Counter-Unmanned Aircraft Systems

Technology Guide

September 2019

Homeland Security
Science and Technology

NUSTL®
NATIONAL URBAN SECURITY TECHNOLOGY LABORATORY

Approved for Public Release

CUAS-T-G-1

The *Counter-Unmanned Aircraft Systems Technology Guide* was prepared by the U.S. Department of Homeland Security, Science and Technology Directorate, National Urban Security Technology Laboratory (NUSTL).

Reference herein to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. government.

The information and statements contained herein shall not be used for the purposes of advertising, nor to imply the endorsement or recommendation of the U.S. government.

With respect to documentation contained herein, neither the U.S. government nor any of its employees make any warranty, express or implied, including but not limited to the warranties of merchantability and fitness for a particular purpose. Further, neither the U.S. government nor any of its employees assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed; nor do they represent that its use would not infringe privately owned rights.

--- Warning ---

Federal law prohibits the operation of certain C-UAS technologies described in this Technology Guide. Only the Departments of Homeland Security, Justice, Defense, and Energy have affirmative authority to take C-UAS actions that would normally violate Federal law. This Technology Guide is not intended to opine upon the legal authorities to operate a C-UAS technology. It is strongly recommended that prior to the testing, acquisition, installation, or use of counter-UAS systems that entities seek the advice of counsel experienced with both federal and state criminal, surveillance, and communications laws. **Entities should conduct their own legal and technical analysis of each UAS detection or mitigation system** and should not rely solely on vendors' representations of the systems' legality or functionality. This is particularly important because potential **legal prohibitions are not based on broad classifications of systems (e.g., active versus passive, detection versus mitigation), but instead are based on the functionality of each system**. A thorough understanding of both applicable law and the systems' functionality will ensure that important technologies designed to protect public safety, by detecting or mitigating UAS threats, are used responsibly and legally.

Images included herein were provided by NUSTL, unless otherwise noted.

FOREWORD

The U.S Department of Homeland Security (DHS) Science and Technology Directorate's (S&T) National Urban Security Technology Laboratory (NUSTL) provides testing and evaluation services and products in order to help first responders and DHS components prepare, protect and respond to homeland security threats.

As a federal government-owned, government-operated laboratory, NUSTL provides independent technology evaluations, assessments and technical reports to first responders and DHS components, enabling informed decisions and helping to ensure that responders have the best technology available to use in homeland security missions. As such, NUSTL is positioned as a preferred and trusted partner with first responder government agencies at the federal, state, local and tribal levels.

This Counter-Unmanned Aircraft Systems (C-UAS) Technology Guide is intended to educate the national first responder community on C-UAS technology. In order to explain how C-UAS technologies operate, this guide provides an overview of small unmanned aircraft system technologies, including key components enabling their operation. The information provided in this guide includes technical, scientific and engineering expertise offered by NUSTL as well as information gathered from May to July 2018 from internet research, industry publications and manufacturer data.

The guide is not intended to provide legal advice and makes no comments, evaluation, or assertions concerning the legality of any specific purchase or operations of C-UAS technologies by individual first responders. Congress has only authorized the Departments of Defense, Energy, Justice, and Homeland Security to engage in limited UAS detection and mitigation activities that would otherwise potentially violate applicable federal criminal laws, including laws relating to surveillance. No one else has been granted that authorization. Accordingly, it is important that other federal, state, local, tribal and territorial (SLTT), and private sector entities without such statutory authority (first responders, including SLTT law enforcement, SLTT governments, and owners and operators of critical infrastructure, stadiums, outdoor entertainment venues, and airports, among others) understand that federal law may limit, prohibit, or govern the sale, possession, or use of UAS detection and mitigation capabilities.

For further assistance, refer to the Department of Justice, Homeland Security, and Transportation Legal Advisory.

POINT OF CONTACT

National Urban Security Technology Laboratory
U.S. Department of Homeland Security
Science and Technology Directorate
201 Varick Street
New York, NY 10014

E-mail: NUSTL@hq.dhs.gov
Website: www.dhs.gov/science-and-technology/national-urban-security-technology-laboratory

Authors:
Bhargav Patel, Mechanical Engineer, NUSTL
Dmitri Rizer, Support Contractor, NUSTL

TABLE OF CONTENTS

1.0 Introduction 6
2.0 UAS Technology Overview 7
2.1 UAV Types and Capabilities 8
2.2 UAV Components and Attributes 9
2.2.1 Propulsion System 9
2.2.2 Flight Controller 9
2.2.3 Payloads 9
2.2.4 Telemetry Data 10
2.3 Ground-Based Control System Components 10
2.3.1 Command and Control 11
2.3.2 Communication Protocol 11
2.3.3 Flight Navigation Modes 12
3.0 Counter-UAS Technologies 13
3.1 C-UAS Processing Chain 13
3.2 Types of C-UAS Sensors 15
3.2.1 Radar 16
3.2.2 Passive RF 18
3.2.3 Electro-Optical/Infrared 19
3.2.4 Acoustic 19
3.2.5 Comparison of C-UAS Modalities 20
3.3 Understanding C-UAS Specifications 20
3.3.1 Radar Parameters 20
3.3.2 RF Sensor Parameters 21
3.3.3 EO/IR Sensor Parameters 21
3.3.4 Acoustic Sensor Parameters 22
3.4 C-UAS Mitigation Technologies 22
3.4.1 Electronic 23
3.4.2 Kinetic 24
4.0 References 25
Appendix A. C-UAS Questions For DHS Components A-1
Appendix B. Environmental Considerations For Using C-UAS Technologies B-1
Appendix C. Definition of Acronyms C-1

LIST OF FIGURES

Figure 2-1 Small UAS Components and Attributes 7
Figure 2-2 Examples of Small UAS Types 8
Figure 2-3 Examples of Ground-Based Controllers 10
Figure 3-1 C-UAS Processing Chain 13
Figure 3-2 Alternate C-UAS Processing Chains 15
Figure 3-3 Illustration of Radar Distance Measurement. 16
Figure 3-4 Diagram Showing How a Phase Array Antenna Works 17
Figure 3-5 Radar Target Location Coordinates 17
Figure 3-6 Example of 3-D Radar Antennas 18
Figure 3-7 Example of a Passive RF Detection Sensor 18
Figure 3-8 Rotating EO/IR Camera Mounted on a Tripod 19
Figure 3-9 Example of a Microphone Array 19

LIST OF TABLES

Table 2-1 UAS Capabilities Examples 8
Table 3-1 C-UAS Processing Chain Stages 14
Table 3-2 Comparison of C-UAS Sensor Modalities 20

1.0 INTRODUCTION

The increasing availability, affordability and capability of commercially available unmanned aircraft systems (UAS), colloquially referred to as drones, provides opportunities for legitimate, nuisance and nefarious uses. Legitimate applications include the use of UAS by public safety officials to protect critical infrastructure and gain situational awareness during emergencies, by the entertainment industry for movies and television and by agricultural and other industries for inspections over large areas. Nuisance incidents include hobbyists operating illegally but without malicious intent. Nefarious applications may include unpermitted surveillance, the distribution of contraband or a terrorist attack.

Many UAS-related incidents involve the unintentional misuse, or nuisance case, of UAS and pose higher safety risk rather than security risk. However, intentional UAS misuse can cause safety issues and security concerns. For example, flying a UAS during a wildfire can force response operations to cease due to safety concerns, and flying a UAS over a prison wall or the U.S. border to deliver contraband is a security concern. Terrorist organizations employing UAS are also a threat (Watson, 2017).

This technology guide is intended to provide background information to improve the understanding of the DHS Components and the national first responder community regarding the technologies that are designed to counter UAS use. As counter-unmanned aircraft systems (C-UAS) continue to evolve, the need to better understand the components and operational considerations of this technology will also continue to evolve. This guide is designed to provide basic scientific and engineering information on the types of C-UAS modalities that are commonly employed in C-UAS systems.

This technology guide first includes a brief overview of small UAS and how they operate. Small UAS, i.e., aircraft weighing less than 55 pounds on takeoff, are sometimes abbreviated as sUAS. sUAS are the only type of UAS addressed in this guide. The abbreviation, UAS, which is used throughout this guide, refers specifically to small UAS or sUAS. The UAS overview is included to facilitate understanding of how various modalities of C-UAS technologies work. C-UAS operations are based on exploiting one or more UAS processes and physical attributes, such as radio and sound emissions, or material properties and flight characteristics. Also included is information on specifications or characteristics that are commonly understood for each mode of C-UAS technology to assist in understanding the technological information that may be used by technology manufacturers. Lastly, this guide also includes a list of questions in Appendix A designed for DHS components with authority to conduct C-UAS activities build a more comprehensive understanding of the various modalities employed by specific C-UAS technology solutions.

