To Jam or Not to Jam:

WhiteFox Defense Technologies, Inc.

Luke Fox
Chief Executive Officer

Ryan Hodgens
Director of Business Development

WhiteFox Defense Technologies, Inc
(805) 250-9690
info@WhiteFoxDefense.com

WHITEFOX
DRONE DEFENSE

WHITEFOX

To Jam or Not to Jam

WhiteFox Defense Technologies, Inc.

Each new industry brings with it a lot of noise and confusion as people evaluate this new market to see what works and what doesn't. Eventually, the dust settles to reveal the most technologically advanced companies. Remember AltaVista? Dogpile? AOL? Now how about Google? Google emerged from the dust by coupling its intuitive design with its cutting-edge technology. The counter-drone industry is no different. It is brand new and riddled with noise. However, when the dust settles, the company that is the most innovative and advanced will, like Google, succeed. In the counter-drone industry, the importance of such a result is not just a matter of technological advancement, but of safety.

Why counter-drone?

Physical barriers have been generally used to mitigate ground-based threats, but there is a new threat that a wall cannot protect against: drones. For less than $1,000, a commercial-off-the-shelf (COTS) drone can be easily purchased and readily provides complete access to the airspace—restricted or not. Whether the pilot is clueless, careless, or criminal, drones pose a variety of different critical safety and security concerns.

What really is jamming?

As this new industry forms, the initial response and solution attempts have come with it. The most pervasive of which uses a method called "jamming." This technology exists in such high numbers because it's easy to create and appears to successfully defeat drone threats. However, all that a jammer really does is disrupt the communication link between the drone and the controller. On top of being highly illegal by FAA and FCC standards, there are two major concerns as to why **jammers are inherently unsafe**:

1. Because drones often operate using radio frequency (RF) signals that are frequently used for other forms of wireless communications (e.g.Wi-Fi, mobile hotspot, wireless handsets for landline telephones) jammers indiscriminately disrupt any and all of these signals. This includes "directional" jammers which typically disrupt all communication frequencies within a 30° spread of the jamming device. With such a wide radius of disruption, these "directional" jammers are highly likely to interfere with critical consumer electronic and business infrastructure, as well as critical emergency services, law enforcement, and military communication systems.

2. When effecting a drone, jammers are initiating the failsafe mode of the sUAS. This means, without control of the outcome, the drone will either drop from the sky or the failsafe will be triggered-which could be any pre-programmed behavior. If a drone merely drops from the sky, there is the inevitability of injuring someone. This creates not just a huge liability, but is a blatant public safety risk. The other jamming mitigation option is for the drone to complete a pre-programmed behavior. Often, this is the “return to home point” function. However, bad actors are known to change the home point to be the coordinates of the target. Jamming the drone's communication then initiates the failsafe of the drone which flies the drone directly to the bad actor's target.

How do I spot a jammer?

As more research is done that proves that jammers are inherently unsafe, many companies are beginning to stray away from blatantly saying they “jam.” When doing your own due diligence, beware of verbiage like: “disrupt,” “break,” “interfere,” “initiate fail-safe,” “disable.” Company marketing materials regularly portray jammers under this light.

Is there a safe way to mitigate drone threats?

In order to minimize the risk of collateral damage and safely mitigate drone threats, a complete drone takeover solution must be employed. WhiteFox's counter-drone product, the DroneFox, detects the RF signal, replicates it, and transmits a “smarter" signal back. This allows the DroneFox to step into the pilot's seat of the drone and —either manually or automatically—command it to return to the launch site, perform a controlled soft landing, disable the motors, or fly to a predesignated and safe location. WhiteFox has been confirmed by top government officials within the U.S. Department of Defense and Intelligence Community to be the only entity who can claim and demonstrate the ability to safely mitigate the heavily encrypted Lightbridge 2: the most popular consumer and terrorist drone communication protocol in the world.

Summary

WhiteFox Defense Technologies, Inc. appreciates the opportunity to discuss the importance of safe mitigation. Our team looks forward to further discussion regarding our approach, methodologies, and solutions to support your mission set.

For access to available DoD After Action Reports (AARs), updates on evolving capabilities, additional whitepapers, counter-drone market analysis from a technical lens, and to determine how WhiteFox can employ their solution to fit your specific needs, contact Ryan Hodgens at: +1 (805) 250-9959 or ryan@whitefoxdefense.com.