guard, serving as the state judge advocate.

[1] https://mcguire.house.gov/media/press-releases/rep-john-mcguire-and-rep-juan-ciscomani-pen-inter-agency-letter-regarding.

[2] See 18 U.S.C. § 3218 U.S.C. § 1030; 18 U.S.C. § 1367; 18 U.S.C. § 2510, et seq.; 18 U.S.C. § 3121, et seq.; 47 U.S.C. § 333, 501-502; 49 U.S.C. § 46502.

[3] 6 U.S.C. § 124n, 10 U.S.C. 130i, 50 U.S.C. 2661.

[4] See generally Advisory on the Application of Fed. L. to the Acquisition & Use of Tech. to Detect & Mitigate Unmanned Aircraft Sys., 2020 WL 4812511, at *4 (OHMSV Aug. 1, 2020).

[5] Id. at *2.

[6] Id. at *4.

[7] Id. at *2.

[8] 18 U.S.C. § 2510(12).

[9] 18 U.S.C. § 2512.

[10] 18 U.S.C. § 1030

[11] 18 U.S.C. § 1367

[12] 2020 WL 4812511, at *1 (OHMSV Aug. 1, 2020).

[13] See U.S. Const. Amend. X.

[14] See Bailey v. Comm, 200 Va. 92 (1958); U.S. v. Black, F. 2d 314 (4th Cir. 1982).

[15]See Foster v. Comm., 13 Va. App. 380, 385, 412 S.E.2d 198, 201 (1991) ("the right to defend another is commensurate with self-defense").

[16] See Diffendal v. Comm., 8 Va.App.417 (1989) (holding that privilege to protect property from trespassers was defense to charge of brandishing a firearm); Montgomery v. Comm., 98 Va. 840 (1900) ("a man may rightfully use as much force as is necessary for the protection of his person and property").

[17] See Graham v. Connor, 109 S.Ct. 1865 (1989).