Reference herein to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise does not constitute or imply endorsement, recommendation, or favoring by the U.S. government. Discussion of C-UAS technology does not imply that these C-UAS capabilities are legal for first responder purchase or use.

2.0 UAS TECHNOLOGY OVERVIEW

Different organizations, agencies and manufacturers often use different terms interchangeably, but for the sake of consistency we will use the Federal Aviation Administration (FAA) definitions throughout, as found in the glossary (CFR Title 14, Part 107.3):

- **Unmanned aircraft**[i] – an "aircraft operated without the possibility of direct human intervention from within or on the aircraft."
- **Small unmanned aircraft** – an "aircraft weighing less than 55 pounds on takeoff, including everything that is on board or otherwise attached to the aircraft."
- **Small unmanned aircraft system** – a "small unmanned aircraft and its associated elements (including communication links and the components that control the small unmanned aircraft) that are required for the safe and efficient operation of the small unmanned aircraft in the national airspace system."

It is useful to think of a UAS in terms of its major components: 1) the aircraft, also called an **unmanned aircraft vehicle (UAV),** and 2) a **ground-based control station (GCS)**, which controls the UAV's flight. A simplified block diagram is shown in Figure 2-1.

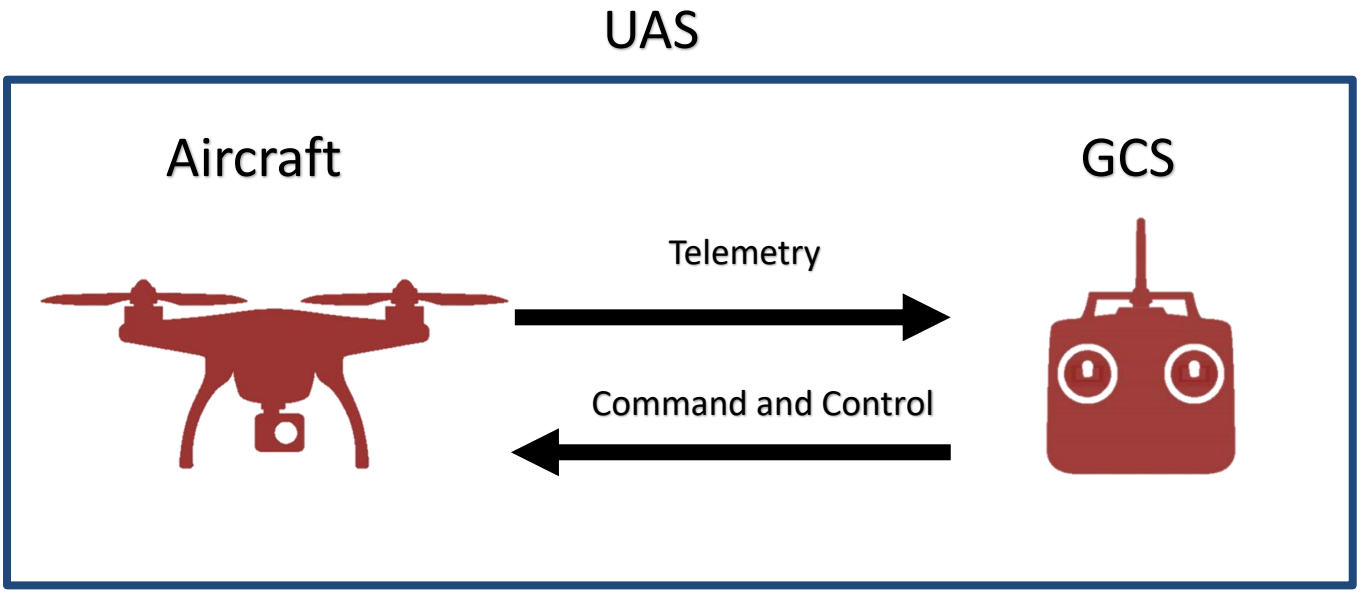


Figure 2-1 Small UAS Components and Attributes

[i] Note that both "aircraft" and "aerial" are used to describe unmanned systems.

2.1 UAV Types and Capabilities

There are two primary types of UAVs: fixed wing and rotocopter, as shown in Figure 2-2. Some UAVs attempt to combine aspects associated with both types; however, these are less prevalent.

- **Fixed wing** UAVs have a motor(s) and propeller(s) to create propulsion in a roughly horizontal direction. The flight path is determined by the manipulation of the flight control surfaces on the wings (i.e., ailerons) and tail (i.e., rudder and elevator).
- **Rotocopters** may have two or more propellers that generate lift in a roughly vertical direction. Rotocopters have no wings and their flight path is determined by independently adjusting the rotation speed of each of their propellers.

Fixed Wing

Rotocopter

Figure 2-2 Examples of Small UAS Types

The available capabilities vary greatly between both types of UAV and makes/models of similar types. Table 2-1 provides examples of capabilities of commercial sUAS, showing approximate data for a range of specifications (e.g., range, speed, flight time, etc.).

Table 2-1 UAS Capabilities Examples

Specification[ii]	Range	Speed	Flight Time	Payload	Altitude
Values	4 to 60 miles	20 to 50 miles per hour (mph)	25 to 120 minutes	0 to 15 pounds	3,300 to 16,000 feet above mean sea level
Examples	DJI Mavic Pro: ~4 miles FlightWave Edge: ~60 miles	Yuneec Breeze: ~20 mph NMS M600: ~50 mph	Parrot Bebop 2: ~25 min FlightWave Edge: ~120 min	DJI Spark: <1 pound DJI S1000: ~15 pounds	Yuneec Q500: ~3,300 feet DJI Mavic Pro: ~16,000 feet

[ii] Table 2-1 provides examples of sUAS capabilities as of July 2018, based on information gathered from a sample of manufacturer websites. Note that the FAA sets operational limitations for UAS flight operations under the Small UAS Rules (Part 107) for specifications such as speed and altitude (FAA sUAS Part 107: The Small UAS Rules).

2.2 UAV Components and Attributes

UAVs can be further deconstructed into many sub-systems and attributes. For the purposes of understanding the capabilities of C-UAS technologies, we will limit this section to just the propulsion system, flight controller, payloads and telemetry data.

2.2.1 Propulsion System

Most small UAVs are propeller driven and powered by one or multiple electric motors. The energy is provided by an on-board rechargeable battery. Small UAVs may also be powered by internal combustion engines, or hybrid gas-electric systems where a generator keeps a battery charged but propulsion is provided by electric motors.

2.2.2 Flight Controller

The flight controller is a small on-board computer that acts as the central hub for directing all inputs and outputs to and from the UAV. Often times the flight controller will include several built-in sensors such as gyroscopes, accelerometers and Global Positioning System (GPS) receivers. The flight controller will direct all operations in the UAV, this includes:

- Managing the amount of power drawn from the battery and power distribution to the various components of the UAV
- Connecting radio frequency (RF) receivers and transmitters (i.e., GPS receivers, command and control (C2) receivers and telemetry transmitters)
- Connecting and operating sensors (i.e., thermal sensors, proximity sensors, etc.) and payloads (i.e., actuators, cameras, etc.)
- Connecting and operating the flight control surfaces (i.e., wings, propellers, etc.) of the UAV.

2.2.3 Payloads

Small UAVs can carry payloads which are additional packages added to the UAV. Payloads may be innocuous, or may be malicious, including:

- Cameras
- Sensors
- Aerosol dispersers
- Medical supplies
- Explosives, chemical, biological or radiological substances, or other weapons
- Hazardous materials
- Radiofrequency transmitters or receivers
- Surveillance equipment
- Other cargo.

Some payloads can be manipulated remotely, for example, the movement and zooming of a camera lens. Many UAS come standard with one or more built-in cameras.

2.2.4 Telemetry Data

Telemetry is the term used to describe information that is transmitted from the UAV to the GCS. This may include:

- Video and audio data
- Battery status
- Altitude
- Speed
- Direction of flight
- Air temperature
- Launch location
- Others.

Telemetry information is generally derived from on-board sensors such as:

- Inertial measurement unit
- Accelerometer
- Gyroscopes
- Temperature sensors
- Cameras
- Infrared sensors
- RF receivers
- Sonar sensors.

2.3 Ground-Based Control System Components

A GCS, or controller, can be a hand controller, laptop, visual display or some combination of these items that transmits commands to a UAV and receives telemetry data from the UAV. The controller facilitates the human interface with the UAS.

