ORION FORUM

Securing the Homeland Against Drone Threats: Policy and the Challenge of Decentralized Authority

FEBRUARY 27, 2026

By Suat Cubukcu, Editor

With contributions from Austin Doctor, Bill Edwards, Scott Parker, and DJ Smith (listed alphabetically)

The rapid proliferation of small unmanned aircraft systems (sUAS) has created both opportunity and vulnerability. While drones increasingly support commerce, public safety, agriculture, and infrastructure inspection, their accessibility also lowers the barrier to misuse. The recent incident in El Paso, which resulted in a temporary yet highly disruptive airspace closure, underscores the real-world consequences of both drone activity and counter-UAS responses. Similar incidents near airports, over mass gatherings, and around critical infrastructure expose regulatory and operational gaps that policymakers can no longer afford to treat as hypothetical.

The expansion of counter–unmanned aircraft systems (C-UAS) authorities under the SAFER SKIES Act marks a turning point. The central question is no longer whether drone threats exist, but whether the United States can build a coherent framework that balances security, innovation, and decentralized execution.

To examine this challenge, Orion Policy solicited insights from subject matter experts Austin Doctor, Bill Edwards, Scott Parker, and DJ Smith on three critical questions:

1. What measures and policy interventions are most critical in limiting access to small drones by malicious actors and mitigating vulnerabilities to drone-related threats in the homeland?

2. How effective are current counter-UAS (C-UAS) technologies for deployment in civilian airspace, especially near airports and in dense urban environments?
3. With the decentralization of C-UAS authority under the SAFER SKIES Act, what major operational and coordination challenges are likely to emerge?

Their responses reveal that the drone challenge begins earlier and demands more coordination than current policy frameworks fully account for.

The Threat Begins Before Takeoff

Much public debate focuses on detection and interdiction. But Austin Doctor argues that this perspective is incomplete. “The drone threat begins at procurement—not at flight,” he explains. From a homeland security standpoint, the objective should be to “harden sourcing pathways and generate points of friction in procurement and assembly.”

This reframing shifts attention to the supply chain. Rather than relying solely on mid-air mitigation, policymakers should consider upstream interventions: point-of-sale registration for higher-risk systems, anomaly detection models to flag suspicious bulk purchases, and structured partnerships with e-commerce platforms, retailers, payment processors, and logistics firms. Doctor notes that outbound and cross-border shipments would benefit from “risk-based assessments that integrate bill-of-lading analysis, routing anomalies, and network mapping.”

The supply chain is not purely physical. Open-source firmware, programming modifications, and AI-enabled operating systems increasingly allow malign actors to adapt commercial platforms in ways that circumvent traditional countermeasures. Monitoring digital supply pathways, therefore, becomes part of a broader resilience strategy. As Doctor concludes, “Supply-chain hardening is an efficient way to raise the costs of criminal exploitation, reduce criminal anonymity, and constrain malign adaptation before drones are deployed.”

Layered Defense Is Operational Reality

Even robust procurement controls cannot prevent every misuse. The drone threat landscape has two dimensions. The most probable risk comes from careless use around airports and

mass gatherings. The most consequential risk comes from low probability but high impact weaponization by malign actors. Both require sustained attention.

No single intervention will solve the problem. A layered “Swiss cheese” approach remains essential. Limiting adversary capability through stronger supply chain controls and tighter registration requirements must be paired with vulnerability reduction at the target level.

Structured vulnerability assessments of critical infrastructure, symbolic locations, and high visibility events should be routine. A dynamic geospatial risk map that identifies high risk zones can significantly enhance situational awareness and interagency coordination.

Scott Parker reinforces this logic from an operational standpoint. “Targeted policy and operational interventions are required,” he notes. Education and awareness campaigns improve understanding of lawful drone activity and indicators of concern. Higher quality reporting enables earlier intervention and reduces the ability of malicious actors to operate undetected.

Parker also highlights a structural oversight. “Most all hazard assessments lack a ‘bird’s eye view,’ leaving exploitable exposures unaddressed.” Integrating aerial vulnerabilities into existing risk management processes forces agencies to account for vertical exposure, not only perimeter threats.

He further notes that “as drone technology and tactics evolve, detection and defeat alone are insufficient.” Hardening, obscuring, and building redundancy into high risk assets reduces consequences even if perimeter defenses fail. Resilience determines whether disruption becomes crisis.

Visibility Creates Decision Advantage

One of the more pragmatic debates concerns access restriction versus universal visibility. DJ Smith questions whether limiting access to drones outright is realistic. Instead, he focuses on the necessity of comprehensive airspace awareness. “If we truly want to create a common operating picture,” he argues, “we need to be able to see all things aloft.” Current exemptions for smaller drones create blind spots. When those platforms are not required to register, they often fall outside Remote ID mandates. As a result, “we cannot see them in our airspace in

most cases," even though that size point represents a significant portion of drones aloft.

Smith challenges earlier assumptions that lightweight drones posed minimal risk. Real world incidents have demonstrated otherwise. His recommendation is direct. Require all drones, regardless of size or weight, to transmit Remote ID or an ADS B style signal.

The operational benefit is discrimination. Once compliant aircraft are visible, enforcement can concentrate on anomalies. Authorities can "focus on those airframes that are dark or not transmitting, narrowing the haystack in the sky." Visibility converts ambiguity into prioritization. In a congested low altitude environment, that distinction is decisive.

The Limits of Technology Alone

Technological mitigation remains indispensable, particularly near airports and dense urban infrastructure. Yet panelists caution against overconfidence. No single C-UAS system is sufficient.

