POLICING THE SKIES

Tal Cohen *considers the rise of Cyber Over RF in counter-drone defence*

In the ever-shifting landscape of global security, the growing prevalence of drones has introduced a new category of threat that transcends borders, conflicts and even conventional definitions of warfare. Drones are no longer exclusive to military forces; they are now widely accessible, affordable and weaponisable by criminals, terrorists and other malign actors. As a result, the counter-unmanned aerial systems (C-UAS) sector has undergone rapid expansion. But with the proliferation of technologies, there also comes complexity. Amid the noise, one approach is beginning to rise above the rest: Cyber Over RF (CoRF).

Originally deployed for reconnaissance or commercial delivery, drones have found far more sinister uses. From smuggling drugs into prisons and surveilling critical infrastructure to disrupting airport operations or conducting battlefield attacks, drones are a force multiplier for those looking to evade traditional security measures. As drone technology becomes more sophisticated, with swarming capabilities, frequency-hopping communications and semi-autonomous navigation, defenders can no longer rely on outdated or singular defence mechanisms. Today, what's needed is precision, adaptability and regulatory compliance – a tall order for many traditional solutions.

Let's consider the standard toolkit. Radar, electro-optical/infrared (EO/IR) cameras, acoustic sensors, RF jammers, GNSS spoofers and kinetic interceptors all bring unique advantages. However, they also carry inherent limitations:

- RF jamming, for instance, indiscriminately disrupts communications at targeted frequencies, risking collateral interference with emergency services and aviation.
- GNSS spoofing can mislead not only unauthorised drones but also legitimate systems, creating a hazardous environment for navigation.
- Kinetic interception, such as net guns or anti-drone drones, introduces physical risk. Even a successful takedown could cause debris damage, especially in populated areas.

Radar and EO/IR depend on line of sight and favourable environmental conditions, and they generally lack built-in mitigation capabilities.

Most significantly, these systems were often designed for battlefield use, where rules of engagement differ substantially from civilian and homeland environments. The real-world deployment of these tools in urban areas raises legal, operational and ethical questions that few systems are built to answer.

Instead of interfering with or destroying drones, CoRF takes control of them

Cyber Over RF isn't just another technology, it's a fundamentally different philosophy altogether. Instead of interfering with or destroying drones, CoRF takes control of them. By interacting directly with the drone's native communication protocol – the language between the drone and its remote operator – CoRF solutions detect, identify and take over unauthorised drones without causing collateral damage or regulatory violations.

The approach relies on a combination of electronic warfare, signal intelligence and cyber exploitation. Through passive RF scanning, protocol analysis and surgical signal injection, the system guides the drone to a safe landing zone. It's lawful, silent and highly precise. And when deployed correctly, it leaves friendly drones and surrounding infrastructure completely untouched. As the technology gains traction, not all CoRF providers are created equal. Security stakeholders evaluating solutions should assess them against five critical criteria:

1. TIME TO MARKET

In CoRF systems, the 'library' refers to the database of known drone protocols, models, firmware versions and control links. It forms the basis for detection and takeover capabilities. Given the rapid evolution of the drone market, a static library is a liability. Providers must:

- Update their libraries frequently (at least every three months)
- Support dynamic protocol decoding for unknown or custom-built drones
- Offer transparency about the last library update date

A leading-edge CoRF solution will not only keep pace with new drone releases, but also improve autonomously using machine learning and AI to identify novel patterns on the fly.

2. HOW EASY IS IT TO DEPLOY AND OPERATE?

Operational success often comes down to how quickly and reliably a system can be deployed in the field. In high-pressure environments like airports, stadiums or government facilities, setup time and ease of use are essential. Ask your provider:

- How many operators are required? A typical system should arrive in 1–2 ruggedised cases (or as a handheld device) and be deployable by a single operator in under 15 minutes.
- What power sources are needed? Leading solutions are battery-powered or run from a vehicle's energy supply.
- What level of training is required? A good CoRF system should come with an intuitive interface and require minimal technical training. RF and cyber experts should not be a prerequisite for operation.

