

EXPERT PAPER



MAXIMIZING MILITARY EFFICIENCY IN DRONE DEFENSE

Effective sUAS defense relies on high-precision RF direction finding and powerful multi-band effectors.

ROHDE & SCHWARZ

Make ideas real



EXECUTIVE SUMMARY

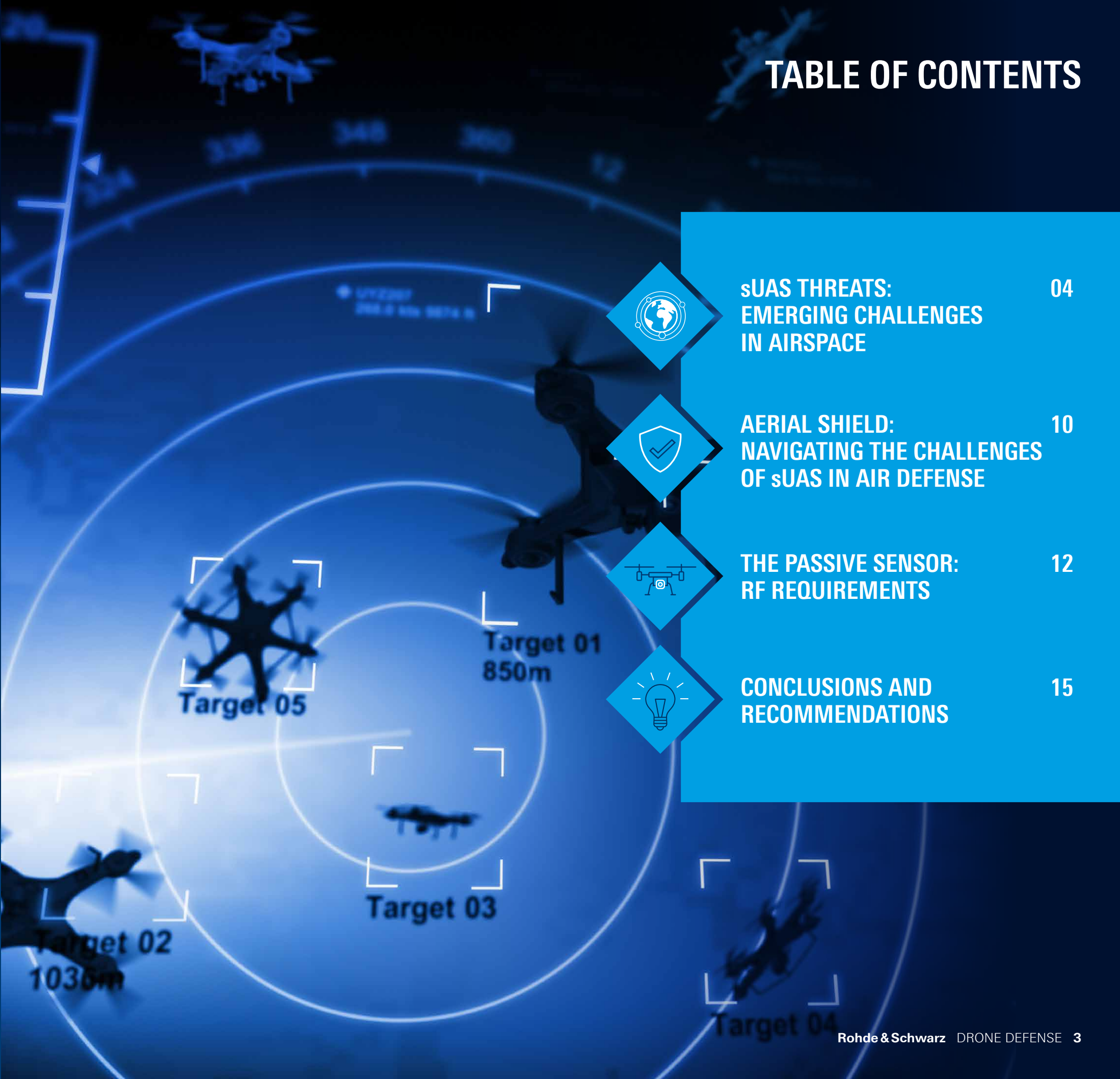
FORTIFYING sUAS DEFENSE WITH RF PRECISION

The strategic importance of sUAS defense
Small uncrewed aerial systems (sUAS) have transformed tactics on the modern battlefield, not only in intelligence, reconnaissance and surveillance (ISR) operations, but also in direct offensive or defensive missions. These systems operate across multiple levels and present a significant challenge to traditional defenses. As the role of sUAS continues to evolve in modern warfare, defense systems must adapt to counter these emerging threats. This adaptation often requires the integration of advanced technologies that are resilient against changes in the fast evolving world of UAS and provide universal capabilities when it comes to the radio spectrum, such as radio frequency (RF) direction finding, which provides the precise detection and tracking capabilities critical for the situational awareness needed to mount an effective defense.