Using a controller, a remote operator can control motor power, flight control surfaces, an on-board camera and other sensors wirelessly. Telemetry, UAV status warnings and notifications can be presented to the remote pilot using a built-in or attached display. Examples of GCS are shown in Figure 2-3.

As shown in Figure 2-3, there are two primary attributes that are associated with the GCS: communication protocols and C2.

Figure 2-3 Examples of Ground-Based Controllers

2.3.1 Command and Control

Command and control (commonly called C2) is the term used to describe the set of commands transmitted from the GCS to the UAV, which leads to changes in the operation of the UAV, such as: speed, direction of flight and altitude. C2 transmissions may also be used to manipulate other payloads and sensors on the UAV (e.g., pan, tilt, zoom and record/capture of an on-board camera) or to transition between different types of flight navigation modes.

2.3.2 Communication Protocol

A communication protocol is a system of rules that allows two or more end nodes of a network to exchange information. Communication protocols define the rules, syntax, semantics and synchronization of communication data between two or more nodes. It may also include information about how data should be compressed, encrypted or recovered from data error issues.

For UAS, a protocol defines how the control, telemetry and video data are to be encoded, transmitted and decoded to facilitate communication between the GCS and UAV. Communication between the GCS and UAV may use standard, or proprietary, protocols.

Examples of UAS-specific protocols include but are not limited to:

- Lightbridge
- Ocusync
- MAVlink.

Communication protocols use special formatting methods to determine message structure. Most protocol messages contain three main parts:

- Header: The portion of a data frame that precedes the message data. It usually contains information such as who the sender and receiver are, protocols governing the format of the message and any synchronization information allowing the receiver to adapt the way it should process signals.
- Message Data: Sometimes called the 'payload,' it is the actual message or fragment of a longer message to be transmitted. For example, it can be a command sent from the GCS to the UAV, or a video frame from on-board UAV camera back to the GCS.
- Footer: A portion of the data packet that may contain control and information fields. The footer is often used to verify error-free reception of the information by the receiving device.

Communication protocols are transmitted via a medium. For UAS the medium is the radio spectrum: wireless RF emissions between 3 kHz and 300 GHz in the United States (Office of Spectrum Management, National Telecommunications and information Administration, U.S. Department of Commerce, 2003).

Most consumer UAVs and their GCS use the same radio bands as Wi-Fi compatible devices (2.4 GHz and 5.8 GHz) to both control the UAV and transmit telemetry information from the UAV to the operator. More advanced and hobbyist platforms can be fitted with modems that transmit and receive data at 433 MHz or 915 MHz.

Three of the four radio bands mentioned: 2.4 GHz, 5.8 GHz, and 915 MHz, are part of the industrial, scientific and medical (ISM) radio bands, defined by the Federal Communications Commission (FCC), which do not require licenses for use to transmit (Federal Communications Commission, 2010). The 433 MHz band is considered to be a regulated band in the United States and is generally reserved for amateur radio operators. According to international standards it is also considered to be part of the ISM radio bands (Federal Communications Commission, 2018). These are the most common transmission bands for commercially available UAS, but any other portion of the radio spectrum could theoretically be used in a custom system.

2.3.3 Flight Navigation Modes

The three common flight navigation modes that are used to remotely operate a UAV are:

- **Manual Navigation:** Under the manual navigation mode, the UAV is directly controlled in real time by a remote, human pilot who manipulates joysticks, buttons and/or knobs on a controller. Manual navigation relies on uninterrupted and continuous radio communication between the UAV and controller. Manual navigation can sometimes include first person viewing (FPV), in which a pilot operates the UAV by relying on a live video feed from the UAV in a display mounted on the remote controller or in headset.
- **GPS Navigation:** Many UAVs are equipped with GPS receivers that tell them where they are in space and time. Relying on the GPS system, UAVs can be pre-programmed to fly autonomously to specified locations (also known as waypoints) or use specified flight paths. This navigation mode can be achieved without any radio emissions from the UAV or GCS, although many UAVs may emit a "heartbeat" signal that occasionally transmits telemetry, for safety reasons, back to the controller. This heartbeat function is a safety feature that can be turned off to avoid radio emissions.
- **Autonomous Navigation**: Some UAVs have the capability of navigating using only their own on-board sensors, as opposed to relying on received signals from the GPS system. These sensors can include, but are not limited to: accelerometers, gyroscopes, magnetometers, video cameras and collision avoidance sensors. In this mode, the UAV can follow moving objects or people, fly towards a stationary object at a distance or navigate by dead reckoning. UAVs relying on autonomous navigation may not emit any radio signals and may be entirely unaffected by any impediments in radio signal propagation or interference.

3.0 COUNTER-UAS TECHNOLOGIES

Various technologies exist to counter use of UAS. These technologies, collectively referred to as C-UAS technologies, employ a variety of sensors and processes that account for or exploit the physical components of a UAS and the communications between the UAV and the GCS.

Federal law prohibits the operation of certain C-UAS technologies described in this section of this guide.[iii] Only the Departments of Homeland Security, Justice, Defense, and Energy have received a legislative exception to those Federal laws to conduct C-UAS. This portion of the Technology Guide is intended to provide background information about C-UAS technology, and is not intended to imply that any agencies other than those listed above have the lawful authority to purchase, possess or use such systems. Please consult with an attorney experienced with both federal and state criminal, surveillance, and communications laws. Entities should conduct their own legal and technical analysis of each UAS detection or mitigation system and should not rely solely on vendors' representations of the systems' legality or functionality. This is particularly important because potential legal prohibitions are not based on broad classifications of systems (e.g., active versus passive, detection versus mitigation), but instead are based on the functionality of each system. A thorough understanding of both applicable law and the systems' functionality will ensure that important technologies designed to protect public safety, by detecting or mitigating UAS threats, are used responsibly and legally.

3.1 C-UAS Processing Chain

A C-UAS processing chain (Figure 3-1) is a framework for approaching the potential threat posed by UAS that can be used by technology developers and public safety officials alike. Terms and definitions within this processing chain may be different depending on the audience (e.g., developers, operators and government agencies), and not all C-UAS technologies are able to address all of the activities identified by this processing chain, or in the same manner.

Figure 3-1 C-UAS P

This processing chain and description can be used as a reference to understand how different C-UAS technologies operate. Table 3-1 defines the terms identified in the C-UAS processing chain.

[iii] See generally, Pen/Trap Statute, 18 U.S.C. §§ 3121-3127, Wiretap Act, 18 U.S.C. § 2510; Aircraft Sabotage Act, 18 U.S.C. § 32(a); Computer Fraud and Abuse Act, 18 U.S.C. § 1030; 18 U.S.C. § 1362; 18 U.S.C. § 1367; 47 U.S.C. § 301; 47 U.S.C. § 302a; and 47 U.S.C. § 333.

Table 3-1 C-UAS Processing Chain Stages

Detect	A ***detection*** is a declaration that a UAS is in the presence of a sensor. Some systems, depending on how thresholds are configured, may report any object in its view as a detection (i.e., birds, commercial planes, etc.), or they may attempt to only alert the operator of objects deemed to be considered UAS, based on system capabilities and configuration.
Locate/Track	A ***location*** is a static estimated report or display of where a GCS or UAV is located at a given moment. The display to the operator of the C-UAS technology can take on many forms, e.g., a heat map display, quadrant alert, or circle to indicate estimated center and location error or line of bearing (LOB). A ***track*** is a compilation of location reports over a period of time. Tracks can be displayed for GCS and/or UAVs. Generally, it is displayed as a line or a sequence of dots.
Classify/Identify	*Classification* is the assignment by the C-UAS technology (either autonomously or by an operator) of a potential target UAS to a high-level category such as UAS type, group, manufacturer and/or specific communication protocol. *Identification* is the assignment by the C-UAS technology (either autonomously or by an operator) of a UAS to a more specific name or category, such as physical address of its modem, or the exact make/model of the UAS. Note that the terms, classify and identify, are often used interchangeably, but can have different meanings for different audiences.
Mitigate	*Mitigate* is often used interchangeably with negate, interdict or neutralize. It describes the methods used to remove or reduce the threat posed by a UAS. These methods include technical means, such as RF or GPS jamming, spoofing/hijacking and kinetic attack; however, these technical methods are likely not legal for any entity other than DHS, DOJ, DOD or DOE to conduct. Mitigation may also include any capability or action associated with finding the sUAS operator and having that person safely land the sUAS, which would likely be permissible if the underlying detection system can be lawfully operated with Federal surveillance laws, as well as FCC and FAA regulatory standards and requirements. These methods will be explained in Section 3.4.

