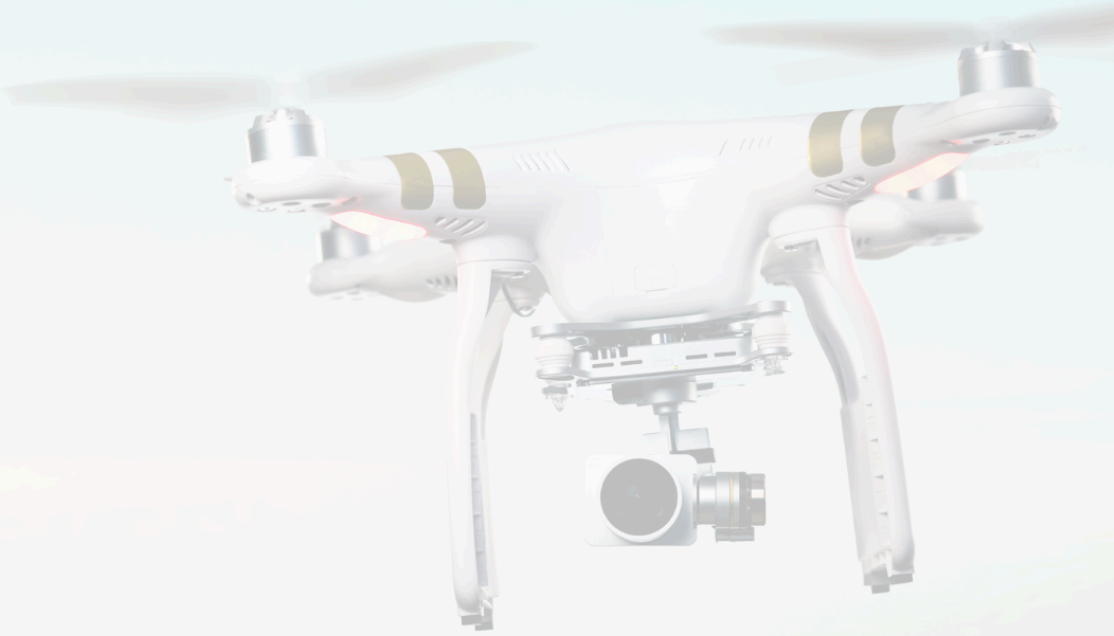
CENTER FOR
CYBERSECURITY
POLICY AND LAW



AFTER ACTION REPORT

MEETING THE HOMELAND UAS THREAT: 2026 TABLETOP EXERCISE

JULY 2026

Executive Summary

On May 12, more than 80 participants representing U.S. federal, state, local, and tribal stakeholders; Canadian government partners; critical infrastructure operators; technology providers; and private-sector organizations participated in the *Meeting the Homeland UAS Threat 2026 Tabletop Exercise* in Detroit, Michigan.

The exercise involved a multi-pronged drone attack from a boat situated halfway between the United States and Canada on Lake St. Clair. The boat served as a launch pad for multiple drone swarms that descended on both sides of key international bridges and the tunnel connecting Detroit, Michigan, and Windsor, Ontario; hit multiple electric grid transformers and substations; and killed dozens of fans gathered for the summer Grand Prix.

Participants were challenged to respond to a rapidly evolving threat environment characterized by incomplete information, competing operational priorities, cross-border implications, and uncertainty about whether additional attacks would follow.

While participants acknowledged significant progress in recent years—including the passage of the Safer Skies Act, which gives trained state, local, tribal, and territorial officials authority to take certain mitigation measures—the exercise highlighted persistent gaps in airspace awareness, available resources, and protections for critical infrastructure.

Some key takeaways:

- **Effective Airspace Awareness Remains a Significant Gap:** Participants consistently identified detection and airspace awareness as the most significant challenge facing both government and private-sector organizations. Without reliable detection, organizations cannot distinguish lawful activity from suspicious activity, nor can they effectively prioritize response actions.
- **Airspace Awareness Suffers from Resource Constraints and Limits on Effective Information-Sharing:** Effective detection requires multi-layered systems incorporating multiple sensor types (*i.e.*, radio frequency, acoustic, and visual), integrated into a single operating platform, and shared across multiple jurisdictions. Few state and local jurisdictions and few critical infrastructure owners and operators currently have the resources and visibility needed.
- **Better Enforcement of Existing Rules Is a Critical First Step:** Better enforcement, and potential expansion of the Remote ID rule, which requires drones weighing more than 250 grams and other drones subject to FAA registration requirements to publicly broadcast identification and location data, would significantly enhance detection efforts. This would enable local officials and critical infrastructure owners to better distinguish between lawfully present and potentially malicious drones.