The power of passive location solutions
Passive RF-based solutions are not only effective but invisible in the radio spectrum and to electromagnetic warfare systems and can be operated without exposing the sensor location. From reconnaissance missions to strike operations, each drone mission and type poses unique challenges that must be addressed through precise classification and tailored countermeasures. By leveraging sophisticated signal processing and real-time data analysis, these passive RF solutions enable commanders to respond swiftly to potential threats without revealing the location of their monitoring assets. This capability is crucial to the development of **multi-layered defense systems** that can meet the demands of today's evolving threat landscape marked by the increasing prevalence and sophistication of small uncrewed aerial systems.

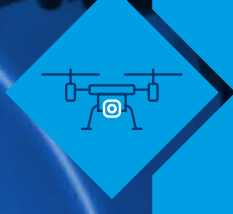
Defending against small uncrewed aerial systems (sUAS) in modern warfare requires advanced technologies like radio frequency (RF) solutions for effective drone detection and initiation of countermeasures. By utilizing sophisticated signal processing and real-time data analysis, military organizations can enhance situational awareness and develop robust multi-layered defense.

TABLE OF CONTENTS



	sUAS THREATS: EMERGING CHALLENGES IN AIRSPACE	04
---	--	-----------

	AERIAL SHIELD: NAVIGATING THE CHALLENGES OF sUAS IN AIR DEFENSE	10
---	--	-----------

	THE PASSIVE SENSOR: RF REQUIREMENTS	12
---	--	-----------

	CONCLUSIONS AND RECOMMENDATIONS	15
---	--	-----------

sUAS THREATS: EMERGING CHALLENGES IN AIRSPACE



TRUE SPECTRUM DOMINANCE: A CRITICAL KEY FACTOR FOR SUCCESS

The increasing threat posed by malicious non-compliant, and non-cooperative sUAS in military scenarios necessitates a comprehensive understanding of their technical and operational parameters. With over 3,000 drone attacks occurring worldwide daily and the intensifying saturation of the electromagnetic spectrum (EMS) caused by RF drones, attaining **true spectrum dominance** is paramount for ensuring robust airspace security and electromagnetic superiority. Effective EMS management and control are critical because they enable military forces to respond to the diverse threat vectors associated with sUAS.

The primary sUAS threat vectors can be categorized into three key areas:

- **Physical threats:** sUAS can serve as delivery systems for explosives or hazardous materials, causing physical harm or damage, as evidenced by their use as 'flying bombs'. Additionally, they can represent an indirect threat as intelligence, surveillance, and reconnaissance (ISR) platforms used for target acquisition and tracking.
- **Harassment and attrition warfare:** sUAS can be employed to deplete adversary resources and provoke costly defensive responses, thereby weakening the opponent without direct military engagement.
- **Psychological effects and propaganda:** sUAS can instill fear and uncertainty among military personnel and be used for psychological operations (PSYOPS) to disseminate targeted misinformation that undermines morale and operational effectiveness.

ESSENTIAL STRATEGIES FOR EFFECTIVE UAS PROTECTION

Countering UAS threats rests on two indispensable pillars: **precise classification and in-depth technical and operational expertise.**

Precise classification enables comprehensive understanding of UAS-specific characteristics, allowing military forces to identify and effectively respond to physical threats, novel tactics and drone based psychological operations. The system employed must be designed to be adaptable, enabling operators to account for changes in UAS communication parameters.

Technical expertise reveals potential attack scenarios, so that emerging challenges can be met with proactive countermeasures. As the threat from sUAS in military operations grows, achieving true spectrum dominance becomes ever more essential for safeguarding airspace. By developing robust defense strategies and innovative surveillance technologies, military forces can combat these threats with precision.

Achieving true spectrum dominance is essential in all military scenarios. It is fundamental to countering the growing threat of sUAS in military operations and enables effective adaptive defense strategies. Such dominance relies on comprehensive situational awareness resulting from integrated advanced surveillance technologies.

