North Dakota Law Review

Volume 93 | Number 3 Article 2

1-1-2018

Counter-UAS Applications Illegal Under 18 U.S.C. § 32 Are Justified When Using a Reasonably Defensible Counter-UAS Strategy That Incorporates Risk and Compliance Categorizations

Joseph J. Vacek

COUNTER-UAS APPLICATIONS ILLEGAL UNDER 18 U.S.C. § 32 ARE JUSTIFIED WHEN USING A REASONABLY DEFENSIBLE COUNTER-UAS STRATEGY THAT INCORPORATES RISK AND COMPLIANCE CATEGORIZATIONS

JOSEPH J. VACEK*

ABSTRACT

Drones fly every day in U.S. airspace, and drone operations are forecasted to continue to grow. With that growth comes novel uses for drones, but some uses of drones constitute nuisances, intrusions onto existing legal rights, or even criminal acts. Currently, federal law under 18 U.S.C. § 32 categorically prohibits destruction or interference with any aircraft, which includes a drone. There are technological defensive measures available should a drone pose a threat, and the affirmative defenses of defense of property, self-defense, and necessity are available should the decision be made to violate 18 U.S.C. § 32. Such an active counter-UAS action must be reasonable in response to the threat level for an affirmative defense to be defensible, and a model compliance categorization that correlates with the threat level is suggested as a reasonable baseline.

*†Joseph J. Vacek, J.D. is a 2006 graduate of the University of North Dakota School of Law. He teaches and researches in the discipline of aerospace law at UND. His research includes counter-UAS law and technology, UAS policy and regulation, remote sensing, UAS insurance, and constitutional and privacy issues related to law enforcement and private drone use. The research for this article resulted in an application for a patent applying an artificial intelligence algorithm to a counter-UAS system. Over the years, he has presented his UAS research to the United States Federal Courts System; the Ninth Circuit Court of Appeals; the Eighth Circuit Court of Appeals; the Knowledge Foundation; the International Aviation and Transportation Safety Board Bar Association; and the American Bar Association.

I. INTRODUCTION

There are more than one million drones operating legally in the United States as of the date of this Article. As of 2018, over 1,000,000 Unmanned Aircraft Systems, referred to as UAS or drones, were officially registered in the Federal Aviation Administration's (FAA) database.[1] To put that in context, there are about 320,000 registered piloted aircraft in the United States, which includes sizes from single-engine training aircraft through transport-category jet aircraft.[2] The timespan in which drone registrations outpaced piloted aircraft registrations was approximately one month once the registration system became available, and drone registrations then doubled in a single year.[3] Clearly, the drone industry has succeeded in entering U.S. airspace and is poised to continue to grow. With that explosive growth comes several problems – some uses of drones are nuisances, intrude onto other legal rights,

1. *FAA Drone Registry Tops One Million*, U.S. DEP'T TRANSPORTATION, https://www.transportation.gov/briefing-room/faa-drone-registry-tops-one-million (last updated Jan. 10, 2018).

2. *FAA: More Registered Drone Operators than Registered Planes*, WASH. POST (Feb. 8, 2016), https://www.washingtonpost.com/politics/faa-more-registered-drone-operators-than-registered-manned-aircraft/2016/02/08/384683d2-cec5-11e5-abc9-ea152f0b9561_story html?noredirect=on&utm_term=.8d3d9377c04c.

3. *Unmanned Aircraft Systems*, FED. AVIATION ADMIN., https://www.faa.gov/data_research/aviation/aerospace_forecasts/media/Unmanned_Aircraft_Systems.pdf (last visited Sept. 21, 2018).

or even constitute criminal acts. Currently, federal law under 18 U.S.C. § 32 categorically prohibits destruction or interference with any aircraft, which includes a drone.

This Article explains how a drone can pose a threat, examines the legal framework that prohibits destruction or interference with a drone, and explores available technological defensive measures. The Article then analyzes whether the affirmative defenses of defense of property and self-defense are available should the decision be made to willfully violate 18 U.S.C. § 32. The Article argues that active counter-UAS actions must be reasonable in response to the threat level for an affirmative defense to be defensible, and a model compliance categorization that correlates with the threat level is suggested as a reasonable baseline.

The model compliance categorization includes three categories: Compliant Operators, Noncompliant-Ignorant Operators, and Noncompliant-Purposeful Operators. The threat level analysis correlated to the compliance categories is derived from a common aviation industry risk matrix, which outputs three risk levels: Low, Medium, and High.[4] The proposed Vacek Model applies this approach to reasonable counter-UAS applications currently illegal under 18 U.S.C. § 32 and presents a defensible solution for responding to UAS intruders.

II. SOME DRONE OPERATIONS HAVE EVOLVED INTO A THREAT

From delivery of contraband to prison yards[5] to drone operators curious as to how close they can fly to airliners on approach to landing[6] to corporate espionage,[7] drones have been found to be useful tools in wrongdoing and crime. Even international terrorist groups such as ISIS have used drones to facilitate their activities.[8] While small drones (under fifty-five pounds) are of limited utility in the delivery of physical items or for long-distance missions, the utility of small drones for relatively short-range intelligence gathering,

4. *See* Safety Risk Management Policy, FAA Order No. 8040.4B (May 5, 2017).

5. Tracy Samilton, *Prisons Work to Keep Out Drug-Smuggling Drones*, NPR (Nov. 15, 2017, 5:11 AM), https://www npr.org/2017/11/15/564272346/prisons-work-to-keep-out-drug-smuggling-drones.