Modern solutions aim for portability and autonomy – two traits that allow even small teams to deploy and maintain robust protection.

3. TOTAL COST OF OWNERSHIP

Budgets are tight, especially for municipalities, law enforcement and critical infrastructure operators. But affordability goes beyond sticker price. Buyers must consider:

- Hardware and deployment costs
- Software licensing and update fees
- Maintenance and technical support packages
- Training and onboarding costs

Some CoRF solutions offer modular pricing, allowing organisations to scale their defences according to operational need. This is often more sustainable than committing to large fixed installations from day one. Additionally, CoRF systems reduce long-term costs by avoiding collateral damage, legal liability and service disruptions – expenses that are often underestimated when comparing with jammers or kinetic systems.

IN THE RACE TO SECURE AIRSPACE, THE GOAL ISN'T BRUTE FORCE, IT'S PRECISION

4. HOW WELL DOES IT WORK?

Effectiveness must be assessed across several different dimensions:

- Detection accuracy: Can the system distinguish between authorised and unauthorised drones?
- Identification speed: Does it detect and classify simultaneously or is there a delay?
- Operator location: Does the system provide GPS coordinates of the operator's location?
- Mitigation reliability: Once detected, does the system successfully take over and land the drone?
- Swarm support: What happens while one drone is being defeated? Does the system keep providing accurate situation awareness?
- Coverage and range: How large an area can it defend? Can it successfully operate in GPS-denied environments?

Modern CoRF systems enable real-time extraction of drone serial numbers, flight telemetry and operator locations. These capabilities not only ensure successful mitigation, but also provide crucial forensic and operational intelligence for follow up.

5. HAS IT BEEN TESTED AND TRUSTED?

The best technology on paper means little without operational validation. Ask vendors to provide:

- Case studies in urban, military or critical infrastructure environments
- User references and testimonials
- Proof of regulatory compliance and export approvals

A solution that has been stress-tested in high-risk areas – such as border regions, military zones, power plants or major sporting events – brings the added assurance that it can handle the real-world complexity of domestic deployment. Some providers

even offer demonstration days or limited pilot deployments to showcase real-time performance. If possible, evaluate the system in your operational setting before making a purchasing decision.

DEFENDERS CAN NO LONGER RELY ON OUTDATED OR SINGULAR DEFENCE MECHANISMS

THE REGULATORY EDGE

In many jurisdictions, broad jamming or destructive mitigation is either illegal or heavily restricted. CoRF sidesteps these constraints by targeting only the unauthorised drone with protocol-level precision. This makes it uniquely suited to urban and homeland security applications, where both human safety and legal compliance are non-negotiable. In fact, CoRF is one of the few C-UAS technologies that aligns with FAA guidance on non-interference. That alone positions it as a strategic asset for any country serious about long-term airspace governance. As drones evolve, C-UAS systems must evolve faster. The nature of the threat will change; what matters is the agility and intelligence of the response. CoRF, with its software-defined architecture and cyber-aware methodology, is inherently future-proof.

Look for providers who:

- Offer over-the-air updates
- Leverage AI and machine learning for pattern recognition
- Actively contribute to international drone defence standards

These traits will ensure your investment continues to deliver value as threats, policies and technologies shift over time.

In the race to secure airspace, the goal isn't brute force, it's precision. As regulators tighten the rules and drone threats multiply, only one technology offers the control, legality and scalability required to meet the moment: Cyber Over RF. But adopting CoRF isn't just about acquiring new tech. It's about choosing the right partner – one that is agile, proven, affordable, easy to use and aligned with operational realities.

In the coming years, airspace defence will shift from primarily focusing on preventing flight. It will be about commanding it. CoRF makes that possible. The time to take control is now ●

Tal Cohen is a Lieutenant Colonel in the Israeli Air Force (Res.) and the founder of the Israeli National C-UAS Taskforce. Since 2020, he has been the CTO of Sentrycs.

CoRF sidesteps constraints by targeting only the unauthorised drone with protocol-level precision