THE ROLE AND RISKS OF sUAS IN MILITARY OPERATIONS



To counter the growing threat of sUAS, an in-depth understanding of the tactics, techniques and procedures of sUAS operations and the connected risks and possible countermeasures is necessary.



In **close-combat scenarios**, sUAS can deliver payloads such as explosives directly to opposing positions. This capability is enhanced by a permanent control link, which allows for real-time command and adjustments during missions, while GNSS signals can optionally be used for navigation. Additionally, a permanent video downlink enables continuous tracking and positive target identification, enhancing strike effectiveness.

Given the increasing availability of commercial drones and components, understanding their implications in military

contexts is crucial. Their widespread accessibility elevates the threat they pose, since they can be easily acquired and operated by both state and non-state actors for a comparatively modest investment. Once equipped for precise strikes, these drones pose a significant danger in the hands of adversaries because they enable precisely targeted attacks with minimal risk.



TRANSITION TO ISR MISSIONS

sUAS play a vital role in providing eyes in the sky for real-time battlespace awareness, aiding in rapid target acquisition and battle damage assessment. Specifically designed for **intelligence, surveillance and reconnaissance (ISR)** missions, these drones enhance battlefield situational awareness by operating at higher altitudes—up to 6,500 meters with a range of approximately 50 kilometers. They are typically controlled via uplink communication, which allows operators to direct their flight path and adjust missions in real-time.

While GNSS signals are often used for navigation, onboard navigation through image analysis can also be employed, providing flexibility in environments where GPS signals may be unreliable or jammed. Additionally, ISR drones enable live monitoring via video downlink, enabling real-time intelligence sharing with command centers.

Drones can also act as repeaters to enhance both uplink and downlink communication, ensuring robust connectivity and data transmission integrity. This capability allows sUAS used for ISR missions to provide timely and accurate information, enabling commanders to make informed decisions and effectively coordinate actions in the battlespace.



THE COMPLEXITY OF AUTONOMOUS OPERATIONS

Given the operational capabilities of sUAS, it is also important to examine the complexities introduced by **autonomous operations**, which significantly alter the threat landscape. Operating on pre-programmed paths with minimal human supervision, autonomous systems can precisely target critical infrastructure and command centers. They often utilize GNSS or inertial sensors for autonomous flight and accurate navigation even in challenging environments. While these systems may include an optional control or telemetry link (such as 4G), they typically do not send signals in mid-flight, relying instead on short data bursts for target confirmation. They operate discreetly, often utilizing passive communication methods, which makes them difficult to detect and intercept. By minimizing acoustic signatures and employing low-probability-of-detection communication techniques, these systems complicate attempts of adversaries to defeat them and present a serious challenge to defense forces charged with protecting vital assets.



THERE ISN'T A SIMPLE, DIRECT ANSWER FOR CATEGORIZING THREATS POSED BY SMALL UAS, AS THESE THREATS ARE COMPLEX AND CAN VARY SIGNIFICANTLY DEPENDING ON THE SPECIFIC UNITS INVOLVED.



COUNTERMEASURES:
THE POWER OF JAMMING
AND SPOOFING IN COUNTER-
UAS OPERATIONS

To effectively counter evolving sUAS threats, knowledge of jamming and spoofing in counter-drone operations is indispensable. These tactics are critical countermeasures against sUAS operations aimed at disrupting adversarial capabilities. Jamming involves intentional interference with communication signals, effectively denying control links and navigation systems, such as GNSS, to disrupt the hostile drone operations. When successful, drone operators lose control and communication with their aircraft, making it difficult or impossible for opposing forces to execute their missions.

Effective jamming of sUAS in military scenarios requires wideband jamming equipment that is not limited to typical ISM bands. Non-reactive jamming can be effective in point protection use cases where specific areas or assets need to be safeguarded without the need for an immediate response to detected threats. For area protection, however, a reactive jamming approach is typically required that provides sufficient jamming range while avoiding disruption of friendly operations and allowing for a more dynamic response to threats as they arise.

Spoofing is another drone defense tactic that is becoming increasingly important. It involves deceiving a system by sending false signals to mislead a drone into incorrectly determining its location or receiving commands from an adversary disguised as those coming from a legitimate source. Both tactics are vital in modern military operations and enhance drone defense through asset protection and maintaining airspace security. By undermining the effectiveness of sUAS, they ensure that friendly systems can operate in a protected environment.