Different organizations, technology developers and groups may use different C-UAS processing chains with different definitions. Figure 3-2 illustrates some of the different C-UAS processing chains used by industry and government.

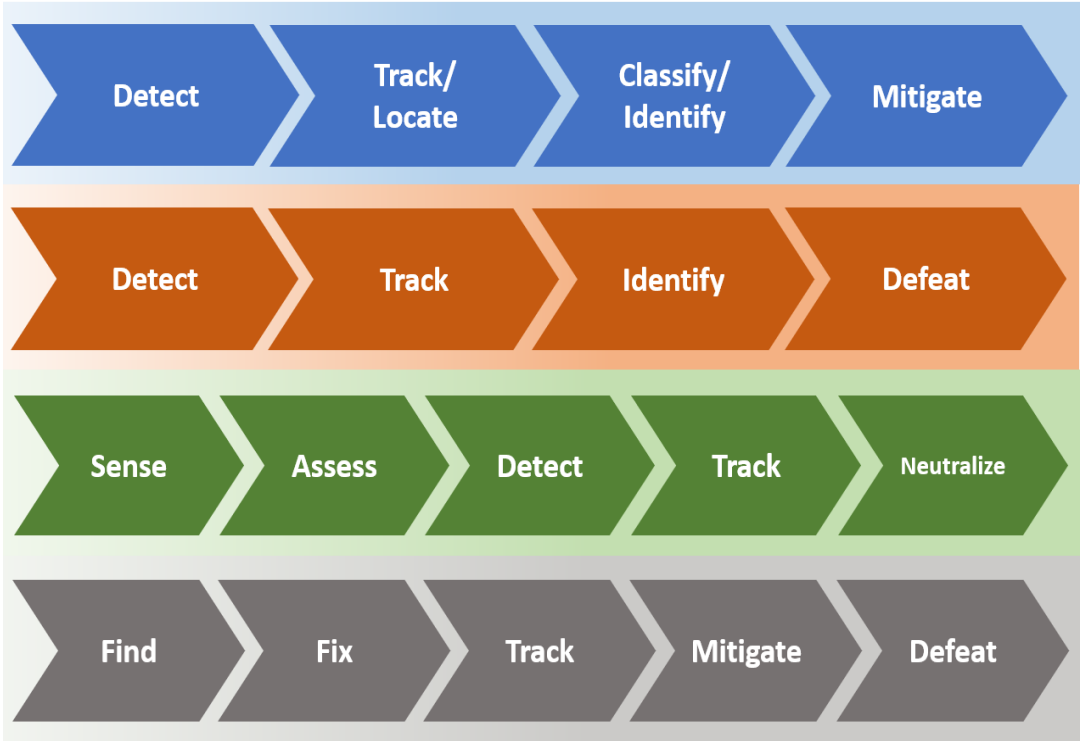


Figure 3-2 Alternate C-UAS Processing Chains

3.2 Types of C-UAS Sensors

There are four modalities (or types) of sensors that are commonly used in C-UAS operations to detect, locate/track and classify/identify UAS. Mitigation activities and methods are covered in Section 3.4. The four common modalities are:

- Radar
- Passive RF (sometimes referred to as electronic surveillance measures (ESM))
- Electro-Optical (EO) and Infrared (IR) cameras
- Acoustic.

Sensor modalities are sometimes described as being either active or passive. A radar is an active sensor, since it transmits radio signals—a type of directed energy—in order to elicit a response from the target of interest. The other sensors typically used in C-UAS technologies are passive, meaning they only receive a stimulus, for example, in the form of radio signals, light, or sound. Some C-UAS technologies use multiple sensor modalities to form an integrated system.

3.2.1 RADAR

Radars operate by transmitting a radio signal of known frequency and power in a focused direction and then detecting the reflected signal that is bounced back from the target. Doppler radars are the most common type of radar used in C-UAS technologies. Doppler radars differentiate the return signal based on a frequency shift from the original transmitted frequency, which allows the radar to dismiss the detection of stationary objects (see Figure 3-3).

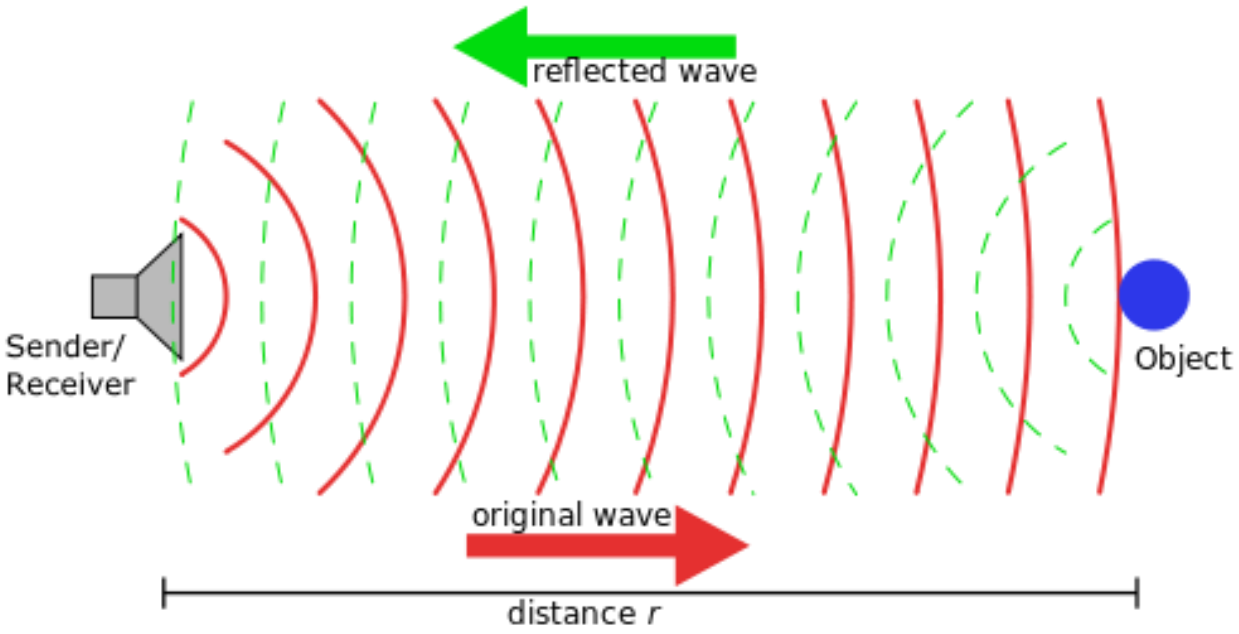


Figure 3-3 Illustration of Radar Distance Measurement.

Image courtesy of Wikimedia (https://commons.wikimedia.org/wiki/File:Sonar_Principle_EN.svg)

Radars can be two dimensional (2D) or three dimensional (3D); 2D radars provide direction and distance to the target, while 3D radars also provide the target's altitude. Two dimensional radars typically use a single antenna that rotates to cover the desired field of view. These radars may provide the UAS's distance from the radar (or the target's range) and its bearing or azimuth (degrees from true North in horizontal plane).

Three dimensional radars use phased array stationary antenna panels with multiple internal antennas (array) on a single panel. This type of radar can change the direction of the RF signal it emits by manipulating the phase of the signal emitted by each of the internal antenna elements–much like focusing a lens on a camera (see Figure 3-4).

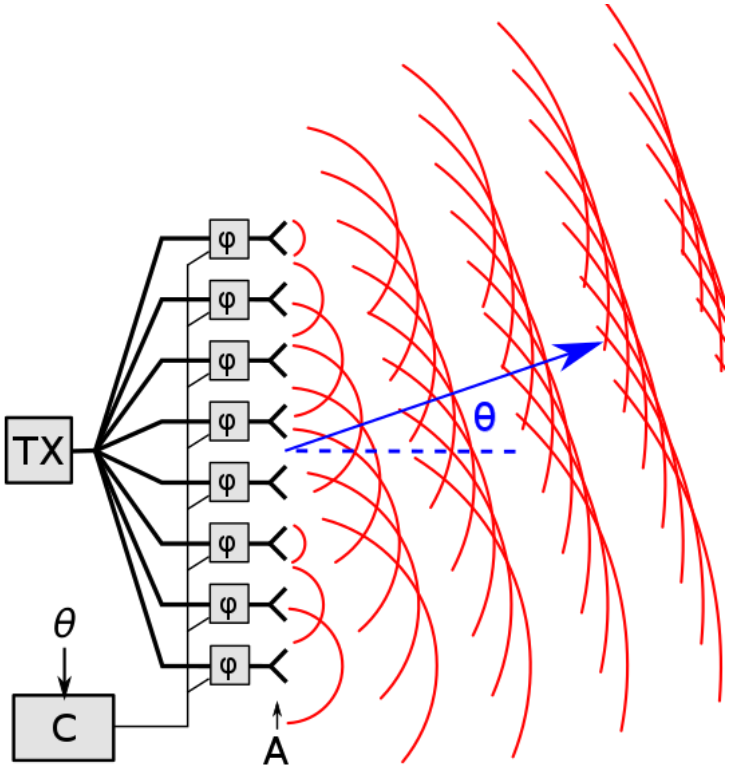


Figure 3-4 Diagram Showing How a Phase Array Antenna Works

Three dimensional radars provide the target's elevation angle in the vertical plane in addition to its range and azimuth. Figure 3-5 depicts target location coordinates for 2D and 3D radars.

