sentrycs

Act Now to Protect Critical Infrastructure Against Drones

By: Dawn Zoldi (Colonel, USAF Ret.)

Act Now to Protect Critical Infrastructure Against Drones

Attacks and attempted attacks on critical infrastructure in the United States, ranging from nuclear power plants to power grids and energy facilities, have ramped up over the past several years. These attacks have become increasingly complex as perpetrators have started employing uncrewed aircraft systems (UAS) to target these facilities.

As these attacks continue, the limited legal authorities for a handful of federal agencies to detect and mitigate rogue UAS remain on track to expire. The current threat posture requires not just a continuation of limited Federal law enforcement agency authorities, but an expansion of such authorities to those in a position to defend our critical infrastructure: local law enforcement and critical infrastructure owners.

The UAS Threat in General

UAS present a sophisticated threat because of their unique characteristics. Unlike traditional weapons, UAS provide unparalleled physical and cyber access because they can overfly traditional security measures to conduct surveillance, inflict damage and access unsecured networks and critical operational components.

They are also cheap and easy to buy commercially off-the-shelf (COTS). The 2023 Annual Threat Assessment by the U.S. intelligence community warned that “foreign intelligence services are adopting cutting-edge technologies—from advanced cyber tools to unmanned systems to enhanced technical surveillance equipment—

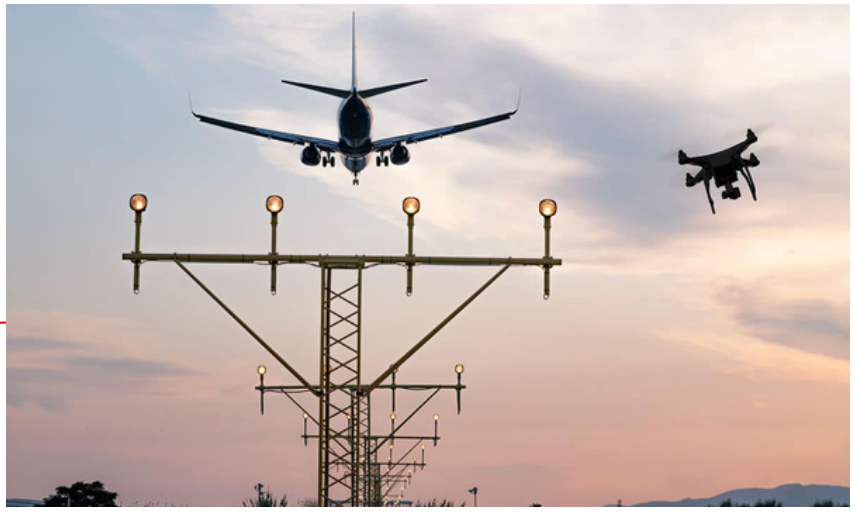
that improve their capabilities and challenge U.S. defenses. Much of this technology is available commercially, providing a shortcut for previously unsophisticated services to become legitimate threats." (Emphasis added). The recent events in the Russia-Ukraine war have literally battle-proven this assessment.

Beyond foreign battlefields, and much closer to home, UAS continue filling the U.S. national airspace. In its Aerospace Forecast for Fiscal Years 2023-2043, the Federal Aviation Administration (FAA) estimated that the recreational small UAS fleet will peak over the next 5 years, from the current 1.69 million units to approximately 1.82 million units by 2027. This equates to a cumulative annual growth rate of 1.6% over that period. The size of the registered commercial drone fleet (those weighing > 0.5 lbs up to 55 lbs) amounted to 727,000 aircraft at the end of last year. The FAA forecasts that the commercial drone fleet will increase to about 955,000 UAS by 2027.

While the majority of UAS pilots choose to follow the rules, as UAS numbers surge, so too do the negative encounters with them. This includes hundreds of reported drone sightings around airports every month and thousands of border incursions annually. These events will continue to grow over the coming years. The unique physical and operational characteristics of UAS make them a difficult problem to address. UAS often evade detection. This creates specific challenges for the critical infrastructure community.

The FAA received 2,596 reports of sUAS spotted by pilots in 2021

Source: Embry-Riddle Aeronautical University



The UAS Threat to Critical Infrastructure

The Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) lists 16 critical infrastructure sectors. These include commercial facilities, such as stadiums that facilitate mass gatherings, nuclear reactors, energy resources, financial services, government facilities and others. According to CISA, the private sector both owns and operates the majority of this infrastructure.

