



sentrycs

A New Era of Counter-drone Mitigation

Safe and effective is possible.



New solutions for new challenges

With the proliferation of commercial drones, associated threats are constantly evolving. Until recently, drone attacks were mostly making headlines in a military context, we are now increasingly hearing about drone incidents in civilian contexts such as prison smuggling, airport disruption, criminal explosions, and more.

In an attempt to mitigate these threats, a myriad of tactics has been tested, some of which are successfully field-proven, while others... way less.

In this article, we'll try to bring order to the chaos and provide useful insights into the most advanced counter-drone mitigation technologies available in the market.

Traditionally, drone mitigation technics were split into two main categories:

- Hard kill
- Soft kill

But a new type of technology - based on advanced communication protocol research - has been in the making for several years and is promising to become the breakthrough the drone industry has been waiting for. "Protocol-based Mitigation" is a subset of more comprehensive type of integrated counter-drone solutions, that can not only detect, track and identify unauthorized commercial drones as well as their controllers, but can also mitigate them.

Drone incidents in a civilian setup are on the rise.



Limitations

In order to better understand what alternatives are best for missions and specific environments or use cases, let's go over each one of the above mentioned technologies:

The term "Hard kill" is usually associated with kinetic methods which in most cases ultimately destroy the drone they aim to protect against. Sample tactics used under this category include lasers, using nets to catch drones, colliding a drone against another drone, projectile weapons, and more.

Obviously, once a drone has been "hard-killed" it is of no use in terms of investigation or incrimination.

No reverse engineering can be done and therefore the defense strategy of the defender can not be optimized.

One more limitation to highlight is that users of such solutions have not control whatsoever over the landing point of the threat and over the collateral damage they will cause.

Lastly, no evidence can be collected, hence no actions can be taken against the offender.



Soft kill drone mitigation solutions are irrelevant in urban environments.

The second category, coined "Soft kill" mostly refers to two key technologies: jamming, and spoofing.

Jamming consists in using a transmission-blocking signal to disrupt communications between a drone and its controller.

Once a drone is jammed, it can be forced to either land on the spot or fly back to its home location.

Spoofing consists in emitting a signal that is supposed to confuse the drone so that it thinks the spoofing signal is legitimate, when in fact it is not.



Soft-kill solution advocates rightly claim they have many advantages over hard-kill tactics. By not physically harming the drone they enable to get hold of any evidence the drone might be carrying along with it as well as to better understand what drone was used, was it modified or not, how was controlling it, and more.

Having said that, such solutions are entirely irrelevant in an urban setup, airport, or non-isolated environment as they interfere with other communication signals and GNSS. Imagine taking down Wi-Fi connections in a city or near critical infrastructures, just to takeover a drone. It literally can't fly (pun intended).

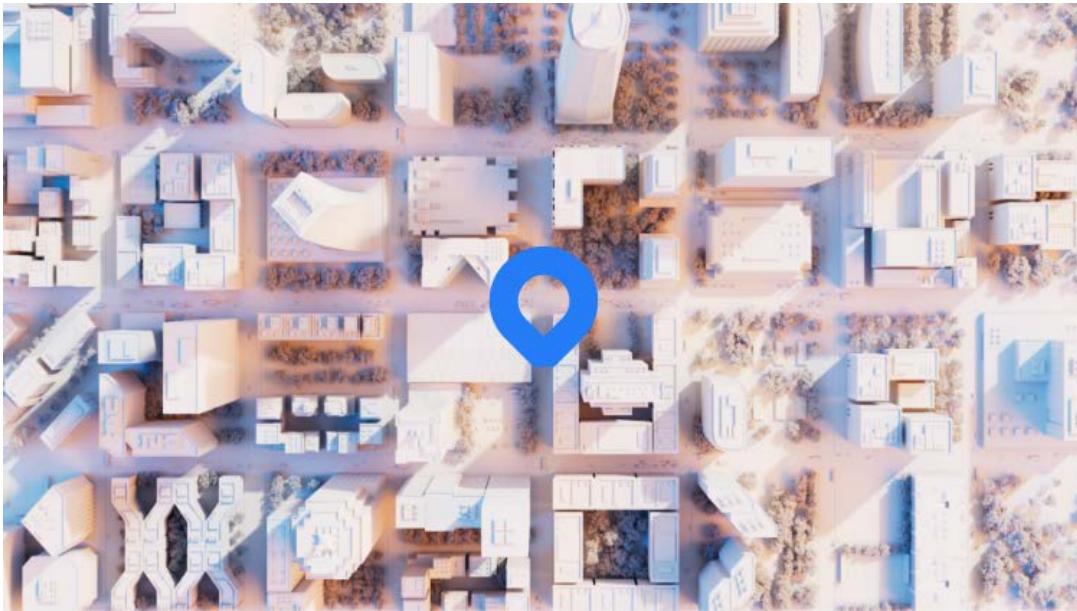
Moreover, although soft-kill methods are not shooting down the drone per se, they are not totally in control of what the drone does once it's been disconnected. They can hopefully ensure it doesn't fall and crash – creating collateral damage; but it often does not know where the drone will land and therefore can't promise the defender will be able to retrieve it once landed.



The Era of Protocol-based Mitigation

Protocol-based Mitigation provides an optimal solution to detect, identify, track and take over the drone as well as locate the controller. It surgically decodes the communication protocol between the drone and its remote control, disconnects the signal between them and pairs itself to the drone. It then sends a short prompt to the drone and makes it believe the system is the remote control.

From that moment on, the system decides when and where to land the drone; in a way that is safe, secure, and in reach of the defender. The drone remains intact, allowing for investigation and prosecution.



Protocol-based Mitigation is the only viable solution in dense and urban environments, as it does not interfere with any other communication signal and ensures the drone is taken over safely, with no collateral damage to people or assets. One more advantage of such systems is that they require little training and can be operated autonomously with a human in the loop only being alerted once the drone is mitigated.



Protocol-based Mitigation technologies, as they name implies, are based on advanced communication protocol research, which knows how to detect, reproduce, and decode such protocols, to then pair itself to the drone and speak to it in the specific and unique language it understands. This process is called “black box analysis”.

Each drone vendor, and each model within the same vendor, uses a different communication protocol. Therefore, the only downside of protocol-based mitigation technologies is that for now, the black box analysis phase and the design of the necessary algorithms takes some time and resources.

Sentrycs has made significant progress in developing a framework that leverages advanced research techniques, automation, and Machine Learning. Our software platform is constantly shortening the black box analysis process and providing the quickest time to market for our solutions.



Table 1 below summarizes the advantage and disadvantages of each drone mitigation technique.


	Non-Kinetic Soft-Kill	Kinetic Kill Hard-Kill	Protocol-based Mitigation
Sample “tech”	Jamming Spoofing	Lasers, nets, hawks, projectile weapons	 sentrycs
Drone Detection	No	No	Yes
BVLOS Detection	No	No	Yes
Drone Tracking	No	No	Yes
Drone Identification	No	No	Yes
Drone reverse-engineering / Evidence collection	Yes	No	Yes
Accuracy	NA	Inconsistent	Superior
Interference with GNSS and communication signals	Yes	No	No
Collateral damage	Yes	Yes	No
Viable in urban environments	No	No	Yes
Training required to operate	Low	High	Low



Table 1 – Pros & cons comparison of main drone-mitigation categories



Get in touch

UAS solution. To discuss your situation in depth or if you would simply like more information on anything in this guide, please visit www.sentrycs.com or reach out: info@sentrycs.com