6. Stephen Shankland, *Drone Hovers Right Above Jet Landing at Las Vegas Airport*, CNET (Feb. 2, 2018, 5:15 PM), https://www.cnet.com/news/drone-hovers-over-jet-landing-at-las-vegas-airport/.

7. Corporate Risk Services, *Drones: Threat from Above*, G4S, http://www.g4s.ca/-/media/g4s/canada/files/whitepapers/usa/drones_threat_from_above.ashx (last visited Sept. 20, 2018).

8. Mark Pomerleau, *In Drones, ISIS Has Its Own Tactical Air Force*, C4ISRNET (Sept. 21, 2017), https://www.c4isrnet.com/digital-show-dailies/modern-day-marine/2017/09/21/in-drones-isis-has-its-own-tactical-air-force/.

surveillance, and reconnaissance is extremely valuable for relatively low expense.[9] The threats posed by such misanthropic or criminal use of drones can be categorized into physical hazards and cyber hazards.

A. PHYSICAL INTRUDERS THREATEN SAFETY OF FLIGHT AND THOSE ON THE GROUND

While small drones arguably pose little threat to large passenger-carrying airliners, their mass combined with velocity (up to 100 miles per hour) results in potentially lethal force in the event of a direct collision with a human – or at least significant injury from the impact or cuts from rotating blades. Should a small drone disintegrate in flight, the falling pieces may reach terminal velocity and injure people on the ground below. Even though the probability of a catastrophic collision between a drone and an airliner is likely quite low, the consequences of such an event would be severe, potentially resulting in hundreds of deaths, both of airline passengers and people on the ground. The current radar systems used by air traffic control and installed in most large aircraft are not sensitive enough to detect small drones. And even if one is sighted by a pilot, the small size of the drone, coupled with the speed of the jet, leaves too little time for evasive maneuvers. Even so, much more probable than a collision with a jet is a small drone creating a safety hazard to those near or below it when it is operated recklessly at a low altitude. The author of this Article recalls being out for a walk through a public park when a highly modified racing drone "buzzed" him at less than ten feet. The author observed the operator to be using first-person-view (FPV) goggles to control it, without an additional visual observer, and in a congested area below trees where several people were exposed to the threat.

B. CYBER INTRUDERS USING UAS AS TOOLS THREATEN CRITICAL INFRASTRUCTURE AND PRIVATE DATA SECURITY

Less immediately threatening, but much more generally risky to the population as a whole, are cyber intrusions facilitated by drone. An easily grasped example of such a risk was the demonstration of a drone-enabled hack of a printer on the thirtieth floor of an office building.[10] Researchers in Singapore in 2015 coupled a smartphone to a drone, tasked the phone with impersonating a Wi-Fi connection, flew the drone up to the thirtieth floor where the printer was located, and intercepted confidential documents being

---

9. *See, e.g.*, COPTERSAFE, http://www.coptersafe.com/ (last visited Sept. 20, 2018).

10. Kim Zetter, *Hacking Wireless Printers with Phones on* Drones, WIRED (Oct. 5, 2015, 7:00 AM), https://www.wired.com/2015/10/drones-robot-vacuums-can-spy-office-printer/.

sent to the printer.[11] Use of drones as mobile electronic espionage units is alarmingly common, to such an extent that an entire cottage industry has developed around detection and alert systems to combat such espionage.[12] The incredibly accurate, detailed imagery and other remotely sensed data obtainable by small drones poses an additional risk to critical infrastructure. The unique perspective offered by a drone operating at up to several hundred feet, coupled with high-resolution stabilized cameras, allows anyone to obtain detailed data for critical infrastructure, such as dams, electrical transmission systems, power generation facilities, airports, public safety agencies and assets, and military hardware locations.[13] Clearly, the capability to easily obtain the tools that allow bad actors to gain access to, or information about, critical infrastructure or private data is potentially devastating. The risks posed to air traffic and people below from recklessly operated drones is also significant. People also generally dislike the idea of drones compromising their privacy. Together, threatening drone operations have raised the question of countering those threats. At least one case responding to a perceived threat from a drone by use of force has already occurred.[14]

III. COUNTER-UAS IS PROHIBITED UNDER 18 U.S.C. § 32

Federal law currently prohibits any counter-UAS (cUAS) activity beyond detection, tracking, and notification of the intrusion.[15] The three relevant sections of 18 U.S.C. § 32 for cUAS purposes state:

> (a) Whoever willfully—
>
> > (1) sets fire to, damages, destroys, disables, or wrecks any aircraft in the special aircraft jurisdiction of the United States or any civil aircraft used, operated, or employed in interstate, overseas, or foreign air commerce;
> >
> > . . . .

11. *Id.*

12. *See* discussion *infra* Section IV.

13. An example of a drone with this capability is the Snipe Nano UAS by AeroVironment. "Weighing less than 5 ounces, the Snipe requires no assembly and can be operation in less than 60 seconds, providing . . . over 15 minutes of immediate organic tactical overmatch – over the wall, down the alley, around the hill." AEROVIRONMENT, https://www.avinc.com/uas/view/snipe (last visited Sept. 20, 2018).

14. *See* Boggs v. Merideth, No. 3:16-CV-00006-TBR, 2017 WL 1088093, at *1 (W.D. Ky. Mar. 21, 2017).

15. *See* 18 U.S.C. § 32 (2012).

