CONTROL, SAFETY AND CONTINUITY

Jeffrey Starr, CMO, D-Fend Solutions takes a closer look at RF-Cyber counter-drone technology – a next-generation approach

Drones are bringing tangible value and benefits to millions around the world and are reshaping the way modern societies function. They are changing the way various fields and industries operate. But, as drones continue to proliferate, there is a portion of bad actors, inexperienced operators and outright enemy combatants who can cause tremendous damage. New technologies are needed to mitigate this threat and thereby help support today's drone-powered society.

> **"RF-CYBER BRINGS A UNIQUE CAPABILITY TO MITIGATE RISK."**

Drones are becoming, faster, harder to detect and more durable. Many can fly long distances and carry heavy payloads and are quite easy to operate, which poses safety and security risks to every type of environment. Drones can be used to attack soldiers and law enforcement teams, target critical facilities, smuggle drugs into prisons or across borders, disrupt major events and pose a danger to plane and other aircraft.

Traditional technologies from the military realm have a role to play in a layered defence strategy, but they are insufficient in certain sensitive scenarios. On the detection side, radars can generate false positives from other flying objects such as birds. Optical camera-based identification solutions are ineffective without a clear line of sight. Acoustic solutions are ineffective in noisy environments, especially as drones become quieter.

More importantly, relating to mitigation, jamming-based solutions are temporary and may disrupt nearby communications and operations. Kinetic solutions involving physical shooting can be risky in crowded situations and can cause collateral damage.

Safe landings for safe outcomes

In this context, a new category of technology has emerged, employing RF-Cyber-detection and takeover mitigation technology. With this technology, systems detect, locate and identify rogue drones in the airspace and then neutralise the threat by providing security agency operators with full control over the drone to fend it off or land it safely in a predefined zone.

During the mitigation takeover process, the rogue drone pilot loses all control of the drone and cannot regain it. Since the system does not rely upon jammers or kinetic technology, RF-Cyber avoids collateral damage, interference, disruption or disturbance. Continuity prevails as communications, commerce, transportation and everyday life proceeds smoothly.

RF-Cyber brings a unique capability to mitigate risk by taking control of hostile drones and, by extension, the incident. The rogue drone lands safely in a predefined safe zone. The technology employs non-jamming, non-kinetic technology that does not require line-of-sight. It also brings the added advantage of distinguishing between authorised and unauthorised drones. The advanced can even operate in an autonomous mode.

It can be implemented in a wide variety of deployment configurations, providing complete operational flexibility and end-to-end counter-drone capabilities for any scenario or environment. Finally, with open APIs, the technology can integrate with command and control systems and can also complement other detection and mitigation technologies in a layered defence.

> **“A NEW CATEGORY OF TECHNOLOGY HAS EMERGED.”**

Operational continuity

RF-Cyber-based systems passively and continuously scan and detect unique communication characteristics of commercial drones. Once detected, the drone’s core identity is discovered, including whether it is authorised or not.

The location can be tracked with a high degree of accuracy, including the take-off position. Authorised drones can continue to function without interruption, while the system tracks the rogue drone. During the mitigation process, the takeover process commences and the pilot loses all control of the drone and cannot regain it. RF-Cyber technology therefore empowers security agencies with operational flexibility across domains, environments and scenarios.

The rogue drone incident lifecycle

RF-Cyber systems are best understood within the framework of a rogue drone incident lifecycle. The system must detect, then issue an alert, then locate and track the rogue drone and identify the drone, take-off and pilot positions. Ultimately, if determined to still be a threat, the system will fend-off or take control and land the rogue drone, for a safe and controlled outcome, as opposed to jamming or kinetic methods where the outcome is unknown and potentially dangerous.

Varied deployment options

RF-Cyber systems should provide operational agility and flexibility. This means that its core elements should be easily set up, transferred, mounted and configured very quickly, even within minutes. Relevant deployment options include stationary including high altitude long range coverage and tactical “on the move” capabilities – also at high altitude and ground level – and vehicular, both military and covert civilian. Finally, a backpack man-portable deployment is needed for the hardest-to-reach scenarios.

Selected, proven, chosen

RF-Cyber systems are already in use by government security agencies. The technology has been proven, tested, selected and trusted by operational units and security agencies in sensitive environments and deployed by agencies in the military, law enforcement and homeland security sectors. The technology has also been selected for large scale events and entrusted to protect high-level VIPs around the world, at major stadiums, arenas and open-air venues.

Core counter-drone concepts

The RF-Cyber counter-drone technology approach is based on core concepts. The first is ‘control’, meaning the best way to control the drone threat is to take control of the drone itself. The second is ‘safety’; achieving a safe landing or fending off the rogue drone as the best possible outcome for safe airspace and continuity. Then, a ‘focus’ on the real risk, the most dangerous commercially available drones. Finally, ‘future’, which means the system provider must foresee the drone future and always stay a drone threat ahead. ▪