WHITEFOX

1241 Johnson Ave. No. 237, San Luis Obispo, CA 93401 || +1 (805) 250-9690 || **DUNS Number:** 080418634

DroneFox Fortify

The First Comprehensive Counter-sUAS Toolkit

SYSTEM RACK AND COMPONENT WEIGHTS

Rack Enclosure: 48 kg (106 lbs)

Alpha: 12.5 (27.5 lbs)

Bravo: 10 kg (22 lbs)

Charlie: 1.4 kg (3 lbs)

Ethernet Switch: 0.57 kg (1.25 lbs)

Display Console: 10.07 kg (22.2 lbs)

Total Weight: 82.5 kg (181.95)

RACK ENCLOSURE DIMENSIONS

Dimensions: 30.625" x 23.06" x 27.0"

Manufacturer's Part:
Lowell LPR-1427FV, 14U Rack w/ vented door

PROBLEM DEFINITION

Physical barriers are often used to mitigate ground-based threats, but there is an emerging threat a wall cannot protect against: small unmanned aircraft systems (drones). For only a few hundred dollars, a commercial-off-the-shelf (COTS) drone can be easily purchased, and readily provide 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. Globally, hobbyist drone pilots are interfering (accidentally or purposefully) with passenger aircraft, firefighting operations, and other restricted airspace above critical infrastructure and other soft targets. ISIS is using COTS Group I and Group II drones to carry out targeted aerial explosive payload drops and for intelligence, surveillance, and reconnaissance (ISR) to coordinate attacks. This leaves critical infrastructure, the public, and VIP targets vulnerable to terrorist threats. Although there are regulations in place that attempt to prevent drone pilots from flying in restricted areas, there is no mechanism to enforce these laws, thereby rendering them largely ineffective. The threat is only rising, while decreasing in cost and increasing in power

DRONEFOX FORTIFY

PURPOSE

DroneFox is a comprehensive small Unmanned Aircraft System (sUAS) threat detection, identification, and mitigation device that is readily integrated, omni-directional, and highly-efficient. DroneFox functions by passively analyzing the radio frequencies (RF) that are being transmitted by the sUAS and enables the user, through a series of proprietary algorithms, to lock out the original pilot and redirect the sUAS.

NOTE: DroneFox is not a jamming device. It is able to safely and securely reroute the sUAS without interfering with friendly or other authorized communications.

REMOTE ANTENNA MODULE

CONCEPT OF OPERATION

Via a built-in or external antenna array, DroneFox works by detecting the RF-signature of the sUAS and immediately applies a perpetual Unique Identification (UID) number for each detected sUAS. This allows for the "whitelisting" of friendly Blue Force sUAS and the "blacklisting" of all others. The DroneFox operator has the ability to select, then mitigate, any number of threat sUAS without affecting Blue Force (or coalition) sUAS operating in the same airspace at the same time. These capabilities are initiated by:

1) Detecting the sUAS within the operating environment of DroneFox

2) Generating a UID number off every sUAS known to be operating in the coalition area and programming those numbers into DroneFox (i.e. whitelisting) so the operator will know which sUAS are "Friend" and which are "Foe"

Proprietary & Confidential. This document is non contractual. Subject to change without notice. Copyright© 2018 WhiteFox. All rights reserved. 190111.

3) Identifying mission critical information about each sUAS through passive SIGINT and data mining of the command & control link. Using forensic analysis to determine inherent safety risk of sUAS and intent of pilot

4) Mitigating the threat by locking out the "threat" pilot and assuming complete control of the sUAS or,

5) Mitigating the threat by overtly or covertly targeting specific command & control functions of the sUAS or,

6) Mitigating the threat by applying a non-jamming and proprietary algorithm that forces a "Loss Link" function of the drone.

CURRENT VERSION

The US Department of Defense (DoD) has established a criterion of eight functions that identify what comprises an effective Counter-sUAS system: Detect, Locate, Identify, Assess, Track, Exploit, Defeat, and Destroy. Depending on the make and model of sUAS, DroneFox is able to provide an operator with elements of seven of the eight primary C-sUAS threat protocols (Detect, Locate, Identify, Assess, Track, Exploit, Defeat) or a combination thereof. DroneFox operator is currently able to Detect, Identify, and Defeat approximately 90% of the commercial sUAS including the ability to Detect, Locate, Identify, Assess, Track, Exploit, and Defeat the most popular sUAS in the world: the DJI Phantom 4. Instead of barrage jamming and disrupting all friendly and non-friendly signals, DroneFox's targeted mitigation technique defeats only the selected sUAS. The mitigation method does not disrupt other communications and allows friendly sUAS to operate. DroneFox provides an operator with mitigation choices to allow for the selection of an appropriate course of action to intelligently mitigating the sUAS threat.

DroneFox has successfully demonstrated the ability to protect an area from threat sUAS out to a distance of over 3km. DroneFox's intuitive and easy-to-use design, combined with superior SIGINT and data mining techniques that allow the operator to see what the likely intent of the sUAS is, and the selective response to safely mitigate the threat, makes DroneFox the only known solution to safely manage a wide range of sUAS threats.

INNOVATION

The WhiteFox team has developed a comprehensive C-sUAS protocol library that encompasses nearly 90% of the worldwide commercial drone market. This library includes the encrypted Lightbridge 2: the most popular drone communication protocol in the world. WhiteFox has been recognized by top government officials within the U.S. Department of Defense and Intelligence Community to be able to demonstrate the ability to passively analyze sUAS RF signals, provide an operator with easy-to-read and mission critical information, and effectively mitigate Lightbridge 2 drones—among others—through non-jamming methods.

As new and different command link protocols and encryptions emerge, WhiteFox adapts to learn best methods of engagement. From PhDs to expert reverse engineers, WhiteFox collaborates to create the program language that allows DroneFox to effectively engage with new and emerging threats, notifying all DroneFox operators when new updates are available.

ADMINISTRATIVE POC

Ryan Hodgens
Director of Business Development
Ryan.Hodgens@WhiteFoxDefense.com || +1 (805) 250-9959

TECHNICAL LEAD

Rich Howe
Vice President of Engineering

Proprietary & Confidential. This document is non contractual. Subject to change without notice. Copyright© 2018 WhiteFox. All rights reserved. 190111.