In the energy sector alone, private entities own over 80 percent of the critical assets that supply fuels to the transportation industry and electricity to homes and businesses across the country.

A key part of that sector, the electric grid, remains vulnerable to attacks that could damage or destroy the more than 79,000 transmission substations across the nation. DHS lists UAS as a common attack vector for these facilities, right alongside ballistic (small arms to high powered rifles) and other physical attacks. In the first known case of a modified UAS to target US infrastructure, in 2020, a still-unidentified perpetrator used a DJI Mavic 2 uncrewed aircraft (UA) rigged with dangling rope and copper wires in an apparent attempt to short circuit the power grid in Pennsylvania (PA).

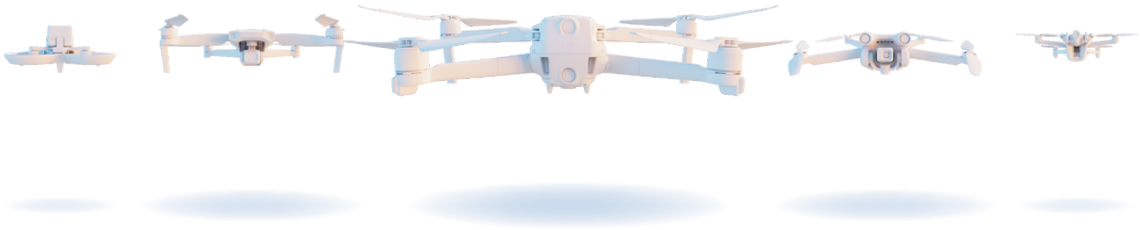
The energy sector does not stand alone in its vulnerability to UAS. Non-modified UAS have been conducting significant numbers of incursions, presumably for surveillance purposes, on dozens of U.S. nuclear reactors and fuel storage sites for years, even prior to the PA substation incident. In 2019, due to a crescendo of UAS sightings around nuclear power plants, the U.S. Nuclear Regulatory Commission (NRC), in conjunction with Sandia National Laboratory, conducted a classified technical analysis on the UAS threat to these facilities. Shortly thereafter, all public discussion from NRC and other Federal agencies on these incursions ceased.

Besides disruption and prohibited surveillance, espionage and intellectual property theft also ranks high among the threats UAS pose to critical infrastructure. The Louisiana Chemical Association, Apple, Facebook, Tesla have all reported incidents of UAS-conducted aerial espionage. Equipped with a variety of sensors, UAS can land on buildings or peer through windows to gather proprietary information.

Perpetrators also employ UAS to drop contraband into prisons. Last year, two inmates at Fort Dix, New Jersey, pled guilty to masterminding a year-long lucrative drone-smuggling operation that distributed prohibited cell phones, cell phone accessories, tobacco and other items to fellow inmates.

While cell phones may appear innocuous, these devices can be worth several thousand dollars inside prisons, have been known to spark riots and otherwise allow inmates to continue conducting their criminal enterprises while incarcerated.

These examples represent but a mere sampling of the many ways that UAS can harass, disrupt, damage, or destroy critical infrastructure facilities and sensitive operations. Detecting and safely mitigating nefarious UAS remains key to successfully preventing these types of UAS-related incidents. However, today only a few Federal agencies can do this legally.



Legal Limitations and Possibilities

Multiple Federal laws and regulations, most written decades ago and well before the UAS threat emerged, continue to hamstring those charged with protecting and defending critical infrastructure in this country. Congress has only affirmatively authorized the deployment of counter-UAS technology by a limited number of Federal agencies: the Department of Defense (DOD), Department of Energy (DOE) as well as certain portions of the DHS and the Department of Justice (DOJ).

In 2017, the DOD became the first Federal agency to receive this legislative authority to detect and mitigate drones. Later that year, Congress amended the Atomic Energy Defense Act to extend similar authority to the DOE. The following year, Congress passed the "Preventing Emerging Threats Act of 2018" as part of the FAA Reauthorization Act (FAARA 2018). It authorized the DOJ (including FBI) and DHS (including the U.S. Coast Guard but not the Transportation Safety Agency or TSA) as approved users of counter-UAS technology.

