National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

# A CRITICAL VULNERABILITY STUDY ON COMMERCIAL DRONE IMPACTS ON US HOMELAND SECURITY

**Major Kyle Amonson, USA**

## JCSP 49

## Exercise Solo Flight

**Disclaimer**

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.



## PCEMI n° 49

## Exercice Solo Flight

**Avertissement**

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.



Canada

CANADIAN FORCES COLLEGE - COLLÈGE DES FORCES CANADIENNES

JCSP 49 - PCEMI n° 49
2022 - 2023

Exercise Solo Flight – Exercice Solo Flight

# A CRITICAL VULNERABILITY STUDY ON COMMERCIAL DRONE IMPACTS ON US HOMELAND SECURITY

**Major Kyle Amonson, USA**

ACKNOWLEDGMENTS

Thank you to **August Cole**, for the feedback and inspiration to attempt Useful Fiction.

Thank you to **COL Robert Rodrigues, US Army Fellow, DOJ,** for providing the legal insight to help me understand the intricacies of the Department of Justice on behalf of the Office of Legal Policy.

Thank you to **Director Brent Cotton**, **C-UAS PMO,** for providing an irreplaceable understanding of the C-UAS challenges on behalf of the Department of Homeland Security.

Thank you to **Dr. Levon Bond**, for the guidance in helping to frame and message this critical concern effectively.

**Key Words:** United States Government (USG), Central Intelligence Agency (CIA), Department of Homeland Security (DHS), Customs and Border Protection (CBP), Department of Defense (DOD), Department of Energy (DOE), Department of Justice (DOJ), Drug Enforcement Agency (DEA), Federal Aviation Administration (FAA), Federal Bureau of Investigation (FBI), Federal Emergency Management Agency (FEMA), National Counterterrorism Center (NCTC), National Air and Space Administration (NASA), National Security Agency (NSA), Nuclear Regulatory Commission (NRC), Interagency Security Committee (ISC), Freedom of Information Act (FOIA), Line-of-Sight (LOS), Beyond-Line-of-Sight (BLOS), Global Positioning System (GPS), Potomac Electrical Power Company (PEPCO), Da Jiang Innovations (DJI), Weapons of Mass Destruction (WMD), Continental United States (CONUS), Outside the Continental United States (OCONUS), Violent Extremist Organization (VEO), Complex Coordinated Terrorist Attack (CCTV)

**List of Figures**



**List of Annexes**

**MALICIOUS UAS: A CRITICAL VULNERABILITY STUDY ON COMMERCIAL DRONE IMPACTS ON US HOMELAND SECURITY**

**FBI Headquarters, Springfield, Virginia, USA**
**11 September 2027**

Tension filled the air in the new FBI Headquarter's press conference room as reporters, cameras, and microphones impatiently waited on the arrival of the FBI Director.[1] In contrast to the unseasonably cool autumn Saturday outside, the room was already hot and stuffy, standing room only. At approximately 10:15 PM, the Director entered the room, flanked by key assistants and agents, visibly stressed from the day's chaos. The Director approached the podium and settled herself and her notes before beginning her speech. This was her first month on the job, and she was already facing a major national crisis.

"Good evening, ladies and gentlemen, I apologize for the delay. As you know, Washington, D.C. was the target of a complex coordinated terrorist attack. While we do not know all the facts at this time, I will tell you what we do know. At approximately 1200 EST, a violent extremist organization conducted a coordinated attack against several key locations and individuals within the District of Columbia Metro region.

Our initial investigation indicates that this attack focused on five main targets and leveraged commercial UAS, also known as small-unmanned aerial systems, for their attacks. We are closely coordinating with the Department of Homeland Security, the Federal Emergency Management Agency, and numerous other interagency partners."

Hands shot up across the room from the journalists eager to learn more about the attacks.

"Director, can you tell us more about the separate attacks and what the goal of those targets may have been," asked a reporter from the rear of the room.

"We are still gathering intelligence on the group responsible and assessing their objectives," stated the Director. "Regarding the targeted sites and individuals, I can tell you that the first attack at the Ronald Reagan International Airport utilized four Da Jiang Innovations, or DJI, Mavic 3 drones, which we believe were all laden with a payload of remote-detonated C4.[2] At Reagan International, it appeared that there were two targets. One was Delta Flight 3893, carrying key diplomatic personnel traveling to an engagement in Israel. Those drones, we believe, were "hand-flown" beyond-line-of-sight (BLOS) into the two engines of the Boeing 767 on takeoff, causing an immediate dual-engine failure with a follow-on crash of the aircraft. The remaining two drones, which we

---

[1] As of March 2023, the FBI is identifying a location to relocate their headquarters, from Washington D.C. to either Virginia or Maryland.
[2] While the DJI Mavic 3 is considerably smaller and less expensive than the DJI M600, it can carry a payload of 4.5kg or 10lbs. Pound for pound, C4 is more explosive than TNT. Frackiwicz Marcin, *The DJI Mavic 3 and it's Customizable Payload Configurations*, TS2, 03 March 2023.

assess were flown via GPS coordinates, attacked the airport's fuel depot and remotely detonated simultaneously, which triggered secondary explosions at the depot."

"The target of the second attack, occurring at 1215, was an assassination attempt on the Vice President as he was entering the Smithsonian National Air and Space Museum to participate in the opening of a new exhibit. This attack consisted of two drones, DJI M600s, also laden with C4.[3] We believe these were hand-flown, BLOS, but due to the delay in the Vice President's arrival to the event and the coincidental law enforcement reaction due to the Federal Aviation Administration personnel located in the next adjacent building calling in the small unmanned aerial system (sUAS) sighting, these two drones were detonated at the entrance of the building prior to the Vice President's arrival. While the Vice President is safe, the dual explosions caused significant injuries to law enforcement personnel and damage to the building."

"The third attack targeted power transmission and distribution substations owned by the Potomac Electrical Power Company, created as part of the PEPCO Capital Grid Project. The simultaneous attacks on the Takoma, Harvard, Champlain, and Mount Vernon substations caused significant damage to the PEPCO transmission line. Thousands are still without power. We assess this was carried out with four DJI M600 drones, GPS programmed and modified with plastic explosives."

"Excuse me, Director, when and where does the FBI believe the next attack will be," injected a journalist from the middle of the crowd, clearly in shock from the emerging news.

"Thank you for the question," stated the Director. "We do not believe there are more attacks planned at this time but remain in a high emergency and readiness state," as she quickly refocused on her notes. "The fourth attack consisted of two DJI M600 drones targeting the D.C. Central Detention Facility and Correctional Treatment Facility in Southeast D.C. We assess these two drones were GPS programmed to detonate at the internal and external security fencing of the DOJ facilities. Due to this security breach, several dozen inmates have escaped. The D.C. Metropolitan Police have located many inmates, but several have yet to be found. We do not know if any escaped inmates have specific ties to the group that prosecuted the attack."

"The final attack occurred at Nationals Stadium during the preparations for the city cultural festival utilizing the venue. We are still determining the target for this specific attack, or if there was a specific target. The stadium attack was prosecuted with three DJI Mavic 3s, initially believed to be hobbyist drones photographing the festival. Each drone had an explosive payload, and we are still assessing the injuries and loss of life at this time."

---

[3] According to DJI's website, a DJI Matrice (M) 600 weighs 20 pounds, can carry a 13-pound payload, can hover for 16-40 minutes depending on payload, and can fly up to 40 miles an hour as high as 8000 feet. The DJI M600 costs roughly $4,600 USD.

For a short period, the press in the room fell silent, as many of them were unaware of the scope of the attack due to the power outages limiting information flow following the substation attacks. The press conference continued for a half hour, with the Director providing updates on the various investigations. After the briefing, the director collected her notes and finally addressed the crowd.

"As we assess the likelihood of further attacks, I assure you that we have every available asset working on this investigation and supporting the D.C. Metro Law Enforcement. We pray for the first responders coordinating a multi-state response to the devastation within the District. Our very freedom came under attack in a series of deliberate and deadly terrorist attacks.[4] This will not break us. We will not let the hatred win."