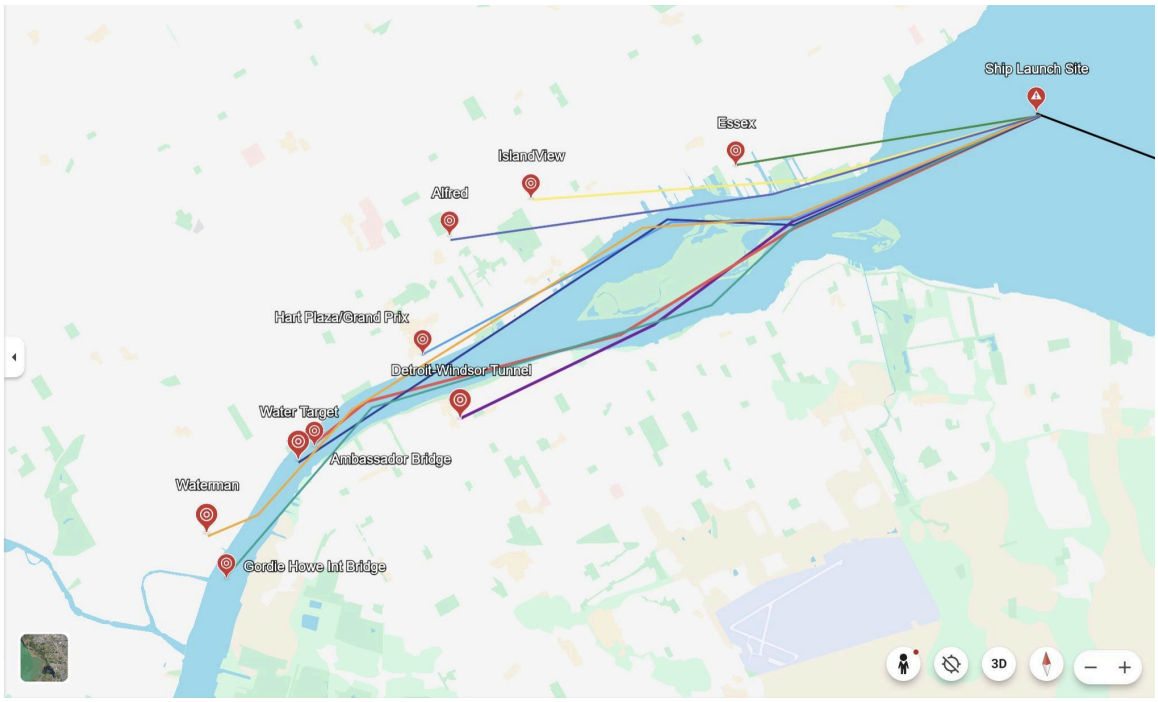
- **Critical Infrastructure Remains Vulnerable:** The event highlighted the vulnerabilities of critical infrastructure to potential drone threats, the importance of critical infrastructure owners and operators being able to manage their airspace, and gaps in authorities to mitigate. The discussion also focused on the promise—and limits—of the Federal Aviation Administration's long-awaited Section 2209 Notice of Proposed Rulemaking, which was issued just days before the event. Once final, it will establish a process by which critical infrastructure entities can request flight restrictions for unmanned aircraft systems above certain fixed facilities.
- **Cross-Border Coordination Is Strong but Requires Further Formalization:** The Detroit–Windsor region benefits from longstanding relationships between United States and Canadian law enforcement entities and other officials. However, the two regions operate under differing authorities, operational procedures, and legal frameworks for responding to airborne drone threats. Participants urged further coordination, both at the operational and policy and regulatory levels, to support integrated detection and response plans.
- **Counter-Drone Measures Should Be Integrated into Core Security Planning:** Management of the threat posed by malicious drones should be integrated and normalized as part of core security planning. While participants expressed confidence in general emergency response capabilities and coordination, the risk of threats from the sky adds new complexity. Participants raised unresolved questions about who would be directing the response operations in a multi-jurisdictional incident involving complex airspace management challenges, among other public safety and infrastructure protection concerns.