ASSESSING THE RISKS:
HOW sUAS CLASSIFICATION
SHAPES MILITARY
STRATEGY

To fully understand the threats posed by sUAS mentioned above it is useful to consider them in terms of categories based on operational threat levels and environment. Fixed assets are at greater risk due to their vulnerability to sophisticated engagements planned over extended periods, while forward-deployed units face a similar threat landscape but grapple with limitations in sensor availability and defensive capabilities.

To mitigate these challenges, analysis of the specific risks and selection of counter-UAS measures are essential for protecting military operations from both commercial and military drones across various environments. These risk assessments are critical for enabling the safety of operating bases, airfields, port facilities and ground forces.

Understanding the specific assets at risk is a vital aspect of selecting effective countermeasures. Categorizing based on their operational risk and vulnerability can help determine which assets are most vulnerable to which risks.

sUAS can deliver payloads and conduct surveillance with low risk to the pilot and their increased use in military operations presents significant challenges both directly and indirectly. Effective countermeasures such as jamming and spoofing are essential for disrupting adversarial drone operations and maintaining airspace security, while a structured, multi-layered monitoring strategy is necessary to protect military assets against evolving sUAS based threats.

Categorization of military assets under threat

Asset type	Location	Description	Risk level
Fixed/semi-fixed	Forward deployed	Assets such as permanent installations or semi-permanent forward operating bases (FOBs)	High risk; susceptible to engagements
	Rear elements	Fixed or semi-fixed installations located further from the front-line, such as command centers or bases	Moderate risk; susceptible to engagements
Mounted/mobile	Forward deployed	Mobile units or vehicles directly on the front lines, such as tactical vehicles or forward-deployed weapon systems	Moderate to high risk; vulnerability to direct strikes
	Rear elements	Mobile units stationed farther from the front but still in the operational area	Lower risk than forward deployed
Dismounted personnel	Forward deployed	Personnel or small units at the forward edge of the battle area	High risk; exposed to direct engagement with limited protection
	Rear elements	Personnel or units positioned further from the frontline but still within range of threats	Lower risk; more time to react, but still vulnerable to targeted engagements

Tailored defense measures against sUAS threats

Effective defense against sUAS threats requires a comprehensive approach to categorizing drone threats and implementing tailored defensive measures, with an emphasis on early detection and adaptability, as outlined in the following table:

Elements of defense measures	Description	Defense measures
UAS classification	Categorize UAS based on type, size, range, control method and mission objective	Tailored comprehensive approach based on UAS classification, enabling precise tactical responses
Covert operations	Forward-deployed units exposed to detection risk due to the use of active sensors, which can be tracked	Passive detection systems to monitor threats without revealing positions
Protection for mobile units	Mobile units and temporary positions are typically farther from the front line and can use active sensors without concern for revealing their position	Active Sensors to detect potential threats early and at long range. Effectors (e.g. jammers, weapon systems) for self-protection and close area protection
Tactics, techniques and procedures	Analyzing and adapting existing UAS defense technologies and strategies to meet evolving threats	Continuous review of current systems and flexible adaptation to new UAS threat types

AERIAL SHIELD: NAVIGATING THE CHALLENGES OF sUAS IN AIR DEFENSE

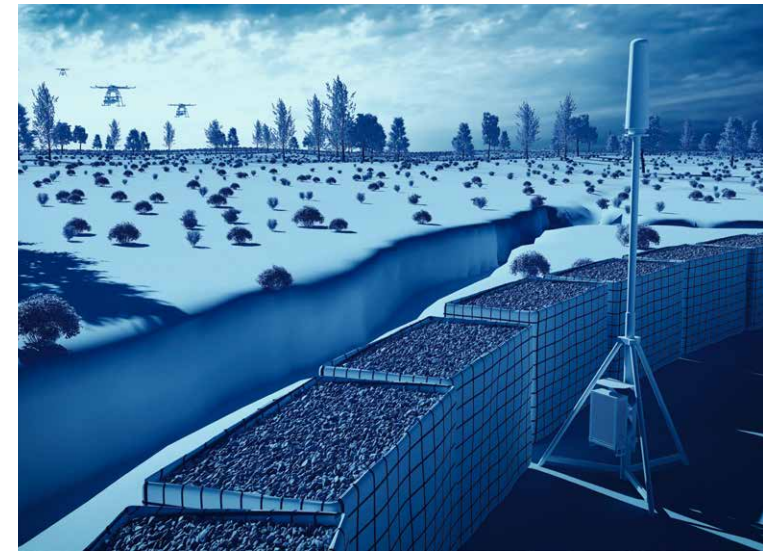


To protect forces, defense systems must ensure broad area coverage while safeguarding specific assets. Ground based air defense (GBAD) units neutralize threats with a so-called kill chain consisting of the following steps: detect, track, identify, decide, counter and assess.