A major gap remains. Some of the biggest and most likely threats to critical infrastructure reside at the state and local level. Federal agencies simply lack the resources and capacity to protect it all.

During last summer's hearing in the Senate's Homeland Security and Governmental Affairs Committee, Acting DHS Assistant Secretary for Counterterrorism, Samantha Vinograd, testified on the evolving threat that UAS pose to the U.S. and the inability of the Federal government to keep up with it. She explained that during the agency's 70 counter-UAS joint protection operations at large events, Federal Bureau of Investigations (FBI) teams detected 970 noncompliant UAS in restricted airspace. The TSA reported 65 cases where commercial airline pilots had to take lifesaving evasive actions to avoid UAS collisions.

Ms. Vinograd said, “DHS relies on partners all around the country to help protect the homeland. We can’t be everywhere.” She continued. “What we know is that the threat posed by UAS is widespread across the country, and it is critical that our partners have the authority to help protect the homeland.”

Those partners include more than just the FBI’s three-member strong counter-UAS team. These over-extended professionals can only cover less than one percent of the requests for support. Necessary partners in this effort must include local law enforcement and critical infrastructure owners and operators. The current Administration recognizes this, as do members of Congress - on both sides of the aisle.

In April 2022, the Biden Administration released the Domestic Counter-Unmanned Aircraft Systems National Action Plan (CUAS Plan), the first whole-of-government plan to address UAS threats in the homeland. It aims “to expand where we can protect against nefarious UAS activity, who is authorized to take action, and how it can be accomplished lawfully” through 8 recommendations for action. Among other things, those recommendations include working with Congress to expand counter-UAS authorities to several other Federal agencies (e.g., State, Central Intelligence Agency and NASA) as well as to state, local, territorial and Tribal (SLTT) law enforcement agencies and critical infrastructure owners and operators.

Several months later, Senator Gary Peters, Johnson, Sinema and Hassan introduced the bi-partisan Safeguarding the Homeland from the Threats Posed by Unmanned Aircraft Systems Act of 2022. Similar to the White House’s CUAS Plan, it proposed to reauthorize Federal government counter-UAS authorities and extend authorities for tracking and detection to SLTT agencies as well as critical infrastructure. It also included a pilot program to expand mitigation capabilities to 12 state and local government agencies each year, conditioned on proper vetting, training and use of similar operational and privacy rules as their Federal counterparts. This bill did not pass, but should have.

Safe Technologies

One of the primary holdups for this type of legislation seems to stem from concerns relating to the safety of counter-UAS technologies in general and in highly sensitive environments, such as near communications-laden airports.

For the past 5 years, under the authority Congress granted it in Section 383 of the FAARA 2018, the FAA has been testing and validating counter-UAS technology in the airport setting. Admittedly, some mitigation tools such as kinetic or jamming technologies create a risk of collateral damage. On the other hand, several safe and proven mitigation solutions exist. These have been employed successfully outside of the U.S.

A currently available and safe counter-UAS solution, operates by replacing the controller's RF signal with a command to land in a pre-defined safe landing zone. The takeover and safe landing can be manually triggered or occur automatically when a UAS enters a designated no-fly zone. This allows the drone operator to be identified and located as well as easily, and safely, taking over a UAS with no collateral risk. This eliminates the risk of damage to civilians and physical property, including the overtaken UA.

One such company, Sentrycs has developed an autonomous and fully integrated counter-UAS solution based on protocol analytics to protect rural and dense urban areas from unauthorized UAS, without the false alarms, interference or collateral damage that other Detection-Tracking-Identification (DTI) and mitigation technologies, such as radars, radio frequency (RF) scanners, directional jammers, or Global Positioning System (GPS) spoofers present.

Sentrycs detects rogue drones with plug & play 24/7 autonomous monitoring and alerting, even during nighttime and without direct line of sight. It tracks them by reading

the RF signal to monitor the UAS' height and speed, and to locate both the UAS coordinates and the last known location of the remote control for it (typically also the pilot's location). It identifies the UAS by providing user-level identification including UAS vendor, type, and serial number. Finally, it mitigates the threat by replacing the UAS control signal with a different set of instructions, bringing it to a safe altitude, and landing it safely in a pre-designated area. To further foster a safe and secure environment, Sentrycs remains resistant to nearby RF noise and creates no RF interference with other communication signals. The Sentrycs solution is one of several similar cyber takeover solutions that have been employed safety and successfully around the globe and do not require an additional five years of testing. They are ready for use now against the threats that will keep coming.