> (5) interferes with or disables, with intent to endanger the safety of any person or with a reckless disregard for the safety of human life . . . ; [or]
>
> . . . .
>
> (7) communicates information, knowing the information to be false and under circumstances in which such information may reasonably be believed, thereby endangering the safety of any such aircraft in flight;
>
> . . . .
>
> shall be fined under this title or imprisoned not more than twenty years or both.[16]

A. UAS ARE AIRCRAFT UNDER *HUERTA V. PIRKER*

As a preliminary matter, the question of whether a UAS is actually an aircraft subject to 18 U.S.C. § 32 and other federal laws and regulations governing the use and operation of aircraft, was answered in the affirmative in *Huerta v. Pirker*.[17] Since *Pirker*, the FAA has promulgated regulations for small UAS[18] and attempted a registration scheme.[19] With the definitional status of UAS – specifically small UAS – settled, regulatory enforcement and policing of rulebreakers becomes pressing, especially so considering the rapid growth of small UAS operations. The relevant question is what defenses are available to property owners or people when UAS operators violate property rights or threaten an individual's physical safety. At first glance, 18 U.S.C. § 32 appears to prevent any such self-help measures, but at least three potential exceptions exist due to the special nature of UAS operations.

B. AT LEAST THREE POTENTIAL EXCEPTIONS EXIST TO THE CATEGORICAL PROHIBITION ON DESTRUCTION OR INTERFERENCE WITH AN AIRCRAFT

While the relevant language of 18 U.S.C. § 32 appears to categorically prohibit destruction or interference with an aircraft, the specific prohibitions were drafted to apply to manned aircraft. This arguably leaves open the possibility of some exceptions for cUAS as currently written, as long as the cUAS process and actions are reasonable. The possible exceptions are related to technological cUAS actions that are simply impossible to execute upon

---

16. *Id.* § 32(a).
17. Pirker, N.T.S.B. Order No. EA-5730, No. CP-217 (Nov. 18, 2014).
18. *See* 14 C.F.R. § 107 (2018).
19. *See infra* Section IV.A.2 for a discussion on registration and statutory hurdles.

manned aircraft. They are: (1) partial temporary disablement by electronic means; (2) interference or disablement unrelated to safety of human lives; and (3) communicating false information to a UAS that does not endanger the safety of the aircraft.

1. *Partial Temporary Disablement by Electronic Means*

Subsection (a)(1) criminalizes a number of actions directed towards aircraft; the list includes setting fire to, damaging, destroying, disabling, or wrecking. Words are known by the company they keep, and all of the listed statutory actions result in significant harm to an aircraft and would put it, to some degree, in a state of emergency – or at least urgency. An intruding drone subject to a cUAS system that triggers the drone's "return to base" function,[20] for example, has indeed been prevented from completing its original planned flight, but it is not damaged, destroyed, or even disabled. Such a command is similar to an air traffic control clearance to an airliner that directs the pilots to a different destination (to avoid bad weather, for example) and is not equivalent to the category of harm intended by the statute. The intruder drone simply follows the new command and returns to its base, which it would also do automatically if it lost its communication link with its operator, or the operator could issue the command if the drone's location became lost. But a cUAS system's interference by commanding a return to base function is still an interference, which implicates 18 U.S.C. § 32(a)(5).[21]

2. *Interference or Disablement Unrelated to Safety of Human Lives*

Subsection (a)(5) prohibits interference or disablement of an aircraft with intent to endanger the safety of any person or with a reckless disregard for the safety of human life.[22] The disablement issue has been treated above, and a cUAS system command to return to base is clearly interference. However, as long as the safety of any person on the ground (since UAS are not piloted and carry no passengers) is not endangered or recklessly disregarded, it appears that the interference would not be proscribed by the statute. Which cUAS actions endanger safety or recklessly disregard human lives is a question of fact and of reasonableness, and a rubric for determining such cUAS actions is discussed in detail later on in this Article.[23]

---

20. For a more detailed technological discussion, *see infra* Section IV.A.
21. *See* 18 U.S.C. § 32(a)(5) (2012).
22. *Id.*
23. *See infra* Section IV.B.2.

3. *Communicating False Information to a UAS That Does Not Endanger the Safety of the Aircraft*

Subsection (a)(7) prohibits "communicating false information to an aircraft knowing the information to be false and under circumstances in which such information may reasonably be believed, thereby endangering the safety of any such aircraft in flight."[24] A return to base command given by a cUAS system is an intrusion into the communication channels between the drone and the operator and would be a false command under the statute because the operator did not give the command. Since the drone obeyed the cUAS "false" command and returned to base, such an action violates the first part of 18 U.S.C. § 32(a)(7).[25] Similar to the analysis of subsection (a)(5), however, endangerment is also a required element.[26] Here, endangerment is tied to the aircraft's safety rather than human safety. As long as the cUAS command does not override the drone's normal safety-compliance software,[27] if installed, or cause an accident, this part of the statute is probably not violated either.

IV. DEFENSIVE MEASURES ARE AVAILABLE

Counter-UAS includes a range of technological defenses, either passive or active. Passive detection and tracking of intruding drones, as well as alerting the property owner or the police, do not violate 18 U.S.C. § 32 because these actions endanger neither aircraft nor bystanders and therefore fall outside the scope of the statute. Active countermeasures implicate 18 U.S.C. § 32 and may fall into an apparent exception from the statute or clearly violate it.[28] Should an active cUAS action such as an electromagnetic pulse, frequency jam, or physical incapacitation or destruction of the drone occur, it more than likely violates 18 U.S.C. § 32.[29] However, the affirmative defenses of defense of property and self-defense may cover such cUAS action if the actions were objectively reasonable.

