SANDIA REPORT
SAND2019-2801
Printed March 2019

Sandia National Laboratories

Counter-Unmanned Aircraft Systems Market Survey

Scott Brooks; Carol Jacobus; Camron Kouhestani; John Stikar; Erik Faye

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico
87185 and Livermore,
California 94550

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology & Engineering Solutions of Sandia, LLC.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone:	(865) 576-8401
Facsimile:	(865) 576-5728
E-Mail:	reports@osti.gov
Online ordering:	http://www.osti.gov/scitech

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone:	(800) 553-6847
Facsimile:	(703) 605-6900
E-Mail:	orders@ntis.gov
Online order:	https://classic.ntis.gov/help/order-methods/

ABSTRACT

More than 300 counter-unmanned aircraft system (CUAS) products were identified in our market survey by reviewing and comparing existing market surveys and reports, academic and commercial compilations, CUAS demonstration event reports, and other documents. Of these, Sandia collected technical data on more than 200 of these products through a combination of manual research and a request for information posted to www.fbo.gov. Technical product information has been compiled into a database that can be filtered by key technical characteristics to find products that match high-level requirements. The CUAS market is shifting from an emerging to a growth industry. Many companies are partnering or collaborating with peers to combine benefits from their core strengths and technologies into more complete solutions. These companies want to know the government's CUAS requirements, so they can design and deliver a product tailored to the application space or requirements.

ACKNOWLEDGMENTS

- Tim Bennett and Shane Cullen, program leads at DHS S&T, for guidance, funding, and foresight to conduct a market survey and compile a database of technical data
- Carol Jacobus and the Sandia National Laboratories Business and Competitive Intelligence research department, whose expertise and capabilities were critical to the success of the research
- John Stikar and Erik Faye, technical writers at Atkins Global Nuclear Solutions, for compiling the survey data and assistance with the report

CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

The U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T) asked Sandia National Laboratories (Sandia) to survey the Counter-UAS (CUAS) market and compile information that could be used to facilitate selection of technologies for testing, acquisition and deployment. This report summarizes the results of that work and includes a compendium or listing of identified CUAS products, with technical data collected on as many of those as possible within the timeframe of the study. The database of products and their technical characteristics is stored on the Sandia External Collaboration Network for download by authorized DHS S&T personnel. This information may help component agencies of the DHS identify potential candidate CUAS products for further consideration and evaluation in support of agency missions related to CUAS deployment.

The market survey was conducted over an approximately two-month period starting in late 2018. This work should be revisited in the future to refine and update the information in keeping with rapidly evolving technologies and their integration into COTS products. Key takeaways include the following points:

- Approximately 316 CUAS products were identified from 195 manufacturers
- Sandia was able to collect technical data on approximately 223 of those products. Technical data was collected through manual research for 150 of those products, and through responses to an RFI posted to www.fbo.gov for 91 products (some companies responded to both our manual research as well as the RFI).
- Products were identified from 35 countries. The top countries represented are the US (39%), the UK (10%) and Israel (6%). The survey prioritized collection of technical data on US-based companies, followed by close allies, then products from other countries.
- Of the 224 products claiming a UAS sensing capability, 52% use passive RF signals, 41% utilize radar technology, 40% use imaging technology (EO/IR), 13% use acoustics, and 3% require a human to perform the sensing function (e.g., for handheld mitigation systems).
- Of the 214 products claiming a mitigation capability, 71% offer non-kinetic (RF) mitigation, 11% offer kinetic-only mitigation, 9% offer multiple mitigations, and 7% offer an intercepting UAS (UAS-on-UAS).
- The overwhelming majority of COTS products focus on non-kinetic RF means of mitigating UAS, with various proprietary means of link interference, protocol manipulation, take-over, or deception.
- Of the 109 products for which a response was obtained on the question of interoperability, 73 claim they are or have the means to be interoperable with other systems, generally through an application programming interface.

CUAS technologies or products should not be thought of as static solutions with fixed capabilities/features. A common response when communicating with manufacturers about their product was “what are your requrements?” Many manufacturers want to know the government’s requirements and applications, so they can tailor their product to meet more specific needs. Many manufacturers offer their core CUAS technology in multiple platforms and form factors for this very reason. Several manufacturers are partnering to leverage each other’s strengths (sensing, mitigation, C2, integration, etc.) and develop a more comprehensive solution. An emerging trend is the development of resellers and integrators – companies who offer other companies’ products, and expertise in integrating/deploying CUAS technologies.

This page left blank

ACRONYMS AND DEFINITIONS

Abbreviation	Definition
2D	two-dimensional
3D	three-dimensional
AI	artificial intelligence
API	application programming interface
ATO	authority to operate
BCI	Business and Competitive Intelligence
C2	command and control
CONOPS	concept of operations
COTS	commercial-off-the-shelf
CUAS	counter-unmanned aircraft system
DHS	US Department of Homeland Security
DoD	US Department of Defense
DOE	US Department of Energy
EM	electromagnetic
EMP	electromagnetic pulse
EO	electro-optical
EW	electronic warfare
FAA	US Federal Aviation Administration
FOV	field-of-view
GLONASS	GLObal NAvigation Satellite System (Russian version)
GNSS	Global Navigation Satellite System
GPS	global positioning system
GOTS	government-off-the-shelf
ID	Identification
IR	Infrared
km	kilometer(s)
LOB	line of bearing
m	meter(s)
MHz	megahertz
NAR	nuisance alarm rate
NNSA	National Nuclear Security Administration
NTIA	National Telecommunications and Information Administration
OPSEC	operations security
OUO	Official Use Only
POC	point of contact
RC	radio control
RF	radio frequency
RFI	request for information
S&T	Science & Technology Directorate
Sandia	Sandia National Laboratories
TRL	technology readiness level
UAS	unmanned aircraft system
UAV	unmanned aerial vehicle
UK	United Kingdom
US	United States
USD	US dollars
XLST	Extensible Stylesheet Language Template
XML	Extensible Markup Language

This page left blank

1. INTRODUCTION

1.1. Overview

The U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T) asked Sandia National Laboratories (Sandia) to survey the commercial-off-the-shelf (COTS) counter-unmanned aircraft system (CUAS) market and compile information that could be used to facilitate selection of technologies for acquisition and deployment. This report summarizes the results of that work and includes a compendium or listing of identified CUAS products, with technical data collected on as many of those as possible within the timeframe of the study. It builds upon a similar but very brief and high-level market survey Sandia had conducted in 2015 to identify CUAS technologies for a technical conference paper.[1]

1.2. Background

Given the forecasted[2] rise in sales and recent increase in capabilities, UAS have quickly become a security concern due to the ease in which they can aid in intelligence gathering and/or be used as a malicious delivery platform. Multiple threat assessments and reviews of small unmanned aircraft system capabilities have been conducted to understand the risks and consequences of a range of scenarios of concern.[3,4,5] Several years of reporting on flyovers and incursions of unmanned aircraft systems (UAS) over secure or sensitive areas shows that the frequency of these events is high. Federal agencies responsible for protecting facilities, personnel, and critical assets have begun realizing the immediate need for airspace awareness and the ability to mitigate incursions by small UAS.

