WINNING THE COUNTER-UAS DETECTION BATTLE: ADVANCED SDR SOLUTIONS FOR EVOLVING DRONE THREATS

Introduction

The proliferation of small, low-cost uncrewed aerial systems (UASs) has transformed the threat landscape for military and civilian infrastructure worldwide. From the lessons learned in Ukraine to emerging threats at critical facilities like airports, the challenge of detecting and neutralizing small drones operating in complex RF environments has become increasingly complex. Unlike traditional air-defense systems designed for larger aircraft, counter-UAS (C-UAS) operations require sophisticated RF detection capabilities that can identify "needles in a haystack" or individual threatening drones amid dense civilian RF backgrounds cluttered with Wi-Fi access points, cellphones, and broadcast towers.

The evolving nature of drone technology presents a dynamic "cat and mouse" game where adversaries continuously adapt their communication methods, waveforms, and frequency bands. Today's threats range from consumer drones using Wi-Fi and proprietary protocols to advanced systems employing cellular communications that are markedly harder to detect and counter. This technological evolution demands C-UAS systems that can rapidly adapt to new threats while maintaining effectiveness across diverse deployment scenarios.

This whitepaper examines how software-defined radio (SDR) technology enables spectrum dominance in C-UAS operations and how new applications—from 2-watt ultra-compact systems to 8-channel rackmount platforms—provide the technological foundation for next-generation C-UAS capabilities.

The Drone Threat Paradigm

Imagine a forward operating base in eastern Ukraine that faces nightly incursions from small autonomous quadcopters approaching at treetop level, seeking gaps in defenses or conducting reconnaissance for artillery strikes. Traditional air-defense radars designed to track fighter jets cannot reliably detect these smaller-scale threats. The base's survival depends on RF detection systems identifying faint command-and-control signals linking drone to operator.

U.S. Army Photo of the Mobile-Low, slow, small-unmanned aircraft Integrated Defeat System(M-LIDS) by Capt. Austin May.

The threat extends beyond battlefields: Airports halt operations when drones penetrate controlled airspace, military bases report frequent incursions, and critical infrastructure faces potential surveillance or attack. Traditional air-defense radars struggle with small drones hovering at low altitudes—the smaller crafts' minimal radar cross-sections, low speeds, and extremely low flight profiles confound conventional detection. Employing expensive interceptors against inexpensive drones represents an unsustainable defense posture.

Crowded RF Environment

Those tasked with countering ever-evolving drone threats must rely on a myriad of countermeasures, some old, some new, and some not yet invented. Complicating this countermeasure effort is a crowded RF environment. A forward operating base surrounded by a civilian town faces thousands of legitimate RF emitters: Wi-Fi routers, cellular base stations, Bluetooth devices—all transmitting across the same frequency bands used by UASs, both friendly and not. Identifying a single hostile drone's RF signature amid this cacophony requires sophisticated signal processing and the ability to determine where threats originate.

Consumer drones traditionally used Wi-Fi chipsets below 6 GHz, but this landscape is changing rapidly. Today's systems employ frequency-hopping spread spectrum, LTE [Long-Term Evolution] cellular networks for