---

24. 18 U.S.C. § 32(a)(7) (2012).
25. *See id.*
26. *See id.*
27. Two examples of safety-compliance software include geofenced area programs and optical detection and avoidance of obstacle programs. *See, e.g.*, Eddie Schmid, *Geofences and Responsible Drone Flight*, AUTEL ROBOTICS (Dec. 17, 2016), https://www.autelrobotics.com/blog/geofences-and-responsible-drone-flight/.
28. *See supra* Section III.B.
29. *See* 18 U.S.C. § 32 (2012).

A. CURRENT LEGAL COUNTER-UAS MEASURES INCLUDE DETECTION, TRACKING, AND ALERTING

A myriad of detection, tracking, and alerting cUAS systems are advertised to prevent UAS intrusion into sensitive areas, critical infrastructure, or private property.[30] While those systems display technological prowess and offer an initial first step towards effective cUAS, positive identification of a threat and the origin of the threat is necessary in building a defensible cUAS strategy. But no comprehensive database of drones or operators exists. Additionally, a large portion of small UAS are currently not registered due to legal wrangling over registration requirements and the lack of an effective way to enforce those requirements.[31] A mandated Air Traffic Management identification system, ADS-B, is slated to be in effect in 2020.[32] That will help in positive identification for cUAS, but non-compliant intruders still will pose identification problems. Even without such identification, intrusive active countermeasures may still be reasonable even though they violate 18 U.S.C. § 32.

1. *Passive Identification, Tracking, and Alert Systems Are a Step in the Right Direction but Do Not Offer a Meaningful Defense Against Intruding UAS*

There is a wide array of commercially available cUAS systems for purchase that generally advertise to identify, track, alert, and potentially actively engage intruding UAS.[33] All such systems advertised for sale in the U.S. warn potential customers that passive identification, tracking, and alerting is the limit of legal cUAS, but many suggest their products will integrate with an active cUAS system if legally allowed (when located outside the U.S. or operated by a government agency, for example).[34] While identification followed by tracking and alerting forms the basis of any cUAS system, those actions provide information only and are not actually defensive in nature. Of

---

30. *See, e.g.*, DRONE DETECTOR, http://dronedetector.com/ (last visited Sept. 20, 2018); DETECT INC., https://www.detectinc.com/ (last visited Sept. 20, 2018); AARONIA AG, https://www.aaronia.com/ (last visited Sept. 20, 2018); DRONESHIELD, https://www.droneshield.com/ (last visited Sept. 20, 2018); DEDRONE, https://www.dedrone.com/ (last visited Sept. 20, 2018).

31. The National Defense Authorization Act of 2017 restored the 2015 rule for "Registration and Marking Requirements for Small Unmanned Aircraft," 80 Fed. Reg. 78593, which was found to be unlawful in *Taylor v. Huerta*, 856 F.3d 1089, 1093 (D.C. Cir. 2017).

32. 14 C.F.R. § 91.225(a) (2018).

33. *See* sources cited *supra* note 30.

34. *See, e.g.*, DEDRONE, https://www.dedrone.com/products/mitigation (last visited Sept. 20, 2018).

course, any reasonable defense must be based on valid, timely information, and the availability of cUAS systems indicates that the industry and marketplace understand that. There simply are not indiscriminate frequency jammers offered for sale as cUAS systems. Such a system would actually provide defense in that everything using radio communications would be jammed and inoperative, including personal phones and emergency services radios. But that system would not provide any information, tracking, or alert possibility.[35] Indiscriminate cUAS systems raise the very real problem of electromagnetic fratricide, where all other devices within the area are also incapacitated, meaning legitimate communication, control, and navigation functions are disrupted.[36] Clearly, a more selective, discriminating approach is required to successfully counter an intruding UAS without unintentionally disrupting other signals. Therefore, passive identification, tracking, and alert systems address a current need but do not rise to the level of meaningful defense unless followed by action. With action, however, comes potential liability. Before acting, a person or autonomous system authorizing cUAS must positively identify and be certain that the target is a legitimate threat.

2. *Positive Identification of the Threat and Origination of the Threat is a Necessary but Difficult First Step*

It is well established that the doctrine of transferred intent applies in both criminal and tort law. Where an action intended to cause harm "misses" and causes harm to a third party, the liability for the action is the same for the actor.[37] A cUAS system that misidentifies and causes damage to an innocent drone implicates the doctrine of transferred intent. While the defense of a reasonable mistake may be available in such a case,[38] the first step to avoiding liability by transferred intent (and having to raise the reasonable mistake defense) is to ensure the cUAS system can positively identify the threat before actively countering it.

Technologically it is rather simple to sense a nearby drone, and a variety of sensors may be employed to that effect. The sensors in a cUAS system may be visual-spectrum cameras, infrared-spectrum cameras, acoustical-frequency microphones, or radio frequency spectrum sensors, to name a few

---

35. *See, e.g.*, HENSOLDT, https://www hensoldt net/solutions/land/electronic-warfare/vpj-r-multirole-rcied-jammer-family/ (last visited Sept. 20, 2018).

36. DAVID L. ADAMY, EW 104: ELECTRONIC WARFARE AGAINST A NEW GENERATION OF THREATS 284 (2015).

37. *See* RESTATEMENT (THIRD) OF TORTS: TRANSFERRED INTENT § 110(a) (AM. LAW INST., Tentative Draft No. 1, 2015).