Scenario Overview

The exercise scenario involved a coordinated attack launched from a vessel operating on Lake St. Clair. Multiple drones were launched against transportation infrastructure connecting Detroit, Michigan, and Windsor, Ontario, including the Ambassador Bridge, Gordie Howe International Bridge, and Detroit–Windsor Tunnel. Additional attacks targeted electrical substations and transformers across the Detroit metropolitan area, as well as public gathering areas associated with the Detroit Grand Prix.

Participants first received threat reporting indicating elevated drone activity and increasing concerns from government agencies regarding the potential for attacks against critical infrastructure. As the exercise progressed, participants were forced to respond to a coordinated attack while managing incomplete information, social media reporting, public communications challenges, and concerns regarding potential follow-on attacks.

Map of Targets



The exercise included a visual demonstration of the attack, using a simulation that showed the initial launch of the drone swarms, their movement along the Detroit River, and their arrival at the designated targets. The entire attack lasted just over 7 minutes from start to finish.

Breakout Group Observations

In order to enable engaging conversation among all participants, three breakout groups were established during the middle part of the exercise. These groups came back together at the end to share the outcomes of their discussion with the broader group.

Federal Participants

Federal participants focused heavily on questions of authorities, resources, and implementation. Discussions focused on the need to support state and local detection efforts, the importance of training more state and local authorities to be able to take appropriate mitigation measures, consistent with the Safer Skies Act, and the resource limitations that prevent federal authorities from being able to fill all counter-UAS (Unmanned Aircraft System) needs across the nation.

State and Local Participants

State and local participants expressed confidence in existing emergency management structures but lacked clarity as to who would ultimately be “in charge” in the wake of an attack that involved the need to manage and deconflict the airspace.

While some participants wanted permission to just shoot down drones, others warned of the potential collateral damage and risk to lawfully present law enforcement drones and operations, including safety and rescue operations.

Participants expressed frustration with the absence of a nationwide airspace awareness system that covers low-altitude drones. Participants also expressed frustration with the pace of training state and local officials regarding mitigation tools and safeguards—a precondition for state and local officials having the authority to take mitigation measures, pursuant to the Safer Skies Act.

Critical Infrastructure and Private Sector Participants

Private-sector participants highlighted significant concerns about the threat posed by drones and the need for a regulatory and operational framework that better protects against such threats, while also continuing to support the proactive use of drones for safety and security inspections.

Participants expressed concerns about the lack of coordinated airspace awareness, the challenges in distinguishing compliant commercial drone activity from malicious operations, and the absence of authority for critical infrastructure owners and operators to take even non-kinetic mitigation measures (such as sending a drone back to the sender) in response to threats.

Analysis and Recommendations

The exercise underscored the challenges posed by the UAS threat in light of the speed of operation, scale of potential damage, and accessibility of the underlying technology. Traditional security measures designed to protect facilities from physical intrusion are insufficient to protect against aerial threats capable of approaching from multiple directions simultaneously.

Three themes emerged repeatedly throughout the exercise. *First,* detection and airspace awareness are prerequisites for every subsequent response activity. *Second,* while the federal government controls the airspace, the risks are felt and ultimately must be managed locally. *Third,* information sharing, coordinated planning, and joint efforts are essential mechanisms for building trust and improving operational effectiveness. These themes inform the recommendations that follow:

Expand Regional Airspace Awareness and Detection Capabilities

Stakeholders should prioritize investments in layered detection systems that combine radar, radio-frequency, optical, and acoustic sensing technologies. These capabilities should feed a shared operating picture accessible to authorized partners across government and critical infrastructure sectors.

Increase Enforcement and Compliance with Remote ID Requirements

Participants repeatedly identified Remote ID as a critical tool for distinguishing compliant operators from potential threats. The FAA's newly announced DETER program, designed to increase and streamline enforcement of Remote ID and other drone safety rules, is a positive step forward and something that should be fully resourced and prioritized.

Institutionalize Joint Planning and Exercises with Critical Infrastructure Owners

Routine exercises, information-sharing activities, and coordinated planning efforts should be expanded to ensure critical infrastructure owners are fully integrated into preparedness and response activities related to the UAS threat.