Counter-drone solutions must be easily adaptable to the evolving landscape of sUAS technology. They must be rapidly deployable and mobile, ensuring operational readiness when integrated into ground-based air defense systems. Crucially, they must be able to refine detection and identification capabilities to continually evolving threats, particularly those to users in critical operations.



Comprehensive sUAS monitoring requires adaptive coverage. Using a combination of area protection and point protection strategies, defense systems can effectively safeguard assets and ensure timely responses to potential threats.



COMPREHENSIVE sUAS MONITORING: COVERAGE AND PROTECTION STRATEGIES

sUAS monitoring tactics focus on comprehensive detection, tracking and identification across all scenarios. Passive close-range detection and passive long-range solutions must be combined with stationary active detection systems that use radar, for instance. This multilayered approach provides comprehensive situational awareness. In real scenarios, certain detection systems focus on sUAS within close range of key assets, while additional passive sensors are used for area protection against threats to maximize response time.

This protection strategy adapts different combinations of sUAS defense systems to different scenarios. Area protection of e.g. mobile and specialized effector systems secures multiple assets – a surface-to-air missile battery, for instance – within a zone, while point protection is focused on individual high-value assets. This layered approach allows for flexible defense based on asset location and threat level.

THE PASSIVE SENSOR: RF REQUIREMENTS



ESSENTIAL RF CAPABILITIES FOR EFFECTIVE DEFENSE

Key capabilities:

- ▶ **Signal detection and tracking:** high sensitivity for detecting weak or distant signals; accurate direction and distance
- ▶ **Tracking accuracy:** precise tracking of drone movements
- ▶ **Broad coverage:** wide frequency range
- ▶ **Flexible workflow:** options for automatic detection and manual intervention by spectrum experts
- ▶ **RF interference management:** resistance to RF jamming tactics in hostile environments
- ▶ **Ready for the unknown:** resilient against new hostile RF drone technologies

To effectively counter the growing threat of drones, it is crucial to understand the technical aspects of RF-based drone detection and how they work. A robust RF detection system must be able to cover the full spectrum and provide accurate geolocation. Additionally, the system should be able to adapt to signal changes, manage interference and ensure reliable tracking across diverse environments. Key factors contributing to its efficacy include broadband coverage, high sensitivity and portability to enable real-time threat detection and mitigation.

TECHNICAL ASPECTS OF DRONE DETECTION

Drones operate using various RF signals, which presents challenges for detection systems. In designing a detection system, key factors such as sensor selection, signal characteristics and operational frequencies are essential to ensure effective monitoring and identification of potential drone threats.

RF signals: Drones communicate using uplink and downlink RF signals.

- ▶ **Uplinks** (remote control to drone) often employ frequency-hopping spread spectrum signals
- ▶ **Downlinks** (drone to controller) can be analog or digital and may be used to transmit video feeds

Frequencies: Commercial of the shelf drones operate on ISM bands, such as 2.4 GHz, 5.2 GHz and 5.8 GHz. DIY drones may use non-ISM bands as well, such as 433 MHz, 868 MHz and 2.4 to 2.8 GHz, while military drones may use yet other frequencies, making them harder to detect. DIY and military drones often have higher RF output power, increasing their visibility to detection systems.

Communications protocols: Drones can rapidly alter their communication protocols and encryption through software updates. Reverse engineering may not be fast enough to effectively detect and adapt to these changes.

Strategic selection and placement of sensors is crucial for effective monitoring and identification of potential drone threats. Properly configured systems can significantly enhance detection success and enable a robust response to a wide range of drone activity.



CONCLUSIONS AND RECOMMENDATIONS

KEY FINDINGS

The integration of drones into military operations enhances situational awareness and operational effectiveness. However, the threats posed by malicious and non-cooperative sUAS require innovative solutions and adaptive strategies to ensure airspace security.

COUNTERMEASURES

Effective defense against sUAS involves a multi-layered approach that includes tailored countermeasures. Understanding the operational capabilities of sUAS is crucial for developing effective military strategies.

RECOMMENDATIONS FOR MILITARY APPLICATIONS

To counter emerging drone threats, armed forces should invest in future-proof advanced RF based technologies that promote situational awareness and rapid, autonomous threat classification. The systems must be designed in such a way that they can be adapted for use against new threats in the future.