38. *See* Caroline Forell, *What's Reasonable?: Self-Defense and Mistake in Criminal and Tort Law*, 14 LEWIS & CLARK L. REV. 1401, 1421-24 (2010).

common sensors. Visual-spectrum cameras are simply video cameras paired with software that runs an algorithm to filter out images that do not match known shapes or silhouettes of drones.[39] The limitation of visual sensors is obvious—a drone may be of an unknown shape and get past the filter since the software does not recognize it as a drone, or the drone may be disguised to look like a bird and evade detection that way. Adding infrared video can address those problems, as drones are powered by motors and produce heat as a by-product, which is easily sensed by infrared video. Infrared cameras can be defeated by shielding or operating when the background temperature is close enough to the drone's temperature that it is invisible to the infrared camera, however. An acoustic sensor can add sensing capability that visual instruments lack by monitoring ambient sound and identifying particular sound patterns associated with drone flight.[40] The major limitation of acoustic sensors is range, since background noise and wind can sharply reduce their effectiveness. Radio frequency spectrum detectors add a highly accurate detection parameter to cUAS systems. All electronics emit radio-frequency radiation when they operate, which is the basis for how radio works.[41] In cUAS, the drone's motors, communication, control, and navigation functions all emit a variety of electronic signals, which provide an electronic "fingerprint" of a particular drone.[42] Together, sensors aggregating visual, infrared, acoustic, and electromagnetic signals have the highest potential accuracy in detecting and positively identifying an intruding drone.[43]

Well-designed and robust cUAS platforms can even match a particular intruder against an internal database to determine the type of drone from a signal analysis alone, but such databases are proprietary and limited.[44] However, that is only the first step. The drone is the unmanned platform operated by the user, and the user's information—the origination of the threat—also must be determined prior to taking action. While a well-designed and robust

---

39. THOMAS M. LILLESAND ET AL., REMOTE SENSING AND IMAGE INTERPRETATION 190-99 (6th ed. 2007).

40. *See generally* BRENDAN HARVEY & SIU O'YOUNG, ACOUSTIC DETECTION OF A FIXED-WING UAV (2018), www mdpi.com/2504-446X/2/1/4/pdf (presenting results from experiments conducted to investigate the viability of acoustic sensing to form the basis of a non-cooperative aircraft collision avoidance system).

41. *See* WIM H. BAKKER ET AL., PRINCIPLES OF REMOTE SENSING 41 (Klaus Tempfli et al. eds., 4th ed. 2009).

42. *Id.*

43. Still, a home-built UAS would be able to defeat many of those sensors by simple disguise or shielding to prevent signal-sending or identification.

44. *See, e.g.*, Alan Perlman, *Master List of U.S. Certified Drone Pilot Directories & Networks*, DRONE PILOT GROUND SCHOOL (Feb. 6, 2017), https://www.dronepilotgroundschool.com/certified-drone-pilot-directory-list/ (a company offering to sell a version of a list of certified drone pilots for marketing purposes).

cUAS platform can accurately determine the type of intruding UAS by database matching, no such database exists for UAS operators. A large portion of small UAS are currently not registered due to legal wrangling over registration requirements and the lack of an effective way to enforce registration requirements.[45]

The FAA Modernization and Reform Act of 2012 (FMRA) specifically excluded amateur hobbyists from regulation.[46] The FAA later promulgated a rule requiring all small UAS operators to register their aircraft.[47] While many hobbyist operators complied, several sued, citing the 2012 FMRA. The United States Court of Appeals for the D.C. Circuit agreed in *Taylor v. Huerta*[48] that FMRA was intended to exclude hobbyists from all regulation, including registration.[49] In December 2017, Congress then specifically required hobbyists to register their drones.[50] Commercial operators are already required to possess a license to operate small UAS by federal regulation.[51] Eventually due to these registration requirements, all amateur hobbyists will have registered their aircraft. While these two operator databases could be used in identification, there still exists the fundamental problem that a person could operate a drone without either a license or registration. Even the best cUAS system coupled to a perfect database of registered operators still would not be able to identify a rogue operator or determine the origination of the threat, nor would it be able to discern whether a particular drone is flown by a particular operator.

3. *Technological Interrogation May Provide a Viable Identification Solution but Is Not Mandated Until 2020*

A potential solution to gaps in the registered operator database is a requirement that all airborne UAS broadcast a unique identifying signal, similar to the requirement that manned aircraft will have by 2020.[52] An aviation regulatory working group, the FAA's Unmanned Aviation System Identifi-

45. DEDRONE, *supra* note 34.

46. FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95, 126 Stat. 11 (codified as amended in scattered sections of 49 U.S.C.).

47. Registration and Marketing Requirements for Small Unmanned Aircraft, 14 C.F.R. § 11 (2015).

48. 856 F.3d 1089 (D.C. Cir. 2017).

49. *Taylor*, 856 F.3d at 1093.

50. National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, 131 Stat. 1283 (2017).

51. 14 C.F.R. § 107.12 (2018).

