WHITE PAPER

Safeguarding Critical Infrastructure: Defense Against Unmanned Aerial Systems (UAS)

By Landon Jones and Jared Oakden

Security leaders at both public and private utilities are grappling with soaring risks posed by drones or unmanned aerial systems (UAS). Specifically, they are focused on understanding the magnitude of this threat, identifying preventive measures, and sharing strategies to counter the escalating threat posed by UAS.

Identifying the Threat

Unmanned aerial systems (UAS), commonly referred to as drones, are remotely and sometimes autonomously controlled aircraft capable of carrying diverse payloads, including cameras and sensors. While drones have beneficial applications — including firefighting, search-and-rescue operations, visual inspection, disaster relief and border security — these aircraft also can be deployed for malicious activities, posing a significant threat for utilities.

Drone-related threats to utilities include surveillance, sabotage, delivery of explosive payloads or hacking devices, creating a short circuit, or deliberately crashing into and damaging sensitive equipment. Data collected by the Electricity Information Sharing and Analysis Center shows an increase in UAS incidents at utilities during the past three years. This signifies an increased risk to our nation's critical infrastructure. UAS, in these instances, have been deployed to disrupt or invade the privacy of utility personnel and customers. Furthermore, their presence near power lines, substations, generation facilities, liquefied natural gas (LNG) storage plants, and other critical infrastructure is hazardous and may cause disruptions to operational continuity.

Methods of Attack

UAS events vary in type and impact. Broadly, UAS events fall into three distinct categories:

1. **UAS sighting.** This classification includes instances where utility personnel or contractors visually detect a UAS flying directly above or around a critical infrastructure site, lasting from brief moments to extended periods. Importantly, sightings typically do not result in service disruptions for the utility.
2. **UAS findings.** A UAS finding occurs when utility employees or contractors discover a downed UAS within the site perimeter during on-site inspections. The downed UAS is presumed to be the result of factors like lost connection, power failure or loss of control by the operator. Such incidents suggest the UAS was likely operated nearby, potentially for surveillance or attempted sabotage against the site.

3. **UAS incident.** An incident transpires when a UAS is the direct cause of a service disruption for the utility provider. These incidents are typically intentional acts of sabotage, but there have been cases where the UAS-driven incident was accidental.

The majority of UAS events fall within the categories of sightings and findings, while a significantly smaller percentage of events result in a UAS-caused utility service disruption or incident.

Examples of Drone Attacks

Weaponization and Sabotage

In recent years, the accessibility of consumer-grade drones has facilitated their modification to be used as weapons against critical infrastructure equipment. Malicious actors have purposefully sought to exploit this accessibility, with some degree of success, while using UAS to damage critical infrastructure and equipment, thereby disrupting utility operations. Some noteworthy examples of malicious actors using drones for inflict damage infrastructure include:

- An illustrative incident occurred when utility personnel discovered a downed drone on the ground within an electrical substation perimeter. The UAS was modified to transport a lengthy copper wire, potentially designed to drag across the substation's electrical equipment to cause a disruption. Similarly in 2019, utility personnel found a fishing line strung across critical equipment at another utility location. Subsequent analysis concluded that the line was connected to an observed UAS flight, demonstrating the recurring trend of these tactics.
- Another incident involved Greenpeace activists flying UAS over a nuclear power plant in France, dropping smoke bombs onto the roof of a building containing irradiated fuel.

Surveillance and Reconnaissance

Malicious actors can use UAS to conduct surveillance on potential targets — easily and quickly. Information garnered via UAS may include sensitive details about grid operations, vulnerabilities, security protocols and personnel, thereby enabling planning or execution of attacks. Moreover, UAS can disrupt, jam or control signals essential for grid reliability.

Reports from multiple utilities confirm the prevalence of UAS sightings in proximity to critical infrastructure facilities. In these incidents, the flights varied in length, but continued long enough to capture video and images of sensitive equipment.

Intellectual Property Theft

Malicious actors have used UAS to deliver devices that connect wirelessly to computer networks to commit cybercrimes involving theft of trade secrets, technologies or otherwise sensitive information. Additionally, UAS have the capability to introduce malicious software or viruses into targeted systems or devices through wireless connections. Examples of malicious actors using UAS to perpetrate cybercrimes include:

- In a noteworthy incident, environmental activists used a UAS to conduct a live stream flyover of a liquefied natural gas site. The ostensible purpose was to show perceived environmental impacts resulting from the site's operations. While framed as advocacy, this event underscores the potential misuse of UAS for unauthorized information gathering.
- A more sophisticated exploitation involved a drone attempting a data infiltration hack on a corporate network. The UAS landed on a building rooftop, then used a modified Wi-Fi Pineapple device, a Raspberry PI, several batteries, a GPD series mini laptop, a 4G modem and another Wi-Fi device.