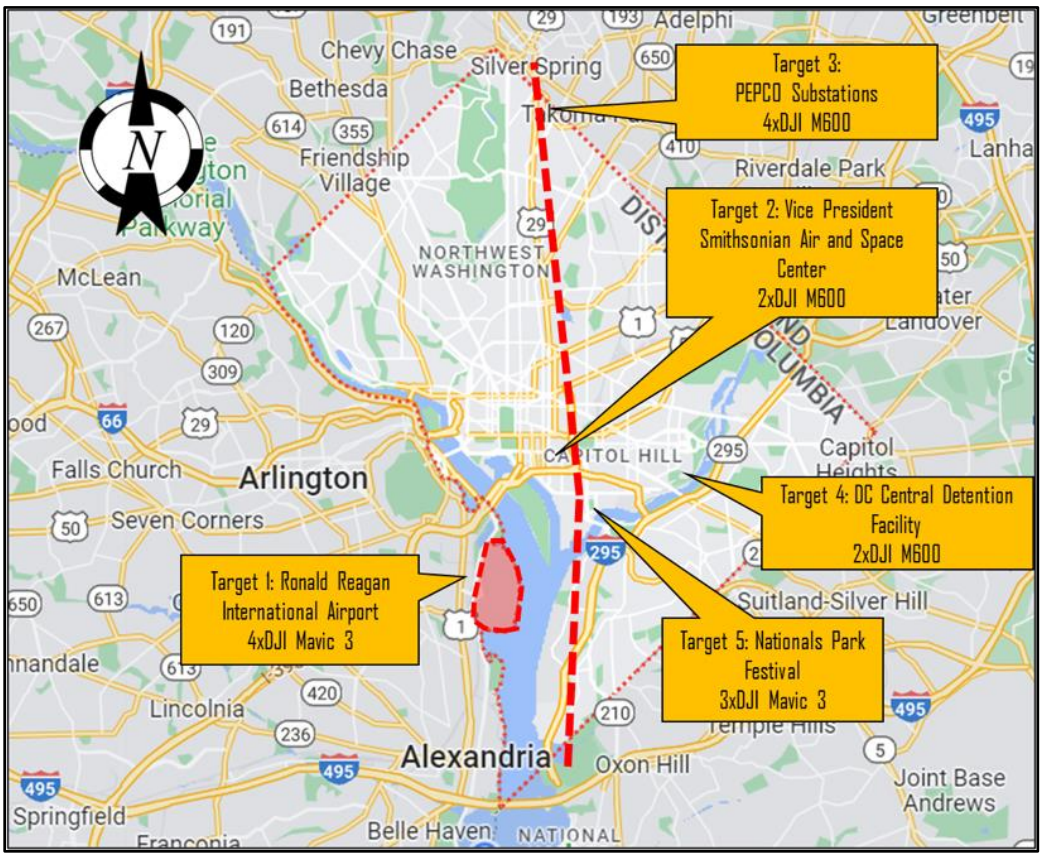



Figure 1: Functional Fiction Narrative Overview

Map Derived: GoogleMaps 02 April 2023

[4] President George Bush, *Address to the Nation After September 11, 2001 Attacks*, https://www.youtube.com/watch?v=WA8-KEnfWbQ.

## Introduction

Looking back on September 11, 2001, even after over 20 years, incites feelings of vulnerability as a violent extremist organization inflicted significant damage on the United States homeland. Since that day, the USG has updated border and travel policies and created numerous homeland security organizations, while countries worldwide took note to quickly address their security vulnerabilities. At its core, 9/11 was a coordinated attack conducted at low cost, utilizing training and technology *initially* used primarily for warfare (pilot training and planes) to inflict maximum damage and chaos.

Modern technological advances have beckoned the age of cyber threats, disinformation and misinformation throughout a range of platforms, leveraging tools from AI bots to deep fake technology, and previously military assets, such as the UAS, are now accessible to hobbyists and terrorists alike. While cyber, EW, space, and information threats still pose their own unique security challenges, the commercial UAS has become commonplace in modern society and provides the access and capability to cause catastrophic damage at extremely low cost and without clear retribution factors.

This essay will seek to understand the critical vulnerabilities that the USG needs to consider concerning the proliferation of commercial UAS. The thesis of this essay is that the rapid development and success of malicious UAS, coupled with the difficulty in countering these systems, will encourage an increase in nefarious domestic UAS employment. Subsequently, while key agencies and departments within the USG recognize the critical threat of malicious UAS, the existing domestic air domain and legal structure precludes both a whole-of-government approach and the necessary authority to interdict domestic UAS threats. This essay will utilize several relevant case studies as an integral part of the research methodology.

## Case Study Overview

The fictional scenario above is not intended to be dramatic. It is designed to display the very real-world vulnerabilities, through useful fiction, that the US now faces with the proliferation of UAS.[5] As written in the Washington D.C. scenario, the cost for employment would be roughly $50,000 USD in total.[6] The damage that 15 sUAS can inflict on a modern city could include crippling critical infrastructure, assassinating government officials, mass casualty attacks, and attacks on DOJ facilities. With many pre-programmable GPS guided UAS, this can be executed with minimal training, leveraging commercial-off-the-shelf (COTS) technology, and BLOS. The four case

---

[5] "Founded by Peter Singer and August Cole, Useful Fiction™ is the deliberate blending of narrative and nonfiction…Useful fiction is a powerful change management tool because it helps people understand and connect with the reasons behind the change." https://useful-fiction.com/why/.

[6] Seven DJI Mavic 3s at $1,800 each, totaling $12,600, and eight DJI M600s at $4,600 each, totaling $36,800, for a grand total of $49,400. This assumes all UAS were purchased new. *This does not factor in the cost of explosive material.*

studies below provide modern examples that directly correlate with each aspect of the fictional attack in the Washington D.C. scenario.

### 1. President Maduro Assassination Attempt, Caracas, Venezuela, 2018

#### *Vulnerability: Targeted Killing, Personnel Security*

The first known assassination attempt on a head of state by commercial drone occurred on 04 August 2018, with Venezuelan President Anthony Maduro as the target. President Maduro was addressing a military parade in the capital city's main avenue when two DJI M600 drones began flying overhead. During the event, security identified the two UAS, at which point they both detonated their explosive payload. Many onlookers initially believed the explosions were fireworks. The first UAS detonated above the viewing stands, resulting in the hospitalization of eight Venezuelan national guard officers. [7] The second UAS exploded nearby, resulting in zero casualties. While the security forces at the event did have cell phone jamming capabilities, they did not have dedicated C-UAS assets.

To this day, many of the facts of this event are still under debate.[8] However, later investigations indicate that a Venezuelan defector group planned this attack outside Venezuela.[9] The group later disassembled the drones, transitioned into Venezuela to carry out the attack, and then reassembled the drones with explosives. A CNN investigation into the assassination attempt stated that their training included "practicing flying the drones high enough to avoid detection, and then swooping down at a steep angle to strike their target in different scenarios: amid green hills over a swimming pool, launched out of a car window, under cover of night."[10]

---

[7] Nick Paton Walsh, Natalie Gallón, Evan Perez, Diana Castrillon, Barbara Arvanitidis and Caitlin Hu, "Inside the August plot to kill Maduro with Drones," *CNN*, 21 June 2019, https://www.cnn.com/2019/03/14/americas/venezuela-drone-maduro-intl/index.html.

[8] Sources inside of Venezuela still state that they believe this was a false-flag attack to "make the government look like victims," and potentially serve as the pretext for a crackdown. Additionally, many of the findings of the Venezuelan government investigation were not released.

[9] Nick Paton Walsh, et al, "Inside the August plot to kill Maduro with Drones," *CNN*, 21 June 2019.

[10] The group ordered the DJIs commercially and modified them to carry explosives, conducting tests and training in rural Colombia. Nick Paton Walsh, *et al*, "Inside the August plot to kill Maduro with Drones," *CNN*, 21 June 2019.


Figure 2: Caracas Drone Attack – Drone 1
Source: New York Times Video – How the Drone Attack on Maduro Unfolded


Figure 3: Caracas Drone Attack – Drone 2
Source: New York Times Video – How the Drone Attack on Maduro Unfolded

Figure 4: Da Jiang Innovations (DJI) Matrice 600
Source DJI Official Website, https://www.dji.com/ca/matrice600

While this example of a defector group targeting a head of state with drones carrying remote-detonated explosives was the first known assassination attempt by UAS at a national level, it is unlikely to be the last. This highlights the first critical vulnerability, personnel security. As the use of drones develops, it will be nearly impossible to ensure an individual's personal security. Whether it is a politician, diplomat, religious figure, or CEO in a high-rise corner office, the UAS can replicate the President Maduro assassination attempt with relatively minimal effort on almost any target. Just as the UAS provides Ukrainian soldiers with the ability to leverage a commercial drone as an ISR platform that transitions to a fires asset once the target is identified, non-state actors and extremists can use an armed UAS, such as a DJI M600 with a 13-pound payload, as a dual role ISR and fires capable airborne weapon.[11]

[11] Benjamin Fogel and Andro Mathewson, *"Will the Drone War Come Home? Ukraine and the Weaponization of Commercial Drones,"* The Modern War Institute at West Point, 08 August 2022, https://mwi.usma.edu/will-the-drone-war-come-home-ukraine-and-the-weaponization-of-commercial-drones/.

## 2. Hershey, Pennsylvania, United States, 2020

## Palo Verde Nuclear Power Plant, Arizona, 2019

*Vulnerability: Key Infrastructure - Power*

"[W]e expect illicit [UAS] activity to increase over the energy sector and other critical infrastructure facilities as use of these systems in the US continues to expand."

- United States Joint Intelligence Bulletin

28 October 2021

On 16 July 2020, a modified DJI Mavic 2 attempted to disrupt the US power grid by short-circuiting an electrical substation near Hershey, Pennsylvania.[12] The UAS operator removed the camera and attached two four-foot nylon ropes connected with copper wires by electrical tape, as depicted in Figure 5 below. The UAS had been stripped of all marking and identifiable features, indicating clear malicious intent.[13]

The primary source for this attack is a Joint Intelligence Bulletin that ABC News acquired from the DHS, published by the DHS, FBI, and National Counterterrorism Center on 28 October 2021. This bulletin stated that because the camera was removed, the operator had to remain within the LOS of the facility to fly the UAS by hand.[14] While the UAS did not achieve the operator's intended effect at the substation, the bulletin stated that "this is the first known instance of a modified UAS likely being used in the US to specifically target energy infrastructure."[15] No operator has been identified, highlighting the difficulties in attribution related to malicious UAS activity.