Privacy Concerns and Remote ID

Privacy and civil liberties are another concern raised about counter-UAS. UAS detection currently collects data that is considered non-public and protected under antiwiretapping laws. With the September 2023 implementation of the FAA's Congressionally mandated Remote Identification rule (RID), those issues will be nullified. Under RID, any small UAS operating in the US must be registered and must have RID broadcast capabilities to legally fly in the national airspace system. RID broadcasts are required to include specific Mission Elements (MEs), including location data, which will go out to the public, law enforcement and security agencies.

There are three ways to comply with RID when flying a UAS in the US: 1) using a Standard RID UAS with built-in RID broadcast capabilities; 2) attaching a Broadcast RID Module to the drone; or 3) flying in specially approved non-RID areas called Federally Recognized Identification Areas (FRIA).

The MEs that RID broadcasts must include: a unique identifier to establish the UAS identity (its serial number or a session ID); latitude, longitude, geometric altitude, and velocity; control station latitude, longitude and geometric altitude (for Standard RID only); time mark and emergency status indication (for Standard RID only). Broadcast Modules will need to broadcast the drone's takeoff location (not control station) and will not indicate an emergency status. Session ID is not an option for Broadcast Modules. These broadcast requirements negate any claim to privacy for this information.

RID, however, is not a silver bullet to detect rogue UAS. Bad UAS actors are unlikely to comply with the rule. Additionally, RID compliance alone does not rule out potential nefarious intent or purposes.

Actions Needed

While the US has, to date, not had an event caused by a UAS cause greater economic or tragic physical damage, the proliferation of UAS makes it unlikely that track record will last. Brad Wiegmann, the Justice Department's deputy assistant attorney general, national security division, warned Congress in last year's Senate hearing that it's "only a matter of time" before a UAS attacks a mass gathering in the country.

UAS threats exist today and will not wait for our laws to catch up. RID is a step in the right direction, but it needs to be supplemented with other legislative language allowing detection by State, local, and tribal authorities as well as critical infrastructure operators. It also does not allow mitigation. Hence, the need for legislative action to permit the organizations who need it to use the technologies that actually do that.

Besides reauthorizing the Federal agencies who have already been deploying counter-UAS technologies for the past 5 years without incident, non-collateral takeover mitigation technologies should be approved and delegated to the lowest level possible.

This includes SLTT and critical infrastructure owners and operators who can more quickly and safely protect the assets that comprise the lifeblood of the nation.

To do this, legislators should review the Peters bill as a baseline. Every relevant Federal and SLTT agency supports it, as does the Association for Uncrewed Vehicle Systems International (AUVSI), the Commercial Drone Alliance (CDA) and the majority of UAS and counter-UAS industry. To remove internal jurisdictional challenges, similar provisions should be included as an amendment to the upcoming FAA Reauthorization Act, just as occurred in 2018 with the original Preventing Emerging Threats Act. Only then will our skies be safe.

About the author

Dawn M.K. Zoldi (Colonel, USAF, Retired) is a licensed attorney with 28 years of combined active duty military and federal civil service to the U.S. Air Force and a Part 107 certified drone pilot. She is the CEO & Founder of P3 Tech Consulting and an internationally recognized expert on uncrewed aircraft system law and policy, featured in CNN, Forbes and Newsweek. Ms. Zoldi contributes to several magazines and hosts popular tech podcasts. In 2022, she received the Airwards People's Choice Industry Impactor Award, was recognized as one of the Top Women in Aerospace & Aviation to Follow on LinkedIn and listed in the eVTOL Insights PowerBook. She is the author of the book Unmanned Aircraft Systems Legal and Business Considerations: A Modern Primer for U.S. Drone Programs. For more information, follow her on social media and visit her website at: https://www.p3techconsulting.com.

Get in touch

There are many factors to consider when thinking of your counter-UAS solution. To discuss your situation in depth or if you would simply like more information on anything in this whitepaper, please visit www.sentrycs.com or reach out: info@sentrycs.com