The 2018 FAA Reauthorization Act granted DHS and others legal authority to detect, identify, monitor, track, warn, disrupt, seize, and use reasonable force if necessary to disable, damage, or destroy an unmanned aircraft or aircraft system posing a threat to covered facilities as designated by the Secretary or Attorney General.[6] Similar legal authorities were previously granted to the US Department of Energy (DOE), National Nuclear Security Administration (NNSA), and the DoD in the 2017 and 2018 National Defense Authorization Act, to protect certain covered facilities.[7,8] These changes have led to an increased interest by DHS component agencies in acquisition and deployment of CUAS. This in turn has led to a need to identify currently available CUAS products and companies and an understanding of the capabilities and characteristics of those products, to support efforts to select and field suitable CUAS for a range of applications.

1.3. Purpose

This document provides a compilation of known COTS CUAS products and summarizes the results of a market survey to collect additional technical information on as many of those products as

---

[1] Birch, et. al., SAND2015-6365 *UAS Detection, Classification, and Neutralization: Market Survey 2015*, July 2015 (UUR).
[2] FAA Aerospace Forecast 2018-2038, Trends in Unmanned Aircraft Systems, March 2018.
[3] Salton, et. al., SAND2015-4329, *Unmanned Aircraft Systems (UAS) Guidance: Policy, Utility, Threats, Vulnerabilities, and Countermeasures,* May 2015 OUO.
[4] Salton, et. al., UAS Threat Addendum to SAND2015-4329 *Unmanned Aircraft Systems (UAS) Guidance: Policy, Utility, Threats, Vulnerabilities, and Countermeasures,* June 2017, SNSI//NOFORN.
[5] As of October 2018, the Department of Homeland Security, Homeland Security Operational Analysis Center (HSOAC) is in the process of drafting a threat document on small unmanned aerial system capabilities.
[6] FAA Reauthorization Act of 2018 (Public Law 115-254)/H.R. 302 Div H, Sec 1602, 1603.
[7] National Defense Authorization Act for Fiscal Year 2017, Public Law No: 114-328, Sec 1697, Sec 3112, Sec 1697.
[8] National Defense Authorization Act for Fiscal Year 2018, Public Law No: 115-91, Sec 1692, Sec 3112.

possible within a two-month period starting in late 2018. This work should be revisited in the future to refine and update the information in keeping with product updates and advances in rapidly evolving technologies and their integration into COTS products. Additional benefits and purposes of this report include:

- Compilation of known COTS and government-off-the-shelf (GOTS) CUAS products available on the global market as of late 2018
- Survey of potential GOTS and COTS CUAS technologies for acquisition and deployment for DHS S&T
- Acquisition and deployment considerations for DHS S&T and its components
- Selection for testing and evaluation
- Provide criteria to facilitate down selection of available CUAS technologies

1.4. Research Scope of Work

The scope of the effort was to identify as many distinct CUAS products and companies as possible including all technologies and product types, available globally. However, efforts to research individual products to obtain additional technical and descriptive information were executed in a prioritized manner. Both component and system technologies were included in the market survey. The research prioritized domestic CUAS products followed by foreign products from allied nations, especially those with a mitigation capability. Information on other foreign systems including those with kinetic mitigations was collected as time allowed.

1.5. General Comments

The following assumptions, constraints and unknowns are applicable:

- Market and technical product Information was collected between October and November 2018 and therefore represents a limited snapshot of the CUAS market at that time.
- Technical data was collected through researching manufacturer websites, product brochures, email and telephone interviews with CUAS product points of contact (POCs), and reviewing test/demonstration event reports.
- While the survey was global in terms of identifying CUAS products, the collection of technical data prioritized US-based companies over foreign companies.
- Given the rapidly evolving nature of CUAS technologies and industry, it is unclear how many identified CUAS products or companies outside the US are continuing to offer their product at this time. A few US companies we spoke with indicated that they had stopped offering their product as the market was too saturated at this point.
- It is possible that some new start-up companies recently formed are not contained within the purview of this report.

1.6. Document Structure

Section 1 provides the overview and background for this CUAS market study.

Section 2 provides explains the market survey approach and process steps used to conduct the survey.

Section 3 provides summary tables and information on the data collected and describes key observations and takeaways from the market survey.

Section 4 provides an overview of CUAS applications and platform considerations including the threat engagement sequence, trends in platforms and technologies, temporary measures, and CUAS performance requirements. Impacts on technology selection and deployment are presented.

Section 5 summarizes conclusions of the CUAS market based on this market survey and offers next steps, such as down-selection and continued research into lower priority systems that could not be completed in the timeframe for this report, as well as review of collected data in support of specific component CUAS needs.

Appendix A contains the Request for Information form that was posted on www.fbo.gov.

Appendix B contains the masterlist of CUAS products identified through the research. Limited product information is presented in the masterlist as a brief overview; the full set of technical data is contained in the accompanying database.

Appendix C provides general characteristics of common UAS sensing and tracking mitigation technologies.

Appendix D provides general characteristics of common UAS mitigation technologies.

Appendix E provides a brief overview of a systems engineering framework for designing, characterizing, and evaluating a physical security system as the basis for the CUAS kill chain.

This page left blank

2. MARKET SURVEY METHOD

Because survey data was needed as soon as possible to meet DHS S&T program and schedule needs, data could only be collected over a roughly two-month period starting in October 2018. Key objectives of the survey were to identify a global pool of CUAS products with a range of sensing, assessment, tracking, and mitigation capabilities for a wide range of potential application spaces. The specific DHS application spaces were unknown at the start of the research so the data collection focused on general capabilities and performance attributes. The survey intentionally included data collection on products regardless of whether they were marketed as a component technology or as a partial/complete 'system.' Systems are products marketed as collections of technologies and command/control functions to yield a complete solution with capabilities in all or nearly all aspects of the desired CUAS kill chain: sensing, assessment/identification, tracking, mitigation. The market survey was conducted using the process illustrated in Figure 2-1. Each step is explained in greater detail below.

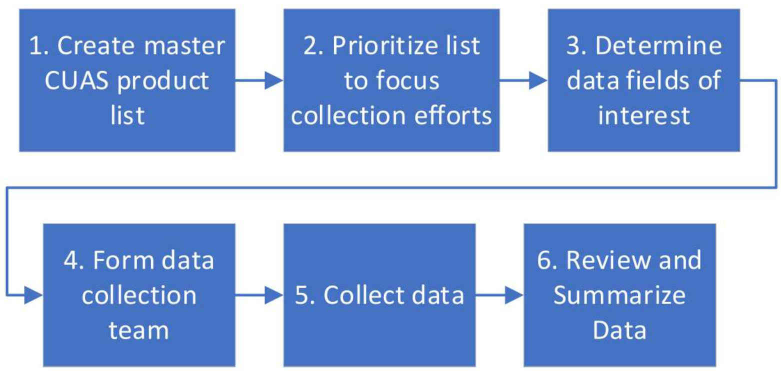


Figure 2-1: Key Steps in the Markey Survey

2.1. Create Master CUAS Product List

A master list of known CUAS products and companies was created by reviewing and comparing existing market surveys, market analysis reports, academic and commercial CUAS databases and compilations, CUAS demonstration event reports, other DHS documents, and systems encountered during prior interactions with CUAS companies. These sources included the following:

1. 9AB0-16, *Global Defense Counter-UAS Technologies Market, Forecast to 2022*, Frost & Sullivan, October 2017
2. 9AB0-22, *Global Commercial Counter-UAS Technologies Market, Forecast to 2022*, Frost & Sullivan, October 2017
3. Arthur Holland Michel, COUNTER-DRONE SYSTEMS, Bard College Center for the Study of the Drone, February 2018
4. "Counter UAS industry directory," March 2018.V1, www.unmannedairspace.info
5. DF0152SR, "Global Military UAV Market 2018-2028," Strategic Defence Intelligence, May 2018 PowerPoint presentation
6. "Anti-Drone Market Analysis and Segment Forecasts to 2024," Grand View Research, 2018
7. Huw Williams, Derrick Maple, Chris Hawkins, MN Wasif, Scott Johnson, Geoff Fein, "Technical Outlook For Global C-UAS Capabilities," Jane's by IHS Markit, April 2017 PowerPoint presentation

8. NI-BRIS-004/01, *BRISTOW 18 Final Report*, Nexus Imaging Ltd., funded by the UK Centre for the Protection of National Infrastructure and the Defence Science and technology Laboratory, June 2018
9. 2017 Department of Homeland Security TACTIC II event participant list
10. 2014-2018 BlackDart event reports and participant lists
11. 2017-2018 Hard Kill I, II event reports and participant lists
12. 2015-2016 Desert Chance I, II, III event reports and participant lists
13. Homeland Security Systems Engineering and Development Institute Assessment of Current Kinetic/Non-Kinetic Options, June 30 2016 (OUO)
14. 2017 Adaptive Red Team/Technical Support and Operational Analysis 17-4 event participant list
15. 2016 and 2017 National Nuclear Security Administration (NNSA) CUAS test event reports and participant lists
16. Birch, et. al., SAND 2015-6365 *UAS Detection, Classification, and Neutralization: Market Survey 2015*, July 2015 (UUR)

The most useful sources of information proved to be the first four sources, which included the Counter Drone Systems report from Bard College's Center for the Study of the Drone, purchased market reports from Frost and Sullivan, and the Counter UAS Directory from www.unmannedairspace.info. The next most helpful sources were the event reports, which identified products that had been demonstrated at numerous events over the past few years. Each of the sources were reviewed and cross checked to develop as current and complete of a list as possible. The Counter Drone Systems report from Bard College was extremely helpful in that it listed the country of origin, website, platform, sensing technology, and mitigation technology for approximately 235 products. The Bard College list served as the basis for our initial master list, and additional products were added (or removed) as they were identified and researched.

Several challenges exist in creating a master list of CUAS that prevented complete accuracy of information. Many of these challenges are explained in the Official Use Only (OUO) version of the report.[9]

Additionally, because the commercial industry is transforming from a nascent to a growth industry,[10] many companies have partnered with complementary peers, changed partners and government sponsors, entered into joint marketing arrangements, modified product names and lines as capabilities have increased, or have simply left the market altogether as it is becoming increasingly crowded. The result is that some product names have changed or modified over time. The current list represents a snapshot of the main players in today's market, and not a historical list of all products previously offered. For these and other reasons, the reader may be familiar with a product but not see it in the master list. In the end, more than 316 CUAS products were identified and placed on the master list.

2.2. Prioritization

Because time available for researching and collecting technical data on products in the master list was very short, the master list was prioritized to focus data collection efforts on the most relevant

[9] Brooks, et al., *Counter-Unmanned Aircraft Systems Market Survey*, SAND2019-1468, Sandia National Laboratories, February 2019 (OUO).
[10] 9AB0-16, *Global Defense Counter-UAS Technologies Market, Forecast to 2022*, Frost & Sullivan, October 2017.

products and characteristics. Because DHS was interested specifically in neutralization/mitigation capabilities, products known to have a mitigation capability were prioritized higher than those that did not have a mitigation capability. Additional priorities and the rationale behind them are described in further detail in the OUO version of the report.

2.3. Determine Data Fields of Interest

The data collection team identified a range of data fields and types of information to be collected as individual products were researched. The objective was to collect general and consistent product information that would support product filtering and sorting of interest to DHS S&T. Because performance and operational requirements were not available at the time of the market survey, the data collection also focused on identifying a range of products that meet a wide range of application space and requirements. Mitigation capabilities were a large focus given that legal mitigation authorities had recently been granted.[11] Because the process was largely manual in nature (calls, emails, and researching product literature and websites), the amount of data that could be collected needed to be balanced against available resources and the time allowed for data gathering. After several drafts, including review and comment by DHS S&T, the team settled on the data fields described and discussed below.

2.3.1. General Product/Company Information

Most of these fields are self-explanatory and used to establish basic facts on the company, product, and POCs.

Country of Origin – *Where is your product manufactured?* The survey was not limited to domestic products. However, knowing the country of origin allows a user to sort or filter results by country. This is important given laws that restrict (but do not prevent) purchasing of foreign products for government use, and the fact that it can be challenging to meet information assurance/cyber accreditation requirements for foreign systems connected to a domestic network, especially if that network contains any sensitive information.

Number of Customers – *How many customers have purchased this product?* This question provides the number of unique customers that have already purchased this product. This can be considered a proxy for the maturity or popularity of the product, or an indication of how long it has been available on the market. As the market for CUAS has only been around for about 8 to 10 years, and products are still maturing, this number is generally low for most manufacturers.

Customer List – *Please provide a sample listing of customers who have purchased this product.* Provides a listing of the customers (or highlighted set of customers) that have purchased the product. The customer list may help some agencies as they seek to identify systems that may already be in place at other government agencies (both domestically and foreign). It may be possible to obtain feedback from these entities on their experience and satisfaction with the product prior to procurement.

Number of Systems Deployed – *How many units of your product have been deployed or are operational worldwide?* This number provides an indication of how many units have been produced and fielded to date. Lower numbers (less than 10) may indicate developmental or prototype quantities; higher quantities may be an indication of the maturity of the product, the production line, service and engineering support, and lower likelihood of product abandonment in the future.

[11] 2018 FAA Reauthorization Act, or H.R. 302, Section 1602.

Status – *What is the maturity or level of development of your product?* This field was used as a measure of maturity based on the information collected above (i.e., number of customers, customer list, and number deployed). For data consistency, this field is limited to a drop-down box with the following choices:

Prototype
New Product/Updated
In Production/Operational
Unknown
No Longer Offered

2.3.2. Cost Information

Fields in this section of the data collection sheet provide information helpful in estimating potential costs in designing, acquiring, deploying, and operating the CUAS for a given application. Cost information reflects today's pricing and may not be accurate going forward.

Unit Cost – *What is the cost of the complete/full system with all typical components?* Care must be taken when comparing unit costs, as costs for component technologies will be substantially lower than for more integrated or complete suite or set of solutions. Actual pricing in whole dollars was reported wherever possible. In most cases, except for products that truly were prototypes, the manufacturer was willing to supply a typical unit/system price. For ease of data consistency, if an actual unit/system price could not be obtained, the following drop-down choices were used by the team in estimating the costs based on manufacturer responses, similar products, or our own familiarity with the product.

≤$50k
≤$100k
≤$500k
≤$1,000k
≤$2,500k
≤$5,000k
>$5,000k

Area Coverage – *What size area can be protected by one unit? (Please use km^2)* Total area that can be covered with a single unit helps in estimating the number of units that may be needed to protect a given area or perimeter. Most companies do not typically report area coverage – instead they report a length (e.g., 5 km) or a field of view (FOV). Attempts were made where possible to calculate and report this number in terms of km^2 based on the information provided.