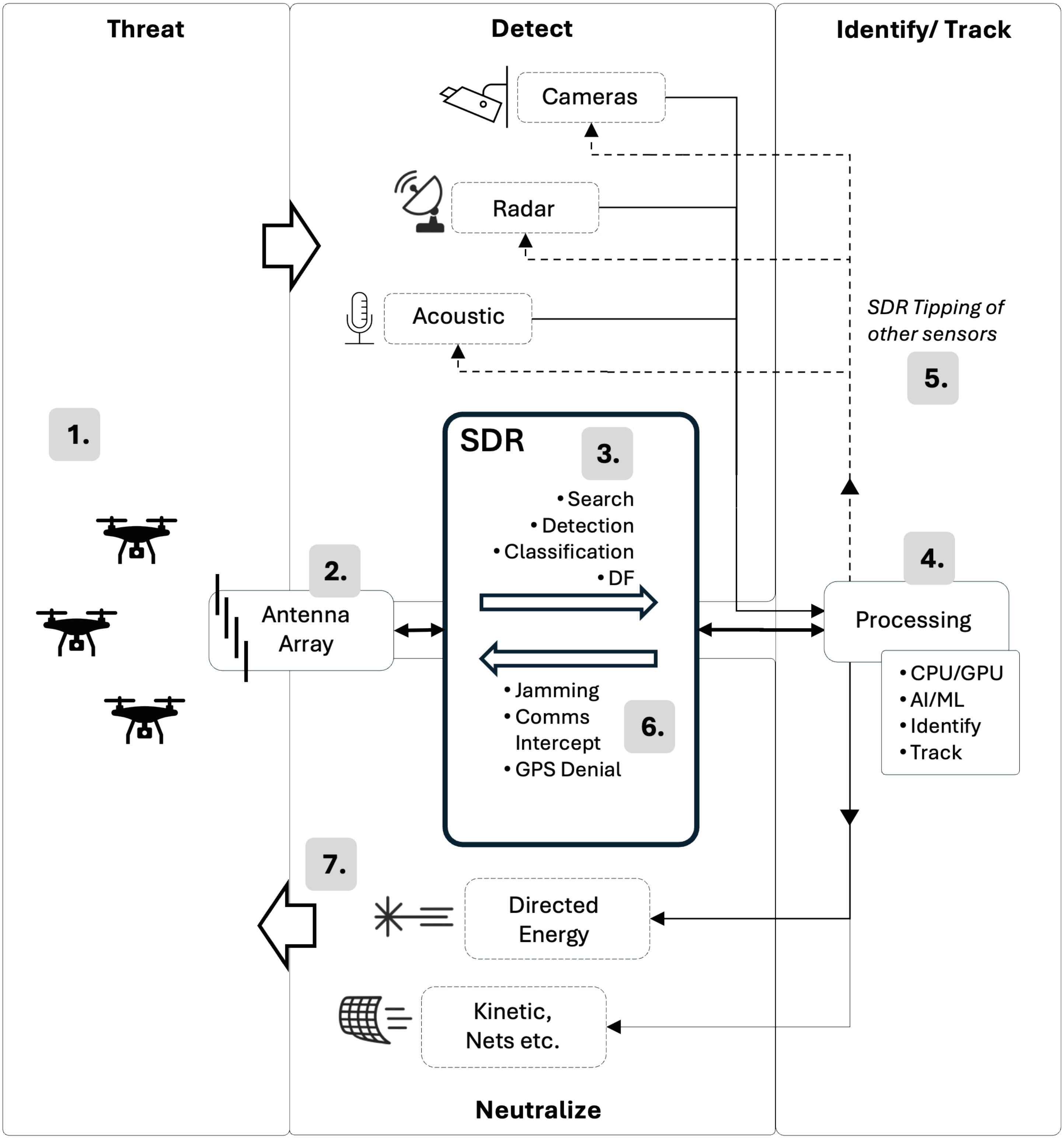


Figure 1: Illustration of core C-UAS system functions, from multi-sensor search and detection through SDR-based signal processing and final neutralization effects such as jamming, GPS denial, and directed energy.

command and control, or newer bands where detection capabilities remain less mature. Cellular-connected drones may well represent the most troublesome form factor: communicating through standard LTE networks, they appear as ordinary cellphones. Distinguishing drone connections from thousands of legitimate devices requires analysis of subtle patterns—handoff frequencies, data-transmission characteristics, movement patterns, and the like.

In such cases, direction-finding and geolocation capabilities become critical. Phase-coherent RF reception across multiple channels enables angle-of-arrival estimation and RF geolocation—core C-UAS functions answering not just “Is there a threat?” but “Where is it coming from?”

Multimodal C-UAS Approach

The answers to each question lay on different levels of response. Effective C-UAS operations must employ layered detection strategies that fuse multiple sensor modalities such as determining if a threat exists then tracking it back to its source. RF detection serves as the primary long-range sensor, capable of detecting drone command-and-control links at extended distances. Phase-coherent multichannel SDRs enable direction-finding and beamforming, pinpointing threat locations. When RF systems identify potential threats, complementary sensors provide confirmation: radar tracks movement and determines precise position, velocity, and altitude; cameras enable visual identification; while acoustic sensors detect characteristic motor signatures.

The C-UAS response process progresses through distinct phases. During detection, RF sensors scan assigned frequency bands for drone-characteristic signals. Machine-learning (ML) algorithms classify detected signals, distinguishing drone communications from background noise. Multichannel phase-coherent reception determines bearing to targets. In this way, when potential threats emerge, sensor fusion builds comprehensive threat pictures feeding operators making engagement decisions.

Threat neutralization methods vary, based on the tactical situation. RF jamming disrupts command-and-control links, forcing autonomous drones to execute preprogrammed behaviors—often returning to launch points or landing immediately. Directed-energy weapons physically disable drones, while kinetic effectors range from specialized projectiles to net-launching systems. Advanced approaches can involve communications takeover, where C-UAS systems exploit vulnerabilities to assume command of hostile platforms—an application requiring both receive and transmit capabilities.