52. *Id.* § 91.225.

cation and Tracking Aviation Rulemaking Committee (FAA ARC Committee) released its final report in December 2017, highlighting two methods to require UAS to broadcast identification for electronic interrogation.[53] The two methods are direct broadcast and network publishing.[54] Direct broadcast is most similar to the system that aircraft use, called ADS-B, or Automatic Dependent Surveillance Broadcast, where each UAS would transmit an identification signal that can be received by any receiver within broadcast range.[55] The most significant drawback with this method is that transmitting a signal strong enough to provide meaningful identification data requires significant battery power, which is already quite limited on small UAS.[56] The second method, network publishing, would allow UAS to transmit at lower power using location data via an approved Internet-based database that would then be available to users for identification information.[57] The most significant drawback with this method is that both the UAS and the interrogation system must be connected to the Internet to provide positive identification.[58]

The final report recommended both methods be combined in a way that reduces the drawbacks of each individual method as much as possible while providing the benefits of the best of each method, depending on the circumstances.[59] In the cUAS context, intruders with bad intent still pose a problem that a technological interrogation system such as ADS-B cannot address, which is that bad actors may choose to ignore or disable their onboard interrogation/identification system. Even more problematically, the final report from the FAA ARC committee recommended that the interrogation requirements be applied to operators only, not to manufacturers.[60] If that recommendation is adopted, the natural inclination of consumers to demand lower prices will induce manufacturers to continue to manufacture small UAS without ADS-B equipment installed, resulting in a large class of UAS that are essentially unidentifiable – unless the operator elects voluntarily to register it. Persons seeking to protect their property or themselves from intruding drones appear to have little choice: the technological limits and relatively generous regulatory requirements described above result in a rather high probability that a drone will not be positively identified, even with the best

53. UAS IDENTIFICATION AND TRACKING AVIATION RULEMAKING COMMITTEE, FED. AVIATION ADMIN., ARC RECOMMENDATIONS FINAL REPORT 31-32 (2017).

54. *Id.* at 33.

55. *Id.* at 39

56. *See* ROBERT C. STRAIN ET AL., MITRE CORP., A LIGHTWEIGHT, LOW-COST ADS-B SYSTEM FOR UAS APPLICATIONS 1 (2007).

57. ARC RECOMMENDATIONS FINAL REPORT, *supra* note 53, at 33-34.

58. *Id.*

59. *Id.* at 2

60. *Id.* at 3

passive countermeasures. It is only reasonable, then, to determine whether active countermeasures may be engaged to defend from an intruding drone.

4. *Even Without Identification, Active Countermeasures Such as Electromagnetic Pulses, Frequency Jamming, Physical Incapacitation or Destruction or Capture May Be Reasonable Responses to Intruding Drones*

It is axiomatic that no person should be required to submit to another's wrongful act, even though defending oneself from it is a wrongful act on its own. Similarly, the prohibitions of 18 U.S.C. § 32 notwithstanding, no person should be subject to a wrongfully intruding drone and have no recourse of defense. Defensive countermeasures such as electromagnetic pulses, frequency jamming, physical incapacitation, destruction, or capture are all available to some extent. For any unfamiliar with those terms, an electromagnetic pulse, or EMP, in the cUAS context is a directed burst of energy strong enough to damage electrical equipment.[61] The strength of an EMP required to damage a drone depends on how well shielded the drone is. Poorly designed electronic equipment can be highly susceptible to very weak EMPs – an example of that is how a small static charge from walking on carpet can ruin a completely unprotected microprocessor.[62] Frequency jamming is simply transmitting a stronger signal on the same radio frequency as the information signal, which overpowers it and disrupts the information flow.[63] Physical incapacitation, destruction, or capture are self-explanatory and may be accomplished in a variety of ways in the cUAS context. Whether one or more of these countermeasures is appropriate in a given context will be discussed below. First, the foundation for using such countermeasures must be built, and that foundation rests upon the bedrock principle of the right to defend oneself or one's property from harm.

B. THE AFFIRMATIVE DEFENSES OF DEFENSE OF PROPERTY AND SELF-DEFENSE ARE AVAILABLE

Defense of property and self-defense both justify conduct that, while violative of the law on its own, is allowable because the wrongfulness of the original act outweighs the wrongfulness of the defensive act. Justification for defense of property exists when a person uses "reasonable force to protect his

---

61. DEP'T OF DEF., ELECTRONIC WARFARE FUNDAMENTALS A-14 (2000), http://falcon.blu3wolf.com/Docs/Electronic-Warfare-Fundamentals.pdf.

62. *Part 1: An Introduction to ESD*, ESD ASS'N, https://www.esda.org/about-esd/esd-fundamentals/part-1-an-introduction-to-esd/.

63. DEP'T OF DEF., *supra* note 61, at 9-1.

property from trespass or theft, when he reasonably believes that his property is in immediate danger of such an unlawful interference and that the use of such force is necessary to avoid that danger."[64] The amount of force used to defend property must be reasonable,[65] and therefore "[i]t is not reasonable to use any force at all if the threatened danger to property can be avoided by a request to the other to desist from interfering with the property."[66] The Model Penal Code requires a person to make a request to desist before using force, unless that would be useless or dangerous.[67] Justification for self-defense exists when a person who is not an aggressor uses "a reasonable amount of force against his adversary when he reasonably believes (a) that he is in immediate danger of unlawful bodily harm from his adversary and (b) that the use of such force is necessary to avoid this danger."[68] While there is much nuance in the law regarding the duty to retreat,[69] imminence of attack,[70] or injuries to third persons,[71] those considerations apply to other persons, not to objects (like drones).[72] While defending oneself against a drone might conceivably result in injury to a third person, this analysis is focused solely on the question of the applicability of affirmative defenses to cUAS under 18 U.S.C. § 32.

