DETECT, TRACK, DISRUPT

Graeme Forsyth *explains why mastering the RF spectrum is key to countering the UxS threat to national security*

Uncrewed systems (UxS) are steadily reshaping the risk landscape for both civilian and critical infrastructure, with their growing use for sabotage, surveillance, and disruption becoming an increasing concern. As these incidents become more frequent, the need to address the expanding and increasingly bold deployment of drones is clearer than ever.

In recent months, Russia has coordinated attacks on Ukraine's critical national infrastructure using adapted Iranian-made Shahed kamikaze drones. In the Middle East, Iranian drone strikes against infrastructure in Kuwait and Bahrain – including airport radar systems – highlight the expanding impact beyond the battlefield.

Notably, attacks on Amazon Web Services facilities in the UAE and Bahrain disrupted cloud services across the region, prompting the World Economic Forum to urge that AI facilities be recognised and protected as critical infrastructure. From minor air traffic disruptions to covert surveillance of sensitive sites such as airports and military bases, adversaries are growing increasingly bold, and the threat is expanding beyond the skies.

Submarines and unmanned underwater vehicles pose a significant risk to essential infrastructure beneath the surface. Increasingly used as tools in 'gray zone' warfare, these systems have the potential to damage undersea pipelines and communication cables that are critical to national security and global connectivity – destabilising infrastructure without provoking open conflict. Recent activity has even seen the deployment of specialised spy ships to map and potentially sabotage vital assets, underscoring the evolving nature of the threat. Russian underwater sensors have also been detected near British critical infrastructure and, as recently as April, forces in the UK and Norway identified Russian vessels attempting to survey underwater cables and pipelines.

The UK and Norway recently identified Russian vessels attempting to survey underwater cables and pipelines

Ukraine has achieved significant results in deploying sea drones against military vessels and Russian naval assets. Furthermore, in March, unmanned surface vessels targeted oil tankers in the Gulf region, posing a threat to one of the world's most important oil shipping lanes.

Illustrating the range of threats posed by UxS, mass public gatherings are continuing to see an increase in drone deployment. The upcoming FIFA World Cup this summer has brought renewed attention to the challenge of achieving comprehensive protection at major public events. The global event faces increased terrorism risks – exacerbated by tensions involving Iran and a decline in counter-terrorism expertise – while experts caution that the greatest threat stems from domestic extremists.

Only last year, a drone flew over Twickenham Stadium in the UK during a packed Six Nations rugby match and bearing a Palestine flag. This incident demonstrated how easily drones can breach security, disrupt large crowds, and deliver provocative messages, or worse, highlighting the urgent need for stronger, more resilient defences at high-profile venues.

When it comes to nuclear facilities, the International Atomic Energy Agency recently reported a surge in drones operating near Ukrainian nuclear sites, recording over 160 flights in just two days. Around the same time a major fire broke out in the Chernobyl exclusion zone spanning 1,100 hectares, sparked by a drone impact.

Whether it's protecting an air base, a nuclear facility, or a sporting event, the same core technology and regulatory standards apply. But, despite the escalating risks and evolving nature of attacks, many regions still remain ill-equipped to counter them effectively.

IT'S CRUCIAL TO BE ABLE TO JAM GNSS, COMMAND, CONTROL AND TELEMETRY SIGNALS

The above developments highlight a rapidly evolving domain where adversaries can target vital assets across land, sea and subsurface environments, underscoring the urgent need for comprehensive, multi-domain protection strategies. As UxS technology grows faster, more agile, more affordable and able to strike from longer ranges, passive observation is no longer a viable defence. This is especially true at high-value sites where aircraft are most vulnerable, such as during low-altitude approaches. In this landscape, only active protection strategies can keep pace with the escalating sophistication of the threats.

Demand for countermeasures is rising sharply. We're seeing about an 80 percent increase in interest across Europe as nations seek to strengthen their defences. However, the complex and crowded marketplace – particularly for radio frequency (RF) equipped solutions – makes it challenging for authorities to identify truly effective options or even have the financial resources to adopt them.