Install Time – *Typically, how long does it take to install the above quoted system at a fixed facility? (Assume all required power and communications infrastructure exist at all required locations.)* Typically the required power and communications infrastructure is not ready at the required locations. Except for small portable turnkey systems that only require being switched 'on,' some modification or construction is usually needed to create or extend infrastructure to the agreed-upon CUAS location(s). As costs to extend power and communications to the installed location vary greatly based on many factors, this information cannot be estimated at this time. Instead this field gives an indication of how long it takes to connect and configure or set up the technology at the installation location(s). For data consistency, this field is a drop-down box with the following choices:

A few hours (or less)
1-2 days
3-6 days
1-2 weeks
3-4 weeks
More than a month

Most manufacturers are reporting installation times in the 'A few hours (or less)' or 1-2 days categories, as setup and connection of their component or system to a network or command and control interface takes very little time. Thus this response should be thought of as time required to physically place, connect, turn on, and configure the system.

However, as most users will deploy a CUAS to a fixed site or implement it in a way that ensures consistent and sustainable long-term operation, additional deployment time will likely be needed for extending supporting infrastructure or for formal acceptance and operation approval. The time to conduct these activities is not taken into account in this question as it will vary greatly with requirements. In general these activities may include the following:

- Pre-installation siting surveys and design/configuration per site-specific requirements
- Post-installation contractor verification/assurance testing
- Network communications setup and configuration
- Spectrum/frequency coordination, surveys, allocation, and approval, and possibly National Telecommunications and Information Administration (NTIA) approvals
- Information assurance and cyber security reviews
- Safety evaluations
- Network/cyber Authority to Operate approvals
- Training and certification of operators
- Site-specific policy and CONOPS updates
- Site-based testing and performance evaluations

The above activities may take more than six months to complete depending on the site-specific CUAS design and any approval processes and requirements.[12]

Annual Cost – *Although annual support costs might vary with the implementation, what are the typical total annual maintenance, support, and update costs (e.g., full service contract)?* Annual costs can vary greatly depending on agreements or customizations that can make this cost difficult for some companies to quantify. Those that offer a set annual maintenance fee, update fee, software access fee, or customer support fee are able to report that cost. Some companies do not charge for customer support. For

[12] Cite the NNSA CUAS deployment report for Los Alamos National Laboratory. NNSA spent nearly 16 months in total obtaining all the required approvals and authorizations needed. They were one of the first non-military agencies/departments to deploy a CUAS. This time is anticipated to be reduced with repeated deployments.

data consistency, if an actual cost could not be reported, the following drop-down choices were used as an estimate of the annual costs.

n/a
≤$10k
≤$50k
≤$100k
≤$250k
>$250k

Many companies reported the annual support costs instead as a percentage of the total purchased equipment costs, as support costs can vary greatly based on the specific configuration. For data consistency purposes, percentages were converted to dollar amounts, using the reported 'unit costs.'

Number of Persons – *How many people does it take to operate all aspects of your CUAS product? That is, alarm monitoring, alarm assessment, tracking, response/mitigation, troubleshooting, etc.* Though highly dependent on CONOPS, this field helps site operators estimate long-term manpower costs associated with operating a CUAS, especially if the posting must be staffed continuously, as is typical of security functions. Nearly all systems can be operated by a single person; a few are able to operate autonomously, but even these will require a system administrator or other person to interact with the system periodically.

2.3.3. Technical Characteristics

These fields describe the technical features and characteristics of the CUAS products, enabling filtering and sorting based on characteristics that are important to a specific CUAS application.

Platform1 – *What is the platform type of your CUAS technology? If multiple platforms are applicable, please list each type separately below.* This field enables filtering of responses by platform type. Some CUAS companies can integrate their product into multiple platforms. Up to three choices were allowed to indicate the range of platforms in which the product is available, or the range of platforms comprising the CUAS. (For example, some systems might use ground-fixed equipment for sensing and tracking, but an aerial platform such as an intercepting UAS for mitigation.)

Platform2 and Platform3 (if applicable)

To standardize responses, the following drop-down choices were allowed. Handheld/person includes a range of products meant to be operated by a person such as a RF-emitting gun, or simply worn by a person but with no interaction required by the person, similar to a body camera worn by local law enforcement agencies. "Other-specify" was added to the request for information (RFI) version of the data collection sheet to allow responders to describe their platform if it did not fit one of the below categories.

Aerial
Ground-Fixed
Ground-Mobile
Handheld/Person
(other-specify)

UAS Sense Technology 1 – *What technologies do you utilize to sense or track the UAS threat? (List all that apply, using a single entry per row. Leave blank if N/A.)* This field captures the individual technologies used for sensing and tracking of CUAS threats. To standardize responses, the following drop-down choices were allowed.

EO
IR
Active RF (Radar)
Passive RF (Signal Emissions)
Acoustic/Seismic Microphone
Human detection
(other-specify)

Because optical system performance can vary by wavelength, and some infrared (IR) technologies can be expensive, electro-optical (EO) and IR were listed as separate entries. Human detection refers to whether sensing or tracking is supplied by a person (e.g., some handheld systems require a person visually acquire a target and track it, to successfully mitigate the UAS). "Other-specify" was added for the RFI version of the data collection sheet to allow entry and description of a technology that does not fit the above choices.

UAS Sense Technology 2 through UAS Sense Technology 5 (if applicable)

RF Sensing Type 1 - *If sensing is based on detection of RF transmissions, what specifically about the UAS is being sensed by your product? (List all that apply but only one per row; leave blank if N/A.)* This field enables up to five entries to describe the aspects of the UAS that are sensed by the CUAS if sensing is based on reception of RF transmissions from the UAS. To standardize responses, the following drop-down choices were allowed.

RC Transmitter/Handset
UAS Telemetry (1 or 2 way)
Transmitted Video
WiFi-Network
Cellular-Communications
Unintended RF emissions

RC transmitter/Handset refers to the controller that a UAS operator holds and interfaces with to remotely pilot the UAS. UAS Telemetry (1 or 2 way) refers to the data link between the UAS and the ground control station or handset that receives UAS flight and health telemetry data. Two way refers to the fact that some ground control stations can upload telemetry data (such as new Global Navigation Satellite System (GNSS) way points or 'missions') to the aircraft in real time using the telemetry link. Transmitted Video refers to video data that may be transmitted by the aircraft during flight. WiFi and cellular options refer to additional communication protocols that can be used for telemetry, video, or remote pilot control links.

RF Sensing Type 2 through RF Sensing Type 5 (if applicable)

Signal Decode – *(Yes, No) If sensing is RF-based, does the system decode the RF transmissions to gather additional UAS information?* This field is used to filter results based on capabilities to read received communication protocols and messages inside the protocols to gather additional information on the aircraft, handset/controller, or information stored inside the UAS. This is a level of capability beyond matching the protocol and frequency hopping pattern to a known protocol to identify a UAS make or model. This more advanced technique allows access to additional information.

Sense Track Range – *What is the typical maximum horizontal sensing/tracking distance (km) for a small (Group 1, <20lbs) UAS?* This is different from the question on how large of an area can be protected by a single unit, as often the area that can be protected by the mitigation technology and UAS alarm assessment capability is smaller than the area that can be sensed by the CUAS. This impacts CONOPS in which airspace awareness is needed beyond the area that is designated as protected or defended or a 'no-fly-zone.' For data consistency, if an actual value could not be reported, the following drop-down choices were used by the team to estimate the distance based on experience with that technology, product, or similar product.