1. *Balancing Defensive Counter-UAS Force with Non-Compliant Operators' Rights by Compliance Categorization Provides the Best Affirmative Defense to a Federal Criminal Complaint or State Civil Claim*

For the purposes of this analysis, intruding UAS can be categorized into three general areas of apparent compliance depending on the nature of the intrusion and data (if any) obtained using a cUAS system. In escalating order of non-compliance and therefore increasing risk, those three areas are: (1) Compliant Operators, (2) Noncompliant-Ignorant Operators, and (3) Non-compliant-Purposeful Operators. The framework presented here isolates the most relevant predictor useful to determine a UAS intruder's threat level, which is the operator's behavior compared to a known set of rules. Such a determination can be accurately made by a software algorithm and would not

64. 2 LAFAVE, SUBSTANTIVE CRIMINAL LAW § 10.6 (3d ed. 2017).
65. *Id.*
66. *Id.* § 10.6(a) (citing State v. Cessna, 170 Iowa 726, 153 N.W. 194 (1915); State v. Woodward, 50 N.H. 527 (1871)).
67. MODEL PENAL CODE § 3.06(3)(a) (AM. LAW INST. 2017).
68. 2 LAFAVE, *supra* note 64, § 10.4.
69. *See id.* § 10.4(f).
70. *See id.* § 10.4(d).
71. *See id.* § 10.4(g).
72. *See id.* § 10.4.

require human input, which lends itself to scalable cUAS systems. While the design of such software algorithms is beyond the scope of this Article, the need for software, rather than a human, to make defensive cUAS decisions is evident by the sheer volume of UAS intrusions currently reported by existing systems in sensitive locations.[73] The threshold requirements of each category will be discussed in detail next.

a. Compliant Operators Would Be Provided the Benefit of the Doubt and Counter-UAS Would Be Limited to Technological Warnings

Compliant Operators are assumed to know the rules and regulations pertinent to drone operation, and that they will follow them. Nonetheless, an operator who knows and intends to follow the rules can still violate them unintentionally. An example of such a mistake could be a commercial UAS operator gathering visual imagery of a bridge for an inspection. During the course of the inspection the UAS is blown off course by gusty winds, momentarily flying over pedestrians on the bridge in violation of federal regulations. Assuming the UAS operator had done due diligence in checking the weather conditions for the flight, the technical violation was unintentional and should not result in punishment. If a cUAS system were in place and a similar intrusion occurred because of a wind gust, the cUAS system should react with appropriately mild defensive measures. To continue with the example, an ideal cUAS system here would have been monitoring the UAS as it was operated outside the boundary line, identifying it either by passive visual/audio/electronic signature or active interrogation.[74] Once the UAS intruded, the cUAS system would compare the vector and time of its intrusion with local weather conditions and geography to prepare a defense. In this example case, the appropriate defense would be a warning, broadcast on the communication frequency of the UAS and relayed back to the operator that an intrusion occurred with a request to exit the protected area. Once the UAS maneuvered outside the boundary, broadcast of the warning signal would cease. A record of intrusions and warnings could be kept and repeat violators could be subject to more formal warnings before aggressive defensive measures would be used.

73. Dan Parsons, *DOD Demands Authority to Destroy Drones in Restricted Airspace*, AVIONICS INT'L (May 9, 2018), https://www.aviationtoday.com/2018/05/09/dod-demands-authority-destroy-drones-restricted-airspace/.

74. *See* discussion *supra* Section IV.A.

b. Noncompliant-Ignorant Operators Would Be Subject to Somewhat Intrusive Technological Verification or Exclusion

Noncompliant-Ignorant Operators would be categorized by comparing their operation of the drone to the rule structure to infer the operator's intent. An example of a noncompliant-ignorant operation would be the operation of an off-the-shelf UAS that has a known signature but is not registered that is then flown as high as the aircraft will go, in violation of the altitude limit of 400 feet. Such behavior is easily quantified as noncompliant-ignorant because the noncompliance is straightforward to determine for a cUAS system. Ignorance can be inferred by the nature of the violation. Non-registration is likely an omission here when paired with the behavior of a maximum altitude flight, since there is little use of a small UAS at very high altitudes. Such Noncompliant-Ignorant Operators would be subject to something more than a mere warning, since their actions are quantitatively more likely to cause harm, albeit unintentionally. In the example of the non-registered drone flying up to maximum altitude, the risk to airline passengers increases, even though insignificantly. Depending on the nature of the violation, a cUAS system could either broadcast a command displayed to the operator (land now!) or code directly to the UAS (return to base).

c. Noncompliant-Purposeful Operators Would Bear the Risk of Destruction or Loss of the Asset

Noncompliant-Purposeful Operators would be categorized by comparing their operation to the rule structure in the same manner as for Noncompliant-Ignorant Operators described above, but the inferred intent is purposeful towards causing harm or criminality. An example of a noncompliant-purposeful operation would be a non-identifiable UAS that has a masked or shielded electronic signature, is not registered, and is continuously flying over critical infrastructure, such as a major airport. The lack of identifying data available to a cUAS system, coupled with the location and nature of the flight, indicate non-compliance and purposeful behavior. Aggressive countermeasures would be the appropriate response in such a case, meaning potential loss or destruction of the UAS, depending on the specific countermeasure used. Countermeasures for capture or destruction must be carefully designed to fit the context in which it is used. In the example given, a UAS flown continuously over a major airport is a significant safety risk and must be mitigated quickly. However, destruction of the UAS is not ideal because

the pieces would fall onto the runways, taxiways, and ramps, effectively closing the airport until all the pieces were cleaned up so as not to be ingested into and damage an aircraft engine.

