When is Drone Interception Considered Legal?

Sep 24, 2017

This post is also available in: עברית (Hebrew)

Are the laws regarding unmanned aircraft systems unsuitable for the current circumstances? US Federal agencies have asked Congress to change laws that prevent law enforcement departments from taking down small UAS that present a threat, according to a senior official with the U.S. Department of Homeland Security (DHS).

The push comes as the Department of Defense (DOD) has issued guidance allowing military installations to destroy rogue drones, according to ainonline.com.

Interagency working groups advising the White House National Security Council (NSC) have recommended changes to Title 18, the federal criminal code, said Anh Duong, UAS program executive officer with the DHS Science and Technology Directorate. "Many years ago, when we wrote those laws, when [Congress] passed those laws, we never anticipated something that will one day fly in the air and be both an aircraft and a flying laptop. We're running [up] against statutes and laws and regulations that restrict the ability of law enforcement to counter drones, so we need to fix those laws."

The Wiretap Act prevents law enforcement departments from intercepting "wire, oral or electronic" communications without a court order; the pen register law prevents the use of pen register or "trap and trace" devices that trace telephone calls, including cellular communications. Loosening those restrictions would allow a DHS law enforcement branch such as the U.S. Secret Service to disrupt or disable the radio frequency link between a drone and its operator—euphemistically to "mitigate" a perceived threat.

"We have a joint interagency proposal at [Congress], to propose certain changes so that we can give adequate authority to law enforcement for countering UAS," she told AIN. "We are talking about two things: whether a particular law enforcement entity has authority to counter UAS and even if that entity does, what kind of technology can [it] use? Certain technologies are illegal because of the Wiretap Act and the pen register act."

Duong added: "The most effective counter-drone technology in order to detect and then do something about it is basically take over the communication between the drone and the ground controller in order to tell it to do something else, and we're not allowed to do that because it's like hacking into somebody else's computer. To be frank, the most effective technologies are the ones that are illegal."

Domestic federal agencies are advancing counter-drone systems and strategies in concert with the DOD. In April, the Federal Aviation Administration announced the creation of no-drone zones over 133 U.S. military facilities, citing a "Special Security Instructions" regulation applying to air defense identification zones. Last month, the DOD said it had issued new guidance to the military services and installations permitting them to track, disable or destroy drones deemed to be threats. The guidance, sent on August 4, followed classified guidance sent to installations in July.