ORION FORUM

The RF Perimeter Has Changed: Why Critical Infrastructure Needs Full-Spectrum RF Awareness and Clear Response Authority

OCTOBER 28, 2026

A quiet radio frequency (RF) display can conceal a dangerous gap in a security plan. An approaching drone may be communicating outside the frequencies being monitored, using a signal the equipment cannot classify, or operating without a conventional radio-control link at all. In each case, the absence of an alert can be mistaken for evidence that the airspace is clear. For critical infrastructure, that mistake can consume the time needed to protect personnel, preserve essential operations, and achieve Decision Advantage. That risk is increasingly difficult to dismiss as a problem limited to sophisticated state actors. Alternative communications methods, components, and configuration guidance are described in public documentation, online communities, and social media. A motivated individual does not have to invent a new technology; in many cases, the individual only has to discover that an alternative exists and learn from work already completed by others. Legacy RF detection concentrated on familiar drone bands therefore remains useful as a layer, but it is a poor foundation for a new protection program facing an adaptive threat. Critical infrastructure needs full-spectrum RF awareness, demonstrated performance, complementary sensing, and clearly established response authority.

The spectrum is moving. The 900 MHz, 2.4 GHz, and 5.8 GHz ranges remain important to drone communications. They should guide initial assessment without defining the outer boundary of RF awareness. The FCC ISM allocations describe particular frequency bands; they do not encompass every frequency a drone can technically use. Control, telemetry, and video

may also travel on different links, so observing one transmission does not necessarily reveal the complete communications architecture. Commercially available equipment already demonstrates how quickly assumptions can age. The RUSHFPV catalog advertises first-person-view video transmitters in ranges extending above 6 GHz and into the 7-8.5 GHz region. Those are advertised specifications, not proof of field performance, threat prevalence, or lawful U.S. operation. They nevertheless show that a permanent detection ceiling built around familiar commercial bands is difficult to defend. Militarnyi reporting in July 2026 described Russian Boomerang FPV drones using video links above 6 GHz and up to 7.2 GHz, providing an operational example of the same trend.

The change is not simply a march toward higher frequencies. Resilience can come from changing bands, using more than one band, altering the waveform within a familiar band, or transmitting in short bursts. ExpressLRS documentation, for example, describes Gemini Xrossband operating simultaneously in the 900 MHz and 2.4 GHz bands. A detector may therefore cover a frequency range and still fail to capture or classify relevant activity occurring within it. Full-spectrum awareness should mean effective observation and analysis across the spectrum justified by the threat assessment, with known limitations and a practical path for expansion. It should never become a marketing claim that one sensor sees every emission or every aircraft.

Public knowledge changes the threat calculation. Open technical information has lowered the barrier to adaptation. Product pages, instructional videos, public repositories, user forums, and social media communities can show a threat actor which alternatives exist, what hardware is available, and where to learn more. This does not make every viewer an engineer. Compatible equipment, practical skill, testing, and persistence still matter. The security implication is narrower and more important: organizations can no longer assume that useful technical knowledge remains confined to laboratories, defense programs, or highly trained specialists. That reality should change procurement. A detector can perform well against the familiar aircraft selected for a demonstration and still leave consequential gaps against plausible alternatives. Buyers should ask what happens when a signal falls outside the signature library, when the communications architecture changes, or when a transmission is brief enough to

occur while a scanning receiver is observing somewhere else. Publicly available knowledge should be used by operators to challenge vendor claims and test their own assumptions before an incident does it for them. The asymmetry is organizational as much as technical. A security program may take years to specify, purchase, install, and replace sensors. A public demonstration can expose a new communications option in an afternoon. Security leaders therefore need a recurring process for reviewing credible technical developments, testing relevant observations locally, and feeding the results back into purchasing decisions, operating procedures, and training.

Hardening changes both detection and mitigation. Drone hardening is not one technology. Different mechanisms create different defensive problems. Encryption protects the information carried by a radio link; it does not remove the RF energy used to transmit that information. Depending on the protocol and sensor, encryption can limit identification or interpretation without making the aircraft invisible to RF detection. Frequency hopping and other spread-spectrum techniques present a different challenge. Rohde & Schwarz technical guidance explains that rapid frequency changes and short transmissions can make interception more difficult and can produce missed detections if the receiver is not configured to capture the relevant activity. Mitigation introduces another dependency. A jammer must affect a connection or navigation function that the aircraft actually needs. Interrupting video may leave control intact. Disrupting a control link may trigger return-to-home, continued autonomous flight, or another programmed behavior rather than a safe landing. UK counter-drone guidance cautions that responses to jamming vary and that aircraft using cellular, satellite, autonomous, or other alternative methods may not behave as defenders expect. Fiber-optic control makes the limitation especially clear. The U.S. Army Center for Army Lessons Learned describes drones carrying command and video over fiber, avoiding the active RF control links on which many detectors and jammers depend. A wider receiver cannot recover a radio transmission that is not present. Autonomous aircraft can create a similar problem when they do not require continuous commands. These architectures do not make RF sensing irrelevant; they demonstrate why RF must be one layer in a broader detection architecture that also includes radar and electro-optical or infrared sensing. Expanding frequency coverage cannot restore an absent signal.