2. *Correlation of the Existing Safety Management Systems Risk Matrix with the Compliance Categorization Yields a Defensible Counter-UAS Strategy: The Vacek Model*

The above described compliance categorization measures only one variable—intent—needed to yield a defensible cUAS strategy. The other necessary variable must measure the risk posed by the intruding UAS. Fortunately, risk measurement tools are common in the aviation discipline, so applying an appropriate one is simple.[75] Assessing the overall risk an intruding UAS poses requires determination of two initial factors—the likelihood of harm and the severity of harm. These factors are well established as valid predictors of overall risk in aviation.[76] First, the resultant risk combination of likelihood and severity of harm would be categorized into an overall risk of either Low, Medium, or High, per the matrix below.[77]

Severity in the cUAS context would depend on the mass, speed, payload, and other relevant characteristics of the UAS as sensed by the cUAS system. Catastrophic severity would be an event on the level of a collision with an airliner full of people.[78] Hazardous severity would be something like overflight of a large crowd of people where there would be no safe landing place.[79] Major severity would be something like flight over a freeway where a collision with a car could result in a major traffic pile-up.[80] Minor severity would be akin to property damage only, and minimal severity would be legal harm only, such as a trespass.[81]

Likelihood would be assessed based upon geographic location and demographics – for example, whether an area is densely populated or sensitive infrastructure is located nearby.[82] Once the overall risk of either Low, Medium, or High is determined, the compliance categorization described above would be applied using a similar matrix approach. For this final step, the output of the risk matrix would be input as a single variable, with the compliance

75. Safety Risk Management Policy, FAA Order No. 8040.4B (May 2, 2017).
76. FAA Airports (ARP) Safety Management System, FAA Order No. 5200.11 (Aug. 30, 2010).
77. *Id.*
78. *Id.*
79. *Id.*
80. *Id.*
81. *Id.*
82. FAA Order No. 5200.11.

categorization of Compliant, Noncompliant-Ignorant, and Noncompliant-Purposeful being the other variable, per the Vacek Model.[83]

An example to demonstrate how the model would work in practice is useful for clarity. Assume for this scenario that a building security manager of a large multi-story office complex in a busy downtown metropolitan area purchases and deploys a cUAS system. The system reports multiple observations of the same drone landing on an upper-story ledge, loitering for between two and twenty-five minutes, then departing. The system identifies the drone as a commercially available "consumer" drone, and the drone is not displaying registration information or broadcasting registration data. Using the Vacek Model first requires a risk analysis using the risk matrix. Because the flights are occurring in a busy downtown area where injury to people below could result from a forced landing, and because loss of control of the drone is somewhat probable due to operations in a complex environment with long loiter times (most small drones can only remain airborne for about 30 minutes), the risk matrix indicates moderate risk for this example.[84]

Applying the compliance categorization to the example is next. The observed behavior of the drone shows repetitive flights and some loitering. There is no indication of permission to land on the building in the example, and the operation therefore is not compliant with existing UAS rules. Because the drone is not registered or broadcasting compliant identification data, Noncompliant-Ignorant status can be presumed at a minimum. According to the Vacek Model, reasonable defensive countermeasures could include non-destructive interference or a "return to base" command. If the cUAS system broadcasts such a command successfully neutralizing the threat, the data would be archived. If the same drone appears again, it can be assumed that the next flight is purposeful, and at that point nondestructive disablement or temporary capture would be reasonable. As the example shows, the Vacek Model is an iterative process, where the data is stored for retrieval by the system as needed to respond to a threat, or for later use to show that the countermeasure was reasonable in the circumstances.

The Vacek Model described above and tested hypothetically using both risk analysis and compliance categorization, yields a defensible cUAS strategy. As long as the cUAS system is able to gather the maximum amount of data available about an intruding UAS and the algorithm processes the data in accordance with the above procedure, active countermeasures that would otherwise violate 18 U.S.C. § 32 will fall under the affirmative defenses of

83. Copyright Joseph J. Vacek, 2017
84. *See* FAA Order 5200.11.

either defense of property or self-defense. However, algorithms are not perfect and there must be a mechanism to correct mistakes and reimburse legitimate UAS users for loss of their property when a cUAS system incorrectly identifies a threat and deploys active countermeasures.

As a final point, the Vacek Model output must be subject to a post-hoc reasonableness analysis to provide a mechanism for wrongly countered UAS operators to recover damages and to improve cUAS decision-making. The courts are well positioned to determine whether a particular cUAS action was reasonable or not, and good cUAS systems will securely archive the data associated with an active countermeasure so it will be available as evidence in future litigation.

V. CONCLUSION

Explosive growth of UAS use by companies small and large as well as general consumers brings nuisance issues, intrusions onto legal rights, and even criminal acts. While 18 U.S.C. § 32 prohibits destruction or interference with any aircraft, including drones, this Article has explained how countermeasures may be justified using the affirmative defenses of either defense of property or self-defense. Any such counter-UAS actions must be reasonable in response to the threat level for an affirmative defense to be defensible, and a model compliance categorization that correlates with the threat level is suggested as a baseline. The proposed Vacek Model includes three categories: Compliant Operators, Noncompliant-Ignorant Operators, and Noncompliant-Purposeful Operators. The threat level analysis correlated to the compliance categories is derived from a common aviation industry risk matrix, which outputs three risk levels: Low, Medium, and High. When applied to counter-UAS applications currently illegal under 18 U.S.C. § 32, the Vacek Model becomes a defensible solution for responding to UAS intruders.