≤150m
≤500m
≤1km
≤3km
≤5km
>5km

Assessment Camera – *(Yes, No) Does your product include an integrated camera to allow an operator to optically verify the cause of an alarm?* An assessment camera with slew-to-cue or similar capability enables a human to determine if the reported UAS alarm is a true alarm or nuisance alarm, by assessing the image to classify the target as a UAS or non-UAS. This capability directly impacts CONOPS and policies surrounding automated responses to UAS alarms, rules of engagement, escalation of force, tracking, and site safety. As confidence in sensing, identification, machine learning, and artificial intelligence technologies improve, some users may determine that cameras are not a necessary component of the CUAS; others may determine that visual confirmation of the cause of the alarm is required prior to engaging the threat. Though it may be suitable, accepting a CUAS with no visual assessment capability is inherently accepting the operational and performance risk associated with any nuisance or false alarms.

Assessment Range – *(Please use kilometers) If so, what is the typical maximum effective range for optical assessment of a small UAS?* This is a follow-up question to the Assessment Camera to understand the *claimed* capability of the camera and operator combination. If the sensing system can sense out to 6 km, but the assessment system can only assess out to 3 km, then effectively the combined protected area is only a 3-km radius. For data consistency, if an assessment range could not be reported on a camera, the following drop-down choices were used to assist with estimation of the capability.

≤150m
≤500m
≤1km
≤3km
≤5km
>5km

UAS Identification – *(Yes, No) Does your product identify the type of UAS (fixed vs. rotary wing) or the make/model?* This field enables filtering on whether this capability is required or on whether it is important to identify the make/model of the UAS. Very few companies claim their product can classify a UAS as a fixed wing or multi-rotor. Systems that claim to identify the make/model are identifying the communication protocol that is often unique to a given UAS platform.

Identification Method – *(Yes, No) If your product can identify the UAS make/model, is an exact match against an internal library required to generate a UAS alarm?* Note that if an exact protocol match is required to report the alarm, and the protocol being used by the UAS is not in the CUAS library or has been modified, then the UAS will not be sensed by the CUAS.

Number of Simultaneous Sense-Track – *What is the number of UAS that can be simultaneously sensed/tracked without degrading system performance/latency?* This field enables filtering or sorting based on the required number of UAS threats that must be sensed and tracked in a given application. Some CUAS sensing technologies can have degraded performance in geolocation or track refresh rates if too many UAS are in the FOV.

Provides UAS Track – *(Please enter Yes, No, or N/A) Does the system provide UAS Track history?* This field enables filtering based on applications that require the ability to track an incoming UAS or output the track history to an evidence file.

Provides Position – *(LOB, 2D geolocation, 3D location, alarm only [no position], N/A) What kind of position information on the threat UAS is provided?* This field is important to design and CONOPS. Airspace awareness can take many forms, but the more information that is available about the UAS position, the more actionable that information is. A line of bearing (LOB) may be suitable, but a responder or operator will not know the distance or altitude of the threat – only the azimuth or general direction. In other applications, a 2D geolocation may be suitable, but the operator will not know the altitude of the UAS. Alarm only systems provide 1D awareness or indication when a UAS is within a given range of the sensor in any direction.

2.3.4. Mitigation Characteristics

The following fields enabled collection of data describing technical characteristics of CUAS mitigation capabilities. This data enables filtering and sorting based on characteristics that are important to specific mitigation requirements, constraints, or applications.

Mitigation Type – *What type of mitigation is used? (Non-kinetic, kinetic, intercepting UAS, multiple, N/A).* This allows grouping of systems by broad mitigation type or category. Non-kinetic refers to mitigations that do not require physical contact with the UAS. Kinetic refers to mitigations that do involve physical contact with the UAS such as projectiles, nets, munitions, and lasers. Intercepting UAS refers to a special case of kinetic mitigation in which a UAS is used to manually or autonomously deliver a mitigation to the threat UAS. Multiple refers to conditions in which the CUAS contains elements of more than one type of mitigation. Additional questions or data fields were created to collect further information on each type of mitigation.

Non-kinetic 1 – *If your product has non-kinetic capabilities, please list all that apply; list each in a separate row.* This set of questions enables description of the types of non-kinetic mitigation used. RF interference refers to deliberate use of radio noise or signals to disrupt communications from one component of the UAS to another, usually by raising the in-band noise levels to drown out the targeted signal. This includes targeting known frequency hopping patterns. GNSS interference refers to similar strategies to prevent reception of satellite navigation signals. Acoustic refers to the use of acoustic energy to disrupt navigation, and electromagnetic pulse (EMP) refers to a short burst of EM energy to damage electrical components. "Other-specify" was added as an option in the RFI questionnaire to allow a responder to describe an alternate means of non-kinetic mitigation. Up to four total responses were allowed in this set of questions, as some products have multiple non-kinetic capabilities.

Non-kinetic 2 through Non-kinetic 4 (if applicable)

RF Shape – *If RF mitigations are used, are the antennas: omni-directional, directional or both?* This data helps describe the shape of RF-based mitigations, and may inform design aspects (e.g., ensuring there is sufficient effectors to fully cover the areas to be protected.). Directional antennas may have intended effects at much longer ranges than omni-directional antennas because the output energy is concentrated into a smaller FOV.

GNSS Band – *Which GNSS bands do you mitigate? (List all that apply, for example, GPS: L1, L2, L5, GLONASS: G1, G2, G3, Galileo: E1, E5, E6, other-specify) Leave blank if N/A.* This field helps identify the number of GNSS bands or constellations that are targeted during GNSS mitigations.

Kinetic 1 – *If your product uses kinetic mitigation(s), please list all that apply; list each in a separate row. (Laser, ballistic, net capture, entanglement, ballistic munition, guided munition, other-specify).* This field allows collection of the type(s) of kinetic mitigations employed. Up to two unique responses were allowed here for instances in which the system may have integrated more than one kinetic mitigation. Net capture and entanglement are distinct mitigations. Net capture refers to the use of a net; entanglement refers to the use of streamers or other non-net structures to cause an entanglement. Ballistic refers to the use of bullets that must impact the UAS; munitions are projectiles that detonate near the UAS to cause damage from fragments. "Other-specify" was added as an option in the RFI questionnaire to allow a responder to describe a means of kinetic mitigation not listed above.

Kinetic 2 (if applicable)

Intercepting UAS 1 – *If your product uses an intercepting UAS (hunter-killer UAS) what mitigation payload capability is utilized? Please list each in a separate row. (Net capture, entanglement, projectile/munition, RF, EMP, other-specify.* This field allows information collection of the type of mitigation that is used as the payload on an intercepting UAS. As more than one type of payload or mitigation might be integrated into an intercepting UAS, up to two unique responses were accommodated here. "Other-specify" was added as an option in the RFI questionnaire so a responder could describe an alternate payload type not listed above.

Intercepting UAS 2 (if applicable)

Kinetic Range – *(Please use kilometers) What is the typical maximum range of your kinetic mitigation capability? For example, net capture, claimed effective distance.* This information allows direct comparison of claimed effective ranges of different kinetic mitigation capabilities. (Unless the data is the result of testing by an independent third party, these values should not be interpreted as actual performance values, which may be lower than what is stated.)