Smith estimates that layered systems, properly integrated, can achieve "probably 65–75 percent efficacy." Radar provides foundational detection but lacks classification and attribution. RF intercept and decoding technologies can identify command-and-control links, pilot location, and Remote ID data. In certain cases, mitigation may involve jamming, kinetic removal, or cyber takeover.

Each intervention, however, carries consequences. Jamming risks interference with legitimate communications. Kinetic responses pose safety concerns in populated areas. Cyber takeover authorities raise legal and liability questions. Particularly in civilian airspace, mitigation must balance urgency with proportionality.

Decentralization and the Coordination Imperative

The SAFER SKIES Act decentralizes C-UAS authority, extending operational roles to SLTT entities and critical infrastructure operators. This expansion promises faster response and broader coverage. But it also introduces friction.

Smith emphasizes that "coordination will be the most important piece," especially in determining who owns an incident before it occurs. Tabletop exercises across the country

demonstrate that significant drone incidents inevitably require whole-of-government responses. He argues that once federal standards for training, reporting, and oversight are established, qualified SLTT and critical infrastructure entities should be empowered to act decisively. “In almost all these types of incidents,” he notes, “response time is always of the essence.”

Scott Parker highlights additional vulnerabilities. The absence of a mature federal validation mechanism, such as an authorized equipment list, risks inconsistent procurement decisions and uneven readiness. A limited cadre of experienced federal operators may constrain effective knowledge transfer. Most importantly, a fragmented national data sharing and reporting architecture impedes development of shared, real-time situational awareness across jurisdictions.

Bill Edwards emphasizes interoperability and governance alignment. Agencies with differing resources and legal interpretations must align on authorities, rules of engagement, and evidentiary standards. Disparate sensor systems and command and control platforms fragment situational awareness and slow response. Without national technical standards, shared certification programs, centralized threat intelligence, and regional coordination centers, decentralization risks producing a patchwork rather than a cohesive national enterprise.

Edwards is unequivocal. Establishing a usable common operating picture is “the single most critical problem to solve quickly.”

The Institutional Test

The small drone challenge is not solely about hardware or frequencies. It is about institutional coherence. Upstream supply chain friction reduces malicious opportunity. Layered defense reduces vulnerability and consequence. Universal identification reduces ambiguity. Interoperable systems reduce fragmentation. Coordinated governance reduces hesitation.

Drones will remain a permanent feature of airspace. The question is whether governance can evolve as quickly as technology. As this panel of experts makes clear, the path forward begins upstream, builds in layers, and succeeds only through disciplined coordination and a unified,

real time common operating picture.

Short Bios of Contributors

Austin Doctor, Ph.D., is the director of strategic initiatives at the National Counterterrorism Innovation, Technology, and Education (NCITE) Center, the Department of Homeland Security center of excellence for counterterrorism studies, and an associate professor in the School of Criminology and Criminal Justice at the University of Nebraska at Omaha. Doctor is a homeland security and homeland defense researcher with a focus on the study of emerging threats, domestic and international terrorism, irregular warfare, and violent non-state actors. You can find him on X at @austincdoctor.

COL(R) **Bill Edwards** is a thought leader and is currently the Director of C-UAS Operations and Training at ENSCO. Before this role, he was the owner of Phoenix 6 Consulting LLC. Most recently, he worked for Building Intelligence, Inc. as the firm's President, and before that was at Thornton Tomasetti, operating as a senior executive. Bill offers over 35 years of combined experience and expertise in operational, technical, and electronic security consulting, counter-terrorism, counter-intelligence, surveillance, and counter-surveillance efforts. Most recently, he has built and led a successful security consulting business group that provides expert advice in any vertical market as it applies to sUAS (drones) to include drone vulnerability and risk assessment, drone emergency response planning, cUAS and Law training, and Left of sUAS Launch planning. He also provides threat, vulnerability, and risk assessment (TVRA), electronic security system design (ESD), and security operations center design (SOC). He also provides a myriad of additional services that include Cybersecurity TVRA, electronic security audits, and red teaming. Additionally, he served as the Director of Intelligence for Theater Special Operations Command-North, which required extensive collaboration and partnering across the U.S. whole of government security enterprise.

Scott Parker is the Founder and Principal Consultant of Aerisq Solutions LLC, where he advises public and private sector leaders on managing cyber and physical risks posed by drones to critical infrastructure. He conducts aerial risk assessments, provides executive-level strategic guidance, and delivers workforce training on drone threat readiness. Previously, he served as Chief of UAS Security at the Cybersecurity and Infrastructure Security Agency, where he built and led the agency's first dedicated UAS Security Program and helped operationalize counter-UAS authorities nationwide. Scott is a retired U.S. Army senior enlisted leader with 27 years of service, including Special Operations, supporting global missions and national-level

security efforts.

DJ Smith has worked in the area of Covert Technical/Tactical Surveillance for over 30 years and served as a Senior Technical Surveillance Agent for the Virginia State Police. A few areas of specialty are Title III Intercepts, GPS Installs, Video-Audio Clarification, Technical Surveillance Counter Measures (TSCM), Mesh-Node Deployments, Surreptitious Lock Bypass &

Safe Penetration including GSA locks & containers, Technical Response to Hostage/Barricade Situations, Cellular Tracking and Geo-locating (DF), Covert Surreptitious Audio/Video deployments, and sUAS & Counter UAS deployment operations.

Orion Policy Institute (OPI) is an independent, non-profit, tax-exempt think tank focusing on a broad range of issues at the local, national, and global levels. OPI does not take institutional policy positions. Accordingly, all views, positions, and conclusions represented herein should be understood to be solely those of the author(s) and do not necessarily reflect the views of OPI.