Countering UxS demands a wider array of sensors and mitigation tools than ever, especially covering evolving threat types and environments from underwater to difficult terrain, which greatly complicate detection and identification. Furthermore, UxS threats frequently employ a variety of communication methods and can operate autonomously, reducing the effectiveness of traditional RF-based countermeasures.

In response, security and defence teams require integrated, adaptable, open-architecture solutions that can adapt to their budgets and address the full range of threats spanning air, land, sea, and subsurface domains.

A deep understanding of the RF spectrum is fundamental to mounting an effective defence against modern uncrewed threats. As UxS and drone technologies increasingly leverage diverse and agile frequency bands for command, control and data transmission, pinpointing and interpreting these signals becomes essential for early detection, tracking, and disruption.

Without clear insight into the RF landscape, security teams risk missing covert communications or failing to distinguish between friendly, civilian, and hostile signals – potentially leading to false alarms or operational blind spots. Mastery of the RF spectrum not only

Picture credit: iStock

enables more precise and targeted countermeasures, but also helps ensure that legitimate communications are safeguarded, reducing collateral disruption and enhancing overall situational awareness.

Conducting an early investment in advanced RF soft-kill solutions means they can be redeployed over time to accurately identify the threat, determine the appropriate response and neutralise the threat. Its high rate of re-use and precision make RF a key ally for security and defence teams.

ONLY LAST YEAR, A DRONE FLEW OVER TWICKENHAM DURING A PACKED SIX NATIONS RUGBY MATCH

Directional jamming is also now possible at far greater distances – from 200m to over 10km. Beyond range, countermeasures must also adapt to faster, more mobile devices and an ever-growing mix of frequencies. Longer-range systems, high spectral purity, directional beams, and agile responses to changing protocols are essential for defeating UxS threats.

For instance, it's crucial for solutions to be able to jam a combination of GNSS, command, control and telemetry signals. This ensures a decisive advantage in countering drone threats while simultaneously safeguarding friendly RF signals from unintended inhibition.

For effective defence, countermeasures also need flexible and mobile mounting options, whether positioned high up for a greater line of sight or deployed on the periphery of a critical national infrastructure site for rapid response.

With hundreds of sites potentially at risk, nations across the world need decentralised capabilities that can respond quickly, safely, and within legal frameworks. The most successful solutions blend extended reach with high signal purity, focused beams, and wide coverage to meet the complexity of today's incursions.

By integrating precise disruption tools with sophisticated RF analysis, operators gain a nuanced understanding of their threat landscape and confidence in their detection and mitigation capabilities. However, the pace of technological change is simply too rapid for any single vendor to consistently provide all the necessary UxS countermeasures.

Taking meaningful steps, even small ones, is essential. In today's environment, more white papers and trade studies offer limited reassurance. Real progress is achieved through hands-on experience. The perfect solution is rarely found on the first try and only practical deployment and learning in the field enable organisations to refine and adapt their unique concepts of operation. What's needed now is thoughtful, measured action, ideally in partnership with a trusted expert, to ensure each step leads to genuine improvement and lasting results.

Open ecosystems and collaborative approaches will become essential, allowing organisations to combine the best and most up-to-date technologies from multiple vendors. This not only ensures greater adaptability and resilience, but also helps decision-makers navigate a saturated market – where distinguishing genuinely effective solutions from fleeting trends or marketing hype can be a significant challenge. By fostering interoperability and drawing on a diverse pool of expertise, teams are better equipped to stay ahead of evolving threats.

Ultimately, by combining field-tested countermeasures with scalable, future-ready platforms, security and defence teams can ensure they are equipped to identify, assess and neutralise drone threats both now and as challenges evolve. As uncrewed threats continue to advance rapidly, ongoing adaptation and collaboration across sectors will be essential. Meeting tomorrow's challenges will require not only the latest technology, but also a shared commitment to continuous learning, open partnerships and the agility to respond to an ever-changing threat landscape ●

Graeme Forsyth, Counter-UxS Product Manager at Enterprise Control Systems, has over two decades' experience in the defence industry with a background in battlespace management, electronic warfare, modern digital architectures and airborne defence systems.

Solutions must be able to jam a combination of GNSS, command, control and telemetry signals

Picture credit: Enterprise Control Systems