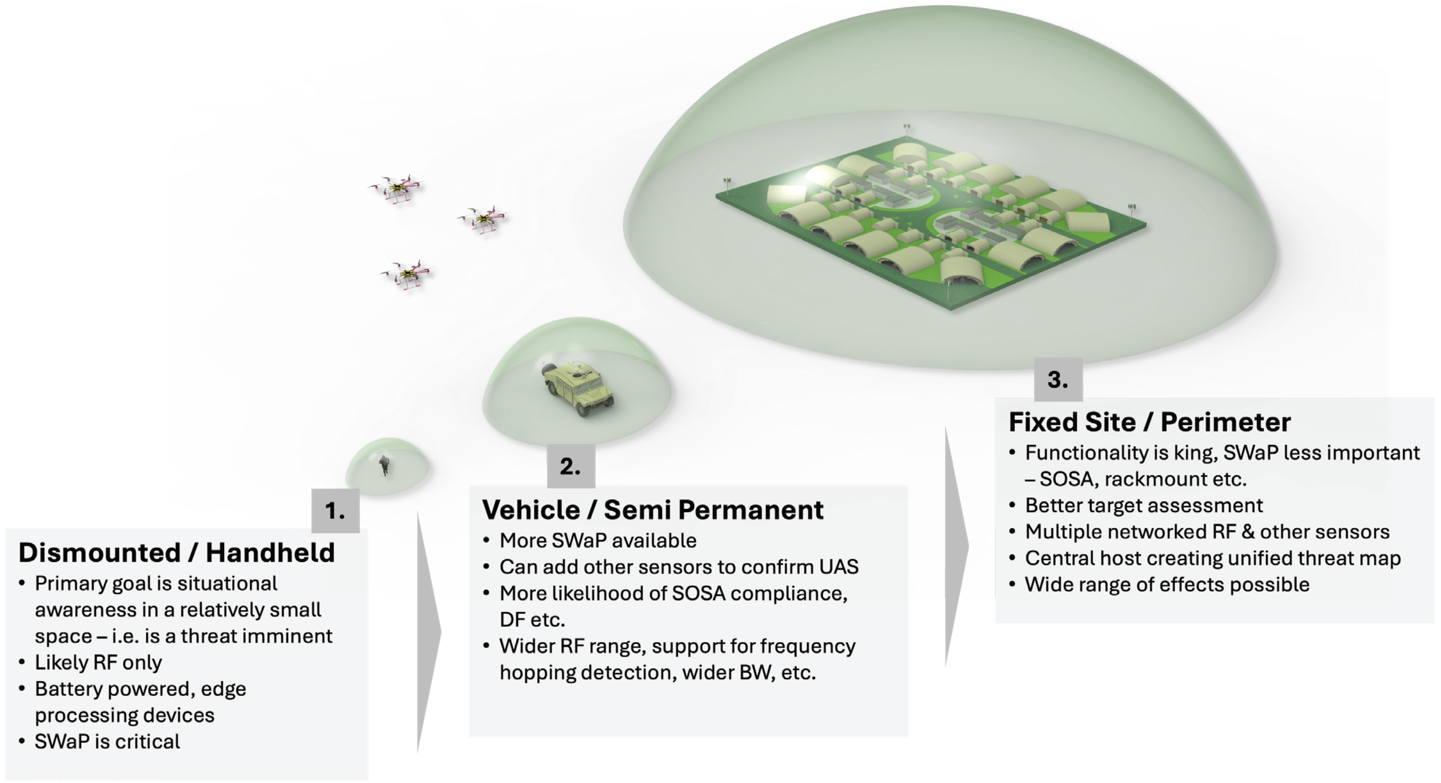
Countering a Diversified and Complex Threat

While multiple levels of C-UAS systems are being deployed, the diversity of drone platforms and communication methods creates sizable problems for designers of counter-drone systems. Manufacturers from numerous countries produce thousands of drone models, with each potentially using different communications protocols, frequency bands, and control mechanisms. Moreover, consumer drones from major manufacturers use multiple proprietary communication standards that have evolved across product generations.

This jumble of platforms and communications protocols creates a perpetual cat-and-mouse game wherein C-UAS technologies must continuously adapt. When systems become effective at detecting and jamming traditional frequency-band drones, adversaries shift to alternatives. Each adaptation then requires C-UAS systems to expand frequency coverage, implement new signal-processing algorithms, and update threat libraries—all while maintaining effectiveness against legacy threats.