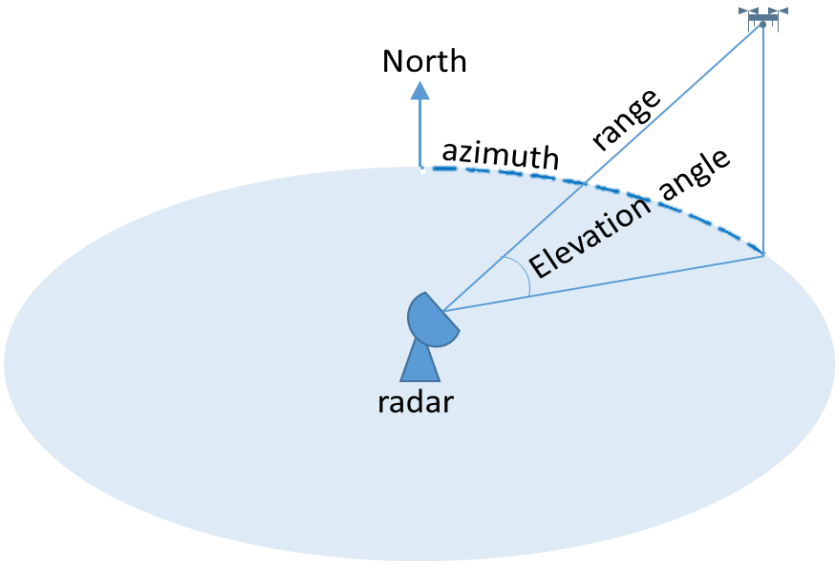


Figure 3-5 Radar Target Location Coordinates

Figure 3-6 shows an example of two 3D radar panels mounted at 90 degrees to each other.

Figure 3-6 Example of 3-D Radar Antennas

3.2.2 Passive RF[iv]

Passive RF sensors rely on antennas to receive, and computers to analyze, RF signals associated with communications between the GCS and the UAV. Systems that use passive RF sensors as their primary sensor are sometimes referred to as ESM. Passive RF sensors analyze the radio signatures and modulations specific to UAS signals and are capable of identifying certain UAS models and manufacturers as well as locating the signal's transmission origin–the UAV and/or the GCS. Most C-UAS that rely primarily on passive RF sensors use libraries of known UAS radio signatures and compare detected signals to those in the library in order to classify or identify UAS. Signature libraries may be periodically updated to include additional UAS signatures and update existing signatures. (WARNING: See footnote iv below). An example of two passive RF detection sensors mounted on a pole is shown in Figure 3-7. Passive RF sensors can employ several different signal processing methods to help locate the source of a UAS associated signal. The more common methods are:

Figure 3-7 Example of a Passive RF Detection Sensor

- Direction Finding (DF)
- Received Signal Strength Indicator (RSSI)
- Time Difference of Arrival (TDOA)
- Frequency Difference of Arrival (FDOA).

[iv] WARNING: The legal analysis and implications of use of any given system are not based on broad classifications of the systems (e.g., active versus passive, detection versus mitigation), but instead are based on the functionality of each system. It is **strongly recommended that prior to the testing, acquisition, installation, or use of counter-UAS systems, including "passive" or "detection-only" systems, that entities fully understand how the system function and seek the advice of counsel experienced with both federal and state criminal, surveillance, and communications laws.**

These methods are explained in greater detail in Section 3.3.2

3.2.3 Electro-Optical/Infrared

EO/IR sensors are digital video cameras that collect environmental information in the visible and infrared light spectrum. This generally incorporates electromagnetic radiation with wavelengths between 400 nanometers and 1 millimeter. IR sensors can be tuned to look specifically at short-wavelength IR, mid-wavelength IR, long-wavelength IR or a combination of the above. See Section 3.3.3 for additional information and uses of different IR bands. When EO/IR sensors are placed on a rotating gimbal and paired with analysis software, these systems are capable of providing wide-area coverage by acquiring and processing real-time full panoramic images. Furthermore, some of these systems are capable of automatically detecting and tracking UAS targets when paired with the appropriate analysis software.

Figure 3-8 Rotating EO/IR Camera Mounted on a Tripod

Some systems use multiple fixed cameras aimed at different angles to provide wide-area coverage. EO/IR sensors are completely passive and are able to detect non-emitting (RF silent) UAS. Some EO/IR sensors are also able to classify and identify UAS. EO/IR camera sensors are often used as secondary sensors, which are cued by location reports from another sensor such as radar or a passive RF antenna.

Figure 3-8 illustrates an example of an EO/IR camera sensor mounted on a rotating gimbal to achieve greater area coverage than is available with a fixed camera.

3.2.4 Acoustic

Acoustic sensors are passive and use high sensitivity microphone arrays coupled with audio analysis applications to detect, track and identify sounds produced by UAV motors and propellers. The spinning of different types of UAV propellers produce unique acoustic patterns, which makes it possible to create a library of these acoustic signatures to identify different types of UAV and determine the general direction of the sound source.

Using triangulation methods with multiple spatially separated microphone stations, the approximate location of a UAV can be determined. An example of a microphone array is shown in Figure 3-9.

Figure 3-9 Example of a Microphone Array

By analyzing the Doppler-induced frequency shift of the source signal over a period of time, some C-UAS may be able to report the approximate speed and direction of the sound source. High levels of sound pollution, like those in urban environments, can degrade the performance of C-UAS that rely on acoustic sensors. Acoustic sensors are ideally employed to “quiet” remote locations such as rural prisons or for border protection applications.

3.2.5 Comparison of C-UAS Modalities

The sensor modalities mentioned in Section 3.2 offer different capabilities, which can vary greatly under different operational environments. These are briefly summarized in Table 3-2. Some sensor modalities require direct line of sight (LOS) to the target to operate reliably, as shown in the table. Additional operational limitations are described in Appendix C.

Table 3-2 Comparison of C-UAS Sensor Modalities

Modality	Active/ Passive	Can Detect		Locate/Track		Identify/ Classify	Need LOS	Affected by Weather	Night-Time Operation
		UAV	GCS	UAV	GCS				
Radar	Active	Yes	No	Yes	No	Limited	Yes	No	Yes
EO	Passive	Yes	No	Yes	No	Limited	Yes	Yes	No
IR	Passive	Yes	No	Yes	No	Limited	Yes	No	Yes
RF	Passive	Yes	Yes	Yes	Yes	Yes	Preferred	No	Yes
Acoustic	Passive	Yes	No	Yes	No	Limited	Preferred	Yes	Yes

3.3 Understanding C-UAS Specifications

Manufacturers of C-UAS technology publish technical specifications of their systems' capabilities. This section is intended to provide an understanding of key parameters usually included in these specifications. Examples of C-UAS technology specifications are grouped by the four system modalities listed in Section 3.2. Mitigation capabilities are not covered in this section.

3.3.1 Radar Parameters

Detection Range. Detection range for radars describes the straight line distance at which a radar system can detect a UAV. This specification is often provided in meters, kilometers or miles. The material, size and type of UAV can cause this distance to vary even under similar environmental conditions. Manufacturer specifications for detection range are usually under ideal circumstances. They should be verified with real world testing to ensure they meet agency requirements.

Field of Regard. At any given instant, radars emit a relatively narrow beam of radio energy. In order to scan a wide area of interest (up to 360 degrees), radar antennas can be mechanically rotated or electronically steered. When choosing a radar, it is important to understand how the type of radar employed relates to the area covered, both in the horizontal and vertical plane. Field of regard describes the total area captured by the radar sensor after it has completed its mechanical rotations or electronically steered scans.