---

[12] According to their website, the Mavic 2 used in this attack is what DJI refers to as their "flagship consumer drone built for pros and enthusiasts." The max speed of the Mavic 2 is 72 kph (or 45 miles per hour). The Mavic 2 only weighs two pounds and costs $1,500 to $1,750 USD, making it considerably cheaper but much smaller than the DJI M600. Weighing only two pounds, the payload capacity is significantly less than other UAS. However, with 30 minutes of flight time, it can carry only minimal cargo, whether that is explosives, drugs, or wire cutters, as seen in a later case study.

[13] Joseph Trevithick, "Likely Drone Attack on U.S. Power Grid Revealed in New Intelligence Report," *The Drive*, 05 November, 2021, https://www.thedrive.com/the-war-zone/43015/likely-drone-attack-on-u-s-power-grid-revealed-in-new-intelligence-report.

[14] While the operator likely flew the UAS by hand in this scenario and leveraged an attack attempting to short-circuit the electrical grid using the copper wire, another tactic would be to fly the UAS via pre-programmed GPS points and execute a kinetic attack via point detonated or remote detonated explosives. This would bypass any potential BLOS jamming and achieve an impact as described in the useful fiction scenario.

[15] United States Joint Intelligence Bulletin, "Modified Unmanned Aircraft System Likely an Attempt to Disrupt Electricity Distribution," 29 October 2021.

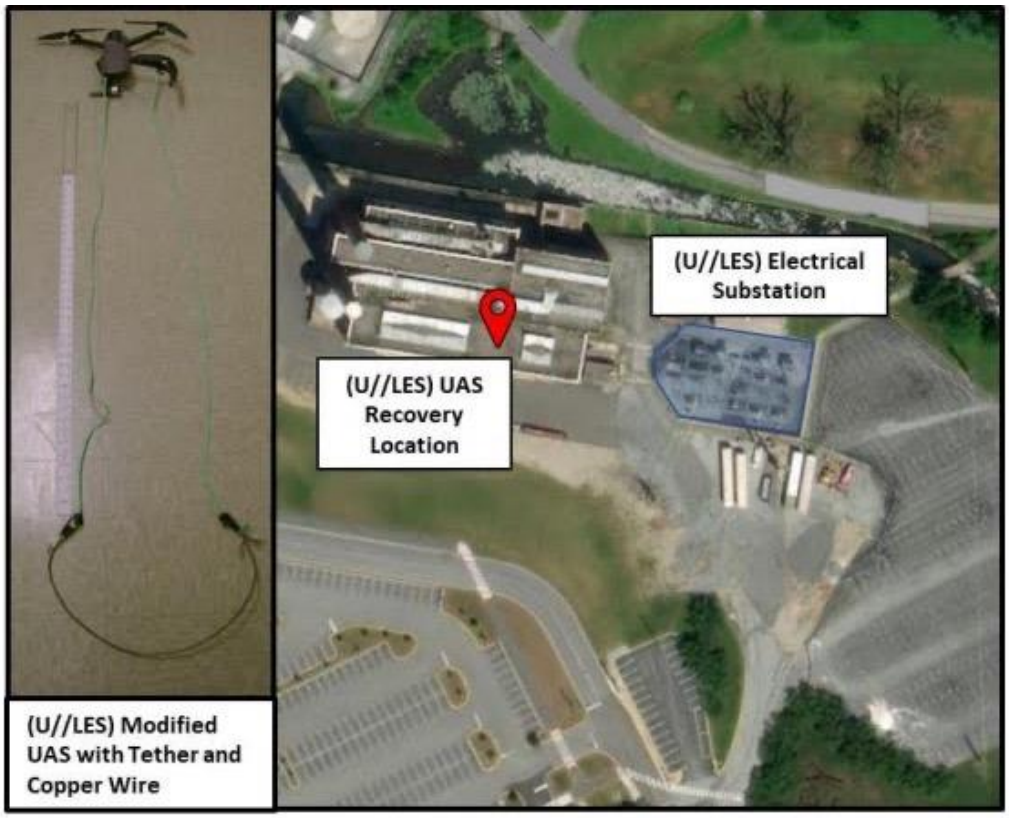



Figure 5: July 2020 Modified UAS (left) and Recovery Location (right)
Source: ABC7 News

Figure 6: DJI Mavic 2
Source: DJI.com

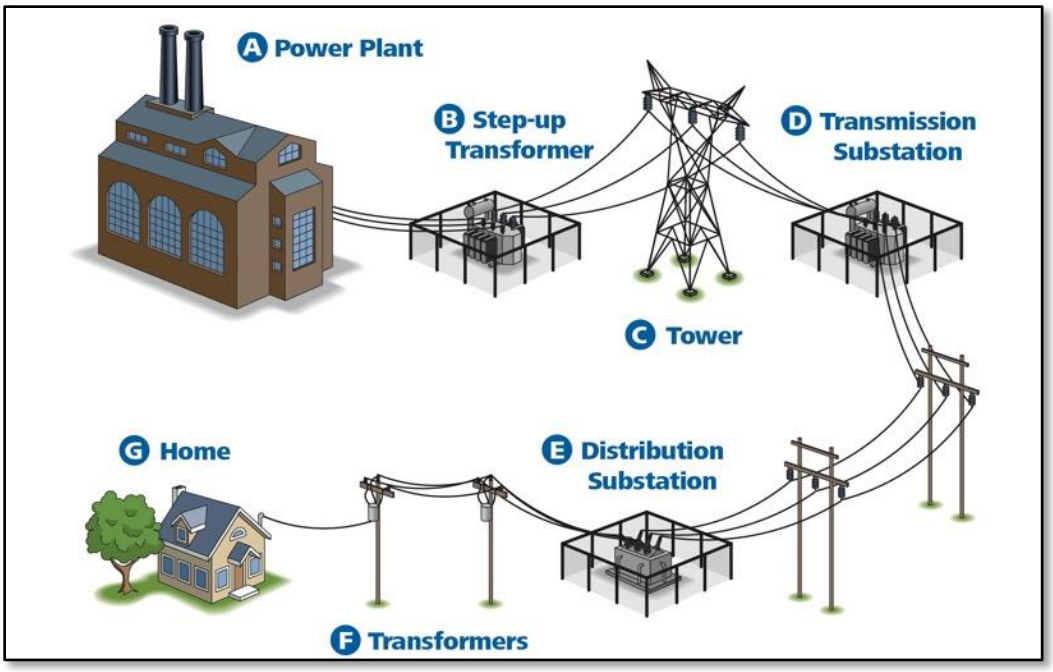



Figure 7: PEPCO Energy Infrastructure 101[16]
Source: PEPCO Energy Education

While the Pennsylvania substation attack was the first known attack on energy infrastructure in the US involving UAS, less than one year earlier, in September 2019, a similar incident highlighted critical vulnerabilities. On 29 September, five to seven sUAS were spotted flying over the Palo Verde Nuclear Generation Station, roughly 24 miles west of Phoenix.[17] Four more drones were reported flying near critical pressurized water reactors the following night. The Nuclear Regulatory Commission stated that this incident highlights the lack of security to protect against adversarial attacks.[18] The DHS, FAA, DOE, and the FBI's WMD Division were immediately involved in the Palo Verde incident.[19] Much of the information surrounding this incident is still under investigation by the DHS. This example, at the US's most powerful nuclear power plant, illustrates how malicious UAS could impact critical US infrastructure. As seen in Figure 8 below,

---

[16] Figure 7 below depicts the critical energy infrastructure, noted in an "Infrastructure 101 Class" provided by the same Potomac Energy and Power Corporation in the fictional scenario, highlighting critical vulnerability across the range of infrastructure from the power plant to the consumer. PEPCO Company, *"Infrastructure 101 – How Transmission Lines Work,"* https://www.pepco.com/SafetyCommunity/Education/Pages/EnergyBasics/Infrastructure101.aspx.

[17] Tyler Rogoway and Joseph Trevithick, "The Night A Mysterious Drone Swarm Descended on Palo Verde Nuclear Power Plant," *The Drive*, 30 July, 2020, https://www.thedrive.com/the-war-zone/34800/the-night-a-drone-swarm-descended-on-palo-verde-nuclear-power-plant.

[18] Nuclear Regulatory Commission, *Executive Summary for "Technical Analysis of Unmanned Aerial Vehicles for Nuclear Power Plans and Category I Fuel Cycle Facilities*," https://www.nrc.gov/docs/ML1930/ML19302E409.pdf.

[19] Tyler Rogoway and Joseph Trevithick, "The Night a Mysterious Drone Swarm Descended on Palo Verde Nuclear Power Plant," *The Drive*, 30 July, 2020.

attacks on power grid infrastructure are increasing every year, and UAS are an effective, non-attributional means to do so.