Accelerate Training and Resource Delivery Under the Safer Skies Act

Federal agencies should expand training capacity and technical guidance so as to expand the pool of state, local, tribal, and territorial officials that can lawfully and safely activate a broader range of detection activities and take needed mitigation measures in response to a credible drone threat.

Ensure Effective Implementation of the FAA's Forthcoming "2209" Rule

Just days before the exercise, the FAA issued its long-awaited proposed rule (with comments due August 5) that would establish standards and processes for critical infrastructure owners and operators to obtain unmanned aircraft flight restrictions over certain facilities. This is important: flight restrictions can provide critically important protections for critical infrastructure, enabling them to better distinguish lawful and unlawful drones and protect their facilities as a result.

The FAA should carefully review comments to ensure sufficient protections for facilities and places where large numbers of people congregate and to ensure that the process for obtaining restrictions can be handled in a timely and effective manner. The FAA should prioritize implementation once the rule is finalized, and Congress should ensure that the FAA is adequately resourced (and staffed) to manage the proposed process.

Develop a Formal U.S.-Canada Counter-UAS Coordination Framework

U.S. and Canadian stakeholders should build on existing relationships by developing shared playbooks, communications protocols, and operational frameworks designed specifically for cross-border UAS incidents.

Conclusion

The threats from UAS are both familiar in their impacts on critical infrastructure and human life and unique in their execution. Traditional methods of defending against adversarial actions, *i.e.*, the "guns, gates, and guards" approach, are inadequate to stop coordinated UAS attacks, as this exercise clearly demonstrated.

Future success will depend on improving airspace awareness, expanding training and preparedness activities, strengthening public-private partnerships, and developing mature operational frameworks capable of supporting cross-jurisdictional and international response efforts.

About Us

This is the second in a series of exercises put on by Venable and the Center for Cybersecurity Policy and Law ("Center"), designed to support local, state, and federal authorities; critical infrastructure owners; and others that host large gatherings in understanding and preparing for the risks posed by unauthorized drone use. Related to these exercises, both Venable and the Center support clients in understanding the current legal and regulatory framework, in putting in place effective frameworks for assessing and responding to threats that emerge, and in working across local, state, and federal government to do so.

We are also actively engaged in ongoing efforts to support critical infrastructure in responding to requests for comments on the FAA's Notice of Proposed Rulemaking, *Designation – Restrict the Operation of Unmanned Aircraft in Close Proximity to a Fixed Site Facility*, which would set standards and procedures for critical infrastructure to obtain flight restrictions over certain fixed facilities. We will also support clients in applying for restrictions once the rule goes into effect.

We also want to thank our partners and sponsors for this event:

ECHODYNE DTE UNIFY.C2

VENABLE LLP

Facilitators:

John Banghart

Venable LLP / Center for Cybersecurity Policy and Law

Jennifer Daskal

Venable LLP / Center for Cybersecurity Policy and Law

Davis Hake

Venable LLP / Center for Cybersecurity Policy and Law

Participants:

Aerisq Solutions, LLC

Ambassador Bridge

Center for Cybersecurity Policy and Law

City of Detroit Homeland Security & Emergency Management

Consulate General of Canada in Detroit

Cooley Law School

Cybersecurity and Infrastructure Security Agency

Detroit City Shield

Detroit International Bridge Company

Detroit Police Department

Divergence Strategy

Downtown Detroit Partnership

Drone Deploy

DTE Energy

Energy-ISAC

Federal Aviation Administration

Federal Bridge Corporation Limited (Blue Water Bridge)

Federal Bureau of Investigation

General Motors

Honeywell

Institute for Critical Infrastructure Technology

Kent County Sheriff's Office

Lantern UAS

Marathon Petroleum

Michigan Department of Transportation

Michigan Drone Association

Michigan Economic Development Corporation

Michigan State Police

National Aeronautics and Space Administration (NASA)

Rainfall Strategies

Rep. Tom Barrett's Office

SPS Aerial Remote Sensing

Stellantis

Synarea Insights

The Tactien Group, LLC

U.S. Customs and Border Protection

UAS Norway

Unify.C2

United States Coast Guard

University of Nevada, Reno

Venable

Wayne Law School

Windsor Port Authority

Windsor-Detroit Bridge Authority