A substation shows why the distinction matters. An electrical substation provides a concrete homeland security example. In September 2025, the Department of Justice announced a guilty plea in a disrupted plot to attack a Nashville-area electrical substation with a drone carrying explosives. The defendant had said he preferred to build the drone himself to avoid law-enforcement detection. The case demonstrates malicious interest in using a drone against energy infrastructure; it does not establish that the planned aircraft used unusual frequencies or hardened communications. For a utility, the planning question is therefore not whether that specific plot used a nonstandard link. It is whether the protection program could recognize and assess a future aircraft whose communications differ from those used during equipment demonstrations. Consider an exercise in which a drone is observed near a substation while the RF picture is inconclusive. A transmission outside the monitored bands may provide no warning. An unfamiliar signal inside those bands may be captured without being recognized. A fiber-controlled or autonomous aircraft may appear only through another sensor. Each condition should trigger an understood assessment process rather than surprise. The utility should baseline its normal RF environment, coordinate authorized inspection flights, and ensure that RF observations can be correlated with radar, imagery, and reports from personnel. An unfamiliar signal alone should not trigger a shutdown. A credible concern may justify moving exposed workers, restricting access, preserving evidence, or coordinating with an authorized responder. Decisions affecting electrical operations should remain with the responsible operations authority. The protection plan must remain useful when identification is incomplete, mitigation is unavailable, or intervention could create additional hazards.

Authority must be decided before the aircraft arrives. This is where spectrum awareness and legal authority must be kept distinct. Technical coverage does not itself authorize interference with communications, takeover of an aircraft, or destructive action. The July 2026 SAFER SKIES implementing regulations establish a framework for eligible state, local, tribal, and territorial law-enforcement and correctional agencies to conduct detection, warning, and mitigation under specified conditions. The Federal Register rule establishes separate Detection and Warning and Mitigation certification structures, while the current regulations prohibit transferring mitigation authority to private contractors. Contractors may provide technical support and certain detection services, but they may not make credible-threat determinations

or execute mitigation actions that require the Act's authority. Critical infrastructure ownership therefore does not confer a general right to jam or seize control of a drone. Utility leaders and public partners should determine before an incident who may collect what information, how alerts will be shared, which agency can make a credible-threat determination, and who can authorize each protective or mitigation action. A drone will not wait for an improvised approval chain. The purpose of planning is not to accelerate every response; it is to resolve authority in advance so the organization can act proportionately while options still exist.

Acquisition should measure warning, not marketing. Procurement should translate these lessons into measurable requirements. A broad tuning range describes where a receiver can operate; it does not establish how much spectrum the system observes simultaneously, how quickly it revisits a channel, or how well it performs amid local interference. The Congressional Budget Office notes that ambient RF activity can shorten detection range and warning time and that RF systems must be adjusted as the electromagnetic environment and drone signals change. Its July 2026 analysis also emphasizes that counter-UAS defenses require continuing hardware and software adaptation as the threat evolves. That distinction matters when vendors use the phrase full spectrum. The requirement may be met by a coordinated set of receivers and analysis tools rather than one device. What matters is demonstrated coverage against the mission threat, the time needed to capture and characterize relevant signals, and the ability to correlate RF observations with independent sensors. Architecture should follow the operational requirement, not a label on a product sheet. Buyers should therefore test representative interference, multiple simultaneous signals, unfamiliar emissions, and the actual configuration intended for use. A clean demonstration range cannot prove performance beside an operating substation, airport, plant, or other complex facility. Tests should distinguish detecting energy from classifying a drone signal, locating an emitter, associating that emitter with an aircraft, and producing a warning that supports a decision. Confidence should remain visible. A bearing toward an emitter is not the same as a verified aircraft position, and a precise-looking symbol should not create false certainty. The acquisition decision should also fund what happens after installation. Antennas and receiver hardware must physically support the required frequencies; software cannot overcome those limits. Signature updates, analysis tools, maintenance, integration, operator proficiency, and

recurring exercises all belong in the total cost of capability/ownership. Vendors should be required to support integration into a common operating picture rather than creating another isolated display. Exercises should include an unfamiliar emission that must be assessed and an aircraft track that produces no RF alert. Both reveal whether the organization can retain useful protective options when its preferred sensor does not supply certainty. Within 3D Physical Security™, Ground, Cyber, and Aerial information should contribute to a common operating picture with Decision Advantage at the center. The responsible person must understand the situation, possess the necessary authority, have viable options, and execute while those options still matter. A 90-second decision window can be used as an exercise challenge, not as a promised warning time. Actual time depends on aircraft movement, sensor performance, site conditions, and the protective action required.

The RF perimeter will continue changing as drone developers diversify communications and reduce dependence on vulnerable links. Critical infrastructure security must change with it. A protection program built around familiar bands, familiar signatures, and familiar aircraft can be overtaken by knowledge circulating in public. Leaders should demand adaptable spectrum coverage, demonstrated performance against realistic signals and hardened architectures, complementary sensing, and lawful response arrangements that have been exercised. The standard is not whether a sensor detected yesterday's drone. It is whether the protection program can keep pace with what a motivated actor can learn and obtain, giving responders enough time to protect people and preserve essential services.

COL (R) Bill Edwards is an Iraq War veteran, owner of Phoenix 6 Consulting LLC, and author of The Perimeter Has Changed: Building and Leading the 3D Physical Security™ Enterprise.

Disclaimer: *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.*