Note that this question only pertains to <u>kinetic</u> mitigations, and not non-kinetic mitigation techniques. This is because there is considerable difficulty in reporting this value for RF mitigation systems as the effect varies by type of RF mitigation and many other factors. The OUO version of the report gives additional details and insight on variables impacting RF and GNSS mitigations.

An alternative method for estimating effective range of RF mitigations in the next market survey would be to request the antenna power and gain specifications on the RF effectors being used, so effective distances can be calculated and normalized based on a specific scenario and assumptions. This was outside of the current scope of research and data collection.

Number of Simultaneous Mitigated – *How many UAS can be mitigated simultaneously (including cases where the UAS are operating on separate frequency control bands)?* This information allows comparison of responses surrounding capability to mitigate multiple UAS or swarms of UAS. The same considerations for RF mitigation discussed in the *Kinetic Range* question apply here.

2.3.5. Test/Demo History

Event 1 – *If you have participated in any CUAS test/demonstration events in the past three years, please list the event name and date (year). Please list each one in a separate row.* The number of times a manufacturer and product has participated in a test or demonstration event may be an indication of the level of interest, ongoing product investment, development, and refinement, or sponsor interest/investment in the product. Tests and demonstration events should be sponsored by a government or separate industry/commercial entity and not by the manufacturer of the product. Documentation of up to 10 unique event entries was allowed.

Event 2 through Event 10 (if applicable)

2.3.6. Product Description

System Description – *Please describe your product? How is it operated? What are the components? What are its capabilities?* This is an unlimited text-entry field allowing the manufacturer to describe the product using their usual marketing descriptions and information. This field provides a more comprehensive overview of the product and its capabilities as the technical specifications and descriptions above may not fully describe the product, its integration or development, or intended operation and optional features. Additionally, manufacturers are able to describe ongoing or planned improvements, sponsorships, partnerships with other CUAS companies and distributors, and other product information not covered by specifications.

Interoperability 1 – *Describe the system's "interoperability." For example, does it have an open software architecture so it can be connected to an existing C2 system? If so, would you provide an API? Is it compliant with any sensor communication standards like TCUT or SEIWG-ICD-0101B*? This is an unlimited text entry field allowing the manufacturer to address interoperability, communication standards, expandability, application programming interfaces (APIs), or their ability to customize the deployment to meet interoperability requirements.

Interoperability 2 – *(Yes, No) Do any of the descriptions listed for Interoperability 1 (or similar) apply?* This field distills the information provided in Interoperability 1 into a simple yes or no response, allowing filtering of the database by whether or not the manufacturer claims the system is "interoperable."

Technical Support – *Please describe any training, operations, maintenance, and troubleshooting support you provide post-sale. (For example, is the support offered onsite or by phone? Is the support free for a given duration? Is a service/subscription contract required for ongoing support? Is there an annual fee for support?)* This is an unlimited text field enabling the manufacturer or data collector to describe the levels of support that are offered and whether or not there is an associated cost after the first year of operation. This helps provide context to the "Annual Cost" field.

2.3.7. References

Reference 1 – *If your product has been assessed or evaluated in any US government agency reports, please provide the report reference information (if known) (e.g., author, title, and date).* Up to 10 reference fields are used to document any references to event or test reports where interested users can review system performance and operation under specified objectives and event constraints. Because event planners have not standardized yet on test protocols, or might only portray the event as a demonstration and not a test, the results can be challenging to compare. However, these reports can provide valuable insight into both strengths and weaknesses especially if the manufacturer was not the equipment operator during the test event. Sandia has collected as many of these as possible within the timeframe of the report.

Reference 2 through Reference 10 (if applicable)

2.4. Data Collection Team

The data collection team consisted of several Sandia staff members with experience in technology development to include testing and deploying CUAS for the NNSA. This prior experience included helping to define performance requirements, CONOPS, issuing requests for proposals and information, meeting with CUAS manufacturers for technical exchanges, obtaining system specifications for test range approval processes, and operating CUAS during test activities for NNSA. This experience was helpful in identifying those key data fields of interest in Section 0.

The data collection team also consisted of several Sandia staff members in the Business and Competitive Intelligence (BCI) department, which partners with technical organizations at Sandia to provide market research and other information to improve strategy and decision making. The BCI team had extensive experience in data collection, market surveys, analysis, and strategy. This experience was helpful in creating the market survey and in reviewing and understanding characteristics of the CUAS market.

2.5. Data Collection

Data collection proceeded in two ways. The first was research and data collection conducted manually by individual team members, and the second was issuing a RFI posted to the FedBizOpp website (www.fbo.gov).

The data collection team manually researched CUAS products following the general prioritization described in Section 2.2. Product websites were reviewed to collect data for each of the fields described above using an Excel-based data collection sheet. Product specification sheets, brochures, briefings, and other materials if available were downloaded and placed into product folders as supporting information. These files were reviewed to determine the values and information that should be entered into the different data fields. Sources listed in Section 2.1 were reviewed as applicable to also support the data entry.

For most products, the data collection sheets could not be fully answered and completed by manually researching and reviewing this information. Technical or business POCs were emailed to obtain as many of the missing pieces of information as possible. On some occasions, a partially completed information sheet was emailed to the product POC, to ask them to review or complete the remaining data fields.

The second way data was collected was through the RFI. The data collection sheet used for manual research was modified for distribution to an external audience as a Microsoft Word protected form that allowed information entry in specific from fields. The RFI form is shown in Appendix A. Suggested response choices were provided for most fields to keep data reporting as consistent as possible, but users were allowed to enter any text. An automated process for uploading completed and returned responses into an Excel database was developed and tested.

2.6. Review and Summarize Data

All manually researched and RFI-submitted data collection sheets were reviewed for completeness and consistency of data reporting. All original survey responses received through the RFI process had to be reviewed and 'scrubbed' by the team to ensure consistency and correctness of the information such that it would support filtering and sorting by key technical characteristics when loaded into the database. For example, fields where a dollar value should have been reported but also included photos or explanatory text had to be modified so only the number remained. Similarly, fields where the respondent needed to select one of the suggested choices, such as type of non-kinetic mitigations, were reviewed and interpreted to understand which choice best described the information being reported. However, because the original versions contain highly useful explanatory and contextual information for each response, they were saved and will be provided under separate cover. The scrubbed versions of the RFI responses were loaded into the database along with the manually researched and collected information to form the CUAS database.

This page left blank

3. MARKET SURVEY RESULTS SUMMARY

Approximately 316 CUAS products were identified from 195 manufacturers. This section provides an overview of the survey results. Appendix B provides a list of all the identified CUAS products and technologies, using only a small subset of the information (columns) that would fit within the margins of this document.

3.1. Summary Data

This section provides summary charts on the data collected. The tables were generated through an automated Extensible Stylesheet Language Template (XSLT) process and are easily updated as the underlying database is updated. Values may not match total numbers of products listed in the database, as technical data was not obtained on all products, and not all RFI responders completed every field (e.g., some declined to indicate a cost or install time).