Current Federal Regulations

In the United States, oversight of national airspace falls under the purview of the Federal Aviation Administration (FAA). The FAA classifies all types of UAS as "aircraft," and, by law, the destruction of an aircraft is a federal crime. Additionally, the Federal Communications Commission (FCC) prohibits interference with radio signals. Common drones use radio frequencies (RF) for remote operation and communication between the controller and the flying device.

The combination of these two laws prohibits damage or destruction of the aircraft in flight and radio interference with its authorized operation. Four federal agencies have the authority to employ UAS technology, including the Department of Justice (DOJ), the Department of Energy (DOE), the Department of Defense (DOD) and the Department of Homeland Security (DHS). Current regulation precludes these agencies from delegating this authority to local or state law enforcement agencies.

The regulations for UAS pilots are described in 14 Code of Federal Regulations (CFR) Part 107 "Small Unmanned Aircraft Systems." This comprehensive set of rules and guidelines accommodates various UAS users, such as recreational, commercial, public and governmental. Key regulations and requirements for UAS operations include:

- **Registration.** UAS operators must register devices weighing more than 0.55 pounds with the FAA. Registration helps with identifying and tracking UAS owners if there is an incident or violation.
- **Commercial operations.** When using UAS for commercial purposes — including aerial photography, surveying or inspection — UAS pilots must follow the rules of Part 107 of the Federal Aviation Regulations. These rules require UAS operators to obtain a remote pilot certificate; fly within visual line of sight; fly below 400 feet; fly only during daylight or civil twilight; fly at or below 100 mph; yield right of way to manned aircraft; avoid flying over people or moving vehicles; and obtain authorization or a waiver for controlled airspace.
- **Recreational use.** UAS pilots flying for recreational purposes, governed by Section 349 of the FAA Reauthorization Act of 2018, must adhere to specific guidelines. Section 349 requires UAS operators to fly only for enjoyment; fly within visual line of sight; follow community-based safety guidelines; fly below 400 feet; fly only in uncontrolled airspace or with prior authorization; register and mark their UAS; and pass an online aeronautical knowledge and safety test.
- **Public entities operations.** Public entities — including federal, state and local governments — are subject to Part 91 of the Federal Aviation Regulations. Part 91 requires UAS operators to obtain a Certificate of Waiver or Authorization (COA) from the FAA. This certificate outlines conditions and limitations for UAS operations in the public interest, including law enforcement, firefighting and search and rescue.

Security Options for Utilities

While utilities may not have as many options as they would like to for mitigating UAS attacks, proactive measures can significantly reduce the risk associated with potential drone incursions into critical infrastructure. Despite current U.S. laws prohibiting direct intervention with drones in flight, utilities can leverage a multifaceted approach to enhance defenses against UAS threats. No single solution will fully mitigate this risk, but there are several measures that can be taken to protect against UAS attacks, including:

- Deploy drone detection and tracking technology.
- Respond to drone incursions.
- Write policies and procedures for drone response.
- Coordinate with local law enforcement.

UAS Detection Technology

Utilities can procure commercially available technology to detect, monitor and track drones. Leveraging various methods including radar, acoustic, optical, infrared and radio frequency detection, this technology is a useful tool to ascertain the frequency and incidence of UAS intrusions. This information is instrumental in evaluating risks and identifying requisite counter-drone measures. Also, some technology can pinpoint the precise location of the drone pilot, a feature principally beneficial for law enforcement response. Technology using jamming, spoofing, hacking, netting, shooting or other capturing methods violates federal laws, which prohibit interference with aircraft navigation or communication systems.

Effective Response Strategies to UAS Incursions

Timely response to UAS incursions can help utilities promptly identify and rectify damage inflicted by drones. These steps can spur further investigation, if necessary. Mere awareness of a UAS incursion is insufficient to mitigate a drone attack. If a utility decides to deploy drone detection technology, timely response is essential for mitigation and deterrence.

Policies and Procedures

To improve response efforts, utilities would benefit from establishing clear roles and responsibilities to address UAS incidents. This involves establishing protocols for how and when to coordinate with law enforcement agencies, FAA officials and local authorities. Written policies and procedures can provide clarity regarding employees' authority by identifying when police involvement is warranted and establishing incident investigation safety protocols.

Law Enforcement Response

The FAA recommends that law enforcement observe and report potential violations of federal drone laws. While local law enforcement lacks the authority to proactively prevent all drone flights over a utility's property, their existing authority empowers them to investigate unsafe or illegal drone use. Beyond federal laws, local or state laws may come into play, especially laws that address the following:

- Trespassing on property.
- Disorderly and unsafe conduct.
- Interference with public safety operations.
- Public and harassment laws

Utilities can coordinate with local law enforcement to investigate attacks and deter future drone incursions. Local law enforcement typically has the knowledge to assist utility owners that are reaching out to federal authorities to investigate suspicious drone activity.

