Incisive Law Article
Aug 2020

Counter-Drone Tech and the Challenges Thereof

incegd.com

Asia, Middle East, Europe

Counter-Drone Tech and the Challenges Thereof

Drone detection technologies have been a blind spot for most governments across the world, and it gains significance in the current times considering that drones are now being used for commercial purposes. Thus, protecting civilians and civilian infrastructure from drone threats is increasingly becoming a broad but a very specific task. Drone threats may arise from as simple a case as of carelessness (such as a drone flying too close to an airport[1]) to as grave and *mala fide* as a drone bearing ammunitions hitting a bridge, or a building (as an act of terrorism)[2].

Counter-drone systems are failing spectacularly against the continued proliferation and use of the drone technology, which is rapidly outpacing the systems put in place to check and adequately safeguard drone 'threats' especially in commercial environment(s).

Counter-drone systems use a variety of different methodologies to detect nearby aircraft at low altitudes, including radar, radiofrequency (RF) sensors and electro-optical / infrared cameras (EO/IR). However, like with all technology, these systems also have weaknesses, which have the potential of being exploited by drone operators. For instance, radars are ineffective at distinguishing between birds and drones, and many radar systems are reliant on line-of-sight plus the object's flight movement to consistently track it.

With the easy availability of drones, the number of drones within the airspace has continued to rise, and thus, it is unsurprising that the availability of counter-drone technologies has likewise increased. But, like with drone threat, the threat posed by counter-drone systems is equally dangerous. A thorough understanding of both the applicable law as well as the technology's functionality is the over-arching need of the hour.

In order to address the conundrum posed by the increasing drone threats to the public and private entities, the U.S. Government has recently released an advisory on the application of federal laws to the acquisition and use of technology to detect and mitigate unmanned aircraft systems ("Advisory")[3].

The Advisory has been jointly issued by the Federal Aviation Administration (FAA), the Department of Justice (DoJ), the Federal Communications Commission (FCC) and the Department of Homeland Security (DHS) and provides a brief overview of the applicable federal laws and specifically addresses two categories: (i) the provisions of the U.S. criminal code enforced by DOJ, and (ii) the federal laws and regulations related to aviation safety and efficiency, transportation and airport security, and the radiofrequency spectrum administered by the FAA, DHS, and FCC respectively.

[1] https://www.channelnewsasia.com/news/singapore/drones-flight-disruption-changi-airport-dangers-risks-11659624

[2] https://www.dw.com/en/drones-could-be-used-in-terror-attacks-eu-security-chief-fears/a-49876427

[3] https://www.justice.gov/file/1304841/download?utm_medium=email&utm_source=govdelivery

Per the Advisory, systems that detect the physical presence of an unmanned aircraft system (UAS), or signals sent to / from the UAS, may violate the federal criminal surveillance laws depending on whether such systems capture, record or intercept the electronic communication to / from the UAS and the type of communication involved.

Similarly, the mitigation capabilities of counter-drone tech may implicate criminal prohibitions against intercepting and interfering with communications, damaging a 'protected computer', and damaging an 'aircraft'[4].

In addition to breaching the federal criminal laws, the acquisition, installation and use of UAS detection and/or mitigation technology may violate other laws and regulations administered by the FAA, FCC and the Transport Security Administration (TSA). Such additional laws may cover (amongst others), laws, rules and regulations in respect of use of airspace, operating certificate(s), interfering with and interruption to air commerce, unauthorised use of spectrum (for radio communications on frequencies requiring individual licenses), sale and operation of jammers for wireless and radio communication(s) etc.

In a nutshell, governments and law enforcement agencies across the world need to be able to look into the sky, see a drone and instantly know whether the drone is supposed to be there or not and if it is not supposed to be there, know exactly where the drone has come from and who is it registered under for the offenders to be brought to justice.

This is exactly what India's institution of the 'Digital Sky' platform[5] aims to achieve. The first-of-its-kind Unmanned Traffic Management (UTM) system facilitates registration and licensing of drones and operators in addition to giving instant clearances to operators for every flight. The controversial "No-Permission, No-Take-off" (NPNT) requirement – long been considered the bane for drone manufacturers and operators in India – might just be the 'simple' answer that sophisticated counter-drone systems are unable to address. The Digital Sky platform allows only those drones that comply with the NPNT protocol to operate in areas demarcated as green and yellow zones, permitting them to fly over almost 70% of the country.

Drone flights over urban areas, near defence and strategic installations, airports and border areas, which are categorised as red zones, will require clearance from relevant security agencies before take-off. This means that for green / yellow zones, operators will get automatic clearance and for red demarcated zones, the security agencies will receive specific clearance request. All data and information is uploaded on to the Digital Sky platform so that there is no scope for arguments to the contrary at a later stage. Once the operator has been identified and intercepted, bringing the alleged offender to justice can be left to the discretion of the judiciary.

[4] In the FAA Reauthorization Act of 2018, the US Congress codified the terms 'unmanned aircraft' as an 'aircraft' that is operated without the possibility of direct human intervention from within or on the aircraft – 49 U.S.C. ss 44801(11).

[5] https://digitalsky.dgca.gov.in/

To conclude, it may be stated that both drones as well as counter-drone tech play a vital role in maintaining a healthy drone ecosystem provided the tech (irrespective of whether it is re the operation of drones or to counter them) is used by private entities in a manner that does not circumvent civil liability, nor does it become a threat to national security.

About The Author

Piyush is an aviation expert and heads the aviation and competition practice as well as the India desk at Incisive Law LLC in Singapore. More details can be found at https://www.incegd.com/en/our-team/piyush-gupta.

If you have any questions regarding this article, please contact:

Piyush Gupta
Head of Aviation & Competition,
Head of India Practice, Singapore
T: +65 6505 3422
E: piyushgupta@incegd.com