Continuous evaluation of existing defense systems and collaboration with industry and allied nations can facilitate best practices and technology sharing, enabling more effective countermeasures. By adopting these strategies, military forces can enhance operational readiness and counter the growing sUAS threat.

ROHDE & SCHWARZ:

SECURING YOUR AIRSPACE WITH TRUSTED EXPERTISE



Rohde & Schwarz is dedicated to addressing the increasing threat posed by malicious and non-cooperative drones with our comprehensive ARDRONIS counter-drone solutions. Our advanced solutions significantly improve drone detection and mitigation, leveraging industry-leading radio frequency (RF) technology.

As the rise of remote-controlled drones poses challenges to aviation and the security of sensitive sites, our system-of-systems approach enables civil and government organizations to effectively detect, identify, locate, track, verify and counter these threats. With ARDRONIS, we provide the capability to automatically classify drone signals, determine the direction of both the drone and its pilot, and disrupt the radio control link, ensuring that potential threats are neutralized before they can reach their targets.



SECURE OPERATIONS, ENHANCED SAFETY: EMPOWER YOUR DEFENSE WITH ADVANCED DRONE PROTECTION SOLUTIONS. BY LEVERAGING CUTTING-EDGE TECHNOLOGIES, WE CAN EFFECTIVELY MITIGATE THE RISKS POSED BY COMMERCIAL DRONES, ENSURING MISSION SUCCESS FOR EXPEDITIONARY FORCES. TOGETHER, WE CAN CREATE A SAFER ENVIRONMENT WHERE SECURITY AND OPERATIONAL EFFICIENCY GO HAND IN HAND!



Explore how ARDRONIS and our RF solutions can give you the edge when managing UAS threats. Whether you're looking for detailed information or a consultation, our experts are here to discuss how ARDRONIS and our other solutions can help you stay ahead in an evolving battlefield.

TRUE SPECTRUM DOMINANCE IN ALL DOMAINS



Today's military missions increasingly rely on information superiority and advanced command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) systems. Control over the electromagnetic spectrum has become essential in achieving strategic military dominance.

Rohde & Schwarz develops, designs, manufactures and implements turnkey end-to-end solutions for secure communications, SIGINT/ EW, intelligence, test & measurement and security in modern warfare. Our solutions contribute to effective C4ISR, enabling customers to achieve dominance in the electromagnetic spectrum for a decisive edge in modern warfare.

SIGNAL MASTERY

Signal testing and generation, secure communications, encryption, signal detection, location, analysis and interception from a single source.

VERTICAL INTEGRATION

Rohde & Schwarz maintains a high degree of vertical integration with nearly its entire value chain inside the company. All products are developed and manufactured in its own factories.

ONE-STOP SHOP

Rohde & Schwarz provides a one-stop shop with the full range of turnkey solutions, from sensors and analysis to effectors across the electromagnetic spectrum.

TRUSTED PARTNERSHIP

As an independent, privately-owned company, Rohde & Schwarz finances its growth with its own resources. The company is not beholden to capital markets or stock market expectations.



NON-TERRESTRIAL
MONITORING



MONITORING
SOLUTIONS



COUNTERING
DRONES



ELINT/RESM



COMINT/CESM



CYBERSECURITY



MOBILE
NETWORK
TESTING



NAVAL
COMMUNICATIONS
SYSTEMS



CELLULAR
NETWORK AND
IP ANALYTICS



TEST &
MEASUREMENT



TACTICAL
COMMUNICATIONS



AIRBORNE
COMMUNICATIONS

Service at Rohde & Schwarz You're in great hands

- ▶ Worldwide
- ▶ Local and personalized
- ▶ Customized and flexible
- ▶ Uncompromising quality
- ▶ Long-term dependability

Rohde & Schwarz

The Rohde&Schwarz technology group is among the trailblazers when it comes to paving the way for a safer and connected world with its leading solutions in test&measurement, technology systems and networks&cybersecurity. Founded 90 years ago, the group is a reliable partner for industry and government customers around the globe. The independent company is headquartered in Munich, Germany and has an extensive sales and service network with locations in more than 70 countries.

www.rohde-schwarz.com

Sustainable product design

- ▶ Environmental compatibility and eco-footprint
- ▶ Energy efficiency and low emissions
- ▶ Longevity and optimized total cost of ownership

Certified Quality Management
ISO 9001

Certified Environmental Management
ISO 14001

Rohde & Schwarz training

www.training.rohde-schwarz.com

Rohde & Schwarz customer support

www.rohde-schwarz.com/support