Table 3-1: Count of CUAS Products, by Country

Country	Count	Country	Count
USA	126	Belgium	3
UK	37	Turkey	3
Israel	18	Brazil	2
France	16	Italy	2
Australia	15	Monaco	2
Switzerland	13	Norway	2
Germany	12	Spain	2
China	10	Taiwan	2
Ireland	9	Bulgaria	1
Denmark	8	Estonia	1
Singapore	6	Finland	1
Netherlands	5	Hungary	1
Russia	5	India	1
Canada	4	South Africa	1
Japan	4	Sweden	1
Poland	4	UAE	1
Belarus	3	**Total:**	**321**

Table 3-2: Summary of Claimed CUAS Status

Status	Count
Deployed/Operational	141
Prototype	41
New Product/Updated	14
No Longer Offering	7
Unknown	2
Total:	**205**

Table 3-3: Count of CUAS Platform Types

Platforms	Count
Ground-Fixed	171
Ground-Mobile	104
Handheld	63
Ground-Based	60
Aerial/UAV	43
Ground-Portable	6
(other-specify) Antenna	4
Maritime-Mobile	3
Any	2
Ground-Fixed (Software)	1
Ground-Mobile (Software)	1
Portable	1
Total:	**459**

Table 3-4: Summary of Claimed CUAS Average Installation Times

Install Time	Count
A few hours (or less)	131
1-2 days	17
3-6 days	4
Unknown	3
1-2 weeks	2
3-4 weeks	1
N/A	1
Total:	**159**

Table 3-5: Claimed CUAS Unit Costs

Unit Cost	Count
Greater than $5,000,000	1
$2,500,001 - $5,000,000	7
$1,000,001 - $2,500,000	9
$500,001 - $1,000,000	13
$100,001 - $500,000	47
$50,001 - $100,000	11
$0 - $50,000	35
Total	**123**

Table 3-6: Types of Sensing Method/Technology

Sensing Technology	Count
Passive RF Signal Detection	114
Radar	92
EO	83
IR	78
Acoustic/Seismic Microphone	26
Human Detection	6
Acoustic	4
Seeker	2
Hyperspectral	1
Integrates with 3rd Party Detection Systems	1
Laser Designator	1
Laser Range Finder	1
LIDAR	1
Terahertz	1
Total:	**411**

Table 3-7: Count of Non-Kinetic Mitigation Types

Type of Non-Kinetic Mitigation	Count
RF Interference	109
GNSS Interference	67
Other RF Techniques	64
Other GNSS Techniques	9
EMP	3
Acoustic	2
High Power Microwave	2
Video Transmission Mitigation	2
Modify RTL Position	1
None (UAS nearby alert only)	1
Optical Blinding	1
Other - Removes Control and Video Links	2
Total:	**263**

Additional summary operations were performed on the CUAS database to develop the following high-level picture of what is contained in the database. Results include the following:

- Products were identified from 35 countries. The top countries represented are the US (39%), the UK (10%) and Israel (6%).
- Of the 224 products claiming a UAS sensing capability, 52% use passive RF signals, 41% utilize radar technology, 40% use imaging technology (EO/IR), 13% use acoustics, and 3% require a human to perform the sensing function (e.g., for handheld mitigation systems).

- Of the 214 products claiming a mitigation capability, 71% offer non-kinetic (RF) mitigation, 11% offer kinetic-only mitigation, 9% offer multiple mitigations, and 7% offer an intercepting UAS (UAS-on-UAS).
- The overwhelming majority of COTS products focus on non-kinetic RF means of mitigating UAS, with various proprietary means of link interference and protocol manipulation.
- Of the 109 responses to the question of interoperability, 73 claim they are or have the means to be interoperable with other systems, generally through an application programming interface (API).

3.2. CUAS Market Observations

Throughout the study, researchers made several observations regarding the CUAS supplier market and product trends in products. In general there is incredible flexibility and desire from manufacturers to understand specific use cases and requirements as best as possible, so they can deliver products that meet those needs. The following observations highlight this fact.

Custom Solutions – CUAS manufacturers are asking for specific requirements from customers and from our survey data collection team, so they can deliver customized solutions. A few manufacturers expressed in phone conversations some difficulty in completing the survey because the answers are largely dependent on the specific configuration desired by the customer, including any optional equipment and capabilities. As an example, many manufacturers claim that they could integrate a kinetic mitigation technology as well as additional non-kinetic mitigations depending on what is required. Or, depending on the area to be protected, additional 'nodes' can be integrated together to provide greater area coverage. For this reason, many of the specifications, specifically the cost of the system, have been estimated by the manufacturer. Thus some manufacturers may not have an 'off the shelf' standard configuration as each deployment might be customized to individual site needs.

Many companies offer CUAS capabilities in multiple form factors or versions – such as a man-packable or handheld version, a mobile/portable/temporarily deployable version, and a fixed site version, each with increasing capability and range. Generally these can be easily integrated together or expanded upon in various ways to meet overall requirements. Examples include the following:

- CACI offers their library-based RF sense, track and mitigate solution in one of three packages: CORIAN, which is a fixed site multi-node configuration; AWAIR, a ruggedized mobile platform for land and maritime vehicles that leverages the CORIAN software; and Small Form Factor, which is a handheld-radio sized platform designed for man-packable/on-the-move applications. Figure 3-1 shows the CACI SkyTracker product line as an example.

Figure 3-1: CACI Skytracker Technology Product Line

- MyDefence offers three CUAS products (Watchdog, Wolfpack, and Eagle). In addition, it offers a solution called "Knox" that refers to any of a number of configurations combined to create a system.

Figure 3-2: MyDefence Technology Product Line

- Whitefox Defense Technologies offers their core mitigation technology in three form factors: a pocket wearable version (Scorpion), a vehicle-portable version (Dronefox Tactical), and a fixed-site rack-mounted version with lots of expansion capability.
- DJI offers their Aeroscope 'awareness-only' solution in three levels of capability – a portable suitcase-sized solution, and the fixed site mast-mounted G-8 and G-16 versions. The G-8 and G-16 versions offer increasing levels of sensing capability, range, and access to all meta-

data transmitted in the DJI C2 protocols, as well as support for network-based integration/communications capabilities. However, the system only reads and reports DJI-developed C2 protocols. Figure 3-3 shows the DJI product line.

Figure 3-3: DJI Aeroscope Product Line

- Several companies offer a full range of CUAS products to include C2 integration and software that can be selected and configured to provide customized capability and coverage from both a sensing and a mitigation perspective. An alternative and equally viable approach is to utilize several companies and a competent technology integrator to assemble a selection of technologies/capabilities to meet a specific set of requirements. Figure 3-4 shows an example from DroneShield.

