D-FEND SOLUTIONS

Evaluating and Comparing Counter-Drone (C-UAS) Mitigation Technologies

Which counter-drone mitigation technology is the most suitable for the use case and scenario? This white note evaluates the strengths and weaknesses of legacy and recent technologies, to help inform discussions and evaluations regarding which technology will best satisfy specific needs.

Radio Frequency (RF) Jammers

Mitigation Technology	Key Challenge
RF jammers	Communication/GNSS interference

RF jammers channel large bursts of RF energy which mask the signal from the controller and prevent the drone from receiving instructions. Some jammers concentrate their radiation in the direction of the drone.

This technology is comparatively cheap, simple to operate and may achieve some desired effect – temporarily incapacitating all drones in the immediate area. These are appealing benefits, but they are accompanied by some significant disadvantages.

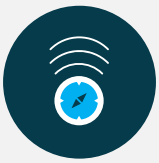
RF noise may interfere with nearby communications systems and/or GNSS, rendering this mitigation technology problematic in many sensitive environments, including the potential of shutting down friendly, authorized drones.

As the jamming effect depends on the strength of the RF noise the jammer creates, its effect relies on the relative strengths of signals the drone receives from the remote controller and the jammer, and this depends both on the power of transmission and on the distance to the drone. The jammer only works if its signal prevails. This condition has several implications:

- The jammer will work only when the drone is far enough from its remote controller but close enough to the jammer
- In case the drone returns home, its pilot can regain control once the drone gets close enough to the remote controller
- In case the jammer stops transmitting, the pilot may immediately regain control; this method depends on continuous transmission

Jammers do not gain control over a drone; they only disconnect it from its remote controller. Once disconnected, it usually tries to return to its take-off ("home") position, but it may also hover in place or try to land, and some drones can be programmed to do other emergency default actions. Each of these options may pose a threat (e.g., a drone returning home may fly through sensitive airspace like the take-off corridor of an airport); when the drone flies without control, not even its pilot can prevent damage. Unless the drone is within line of sight, the jammer's operator may not even know whether the drone was disconnected. Jammers may not always permanently eliminate the specific threat, but rather only temporarily block it, since in many cases, the drone will return to its pilot.

Distinct types of jammers have specific strengths and weaknesses:



Directional Jammers

These jammers mitigate drones flying in from a specific direction. This technology offers a longer range than other types of jamming and causes less disruption and signal interference in the immediate environment. It does require continuous transmission to remain in effect. It cannot, by itself, efficiently overcome swarms, which by their nature usually approach from multiple directions.

A narrow beam can also lose its efficacy if the drone starts to fly back to its home location, and the pilot may regain control and fly from a different direction or evade the effective angle of the directional jammer.

Omni-directional Jammers

Omni-directional jammers can mitigate drones from all directions and thus better handle swarms. But it offers a shorter range than directional jammers, meaning the protected area is smaller.

Omni-directional transmission also increases the collateral effect over authorized and non-threatening drones, and over other communication systems in the vicinity.

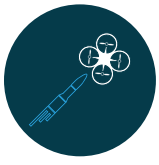
Handheld Jammers

These jammers are mobile and simple to use. The operator just pulls out the device and aims it. Disadvantages: Because this method is manual, a security team member must always have the handheld jammer on his/her person and remain vigilant.

If the operator cannot immediately activate the handheld jammer, or is not paying attention, the chance to mitigate the rogue drone could be quickly lost. Also, handheld jammers operate at a low power level so as not to endanger the health of the operator, but also making the range of the device limited.

This type of jammer is effective in scenarios where a certain sensitive point should be protected, and the threatening drones are in proximity and within eyesight. It is practically useless in cases where a perimeter or a border must be defended as the drone can simply fly high enough to be beyond the range of the handheld jammer.

Kinetic Solutions

Mitigation Technology	Key Challenge
 Kinetic solutions	 Collateral damage risk

Kinetic solutions cause the drone to stop operating by some sort of physical intervention, e.g., a projectile, and they vary in size and portability, ease of operation, cost, and capabilities against specific drone types.

Less favorably, some, though not all, kinetic technologies may require line-of-sight, which is not always available in urban or sensitive environments due to tall buildings, vehicles, signage, etc.

Kinetic solutions aim to cause the drone, in most cases, to fall from the sky, which can create severe collateral damage or human injury. The projectiles themselves may also hit other objects and pose risk, especially in sensitive environments such as airports or critical infrastructure.

Distinct types of kinetic solutions possess associated pros and cons:

Drone-Killing Drone (Net to Tow, Collision, Net Throw or Projectile)

Drone-killing drones can capture unauthorized targets with nets and tow them to a controlled landing. Alternatively, this category can also include drones that attempt to ram into rogue drones and disable them. Finally, some of these defensive drones can shoot nets or other projectiles at unauthorized drones. Accurate hits can be challenging for these methods when trying to mitigate a drone that flies in a non-predictable manner.