Frequency Bandwidth. Radars are active sensors that transmit electromagnetic energy across a specific range of frequencies. This parameter is often specified in hertz or by the Institute of Electrical and Electronics Engineers (IEEE) Standard Letter Designation (521-2002 - IEEE Standard Letter Designations for Radar-Frequency Bands , 2003).

Scan Rate. Defines how fast a radar can scan an entire area of interest (usually 360 degrees), specified in hertz (Hz). For example, 2 Hz means it scans the area twice every second.

Transmit Power. The amount of radio energy transmitted by a radar antenna every second. It is measured in watts (W) and can be as high as several hundred watts. Safe standoff distance is highly dependent on specific radar transmission parameters, such as transmit power, and is usually specified by the manufacturer.

3.3.2 RF Sensor Parameters

Detection Range. Many factors affect RF sensor detection range. These include terrain, LOS to the target or lack of it, RF interference environment and RF reflecting surfaces (e.g., buildings creating multipath). Because of these complications, vendors usually specify detection range as a measure of distance under ideal conditions.

Radio Frequencies. C-UAS RF sensors aim to scan all the frequencies commonly utilized by UAS. This includes but is not limited to 433 MHz, 915 MHz, 2.4 GHz and 5.8 GHz. Some C-UAS sensors are programmable to cover any frequency band from 20 MHz to 6 GHz.

Direction Finding. Most single site RF sensors are capable of determining the approximate direction from which the target signal was received. This is specified in azimuth degrees referenced to true north. The accuracy of this indication is also specified in degrees as a window. For example, ±5 degrees accuracy means that the target source can be anywhere in the specified direction ±5 degrees.

Geolocation. When two or more RF sensors are setup at different locations within the area of interest, it allows for approximate location in two or more dimensions, as opposed to just the direction of the target UAV and/or GCS. There are different ways that a system may display this information, for example, two or more intersecting lines of bearing, a marker on a map, a circle on a map, a heat map with varying color gradients, etc.

Classification. Using a library of stored unique radio signal signatures, many RF C-UAS sensors are capable of determining the manufacturer and sometimes the model of the target UAS. These UAS signatures are updated by C-UAS manufacturers to keep their systems up to date.

3.3.3 EO/IR Sensor Parameters

Detection Range. Detection range is the reported distance that an EO/IR camera is capable of reporting a detection to the operator of a UAV. It can also be interpreted as the distance at which the operator can reasonably discern a UAV from other unidentified flying objects or the furthest distance that integrated video analytics software is able to classify an object as a UAV.

Field Of View (FOV). Field of view is a term used to describe the limits in both the vertical and horizontal direction that an EO/IR sensor is able to see in a single instance. This parameter is often specified in degrees for horizontal and vertical planes. Some manufacturers may mount EO/IR cameras on a rotating platform and report a horizontal field of view of 360 degrees.

Scan Rate. Scan rate describes how fast an FOV can be scanned. This parameter is often reported in either degrees per second or hertz if the system is designed to complete full 360-degree rotations.

Image Resolution. This parameter specifies how much fine detail an image has. Image resolution is often reported as width in pixels by height in pixels. For example, 1280 x 720 means the width of an image contains 1280 pixels and the height of the image contains 720 pixels.

3.3.4 Acoustic Sensor Parameters

Detection Range. This is the reported straight line distance that an acoustic signature should be able to detect a UAV. This parameter may often represent ideal conditions (e.g., a very loud UAV operating in a very quiet environment).

Direction Finding. Similar to RF sensors, acoustic sensors are capable of determining approximate direction of a target sound source. This is specified in azimuth degrees referenced to true north and includes a direction window of ±x degrees.

Geolocation. When two or more acoustic sensors are set up at different locations within the area of interest, it allows for approximate location in two or more dimensions, as opposed to just the direction, of the target UAV. There are different ways that a system may display this information, for example, two or more intersecting lines of bearing, a marker on a map, a circle on a map, a heat map with varying color gradients, etc.

Classification. Using stored unique UAV sound signatures, some acoustic C-UAS sensors are capable of determining the manufacturer and sometimes the model or type of the target UAV.

3.4 C-UAS Mitigation Technologies

As mentioned earlier, mitigation of a threat UAV is not explicitly tied to the techniques mentioned below. Mitigation can also be achieved through finding the UAV operator's location and having that person cease their operation. Employing a system of systems, i.e., multiple detection techniques as well as mitigation technology, as authorized, is likely the most effective strategy to increasing the likelihood of countering any given threat. The following sections describe actions and techniques that are currently prohibited to any agency or entity other than by the Departments of Homeland Security, Justice, Defense, and Energy.

There are two major categories of mitigation techniques:

- Electronic
- Kinetic.

3.4.1 ELECTRONIC

C-UAS mitigation technologies that emit RF signals to jam, interfere with or masquerade as legitimate UAS signals are forms of electronic mitigation.

Some mitigation methods attempt to interfere with the communication between the UAV and GCS, while others attempt to interfere with communication between the UAV and the Global Navigation Satellite System (GNSS).[v]

RF and GNSS Jamming[vi]

RF jamming is when a C-UAS technology aims to neutralize or mitigate a threat UAS by disrupting the RF link (C2 and/or telemetry) between the GCS and UAV. UAS frequencies are emitted from an RF jamming antenna at greater power levels, flooding that frequency bandwidth and preventing actual UAS signals from being received. When a UAS C2 connection is severed or jammed, UAVs often respond according to their pre-programming by:

- Hovering in place
- Attempting to land in place
- Attempting to return home to their original launch location
- Moving to a user-specified location.

GNSS jammers disrupt the UAV's ability to receive spatial and temporal information from these satellite systems. UAVs that lose their satellite link often respond by:

- Hovering in place
- Landing in place at the moment of signal loss
- Attempting to return to their original launch location, if they have other means of orienting themselves in space.

Both RF jammers and GNSS jammers can come in two variants: directional and omni-directional. Directional jammers radiate RF signals in a more focused manner such that the operator can point the jammer in the direction of their intended target. Omni-directional jammers are less discriminate and radiate RF signals in all directions.

(WARNING: See footnote vi below.)

Spoofing

In reference to C-UAS mitigation capabilities, spoofing is sometimes used interchangeably with the term cyber-attacking. It is the exploitation of a weakness or bug in the communication protocol between the GCS and UAV that allows C-UAS technology to potentially take control of a target UAV and/or interfere with its ability to function properly.

---

[v] GNSS is the inclusive term that captures a variety of satellite positioning systems such as, but not limited to GPS, GLONASS, Galileo, and Beidou.

[vi] WARNING: This Technology Guide is intended to provide background information about C-UAS technology, and is not intended to imply that any entity other than the Departments of Homeland Security, Defense, Energy, and Justice have the lawful authority to purchase, possess or use such systems. It is **strongly recommended that prior to the testing, acquisition, installation, or use of counter-UAS systems, that entities consult with an attorney experienced with both federal and state criminal, surveillance, and communications laws.**

There are two methods of spoofing: a man-in-the middle spoofing attack and a GNSS spoofing attack. (WARNING: See footnote vi above.)

A man-in-the-middle spoofing attack operates so that a C-UAS technology is able to receive and/or transmit information that was intended for a UAV or controller by masquerading itself as a legitimate UAS source.

This is commonly achieved through the exploitation of a weakness or a bug in the UAS communication protocol. The C-UAS technology then has the option to potentially:

- Obtain sensitive data from the UAS
- "Eavesdrop" in real-time on both the UAV and controller
- Send C2 inputs to the UAV
- Augment reported telemetry information from the UAV.

A GNSS spoofing attack attempts to mislead the UAV's GNSS receiver by broadcasting fake GNSS signals while pretending to be a legitimate GNSS signal sent by satellites.

To achieve this, the C-UAS technology overpowers the GNSS satellite's RF signals. By injecting fake location signals, the C-UAS is able to mislead the UAV off course.

3.4.2 KINETIC[vii]

Kinetic mitigation techniques often involve some direct physical action for removing or reducing the risk posed by the UAS. More often than not, kinetic mitigation is directed at the UAV in flight as opposed to the ground controller and operator. (WARNING: See footnote vii below.)

Net guns and specialized projectile devices typically shoot a net at the UAV in an effort to entangle the propellers and bring the UAV down. Net guns may look similar to conventional small arms. Specialized projectiles may also be designed to be shot from conventional fire arms such as a rifle.