The emergence of cellular command-and-control links represents a particularly difficult evolution. LTE networks use sophisticated frequency-hopping and handoff mechanisms; detecting these connections requires monitoring multiple LTE bands simultaneously across wide geographic areas, then applying advanced analytics to distinguish drone traffic patterns from normal cellular activity. Newly adopted frequency bands compound the detection barrier as drone manufacturers adopt communications methods outside traditional ISM bands.

Environmental factors can intensify these problems. Urban environments create multipath propagation where RF signals bounce off buildings, complicating direction-finding, while terrain features can attenuate signals and create detection shadows. Electromagnetic interference from power lines, industrial equipment, or other military systems can also mask drone signatures or trigger false alarms.



1.

Dismounted / Handheld

- Primary goal is situational awareness in a relatively small space – i.e. is a threat imminent
- Likely RF only
- Battery powered, edge processing devices
- SWaP is critical

2.

Vehicle / Semi Permanent

- More SWaP available
- Can add other sensors to confirm UAS
- More likelihood of SOSA compliance, DF etc.
- Wider RF range, support for frequency hopping detection, wider BW, etc.

3.

Fixed Site / Perimeter

- Functionality is king, SWaP less important – SOSA, rackmount etc.
- Better target assessment
- Multiple networked RF & other sensors
- Central host creating unified threat map
- Wide range of effects possible

Figure 2: A diagram of typical C-UAS system characteristics by deployment type, highlighting how priorities shift from SWaP-constrained handheld solutions to feature-rich fixed-site systems with multiple networked sensors.

Software-Defined Radio Solutions for C-UAS

One way to overcome these roadblocks is to leverage software-defined radio (SDR) technology as the architectural foundation for adaptable C-UAS systems. Unlike fixed-function receivers, SDRs employ programmable hardware that is reconfigurable through software updates. When new drone protocols emerge, SDR systems can deploy updated software in weeks rather than years. As threats shift frequency bands, systems retune without hardware modifications, a move that directly addresses the rapid evolution of UASs.

SDRs provide multichannel, wide-bandwidth capabilities for comprehensive spectrum monitoring. Systems simultaneously monitor multiple frequency bands to detect frequency-hopping drones. Multichannel phase-coherent reception enables direction-finding through angle-of-arrival estimation, which enables location of threats in what can be a complex electromagnetic environment.

Edge processing enables real-time threat classification at the sensor level. Edge SDRs implement artificial intelligence (AI) algorithms locally, analyzing signals and classifying targets rapidly. For dismounted and vehicle-based applications where bandwidth is limited and response time is critical, accessible CPU and GPU [central processing unit and graphics processing unit] resources can transform the effectiveness of these tools.

Epiq Solutions' C-UAS Technology Portfolio

Engineers at Epiq Solutions bring a suite of comprehensive SDR solutions for counter-UAS operations. They span the complete spectrum of C-UAS deployment scenarios, from dismounted operations to fixed-site perimeter defense. Recent additions to this portfolio include the Matchstiq™ Z4 and Matchstiq™ V40 platforms, which further extend coverage for dismounted and vehicle-mounted C-UAS missions.

Small-Form-Factor for Dismounted Operations

For soldiers and other dismounted operators, the Matchstiq™ Z Series provides handheld SDR options that keep detection equipment within strict SWaP constraints. The *Matchstiq Z2*, for example, consumes only about 2 W of power while providing signal-detection capabilities up to 6 GHz with roughly 50 MHz of instantaneous bandwidth and ~60 dB SFDR, enabling extended battery-powered patrols without sacrificing sensitivity.

The new *Matchstiq Z4* builds on this form factor by adding additional phase-coherent channels suitable for direction finding along with hibernation and low-power semi-sleep modes, making it well-suited to “always-on” surveillance missions that need DF capability at the edge in exchange for slightly higher SWaP.

Matchstiq™ Z4 4-channel 6 GHz SDR with low power wake-up modes

Z-series handhelds measure only a few inches on a side, weigh well under half a pound, and can magnetically mount to a smartphone or other portable host, drawing power and data over a single USB-C connection.

Platform SDRs for Vehicle-Mounted Systems

For vehicle-mounted C-UAS systems, designers need multichannel coverage, wide bandwidth, and enough on-board compute to run DF and classification at the edge. The *Sidekiq™ NV800* provides eight receive channels with 50 MHz of instantaneous bandwidth, consuming roughly 25 W while delivering about 75 dB SFDR, giving vehicle platforms the multichannel RF front end needed to track multiple simultaneous threats.

