EMERGING RISKS: THE CYBER-PHYSICAL DRONE THREAT

DEFEND TODAY, SECURE TOMORROW
Threat Actors

Careless & Clueless
- Overwhelming majority in U.S.
- Operate Common Commercial Off The Shelf (COTS) multi-rotor platforms
- Unintentionally or unknowingly violate flight restrictions or fly unsafely
- Effective detection and tracking by most radio frequency sensors when present
- Operators likely not trying to avoid detection or intervention from LE

Intentional & Criminal
- May modify the COTS drones to carry/drop payloads
- Often conduct planned operations with intent to evade detection.
- Drone modifications may make detection, tracking, and identifying the operator difficult

Terrorists & Paramilitary
- May modify the COTS drones during guerilla warfare
- Detection, tracking, and mitigation are made difficult due to modifications
Tactics

Smuggling
Disruption
Weaponization
Surveillance/Reconnaissance
Cyber
October 2018 - September 2020: 235 pre-operational incidents were reported at or near domestic chemical facilities in Louisiana.

December 2019: A chemical plant in New Jersey found a grounded drone with a memory card containing footage of the facility.

April 2021: A "fairly-large" drone was observed by a Pennsylvania facility employee around the Liquid Propane farm, then flew across the Plant about 20-30 feet above the ground.
Security Measures

- Know the airspace, flight restrictions, and who has authority to take action.
- Consider using detection technology to enhance awareness of the airspace above facilities.
- Use “No Drone Zone” signage.
- Update security plans to incorporate drone response actions.
- Provide training and conduct exercises on recognizing suspicious indicators and responding to drone incursions.
- Establish render safe and handling procedures in the case of a crashed drone.
- Build strong partnerships between federal, state, and local law enforcement, recreational drone user groups, and critical infrastructure owners and operators in the area.
- Connect with a Protective Security Advisor (PSA) and conduct a site survey of the venue and surrounding area. Take note of critical assets, nearby property types, potential drone launch points, and options for positioning detection equipment.
The Domestic C-UAS NAP proposes **eight key recommendations** to include legislative action to address shortfalls in existing authorities.

1. **Work with Congress** to reauthorize and expand existing C-UAS authorities.
2. **Establish a list** of U.S. government authorized detection equipment.
3. **Establish oversight mechanisms** for purchasing C-UAS equipment.
4. **Establish a C-UAS training center.**
5. **Create** a Federal UAS incident tracking database.
6. **Establish a mechanism** to coordinate research, development, testing, and evaluation.
7. **Work with Congress** to enact a comprehensive criminal statute.
8. **Enhance cooperation** with the international community.
For more information:
cisa.gov/uas-critical-infrastructure

Questions?
sUAS Security
Email: suassecurity@cisa.dhs.gov