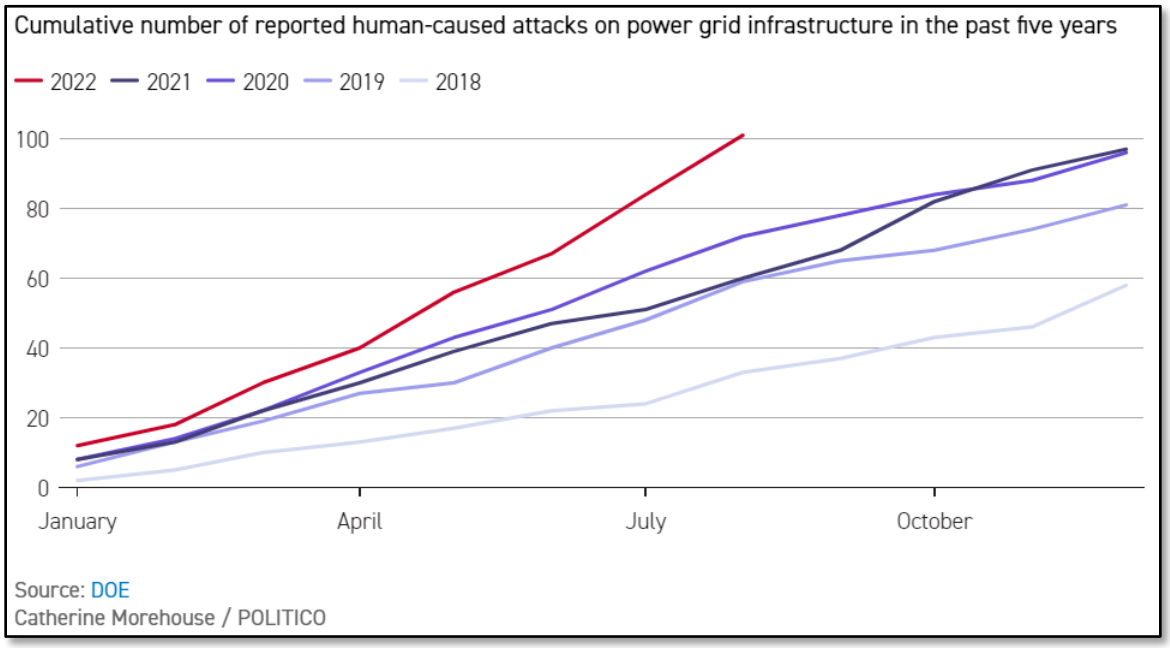



Figure 8. Graph - Increase in Attacks on US Power Grid
Source: POLITICO / Department of Energy

### *3.* United Arab Emirates and United Kingdom Airports

*Vulnerability: Key Infrastructure, Transportation Focused*

On 17 January 2022, Houthi rebels conducted a coordinated attack in the United Arab Emirates on an oil facility owned by the Abu Dhabi National Oil Company and the Abu Dhabi International Airport. At the oil facility, the drones struck three fuel transport trucks among 36 storage tanks that supply fuel for the trucks. At the International Airport, the UAS started a fire that was, luckily, in an extension of the airport currently under construction with minimal personnel. This attack leveraged multiple UAS, a tactic common to the Yemen-based Houthi rebel group, and resulted in three fatalities and six wounded.[20]

In an unprecedented decision following the fatal drone attacks, the UAE swiftly banned recreational drones in the country. The UAE General Civil Aviation Authority has provisions for *commercial* drone operators to apply for work permits, but the

[20] Aya Batrawy, "Drone attack in Abu Dhabi claimed by Yemen's rebels kills 3," *Associated Press*, 17 January 2022, https://apnews.com/article/business-dubai-united-arab-emirates-abu-dhabi-yemen-8bdefdf900ce46a6fd6c7bc685bf838a.

consequences for operating drones can include up to six months in prison and $27,000 USD fines.[21]

Drone incursions at airports have been a recurring theme since hobbyist drones became commonplace. However, two of the most significant airport disturbances occurred in the United Kingdom within the same six-month period. The first was at the Stansted Airport in Essex, which occurred in 2018 (and again in 2021.) The second was at Gatwick Airport in West Sussex, in December 2018. At Stansted Airport, a UAS was flying nearly 20 times its allowable altitude when it had a near miss, within 50 feet of a Boeing 737 on arrival at the airport.[22] After this specific event, the British Civil Aviation Authority noted that between 2014 and 2017, UAS near misses increased from six to 93.[23] Three years later, also at Stansted Airport, another UAS came within *6 feet* of a Boeing 737 on approach to the airport. The captain identified the UAS at 2800 feet.[24]

At the Gatwick International Airport, UAS encroachments resulted in 140,000 passengers affected and 1,000 flights diverted or canceled within *just three days* in 2018. On the first day, two drones were initially sighted on the airfield, resulting in initial closures. Within the same day, six more had been reported, and by the next day, nine UAS had been reported above the airfield. Each time Gatwick prepared to open the runways, additional UAS were spotted and reported. Over three days, the British Government had to deploy military units to the airfield to establish security against UAS they could neither detect nor identify. *The Guardian* states, "Sussex police and Gatwick maintain it was a sophisticated, malicious, and well-planned attack." No culprit was ever identified.[25]

When asked about the potential damage of a UAS colliding with an aircraft, a representative from the British Airline Pilots Association stated that "we don't know what would happen, but because drones have hard, lithium-ion batteries, if one hits a jet engine, it will not only stop it but potentially cause an uncontained engine failure, with bits of metal flying off penetrating the cabin and fuel tanks. And if a drone hits a helicopter or light aircraft, that will almost certainly result in catastrophe."[26]

---

[21] Khitam Al Amir, "UAE extends ban on flying drones," *Gulf News,* 21 February 2022, https://gulfnews.com/uae/uae-extends-ban-on-flying-drones-1.85906816

[22] 400 ft is the max allowable altitude. Chiara Giordano, "Drone came within 15m of plane landing at Stansted," *Independent*, 15 December 2018, https://www.independent.co.uk/news/uk/home-news/drone-15m-boeing-737-plane-stansted-airport-near-miss-a8684766.html; BBC, "Stansted Airport: Drone came within 6ft of Boeing 737, report says," *BBC*, 03 December 2021, https://www.bbc.com/news/uk-england-essex-59519694.

[23] Chiara Giordano, "Drone came within 15m of plane landing at Stansted," *Independent*, 15 December 2018.

[24] BBC, "Stansted Airport: Drone came within 6ft of Boeing 737, report says," *BBC*, 03 December 2021.

[25] Samira Shackle, "The mystery of the Gatwick drone," *The Guardian*, 01 December 2020, https://www.theguardian.com/uk-news/2020/dec/01/the-mystery-of-the-gatwick-drone.

[26] Gwyn Topham, "Drones in four near-misses at major UK airports, air investigators reveal," *The Guardian*, 29 January, 2016, https://www.theguardian.com/technology/2016/jan/29/drones-near-misses-major-uk-airports-heathrow-stansted.

The United Kingdom responded to the chaos in Gatwick with a military reaction but stated that in the future, it "would not be right" to ask the military to respond to similar incidents. The UK is pursuing military-grade C-UAS equipment for all airfields and discussing utilizing similar equipment for prisons, power stations, and military installations.[27] Another recent notable C-UAS airport initiative was Canada's employment of a detection system at the Ottawa Airport in preparation for President Biden's visit in 2023.[28]

### *4.* Department of Justice / Law Enforcement

*Vulnerability: Correctional Facilities / Law Enforcement Officers / Sporting Events / DOD Facilities*

As demonstrated, commercial UAS threats transcend a single agency, with issues proliferating throughout the DOD, DHS, FAA, and DOE. The DOJ is no exception. On 4 July 2017, Inmate Jimmy Causey fled a state correctional institution in South Carolina "after leaving a paper mâché doll in his bed to fool guards into thinking he was asleep."[29] In a press conference, the director stated, "We believe a drone was used to fly in the tools that allowed him to escape," assessed as wire cutters.[30] Additionally, documents obtained by *USA Today* through a FOIA request to the DOJ, indicate that numerous federal and state institutions have "uncovered more than a dozen attempts to transport contraband - including mobile phones, drugs and porn" into prisons.[31]

In Mexico, cartels have developed tactics, techniques, and procedures to leverage UAS against local police. In April 2021, two drones laden with explosives were used to attack a group of police officers. Earlier that year, UAS rigged with explosives and ball bearings were discovered while searching cartel assets. In November 2022, the same cartel utilized a similar tactic, dropping handmade explosives from drones onto a police station in Jalisco, killing two municipal officers.[32]

---

[27] BBC, "Airport drone disruption: All major UK airports to have 'military-grade' protection," *BBC*, 10 January 2019, https://www.bbc.com/news/uk-46827542.

[28] Scott Simmie, *"Ottawa International Airport, INDRO, Provide Drone Detection During Biden Visit,"* INDRO Robotics, accessed 10 April 2023, https://indrorobotics.ca/2023/03/25/ottawa-international-airport-indro-provide-drone-detection-during-biden-visit/.

[29] Doug Stanglin, "Prison officials say escaped inmate likely used wire cutters dropped by drone," *USA Today*, 7 July 2017, https://www.usatoday.com/story/news/2017/07/07/prison-officials-say-escaped-inmate-likely-used-wire-cutters-dropped-drone/459828001/.

[30] Doug Stanglin, Prison officials say escaped inmate likely used wire cutters dropped by drone, *USA Today*, 7 July 2017.

[31] Waseem Abbasi, "Inmates fly mobile phones, drugs and porn into jail - via drone," *USA Today*, 15 June 2017, https://www.usatoday.com/story/news/2017/06/15/inmates-increasingly-look-drones-smuggle-contraband-into-their-cells/102864854/.
Following the Gatwick Incident, the UK already implements C-UAS systems in select prisons. Samira Shackle, "The mystery of the Gatwick drone," *The Guardian*, 01 December 2020, https://www.theguardian.com/uk-news/2020/dec/01/the-mystery-of-the-gatwick-drone.

[32] Luis Chaparro, "A Cartel Used Armed Drones and a Plane to Bomb Police," *The Vice*, 28 November 2022, https://www.vice.com/en/article/xgyp4w/mexico-cjng-airplane-drones-jalisco-police.