The drone-killing drone needs to "dog-fight" or chase the rogue drone, and it is extremely challenging to do so through an autonomous system or through drones that are controlled by a pilot from the ground. This method can also result in collateral damage from a plummeting drone and projectile.

Intelligent Shooter

Intelligent shooters possess a system mounted on a rifle that enables accurate shots against nearby drones. A special scope performs a calculation before the shot. The probability of a hit, compared to other kinetic methods, is therefore increased. This technology is more economical and may play a role in a multi-layer counter-drone system, particularly in rural, or open-field environments. This technology is accurate up to a few hundred meters (generally, less than 250 meters) and may face difficulties to hit smaller drones. The security team must act immediately – drones fly fast, and there are only a few seconds to respond.

Lasers

Mitigation Technology	Key Challenge
 Lasers	 Accuracy affected by weather conditions

These high-energy devices warrant their own sub-category. By emitting an intense beam of light, laser-based systems can destroy the drone structure, or its electronics. Lasers destroy drones and can confront many types of drones. On the downside, they require line-of-sight, burn the drone to pieces (destroying intelligence) and can also result in plummeting drone fragments. Collateral damage is possible, and obstacles such as buildings or other flying objects may pose challenges.

For these reasons, lasers may, in some cases, be less suitable for sensitive environments. It is also more difficult to hit smaller drones using lasers.

Electromagnetic Pulse (EMP)/High Power Microwave (HPM)

Mitigation Technology	Key Challenge
 Electromagnetic Pulse (EMP)/High Power Microwave (HPM)	 Significant collateral damage to electronics in area

This is a radiation-based technology. It utilizes a high-powered burst of electromagnetic energy in short blasts, potentially damaging everything electrical in the area. EMP works indiscriminately and can cause heavy collateral damage. For instance, it can permanently damage nearby electronics or computers, damaging their circuits. EMP is often viewed as a last resort option.

GNSS Spoofing

Mitigation Technology	Key Challenge
 GNSS electromagnetic	 Navigational disruption

Global Navigation Satellite System (GNSS) spoofing broadcasts a false GNSS signal such as GPS in a specific area. A GNSS receiver that receives the spoofed signal may determine its location wrongly. By controlling the perceived location of a drone, it may be possible to cause it to fly in a desired direction and thus navigate it. Alternatively, it can prevent the drone from flying according to a pre-programmed flight plan or from returning home.

In terms of disrupting the environment and affecting continuity, this technology can be even more problematic than jamming. Every navigation device in the area may receive the spoofed GPS signal and determine a wrong global position.

GPS spoofing could affect, for instance, civilian cars' navigation systems, or drivers' navigation apps, causing confusion, accidents and worse. It may also disrupt friendly drone operation. This technology obviously should not be used near friendly authorized ships, planes or helicopters.

RF-Cyber Takeover

Mitigation Technology	Key Challenge
 Cyber takeover	 Overcoming advanced drone protocols

RF cyber-takeover is a non-jamming, non-kinetic technology that transmits a precise and short signal that takes control over the rogue drone. This technology focuses on the RF communications between the pilot's remote controller and the drone, and then intervenes with it, taking over command of the drone. It then directs the drone to follow a predetermined route and to safely land in a prearranged location. This surgical mitigation may occur within certain range, aligned with the needed power output required to intervene with the rogue drone's communication link.

This RF cyber-takeover is end-to-end, meaning it seamlessly flows from the initial rogue drone detection, all the way through to takeover and then safe landing. It can also be deployed automatically, eliminating the chance of human error.

Unlike the other mitigation technologies, RF cyber-takeover preserves continuity by avoiding collateral damage or interference with other communications systems. It can also distinguish between authorized and unauthorized drones, enabling an organization's authorized drones to keep functioning during the mitigation of rogue drones.

As it depends on a short transmission, it may also contend with swarms of unauthorized drones by quickly mitigating each of them in their own frequency and transmission patterns.

Because RF cyber-takeover mitigation does not destroy the drone, like lasers or EMP, organizations can reap the benefits of the intelligence inside the drone (as allowed by applicable laws, of course).

RF cyber-takeover focuses on specific RF-based manufactured or Do-It-Yourself commercial drones and overcoming their specific protocols.

Operational Considerations

Entities permitted to lawfully employ counter-unmanned aircraft system (C-UAS) technologies should be aware of some environmental considerations that can directly impact how such technologies operate. These considerations may include limited line-of-sight, radio frequency (RF) noise, and radio signal propagation.

In addition, mitigation of a drone is not bound to the techniques mentioned above. Mitigation can also be achieved through finding the drone operator's location and having that person cease their operation. Incorporating multiple layered mitigation technologies is the most effective strategy to increase the probability of countering any given threat.

For more information, please visit: www.d-fendsolutions.com