Laser weapons and high power microwaves use the highly directional nature of these light and radio beam sources to physically damage or destroy the UAV (in the case of laser) or physically damage or destroy the UAV's electronic circuits (in the case of microwave). In both cases large amounts of electromagnetic energy are focused into a narrow beam and directed at the target UAV. These mitigation technologies are primarily in use by the military, and not readily available to other Federal Departments.

Another kinetic mitigation system involves the use of UAS to counter other UAS; that is, large UAVs with nets are used to entangle and capture smaller UAVs.

Use of birds of prey such as eagles and hawks has also been explored for use as kinetic mitigation techniques. In the Netherlands, birds of prey were trained to capture a target UAV in flight and bring it to the trainer (Dutch police fight drones with eagles., 2016).

[vii] WARNING: This Technology Guide is intended to provide background information about C-UAS technology, and is not intended to imply that any entity other than the Departments of Homeland Security, Defense, Energy, and Justice have the lawful authority to purchase, possess or use such systems. It is **strongly recommended that prior to the testing, acquisition, installation, or use of counter-UAS systems, that entities consult with an attorney experienced with both federal and state criminal, surveillance, and communications laws.**

4.0 REFERENCES

521-2002 - IEEE Standard Letter Designations for Radar-Frequency Bands . (2003). Retrieved from IEEE Xplorer Digital Library: https://ieeexplore.ieee.org/document/1160089

CFR Title 14, Part 107.3. (n.d.). Retrieved from Electronic Code of Federal Regulations e-CFR. https://ecfr.io/Title-14/pt14.2.107

DHS/S&T/PEO-UAS. (2017, February 24). *Solicitation: PEO_UAS2017_1.* Retrieved from Federal Business Opportunities: https://www.fbo.gov/spg/DHS/OCPO/DHS-OCPO/PEO_UAS2017_1/listing.html

Dutch police fight drones with eagles. (2016, September 12). Retrieved from BBC News: https://www.bbc.com/news/world-europe-37342695

FAA sUAS Part 107: The Small UAS Rules. (n.d.). Retrieved from Unmanned Aircraft Systems: https://www.faa.gov/uas/media/faa-uas-part107-flyer.pdf

Federal Communications Commission. (2010). *FCC Title 47, Part 15, Subpart C.* Retrieved from Government Publishing Office: https://www.gpo.gov/fdsys/pkg/CFR-2010-title47-vol1/pdf/CFR-2010-title47-vol1-part15.pdf

Federal Communications Commission. (2018, October 5). *Federal Communications Commission Office of Engineering and Technology*. Retrieved from FCC Online Table of Frequency Allocations - 47 C.F.R. § 2.106: https://transition.fcc.gov/oet/spectrum/table/fcctable.pdf

Office of Spectrum Management, National Telecommunications and information Administration, U.S. Department of Commerce. (2003, October). *U.S. Frequency Allocation Chart*. Retrieved from National Telecommunications and information Administration: https://www.ntia.doc.gov/files/ntia/publications/2003-allochrt.pdf

Watson, B. (2017, January 12). *The Drones of ISIS*. Retrieved from Defense One: https://www.defenseone.com/technology/2017/01/drones-isis/134542/

Appendix A. C-UAS Questions For DHS Components

This appendix is a list of questions can that be used to help the Department of Homeland Security Components, and other entities with C-UAS authority, build a more comprehensive understanding of the nuances, capabilities and limitations of counter-unmanned aircraft system (C-UAS) technologies. These questions do not address legal authorities to operate a C-UAS technology and DHS or other federal partners with C-UAS authority must follow the appropriate guidance, policies and rules regarding the actual operation of C-UAS capabilities.

General C-UAS

- What types of unmanned aircraft systems (UAS) will your system detect? What types will it not detect? Will it also detect the ground control station and provide its location?
- How many different sensor modalities (i.e., radar, electro-optical/infrared, passive radio frequency (RF), acoustic) does the C-UAS technology have?
- Do any of the sensor modalities serve as the primary sensor type for detection that cues or activates a secondary or tertiary sensor?
- Is the C-UAS technology stationary (fixed to a specific site) or mobile (can easily be moved from site to site)?
    - Can the mobile system be used while moving (e.g., mounted on a vehicle)?
- How many people does it require to set-up and deploy the C-UAS at a new site?
- How long does it take to set up the system?
- What are the calibration requirements for the C-UAS technology?
- What training (type and time) is required to become a novice user? Proficient user? Advanced user?
- What is the required operator workload?
    - Does the C-UAS technology require constant monitoring/human interaction?
    - How well does your system separate UAS from birds, cars, people, etc.?
    - How does it do that? Is it automatic?
- Does the system have an open application programming interface (API) that allows end-users or third party vendors to:
    - Develop new software features, interfaces and capabilities?
    - Add additional sensors or mitigation capabilities?
- Does the system have a mitigation capability? If so, which method best describes how the mitigation capability works?
    - RF broadband jamming: flooding certain frequencies of interest with RF emissions at high power levels?
    - Spoofing: taking advantage of vulnerabilities in the communication protocol, UAS software or UAS hardware to take over, hijack or disrupt UAS operations?

    - Kinetic attack: physically disrupting UAS operations (nets, projectiles, lasers)?
- Is there any portion of the system that reads and interprets any part of the messages between the UAS and the ground controller?
- Is there any portion of the system that transmits messages to the UAS or attempts to jam its communications?
- How does the graphical user interface (GUI) alert the operator to the following:
    - Detection of a UAS aircraft and/or ground controller?
    - Location/track of a UAS aircraft and/or ground controller?
    - Identification or classification of the UAS (Is it a UAS? What kind?)?
    - For desired modifications, can a user or another vendor make them?
- How does the system handle multiple detections at the same time?
- How is maintenance and updating of the system done and what is the cost for updates?
- Do you have any test results for the environment in which I am interested?
- Is there any safety issue or "keep out zone" for your system?

Radar Sensor

- What bandwidth and power levels does the radar emit?
- What certifications does the radar have?
- Is it a single antenna rotating radar or a phased array/multi-panel stationary radar?
- What is the radar's azimuth field of regard? For example, a single radar panel may only cover a 90-degree field of regard, requiring four panels to get a full 360-degree coverage of a protected site.
- What is the radar's elevation field of regard? For example, a radar with a very narrow elevation field of regard would be unable to detect threats at very high or very low altitudes.
- How does the radar discern signal (UAS) from noise (birds, planes, ground traffic, etc.)?
- What is the maximum range of detection?
- How long does a UAS need to be within the radar's line of sight to be accurately reported as a UAS?
- What is the relationship between the probability of detection and distance from sensor to the target?
- What are the safe standoff distances when the radar is active?

Passive Radio Frequency Sensor

- What UAS RF signatures and communication protocols are currently part of the detection library? What is missing from the current library?
- How would the library of fielded equipment be updated to include new UAS of concern?
- Are end users provided with a method and means of updating their own library should a custom UAS be seized?
- What is the rate of library updates since the product has been on the market (e.g., once a month, once a week)?
- Does the system have a "white-listing" capability allowing it to recognize known UAS approved for operating in the area?
- What is the estimated error associated with the reported line of bearing (e.g., 2 degrees, 5 degrees)?
    - What type of conditions affect that error?
- Beyond line-of-bearing, does the system also report on estimated range/distance of the UAS?
- Under ideal operating conditions (i.e., open field with low RF background noise), what is:
    - The maximum distance for detecting a UAS and providing a line-of-bearing?
    - The maximum distance a UAS can be from the C-UAS and still be classified/identified as a UAS?
- What is the noisiest RF environment in which the system has been used or operated?
    - What effect did that environment have on detection, location and classification?
- How long does a UAS signal need to be received by the C-UAS for it to accurately report a UAS (e.g., in urban environments there may be very short periods of line of sight exposure to a UAS or ground controller, on the order of 2 to 5 seconds)?
- Will multiple antennas provide triangulation/geolocation of the UAS/ground controller?
    - If yes, is it simply a plug-and-play upgrade or is there additional configuration needed?
- What is the relationship between the probability of detection and distance between sensor and the target?

Electro-Optical/Infrared Sensor

- What is the camera's azimuth field of regard?
- What is the camera's elevation field of regard?
- How does the camera discern signal (UAS) from noise (birds, planes, ground traffic, etc.)?
- What is the maximum range of detection?
- How long does a UAS need to be within the camera's line of sight to be accurately reported as a UAS?
- What is the probability of detection (as a function of range)?