Additionally, a DHS Report on the Illicit Threats from UAS stated that in "September 2011 a U.S. citizen was arrested for planning to attach explosives to a UAS and attack the Pentagon and U.S. Capitol." In 2015, a quadcopter crashed on the White House lawn, sparking an intense investigation that highlighted a key gap in national security.[33] Another potentially dangerous incident occurred in 2017 when "a UAS flew over the San Francisco 49ers and Oakland Raiders NFL stadiums, dropping leaflets and causing panic."[34] The increasing threat of malicious UAS is a critical vulnerability for nations around the world. The first step to closing that vulnerability gap is to recognize the range and variety of threats and issue guidance for realistic solutions. The US has recognized the threat but will first need to synchronize policy and solutions to effectively harden homeland security against UAS.

**Recognizing the Vulnerability and Implementing Solutions for Risk Mitigation**

As depicted in the preceding case studies, the scenario described in the useful fiction introduction is not only feasible, but the conditions for each event *have already happened* in separate times and places around the world. Commercial drones are becoming more capable, less expensive, and more intuitive to operate. The DHS released an Interagency Security Committee publication overviewing the current domestic threat of UAS. Several activities listed were hostile surveillance, smuggling or contraband delivery, disruption of government business, and weaponization.[35] Examples of threats depicted by the DHS are listed in Figure 9 below:

---

[33] Carol Leonnig and Craig Whitlock, "Drone incident at White House highlights long-studied, still-unsolved security gap," *The Washington Post*, 26 January 2015, https://www.washingtonpost.com/politics/drone-incident-at-white-house-highlights-long-studied-still-unsolved-security-gap/2015/01/26/ed2e7f9e-a594-11e4-a7c2-03d37af98440_story.html.

[34] U.S. Department of Homeland Security, Illicit Threats from Unmanned Aircraft Systems (UAS) (2018) (on file with Senate Committee on Homeland Security & Government Affairs).

[35] Department of Homeland Security, Interagency Security Committee, Protecting Against the threat of Unmanned Aircraft Systems (UAS) https://www.cisa.gov/sites/default/files/publications/Protecting%20Against%20the%20Threat%20of%20Unmanned%20Aircraft%20Systems%20November%202020_508c.pdf.

| Threat Actor - Capability Level | Likely UAS type | Possible scenario use | Flight Method | Range |
|---|---|---|---|---|
| Low | Multi-copter | Disruption, surveillance | Line of Sight (LoS) with First Person View (FPV) assistance | 400m |
| | Multi-copter + additional payload | Delivery of restricted item/ explosives | LoS with FPV assistance | 400m |
| Medium | Multi-copter | Disruption, surveillance | FPV | 1km |
| | Multi-copter + additional payload | Delivery or restricted item/ explosives | FPV | 500m |
| | Fixed-wing | Disruption, surveillance | GPS with FPV assistance | 5km – 30km |
| | Fixed-wing + additional payload | Delivery or restricted item/ explosives | GPS with FPV assistance | 5km – 30km |

Figure 9: Examples of UAS as a Threat
Source: Department of Homeland Security, Interagency Security Committee

Commercial drones are so simple to weaponize that within the first day of Russia's invasion of Ukraine in 2022, Ukraine's Minister of Defense "appealed for civilian drone owners to donate their commercial drones to defend Kyiv."[36] The US recognizes the threat of malicious UAS. However, the barriers to employment for a successful C-UAS strategy are incredibly complex. The top four most significant challenges to domestic C-UAS are:

- Air Domain Awareness and Threat Discrimination
- Authority to Interdict in the Context of Antiquated Legislation
- Whole-of-Government Approach
- Regulatory and Legal Framework

To synchronize and develop a national C-UAS plan in actual detail, the United States needs air domain awareness, the authorities to enable C-UAS mitigation, a regulatory and legal framework for prosecution, and a whole-of-government approach to coordinate these efforts.

### Air Domain Awareness and Threat Discrimination

"C-UAS is just one small piece of a wholistic security architecture needed to ensure safe and secure integration of commercial UAS into the national airspace system. We must have domain awareness equivalent to that of manned aviation consisting of an FAA "compliant UAS" air picture and a non-compliant or nefarious overlay provided by security partners. This combined air picture is needed to

[36] Benjamin Fogel, Andro Mathewson, *"Will the Drone War Come Home? Ukraine and the Weaponization of Commercial Drones,"* The Modern War Institute at West Point, 08 August 2022.

improve threat discrimination, which is necessary to conduct precision C-UAS activities in the domestic environment."

- Director Brent Cotton, DHS Director of C-UAS
Author Interview, 14 April 2023

To implement a realistic strategy for C-UAS, the USG must recognize the environment of the 21st century in which C-UAS systems would be employed. First, the FAA bifurcates C-UAS technology into two main categories – detection and mitigation. Detection is achieved through sensors, whether they are radio frequency, electro-optic, acoustic, or radar, to detect, identify, monitor, and track the UAS. Mitigation or countermeasures include "the capability to disrupt, disable, destroy, take control of, and/or provide alternate flight instructions to a UAS."[37] These can include any range of jamming or interdiction techniques, through a variety of capabilities from kinetic to non-kinetic means including projectiles, directed energy lasers, and even predatory birds.

As depicted in the case studies, the UAS operator does not require LOS to attack fixed structures, enabling them to program GPS coordinates to "set and forget" the attack from a standoff. If the UAS attack has pre-programmed attack headings, it will be less vulnerable to jamming attempts to sever the link back to guidance. When an operator is hand-flying the UAS from LOS or BLOS, this introduces a vulnerability to jamming and other C-UAS interference. However, the C-UAS system would still have to rapidly detect, identify, and interdict a small flying object within the potentially complex and congested civilian infrastructure. Introducing kinetic defeat capabilities in this scenario includes an immediate risk of collateral damage and civilian casualties, lending many CONUS C-UAS efforts to focus on detection, identification, and finish capabilities through non-kinetic effects.

However, before discussing legislation, organization, and regulation, the DHS (which the TSA is a part of) and FAA must recognize that (a) *registered* commercial UAS will need to integrate with the national airspace, (b) hobby UAS will continue to operate below 400 feet, many of which are not registered, and (c) law enforcement will need to understand which is which to make a rapid threat discrimination, regardless of environment or location. The Preventing Emerging Threats Act of 2018 (Title 6 U.S.C. § 124n) authorizes the DOJ and DHS to mitigate credible UAS threats by detecting, identifying, monitoring, and tracking UAS.[38] *However, it is estimated that over 20 million drones have been sold in the US and, as of 2023, only 1.1 million UAS registered*

---

[37] Federal Aviation Administration, Unmanned Aircraft System Detection - Technical Considerations, 26 March, 2019, http://www.faa.gov/airports/airport_safety/media/Attachment-3-UAS-Detection-Technical-Considerations.pdf.

[38] Interagency Security Committee, Protecting Against the Threat of Unmanned Aircraft Systems (UAS), November 2020, https://www.cisa.gov/sites/default/files/publications/Protecting%20Against%20the%20Threat%20of%20Unmanned%20Aircraft%20Systems%20November%202020_508c.pdf.

*with the FAA*.[39] In the incredibly congested airspace around major airports, or sports and government venues in urban settings, threat discrimination without a clear air picture is impossible.

**Authority to Interdict in the Context of Antiquated Legislation**

The second most significant barrier to domestic C-UAS involves a series of laws enacted in the era of landline home phones and introduces the complexity of civil liberty. The problem is two-fold. First, the FAA categorizes UAS as aircraft, meaning that UAS receive the same legal protection as planes. Essentially this means that it is illegal to seize or exercise control of an aircraft, in addition to other laws that inhibit CONUS agency and department personnel from acting against a malicious UAS.[40] The second set of laws impeding domestic C-UAS are a variety of dated acts that "make it illegal to intercept any wire, oral, or electronic communication, or to access a computer without authorization," effectively, making it impossible to use the electronic transmission to track down the operator of the drone.[41] These acts specifically tie to civil liberties involved with frequency transmission, written to prevent wiretapping, and have not been updated for modern applications.

However, in 2018 the United States passed the Preventing Emerging Threats Act (Title 6 U.S.C. § 124n), detailed in Annex C, as part of an FAA Authorization Bill, with an expiration date of 5 October 2022. This act provides the DHS and DOJ authority to protect "critical facilities and assets when there is a national security risk to public safety posed by UAS."[42] The bill also requires the DHS to complete a risk assessment on which facilities are most at risk. The Preventing Emerging Threats Act authorizes the DHS and DOJ to mitigate credible UAS threats by:

- Detecting, identifying, monitoring, and tracking UAS without the prior consent of the operator by means of intercepting or otherwise accessing wire, oral, or electronic communications used to control the UAS.

---

[39] National Conference of State Legislatures, Current Unmanned Aircraft State Law Landscape, 27 March 2023 https://www.ncsl.org/transportation/current-unmanned-aircraft-state-law-landscape; Director Brent Cotton (DHS C-UAS PMO) in discussion with the author, April 2023.