Industry Response to UAS Threats

Numerous utilities recognize the credible threat posed by drones and are actively maturing and enhancing their response capabilities. Some utilities are in the nascent phase of evaluating the efficacy of counter-drone technology. Concurrently, a few utilities have successfully implemented UAS detection technologies.

The graphic below represents various levels of maturing regarding drone security measures.

Key Considerations for Selecting UAS Countermeasures

There are several factors that influence the decision-making process for utilities when implementing UAS countermeasures. These considerations include:

- **Location.** Population density typically impacts UAS activity, with urban areas experiencing higher incursion rates compared to rural locations. Location is an essential factor when considering alarm rates and the capacity to assess the volume of alarms produced by UAS detection technology.
- **Pilot study.** Conducting a pilot study by temporarily deploying the chosen technology is valuable for utilities. The study not only assesses the effectiveness of various technologies but also provides insights into potential UAS incursions, facilitating strategic decision-making.
- **Cost.** A holistic assessment of the total cost, including installation and maintenance, is helpful for utilities in selecting and maintaining counter-drone systems.
- **Supporting technology.** Identifying complementary technologies to support drone detection, including PTZ cameras for alarm assessments, facilitates comprehensive security measures.
- **Configuration and integration.** Most utilities are equipped with electronic security systems and security operation centers to monitor and assess alarms. The integration of new UAS monitoring technology into existing security systems requires careful consideration to optimize the synergy of new and current capabilities.
- **Resources.** Underestimating the staffing required to operate new systems is a common pitfall. For UAS detection, important considerations include the staffing required to monitor and assess alarms, and the personnel needed to respond to alarms.
- **Policy and procedure.** Written policies and procedures are important when deploying new security measures to address emerging threats. These procedures should guide alarm assessments and response to UAS alarms.
- **Law enforcement coordination.** Demonstrations for local law enforcement agencies can enhance the agencies' familiarity with countermeasures, security systems and their role when responding to UAS incursions. Additionally, tabletop exercises with local law enforcement provide opportunities to understand what police can and will do in response to UAS incursions.
- **Regulations.** The evolving legal landscape regarding UAS, as well as offensive and defensive security measures, requires a proactive approach for monitoring regulatory changes. Regularly receiving updated information from industry groups and local governments can facilitate compliance with regulations.

Drone Countermeasures	Level 1	Level 2	Level 3	Level 4	Level 5
Identified drones as a threat.	x	x	x	x	x
Studied the feasibility of detection and tracking technology.		x	x	x	x
Developed drone response policy and procedure.			x	x	x
Deploy and integrate counter-drone technology.				x	x
Implement policy and procedure with employee training.					x
Coordinate and exercise with law enforcement.					x

***Figure 1:** Steps and levels for utilities and asset owners to address drone threats.*

Looking Toward the Future

The passage of remote ID requirements in mid-2021 marked a significant step toward addressing UAS incidents. Remote ID enables UAS in flight to provide identification and location information that other parties can receive via broadcast signal. This technology helps the FAA, law enforcement and other agencies locate the operator when a UAS appears to be flying in an unsafe manner, or if the UAS has entered a secure premise where it is not allowed to fly. Starting in September 2022, all UAS manufacturers were required to integrate remote ID capabilities into their devices. If UAS lack an internal remote ID, a device called a broadcast module can be affixed to comply with requisite rules and regulations.

While the original deadline for all UAS — including those flown for reactional, business or public safety purposes — to comply with Remote ID requirements was Sept. 16, 2023, the FAA provided an extension until March 16, 2024.

In 2022, the Biden Administration unveiled the Domestic Counter-Unmanned Aircraft Systems National Action Plan, which provided an expansive strategy to combat malicious UAS activity. Specifically, the plan seeks to expand the number of locations that can be protected against nefarious UAS activity, identify who is authorized to take action, and explain lawful actions that can be taken to protect assets. Congress did not advance the plan in 2023, but instead reauthorized existing authorities.

In May 2023, lawmakers introduced a new bill titled "Safeguarding the Homeland from the Threats Posed by Unmanned Aircraft Systems Act of 2023." This proposed legislation would incorporate essential components of the Biden Administration's updated counter-UAS legislative action plan while bolstering existing authorities to address current and future threats.

Conclusion

The threat of drones emerged quickly and is rapidly changing, while countermeasures and associated technologies to mitigate UAS are continually advancing. Simultaneously, the regulations governing both drones and drone countermeasures continue to evolve. Security professionals are seeking to understand the threat and identify the optimal mitigation strategy. Utilities nationwide exhibit varying degrees of preparedness to address the threat posed by UAS. Fortunately, there are options available to utilities to assess the threat and chart a path forward.

About Burns & McDonnell

Burns & McDonnell is a family of companies bringing together an unmatched team of engineers, construction and craft professionals, architects, and more to design and build our critical infrastructure. With an integrated construction and design mindset, we offer full-service capabilities. Founded in 1898 and working from dozens of offices globally, Burns & McDonnell is 100% employee-owned. For more information, visit **burnsmcd.com**.