Acoustic Sensors

- Which UAS acoustic signatures are in the detection library? Which are missing?
- How would the library of fielded equipment be updated to include new UAS of concern?
- Under ideal operating conditions (i.e., open field with low noise background) what is:
    - The maximum range for detecting a UAS? Providing a location or track?
    - The maximum distance a UAS can be from the sensor and still be classified/identified as a UAS?
- What is the noisiest environment the system has operated in?
    - What effect did that environment have on detection, location and classification?

Appendix B. Environmental Considerations For Using C-UAS Technologies

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

Line of Sight: Line-of-sight describes the environmental situation between two nodes or points of interest when there are no visual obstructions or barriers between them. C-UAS technologies perform optimally when there is clear and direct line of sight between the C-UAS sensor(s) and the target(s) of interest (unmanned aircraft vehicle (UAV) or ground controller). Some C-UAS sensors can continue to report useful information to an operator even when there is no line of sight, but generally the overall performance is degraded. For example, the range at which UAS detections can occur may diminish, or location reports may become less accurate and precise.

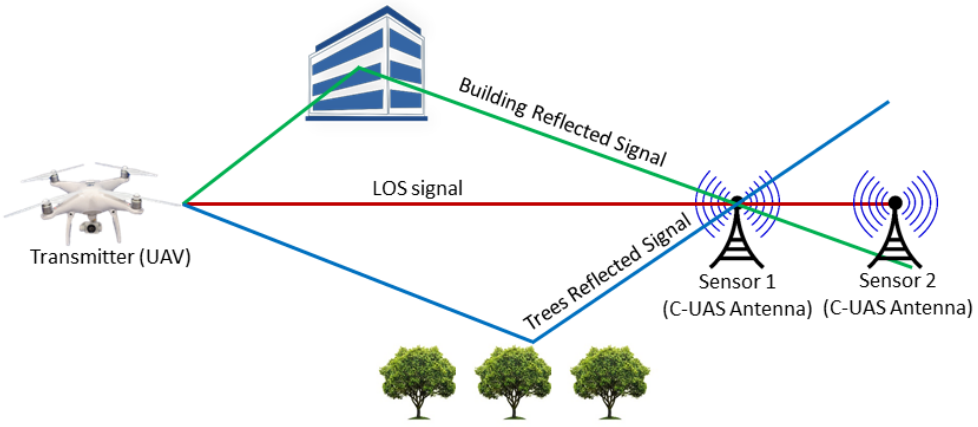
Radio signal multipath propagation: Radio signals emitted by a transmitter (e.g., a UAV) spread in the environment at the speed of light. Just like light, radio signals can be partially reflected or absorbed when encountering obstacles such as buildings, trees, hills and mountains.

An open space environment that is free of obstacles and other radio signal sources is the ideal environment for radio signal propagation and reception, though that is seldom the case. In real-world, geometrically complex environments such as urban areas, a UAS radio signal can travel along many different paths, reflecting off different surfaces before it reaches a C-UAS sensor or receiver.

If a C-UAS sensor relies on an RF signal that was reflected from a surface, as opposed to an unobstructed signal, it can introduce uncertainty to reports on the signal source's location or direction. This uncertainty arises from the fact that the reflected signal has likely travelled a longer distance, and therefore taken longer to reach the C-UAS sensor.

Reflected signals carry less energy than an unobstructed signal. Reflected signals may not be powerful enough to be detected by a C-UAS sensor, especially in an environment like a city where there is a lot of RF noise.

The below figure is an example of how a signal transmitted by a UAV may be reflected and arrive at sensor 1 via multiple paths. Like an echo, reflected and line of sight paths will result in different arrival times at sensor 1 due to distance variations in each path. Also shown nearby is sensor 2, which does not "see" the reflections in this example but does receive the unobstructed signal from the UAV.



Appendix C. Definition of Acronyms

C2	Command and Control. As it relates to UAS, C2 is a hardware and software subsystem that permits transmittal of instructions from the GCS to the UAV, which generally lead to changes in the operation of the UAV.
C-UAS	Counter-Unmanned Aircraft Systems. A sophisticated single, or combination, of systems designed to detect, track, identify and/or mitigate small UAS, perceived as a threat.
EO/IR	Electro-Optical/Infrared. EO/IR sensors are electronic detectors that convert images of visible light and infrared light into electronic signals, allowing processing of such images by computers using sophisticated algorithms.
ESM	Electronic Surveillance Measures. A technology method that uses RF receivers to passively listen and process radio signals of interest within its range. ESM systems are receive-only and do not transmit out.
FAA	Federal Aviation Administration. A national authority with powers to regulate all aspects of civil aviation. These include the construction and operation of airports, air traffic management, the certification of personnel and UAV and the protection of U.S. assets during the launch or re-entry of commercial space vehicles.
FCC	Federal Communications Commission. An independent agency of the U.S. government created to regulate interstate communications by radio, television, wire, satellite and cable.
FDOA	Frequency Difference of Arrival. A technique for estimating the location of a moving radio emitter based on Doppler frequency shift observed from multiple location points. The FDOA emitter target must be in relative motion with respect to each observation point. Time Difference of Arrival (TDOA) and FDOA are sometimes used together to improve location accuracy.
FPV	First Person View. FPV refers to a style of controlling a UAV in flight where one views the world through a camera fitted onto the UAV and uses that ‘first person’ perspective to control the UAV.
GCS	Ground-Based Control System. A land or sea-based control center that provides the facilities for human control of a UAV. For small UAVs, GCS may be based on a laptop, tablet and/or dedicated remote control unit.
GHz	Gigahertz. A unit of measure for a number of cycles per second (frequency) where 1 GHz equals a billion cycles per second. In the context of UAS, GHz is used to describe frequency bands of the radio spectrum used for UAS communications or control.
GNSS	Global Navigation Satellite System. The standard generic term for satellite navigation systems that provide autonomous geo-spatial positioning with global coverage. Common types of GNSS include GPS, GLONASS, Galileo, Beidou and other regional systems.
GPS	Global Positioning System. Originally Navstar GPS, it is a satellite-based radio navigation system owned by the U.S. government and operated by the U.S. Air Force. Using signals from multiple satellites positioned around the world, a receiver and algorithms provide location, velocity and time synchronization for air, sea and land objects.

ISM	Industrial, Scientific and Medical. ISM refers to a group of radio bands (frequencies) or parts of the radio spectrum that are internationally reserved for the use of RF energy intended for scientific, medical and industrial requirements. In the United States, this usually includes 433 MHz, 915 MHz, 1.2 GHz, 2.4 GHz and 5.8 GHz bands.
LOB	Line of Bearing. For C-UAS, LOB is a direction in degrees from true north where a potential UAV and/or GCS target is being detected. It is usually displayed in the shape of a wedge of varying width with its origin in the location of the system detecting the target.
MHz	Megahertz. A unit of measure for a number of cycles per second (frequency) where 1 MHz equals a million cycles per second. In the context of UAS, MHz is used to describe frequency bands of the radio spectrum used for UAS communications or control.
RF	Radio Frequency. RF refers to oscillatory change in a circuit, waveguide or transmission line in the range from around 20,000 times per second (20 kHz) to around 300 billion times per second (300 GHz), roughly between the upper limit of audio and the lower limit of infrared light. Under certain conditions, RF become radio waves of electromagnetic radiation. These waves can propagate at the speed of light, over large distances and through various materials, air and even the vacuum of space.
RSSI	Received Signal Strength Indicator. A measurement of the power or energy present in a received radio signal, measured in milliwatts or decibels, which are referenced to 1 milliwatt.
sUAS	Small Unmanned Aircraft System. These are systems with UAVs weighing less than 55 pounds at take-off. These UAVs are propeller driven, powered by one or multiple electric motors and use an on-board rechargeable battery.
TDOA	Time Difference of Arrival. A method to accurately locate a UAV, GCS or a radio wave emitter by measuring the TDOA of a signal from the emitter at three or more time-synchronized receiver sites or conversely, the signals from three or more time-synchronized emitters at one receiver location (navigation application, e.g., GPS).
UAS	Unmanned Aircraft Systems. UAS refers to the systems and components that allow for the remotely controlled or autonomous flights of UAV vehicles. UAS includes a UAV, a GCS and a system of communications between the two.
UAV	Unmanned Aerial Vehicle. Also referred to as a drone, a UAV is an aircraft without an onboard human pilot that can fly either by remote control from a human operator or autonomously using onboard sensors. UAVs are a component of a UAS, which also includes a GCS and a system of communications.
VTOL	Vertical Take-Off and Landing. VTOL refers to a UAV that can hover, take off and land vertically. This classification can include types of UAV such as fixed-wing, helicopters and other UAV with powered rotors.