[40] Key federal statutes to consider are 18 U.S.C. § 32 Destruction of aircraft or aircraft facilities, 49 U.S.C. § 40103: Sovereignty and use of airspace; and 49 U.S.C. § 46502: Aircraft piracy. The 2017 National Defense Authorization Act did provide the DOD and DOE the authority to conduct C-UAS operations to protect military sites such as missile defense, nuclear deterrence, and other key facilities. The 2017 NDAA did not address the requirements of the DHS and DOJ. United States Senate, Committee on Homeland Security and Governmental Affairs, Preventing Emerging Threats Act of 2018 Report 115-332, https://www.congress.gov/115/crpt/srpt332/CRPT-115srpt332.pdf.

[41] Key legal considerations that impact this aspect of C-UAS are 18 U.S.C. § 2510: wire and electronic communications interception and interception of oral communications and 18 U.S. Code § 3121 - General prohibition on pen register and trap and trace device use. United States Senate, Committee on Homeland Security and Governmental Affairs, Preventing Emerging Threats Act of 2018 Report 115-332.

[42] United States Senate, Committee on Homeland Security and Governmental Affairs, Preventing Emerging Threats Act of 2018 Report 115-332.

- Disrupting control of a UAS without prior consent from the operator by disabling the UAS by intercepting, interfering with, or causing interference with wire, oral, electronic, or radio communications used to control the UAS.
- Seizing, exercising control of, or otherwise confiscating a UAS.
- Using reasonable force to disable, damage, or destroy a UAS.[43]

The DHS and DOJ maintained these authorities when the act was extended through continuing resolutions and reauthorized under the Consolidated Appropriations Act until 23 December 2023. While the DOD and DOE are authorized to conduct C-UAS under a separate United States Code, the DHS and DOJ (specifically the FBI) rely on the continued approval of this act to ensure the essential relief from the application of vintage laws that would prevent C-UAS. Without the continued authorization of the act, the DOJ and DHS would be violating existing US statutes to conduct the most basic C-UAS activities.

However, while the act does provide relief from the statutes in United States Code, it does not empower significant C-UAS employment that could transcend authorities from the DOJ and DHS for state, local, territorial and tribal (SLTT) law enforcement agencies and critical infrastructure owners and operators.[44] Additionally, there are concerns from the FAA and FCC about expanding authorities because C-UAS mitigation technology can potentially disrupt commercial aircraft and public communications if misused. The DHS and DOJ are limited to protecting only designated facilities or assets and high-profile events. The DHS Secretary or Deputy Attorney General must select or designate each facility or event.[45] While this is a step in the right direction, it is far from a scalable solution. It requires the predicated air domain awareness, discussed in the previous section, to enable threat discrimination and interdiction.

**Whole-of-Government Approach**

One clear challenge these case studies represent is the interagency and interdepartmental coordination required for C-UAS initiatives. While reviewing the emerging doctrine, tactics, techniques, and procedures for C-UAS, there are separate publications from the DHS, DOD, FAA, and DOJ, among many others. With nearly every major department involved and affected by malicious UAS, who is the empowered executive agent among key stakeholders?

---

[43] Interagency Security Committee, Protecting Against the Threat of Unmanned Aircraft Systems (UAS), November 2020.
[44] The White House, FACT SHEET: The Domestic Counter-Unmanned Aircraft Systems National Action Plan, 25 April 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/25/fact-sheet-the-domestic-counter-unmanned-aircraft-systems-national-action-plan/.
[45] COL Robert Rodrigues (US Army Fellow at DOJ Office of Legal Policy) in discussion with the author, April 2023.

In 2019 the United States Senate introduced a bill titled the "DHS C-UAS Coordinator Act," which would serve as an amendment to the Homeland Security Act of 2002. This amendment would seek to achieve the interagency coordination and whole-of-government approach that nearly every department and agency desperately needs. The Act's accompanying report stated that the DHS coordinator would "oversee and coordinate with relevant Department offices and components, including the Office of Civil Rights and Civil Liberties and the Privacy Office, on the development of guidance and regulations to counter threats associated with UAS." Among the list of responsibilities, the report on the amendment notes that the C-UAS Coordinator would also coordinate C-UAS intelligence and serve as the DHS liaison with all external state and federal entities while coordinating directly with the private sector. The DHS C-UAS Coordinator Act was not passed.

While the Act was not passed, the DHS *does* have a director of the C-UAS Program Management Office who, while not an SES as the Act intended, coordinates directly with the National Security Council, the Interagency, and a variety of key stakeholders. However, it would not make sense for the DHS to be the sole executive agent for C-UAS in the USG, as the FAA under the Department of Transportation has an massive role. Moving forward, an effective solution would be an interagency task force of both the DHS (that includes stakeholders such as the TSA, and FEMA) and the DOT (that includes the FAA). Arguably, the administration of international airspace is one of the most complex operations in the world, and the DHS would not be successful without the requisite FAA buy-in, and vice versa.

Additionally, based on agency and department, some are pursuing passive or active C-UAS measures, some are pursuing kinetic or non-kinetic approaches, while others are still trying to understand the threat. Through the whole-of-government approach, the DOJ and DHS must attempt to provide guidance to industry by assessing C-UAS law (DOJ-led) that would assess who can leverage *which* C-UAS systems, and *in what way*. However, industry cannot attempt to build an authorized equipment list without detailed legal guidance, yet the DOJ cannot give legal guidance without detailed TTPs of how LEOs will use the equipment. LEOs cannot provide detailed TTPs of what they will use the equipment for without the authority to interdict and specific relief from the United States Code, which Congress is hesitant to permit.

**Regulatory and Legal Framework**

Currently, the regulatory and legal framework surrounding commercial UAS is loose at best. Most UAS incidents in the US are due to careless and clueless operators. Additionally, a majority of UAS operators do not have their UAS registered, further complicating any attempt at air domain awareness. At this time, there are only two charges that the DHS and DOJ can leverage against a UAS operator, (1) violation of national defense airspace and (2) not having a registration.[46] There is no predicating law

[46] If a drone is not registered and is used outdoors, the FAA may impose penalties of up to $27,000. Criminal penalties for the failure to register a drone include fines of up to $250,000 and/or imprisonment. It

that would enable domestic interdiction. There is also no criminal law that prohibits weaponizing drones. Apart from causing fatalities, even the most egregious UAS activity will only result in a misdemeanor, and as such, is less likely to be prosecuted in federal court.[47] By comparison, knowingly aiming a laser pointer at an aircraft or its flight path is a felony with a 5-year maximum sentence. In 2020, a Los Angeles man crashed his UAS into an LAPD helicopter, forcing the helicopter pilot to make an emergency landing. He only received probation for unsafe operation of an unmanned aircraft. [48] At this time the DOJ is proposing federal legislation titled the Crime-Free and Secure Skies Act of 2022 that seeks to address the lack of significant criminal penalties for unlawful UAS activity.

**Executive Response**

Initially proposed by the National Security Council and interagency initiatives, the Executive Branch released The Domestic C-UAS National Action Plan on 25 April 2022. At the highest levels of the USG, politicians acknowledge that "malicious actors have increasingly used UAS domestically to commit crimes, conduct illegal surveillance and industrial espionage, and thwart law enforcement efforts at the local, state, and Federal level."[49] The National Action Plan's three primary goals are identifying *where* to protect, *who* can protect (directly relating to authority to interdict), and *how* it can be accomplished lawfully. This ties back to not only the legal framework that causes direct friction with C-UAS activities but seeks to rectify the privacy laws that will need to be addressed to detect, identify, and mitigate UAS in a wide variety of locations, with the presidential fact sheet specifically mentioning civil rights, civil liberties, and individual privacy.

However, The National Action Plan is contingent on achieving more authority for key stakeholders. Additionally, while it presents strategic goals, it does not identify operational or tactical solutions that an executive agent (interagency task force) would provide. Without an air domain awareness framework, the legislative "teeth" to support

---

is incredibly challenging for law enforcement to enforce this. Additionally, because failing to register is a misdemeanor, it is rarely prosecuted. State of California Press Release, Attorney General Kamala D. Harris Issues Consumer Alert on Drone Registration and Safe Drone Usage, 13 January 2016, https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-issues-consumer-alert-drone-registration-and.

[47] Current Federal UAS Criminal Statue – 18 U.S.C. § 39B Unsafe operation of unmanned aircraft
Any person who operates an unmanned aircraft and:
(1) Knowingly or recklessly interferes with or disrupts the operation of an aircraft carrying 1 or more occupants in a manner that poses an imminent safety hazard to such occupants. This offense is classified as a misdemeanor (1-year maximum sentence).
COL Robert Rodrigues (US Army Fellow at DOJ Office of Legal Policy) in discussion with the author, April 2023.

[48] Richard Winton, "Feds charge Hollywood man after drone collides with LAPD helicopter," *Los Angeles Times*, 19 November 2022, https://www.latimes.com/california/story/2020-11-19/feds-charge-hollywood-man-after-drone-crashes-into-lapd-helicopter; Director Brent Cotton (DHS C-UAS PMO) in discussion with the author, April 2023.

[49] The White House, FACT SHEET: The Domestic Counter-Unmanned Aircraft Systems National Action Plan, 25 April 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/25/fact-sheet-the-domestic-counter-unmanned-aircraft-systems-national-action-plan/.

the tactical detection, identification, and interdiction, the formal designation of a government lead with the authority to coordinate a whole-of-government approach or laws against weaponizing UAS in the first place, the action plan will not be effective.