Sidekiq™ NV800 8-channel fast scanning/ coherent SDR is ideal for search & DF applications

Epiq’s new flagship vehicle platform, the *Matchstiq™ V40*, builds on this architecture by combining a processing design – that leverages ADI’s Apollo wideband mixed-signal front-end platform and AMD’s Versal system-on-chip (SoC) – with approximately 2 GHz of instantaneous bandwidth and RF coverage out to roughly 9 GHz. With Versal SoC processing and high-performance on-board compute resources, the Matchstiq™ V40 enables DF, geolocation, and ML-based signal classification to run directly on the platform at the RF edge. This reduces data backhaul requirements and accelerates engagement decisions for vehicle-mounted and UxS payload C-UAS systems. Optimized for SWaP, the V40 is tailored for vehicle-mounted and UxS payload applications that need to detect both traditional sub-6 GHz control links and higher-frequency UAS waveforms within a compact, deployment-ready form factor.

Matchstiq™ V40 9 GHz direct sampling SDR with up to 2 GHz of bandwidth and integrated DDC/DUCs

SOSA Aligned VPX for Modular Integration

For applications that require a fully integrated 3U VPX RF card rather than a mezzanine-module approach, the *Sidekiq™ VPX400* offers four receive and four transmit channels with up to 450 MHz of instantaneous bandwidth in a SOSA aligned 3U VPX form factor, typically consuming under 40 W. Phase-coherent operation across its channels supports sophisticated direction-finding, while SOSA/CMOSS alignment enables rapid integration into open-architecture EW and SIGINT platforms, substantially reducing deployment timelines and ensuring interoperability.

Sidekiq™ VPX400 SOSA-aligned 6 GHz SDR card with independent and coherent receive and transmit channels (4 + 4)

Rackmount Systems for Fixed-Site Operations

The *NDR358* delivers eight receive channels with 80 MHz instantaneous bandwidth and 90 dB SFDR while Epiq's *NDR818* provides eight channels with 40 MHz bandwidth and 90 dB SFDR. Multiple networked sensors create comprehensive perimeter coverage, with centralized processing fusing data for unified threat maps and integration with jamming systems, directed energy weapons, and kinetic countermeasures.

Future C-UAS Technology Trends

The drone threat is only going to increase in capability and complexity. Emerging communication methods include satellite-based command links, mesh networking between drone swarms, and AI-enabled autonomous operations minimizing RF signatures. Future drones may employ cognitive radio techniques, dynamically selecting frequencies and waveforms to evade detection.
AI will play increasingly critical roles: AI-enabled C-UAS systems will autonomously detect novel drone signatures, predict threat behaviors, and coordinate responses across multiple effectors without human intervention. ML algorithms will continuously improve classification accuracy by learning from operational data, adapting to new threats as they emerge.

Integration with broader electronic warfare (EW) architectures, while complex, can also present opportunities. C-UAS sensors contribute to comprehensive electromagnetic battlespace awareness, while EW systems provide additional countermeasure options. Standards like the SOSA Technical Standard enable interoperability, enabling C-UAS capabilities to integrate seamlessly with existing military systems and accelerating deployment of next-generation technologies as threats evolve.

Conclusion

Small UAS platforms have fundamentally transformed the threat landscape, creating situations that traditional air-defense systems cannot address effectively. The technical complexity of detecting individual threatening drones amid dense civilian RF environments, combined with rapid evolution of drone-communication technologies, demands flexible software-defined approaches that adapt as threats evolve.

Software-defined radio technology provides the architectural foundation for meeting these challenges. SDR's inherent flexibility enables rapid adaptation through software updates, while their multichannel, wide-bandwidth capabilities ensure comprehensive spectrum coverage. In addition, phase-coherent multichannel operation enables critical direction-finding capabilities. Edge processing with accessible CPU and GPU resources delivers real-time AI-powered threat classification essential for tactical operations.

Epiq Solutions' comprehensive SDR portfolio—spanning ultra-small-form-factor edge devices operating at 2 W to high-performance rackmounted systems with 8-channel coherent reception—enables spectrum dominance across the complete range of C-UAS deployments. Moreover, SOSA alignment accelerates integration and deployment while ensuring interoperability with the modular open system approach (MOSA). As drone threats continue to evolve, Epiq's technology foundation provides the adaptability, performance, and scalability essential for maintaining overmatch in the ongoing technological competition.

ABOUT EPIQ

Epiq Solutions develops cutting edge tools for engineering teams and government-focused organizations requiring situational awareness and detailed insight into their RF environments in order to identify and act against wireless threats.

www.epiqsolutions.com
sales@epiqSolutions.com
+1 847 598 0218

3740 Industrial Ave,
Rolling Meadows, IL 60008, USA
© 6th December, 2025

EPIQ