## Conclusion

*Will the United States prioritize domestic C-UAS before the next terrorist attack?* For $1,000 to $5,000, a malicious actor can dramatically impact; a NASA shuttle launch, a DOD ICBM Missile Silo, a DOE Nuclear Site, an international airport, a DOJ Correctional Facility, and conduct a number of nefarious activities against the American people at large, whether it is at a major league sports game or concert. While the sheer amount of documentation acknowledging the UAS threat to the homeland is astounding, the problem lies in air domain awareness, outdated legislation and authorities, lack of coordination, and a broken legal framework for prosecution.

Without rectifying these four foundational issues, the vulnerability gap will remain *until exploited.* The C-UAS efforts will be siloed throughout the government instead of having an interconnected web of security. As technology advances, threats naturally evolve with technology. While the potential of cyber-attacks and technical threats is critical, the USG must understand the catastrophic nature of malicious UAS activity, and the level of domestic coordination required to close the vulnerability gap before it is too late.

Annex A: UAS Categories – United Nations and United States

| Class | Category | Recommended Employment | Normal Aprox Recommended Altitude (AGL) | Range | Examples |
|---|---|---|---|---|---|
| Class III | HALE | Strategic/National | < 65,000 ft | Unlimited (BLOS) | Global Hawk |
| | MALE | Operational/Theater | < 45,000 ft | Unlimited (BLOS) | Heron/Hermes 900 |
| Class II | Tactical | Tactical Formation | < 18,000 ft | < 150 km (LOS) | Hermes 450/Falco Sperwer |
| Class I | Small | Tactical Unit | < 1,000 ft | < 50 km (LOS) | Scaneagle/ Shadow 200 Luna |
| | Mini | Tactical Subunit (manual or hand launch) | <1,000 ft | < 25 km (LOS) | Raven/Aladin Puma/Skylark Heidrum V1 |
| | Micro | Tactical Subunit (manual or hand launch, tethered) | < 400 ft | < 5 km (LOS) | WASPIII/MICADO DJI Phantom 4, DJI Mavic Pro Hovermast 100 |

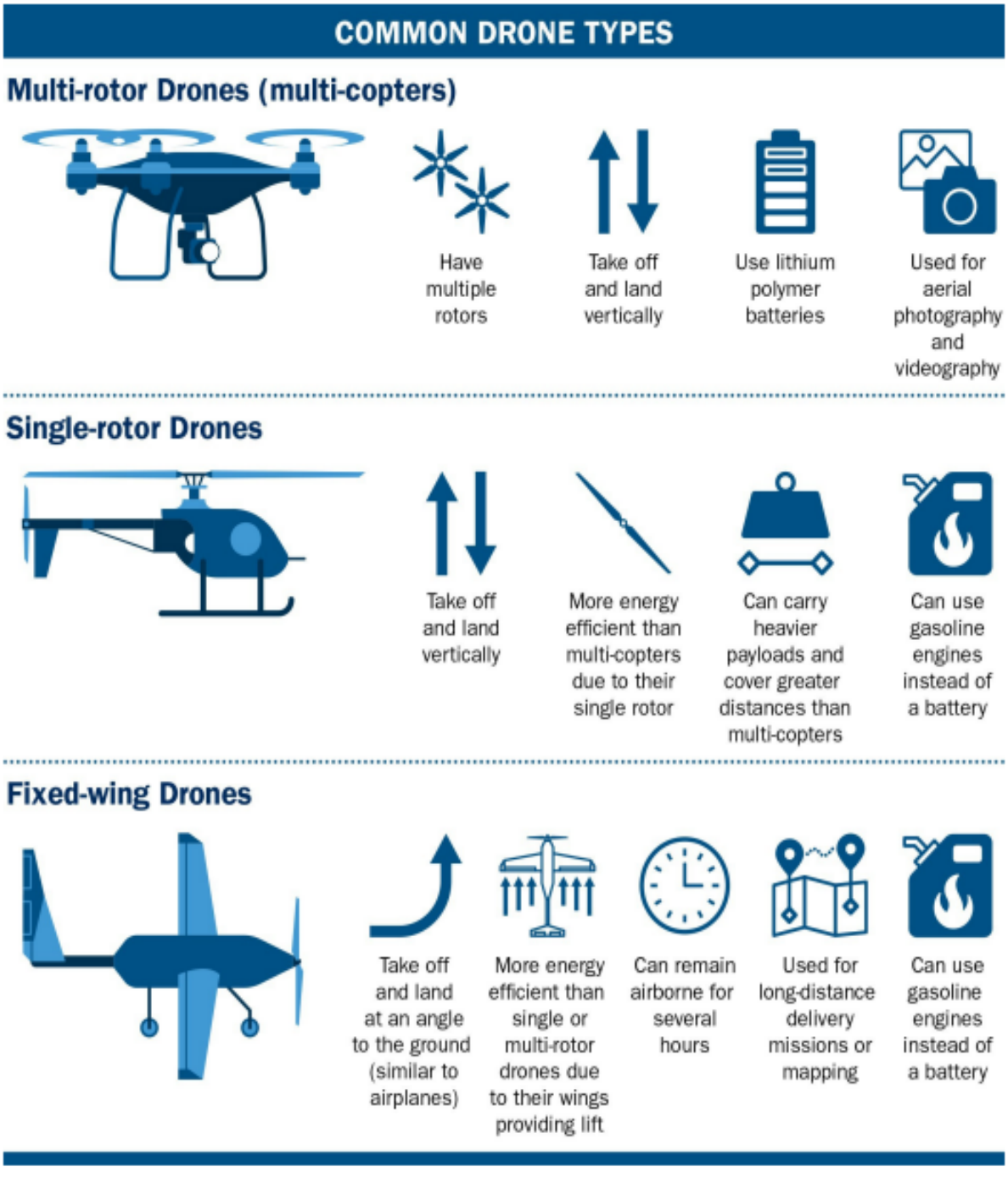
Table 1: UN PKO UAS/RPAS Table
Source: Guidelines - UN Use of UAS Capabilities

| UA Category | Maximum Gross Takeoff Weight (lbs.) | Normal Operating Altitude (feet) | Speed (KIAS) |
|---|---|---|---|
| Group 1 | 0-20 | < 1200 AGL | 100 knots |
| Group 2 | 21-55 | < 3500 AGL | < 250 knots |
| Group 3 | < 1320 | < 18,000 MSL | < 250 knots |
| Group 4 | > 1320 | | Any Airspeed |
| Group 5 | > 1320 | > 18,000 MSL | Any Airspeed |
| Legend: AGL – above ground level; MSL – mean sea level; KIAS – knots indicated airspeed | | | |

Table 2: UA Grouping Table
Source: US Department of Defense, Counter-Small Unmanned Aircraft Systems Strategy

Annex B: UAS Overview and Common Drone Types

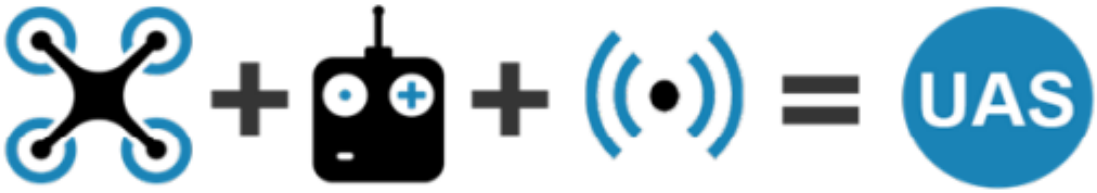
Source: Interagency Security Committee, Protecting Against the Threat of Unmanned Aircraft Systems (UAS), November 2020, https://www.cisa.gov/sites/default/files/publications/Protecting%20Against%20the%20Threat%20of%20Unmanned%20Aircraft%20Systems%20November%202020_508c.pdf



An unmanned aerial vehicle (UAV), or drone, is an aircraft operated without direct human intervention in or on the aircraft. The term unmanned aircraft system (UAS) applies to the UAV and its associated elements, including communication links and unmanned- aircraft control components, which are required for the operator to maneuver safely and efficiently in the national airspace system.[3]

UAS include three key components:

1. A UAV that can operate without a pilot on board.
2. A ground control system (GCS) that allows the pilot to remotely control or monitor the operation of the UAV.
3. A bidirectional link between the UAV and the GCS that provides control, status, and imagery information.



Annex C: H.R.6401 - Preventing Emerging Threats Act of 2018

Sponsor: Sen. Johnson, Ron [R-WI] (Introduced 05/14/2018)

Committees: Senate - Homeland Security and Governmental Affairs

Committee Reports: S. Rept. 115-332

Sponsor: Rep. McCaul, Michael T. [R-TX-10] (Introduced 07/17/2018)

Committees: House - Judiciary; Transportation and Infrastructure; Homeland Security

Introduced in House (07/17/2018)

Preventing Emerging Threats Act of 2018

This bill amends the Homeland Security Act of 2002 to authorize the Department of Homeland Security (DHS) and the Department of Justice (DOJ) to authorize their personnel to act to mitigate a credible threat that an unmanned aircraft system or unmanned aircraft (i.e., drones) poses to the safety or security of facilities or assets, through a risk-based assessment.

DHS may take actions to:

- detect, identify, monitor, and track the drone, without prior consent;
- warn the drone's operator;
- disrupt control of the drone, without prior consent;
- seize or exercise control of the drone;
- confiscate the drone; or
- use reasonable force, if necessary, to disable, damage, or destroy the drone.
- Any drone seized by DHS or DOJ is subject to forfeiture to the United States.

DHS shall: (1) evaluate the threat from drones to U.S. critical infrastructure and to domestic large hub airports; and (2) assess the threat of vehicular terrorism and brief Congress on its findings and on a strategy to improve efforts to support emergency response providers and the private sector to prevent, mitigate, and respond to such threat.

Source:
Congressional Research Service, H.R.6401 - Preventing Emerging Threats Act of 2018, Accessed 4 April 2023, https://www.congress.gov/bill/115th-congress/house-bill/6401

Congressional Research Service, S.2836 - Preventing Emerging Threats Act of 2018, Accessed 4 April 2023, https://www.congress.gov/bill/115th-congress/senate-bill/2836

**BIBLIOGRAPHY**

Abbasi, Waseem. "Inmates fly mobile phones, drugs and porn into jail - via drone." *USA Today*. June 15, 2017. https://www.usatoday.com/story/news/2017/06/15/inmates-increasingly-look-drones-smuggle-contraband-into-their-cells/102864854/.

Al Amir, Khitam. "UAE extends ban on flying drones." *Gulf News*. February 21, 2022. https://gulfnews.com/uae/uae-extends-ban-on-flying-drones-1.85906816.

Arnold, Ross, Andrew Kopeikin, Benjamin Abruzzo, and Christopher Korpela. "Towards a General-Purpose, Replicable, Swarm-Capable Unmanned Aircraft System." IEEE, 2019. doi:10.1109/HST47167.2019.9032896.

Batrawy, Aya. "Drone attack in Abu Dhabi claimed by Yemen's rebels kills 3." *Associated Press*. January 17, 2022. https://apnews.com/article/business-dubai-united-arab-emirates-abu-dhabi-yemen-8bdefdf900ce46a6fd6c7bc685bf838a.

BBC. "Stansted Airport: Drone came within 6ft of Boeing 737, report says." *BBC*. December 3, 2021. https://www.bbc.com/news/uk-england-essex-59519694.

Bertuca, Tony. "SOCOM Puts New Counter-UAS Efforts on Wish List." *Inside the Pentagon's Inside the Air Force* 30, no. 13 (2019): 11.

Chavez, Kerry, and Ori Swed. "Off the Shelf: The Violent Nonstate Actor Drone Threat." *Air & Space Power Journal* 34, no. 3 (2020): 29-43.

Congressional Research Service. H.R.6401 - Preventing Emerging Threats Act of 2018. Accessed April 4, 2023. https://www.congress.gov/bill/115th-congress/house-bill/6401.

Congressional Research Service. S.2836 - Preventing Emerging Threats Act of 2018. Accessed April 4, 2023. https://www.congress.gov/bill/115th-congress/senate-bill/2836.

DJI Technologies. MATRICE 600. Accessed April 2, 2023. https://www.dji.com/ca/matrice600.

Federal Aviation Administration, Unmanned Aircraft System Detection - Technical Considerations, 26 March, 2019, http://www.faa.gov/airports/airport_safety/media/Attachment-3-UAS-Detection-Technical-Considerations.pdf.

Fogel, Benjamin, Andro Mathewson. "Will the Drone War Come Home? Ukraine and the Weaponization of Commercial Drones." The Modern War Institute at West

Point, 08 August 2022, https://mwi.usma.edu/will-the-drone-war-come-home-ukraine-and-the-weaponization-of-commercial-drones/.

Giordano, Chiara. "Drone came within 15m of plane landing at Stansted." *Independent*. December 15, 2018. https://www.independent.co.uk/news/uk/home-news/drone-15m-boeing-737-plane-stansted-airport-near-miss-a8684766.html.

Hambling, David. "Israel Rolls Out Legion-X Drone Swarm For The Urban Battlefield." *Forbes*. October 24, 2022. https://www.forbes.com/sites/davidhambling/2022/10/24/israel-rolls-out-legion-x-drone-swarm-for-the-urban-battlefield/?sh=3ae30bfc4f49.

Leonnig, Carol, Craig Whitlock. “Drone incident at White House highlights long-studied, still-unsolved security gap.” *The Washington Post*. 26 January 2015. https://www.washingtonpost.com/politics/drone-incident-at-white-house-highlights-long-studied-still-unsolved-security-gap/2015/01/26/ed2e7f9e-a594-11e4-a7c2-03d37af98440_story.html

Lykou, Georgia, Dimitrios Moustakas, and Dimitris Gritzalis. "Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies." *Sensors* (Basel, Switzerland) 20, no. 12 (2020): 3537.

Marcolini, Barbara, Christoph Koettl. “How the Drone Attack on Maduro Unfolded in Venezuela.” *New York Times*. 10 August 2018. https://www.nytimes.com/video/world/americas/100000006042079/how-the-drone-attack-on-maduro-unfolded-in-venezuela.html

Nuclear Regulatory Commission, Executive Summary for “Technical Analysis of Unmanned Aerial Vehicles for Nuclear Power Plans and Category I Fuel Cycle Facilities,” https://www.nrc.gov/docs/ML1930/ML19302E409.pdf

PEPCO Company. “Infrastructure 101 – How Transmission Lines Work.” https://www.pepco.com/SafetyCommunity/Education/Pages/EnergyBasics/Infrastructure101.aspx.

Reilly, Briana. "CENTCOM Focuses on Counter-UAS Innovation, Experimentation." InsideDefense.Com's Unmanned Systems Alert (2022). Accessed 17 April 2023.

Rogoway, Tyler, Joseph Trevithick, “The Night a Mysterious Drone Swarm Descended On Palo Verde Nuclear Power Plant.” *The Drive*. 30 July 2020, https://www.thedrive.com/the-war-zone/34800/the-night-a-drone-swarm-descended-on-palo-verde-nuclear-power-plant.

Shackle, Samira. “The mystery of the Gatwick drone.” *The Guardian*. 01 December 2020. https://www.theguardian.com/uk-news/2020/dec/01/the-mystery-of-the-gatwick-drone.

Simmie, Scott. "Ottawa International Airport, INDRO, Provide Drone Detection During Biden Visit." INDRO Robotics, accessed 10 April 2023, https://indrorobotics.ca/2023/03/25/ottawa-international-airport-indro-provide-drone-detection-during-biden-visit/.

State of California Press Release. Attorney General Kamala D. Harris Issues Consumer Alert on Drone Registration and Safe Drone Usage. 13 January 2016, https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-issues-consumer-alert-drone-registration-and.

The White House. FACT SHEET: The Domestic Counter-Unmanned Aircraft Systems National Action Plan. 25 April 2022. https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/25/fact-sheet-the-domestic-counter-unmanned-aircraft-systems-national-action-plan/.

Topham Gwyn. "Drones in four near-misses at major UK airports, air investigators reveal." *The Guardian*. 29 January 2016. https://www.theguardian.com/technology/2016/jan/29/drones-near-misses-major-uk-airports-heathrow-stansted.

Trevithick, Joseph, Likely Drone Attack on U.S. Power Grid Revealed In New Intelligence Report. *The Drive*. 05 November 2021, https://www.thedrive.com/the-war-zone/43015/likely-drone-attack-on-u-s-power-grid-revealed-in-new-intelligence-report.

United Nations Department of Operational Support. *Aviation Manual*, 2020.

United Nations Department of Operational Support. *Guidelines - United Nations Use of Unmanned Aircraft Systems (UAS) Capabilities*. 2019. https://pcrs.un.org/Lists/Resources/07-%20UN%20Military%20Units%20Manuals/United%20Nations%20Use%20of%20Unmanned%20Aircraft%20Systems%20(UAS)%20Capabilities%20Guidelines/2019.05%20UAS%20Guidelines%20February%202019-FINAL.pdf.

United Nations Department of Operational Support. *United Nations Peacekeeping Missions Military Aviation Unit Manual*. Second Edition, 2021.

United Nations Department of Operational Support. *Aerial Command and Control.* Department of Management Strategy, Policy, and Compliance. November 2020.

The United States Department of Homeland Security. Illicit Threats from Unmanned Aircraft Systems (UAS) (2018) (on file with Senate Committee on Homeland Security & Government Affairs).

United States Senate. Committee on Homeland Security and Governmental Affairs, Preventing Emerging Threats Act of 2018 Report 115-332, https://www.congress.gov/115/crpt/srpt332/CRPT-115srpt332.pdf.

United States Joint Intelligence Bulletin, Modified Unmanned Aircraft System Likely an Attempt to Disrupt Electricity Distribution, 29 October 2021.

Wallace, Ryan, Jon Loffi, Michael Quiroga, and Carlos Quiroga. "Exploring Commercial Counter-UAS Operations: A Case Study of the 2017 Dominican Republic Festival Presidente." *International Journal of Aviation, Aeronautics, and Aerospace* 5, no. 2 (2018): 8.

Walsh, Nick Paton, Natalie Gallón, Evan Perez, Diana Castrillon, Barbara Arvanitidis, and Caitlin Hu. "Inside the August plot to kill Maduro with Drones." *CNN*. 21 June 2019. https://www.cnn.com/2019/03/14/americas/venezuela-drone-maduro-intl/index.html.

White, Andrew. "Counter UAS: Developing Solutions to Small Unmanned Air Threats." *Jane's International Defence Review* 54, no. 1 (2021).

Winton, Richard. "Feds charge Hollywood man after drone collides with LAPD helicopter." *Los Angeles Times*. 19 November 2022. https://www.latimes.com/california/story/2020-11-19/feds-charge-hollywood-man-after-drone-crashes-into-lapd-helicopter.