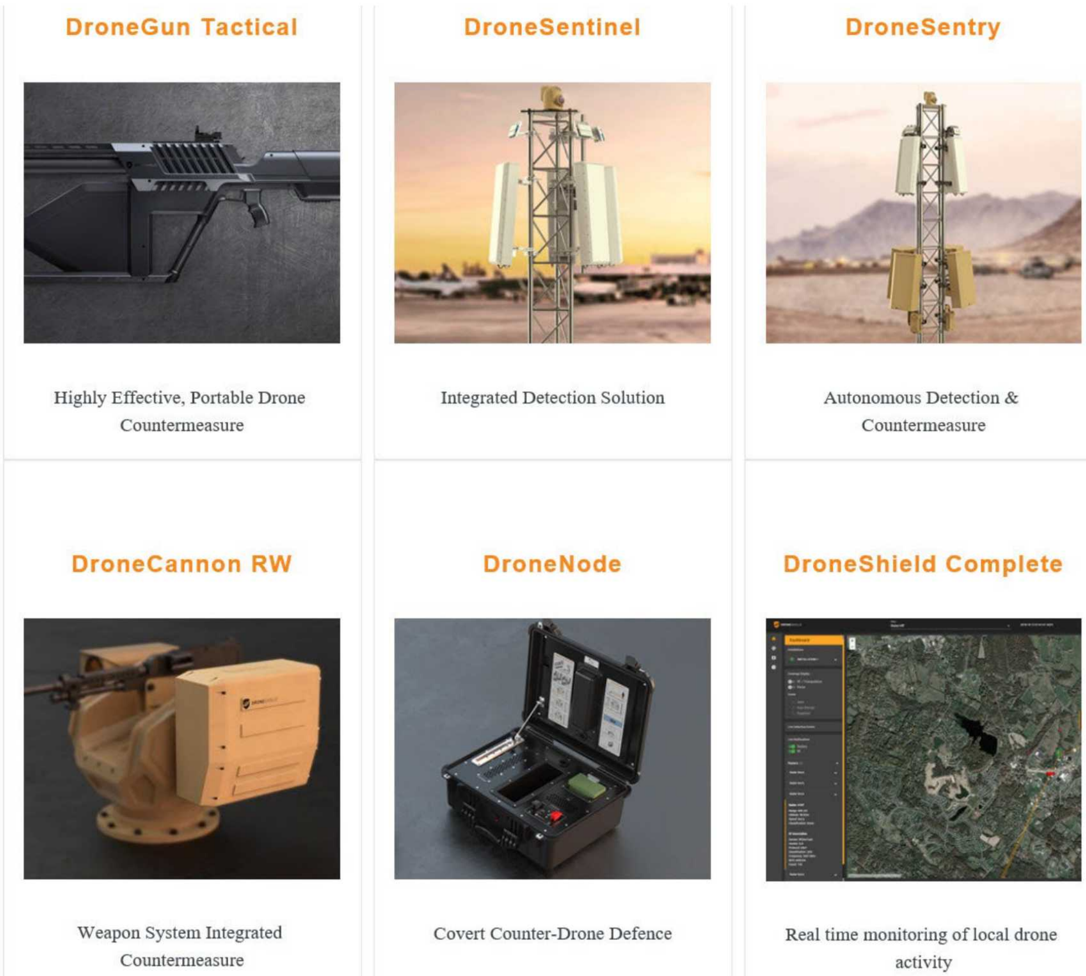


Figure 3-4: DroneShield Product Line Showing a Range of Sensing and Mitigation Technologies

Partnerships – CUAS companies are partnering to leverage each other's expertise and deliver a better overall product or to address needs in new markets. In some cases, defense firms are acquiring or partnering with smaller UAV manufacturers with niche capabilities. Examples include the following.

- The AUDS C-UAS system was developed by a consortium of UK defense companies including Blighter Surveillance Systems (A400 Series air security radars), Chess Dynamics (Hawkeye DS and EO Video Tracker) and Enterprise Control Systems (Directional RF inhibitor). Liteye is the US distributor for this system. It integrates, installs and trains operators in the US.
- DroneShield announced a teaming agreement with Thales in 2018 where Thales will promote DroneShield products in its defense and security CUAS contract bids in Spain.

- In 2018, Liteye and OpenWorks formed an exclusive partnership to offer an integrated low-collateral-damage CUAS defeat layer to Liteye's current offerings for military, law enforcement and security authorities.[13]

- Several companies have entered into partnerships with integrators to ensure incorporation of their component technologies when the integrator bid on requests for complete systems, especially in European markets. Examples include Orbital ATK, Blighter, Openworks, RobinRadar, and Northrop Grumman, each of whom has established relationships with various integrators.

- Companies that have been grouped together in US Government CUAS demonstration events to form more complete kill chain packages have maintained relationships and abilities to integrate with each other.

Resellers and System Integrators – System/C2 integrators have emerged to allow manufacturers to focus strictly on manufacturing and refining their core technologies rather than on integration, C2, sales, and distribution. Integrators claim they can deliver nearly any capability by integrating best-in-class products from across the CUAS industry. Resellers have emerged to capitalize on the emerging market and on opportunities for integration assistance and annual support.

- DJI has successfully monetized the detection and tracking of its own UAS communications links in a product called "AeroScope." Aeroscope is essentially a receiver and base station that reads the radio control and telemetry data of DJI aircraft and reports flight status, path, and other UAS information in real time. Several companies are reselling the capability, assisting with its integration, or offering a CUAS built on the AeroScope platform. This product only identifies, tracks, and reports DJI products. The OUO version of this report gives additional considerations. The threat space covers all platforms and UAS control systems, including fixed wing and hybrid flight/power platforms and tools that facilitate customization of default settings in the flight control software and firmware.[14,15,16] Examples of authorized companies reselling the DJI Aeroscope product include Flymotion, Gresco Technologies, and 911 Security.

- DeDrone uses technology partners to enhance its DroneTracker solution with additional sensors, countermeasures and integration technologies (e.g., Airbus, Battelle, and IACIT). Partners are also used as resellers/integrators of Dedrone's DroneTracker. Example partners include the following:

---

[13] https://liteye.com/openworks-signs-exclusive-agreement-with-liteye-systems-for-north-america/.

[14] For examples of tools that facilitate customized settings for fixed and multirotor flight controllers, see the following links: http://ardupilot.org/plane/docs/common-advanced-configuration.html; http://ardupilot.org/copter/docs/common-advanced-configuration.html; and http://qgroundcontrol.com/.

[15] Salton, et. al., SAND2015-4329, *Unmanned Aircraft Systems (UAS) Guidance: Policy, Utility, Threats, Vulnerabilities, and Countermeasures,* May 2015 (OUO).

[16] Salton, et. al., UAS Threat Addendum to SAND2015-4329 *Unmanned Aircraft Systems (UAS) Guidance: Policy, Utility, Threats, Vulnerabilities, and Countermeasures,* June 2017 (SNSI//NOFORN).

- Atlantic Diving Supply Inc. (ADS) is a reseller for DeDrone DroneTracker. ADS manages the consolidation of solutions and serves as a single POC for the customer, providing technical assistance, equipment, and customer support.
- EIDOS Technologies is a reseller/integrator for DeDrone DroneTracker. EIDOS is a software and data management company focused on security.

- Azgard Group is a reseller/integrator for Department 13's MESMER solution. Azgard Group is a cybersecurity and IT company offering solutions, training, and consulting to both commercial and government customers. The company offers CUAS, sensors, and RF Protocol Manipulation Systems.[17]
- Liteye claims to be a US distributor for AUDS, M-AUDS, M-AUDS-KE, C-AUDS, OpenWorks Skywall 100 and 300 systems, Northrop Grumman, and other solutions. It specializes in the design, manufacture, and supply of CUAS along with helmet-mounted display systems, surveillance radar, and thermal imaging products for use in defense, homeland security, and high-end commercial applications.
- escAerospace (Germany) is a systems integrator and does not offer stand-alone products of its own. It is vendor-independent and integrates drone detection and defense into the existing security engineering. It specializes in comprehensive concept development and intelligent implementation of drone detection and defense solutions.
- DroneShield has several camera solutions it can sell to customers (e.g., DroneHeat, DroneOpt, DroneBeam), although it has found that most customers already have cameras and prefer to integrate into existing cameras or cameras that are best suited to requirements and budget rather than purchasing DroneShield camera products.
- L3 Communications' DroneGuard solution is a C2 and control application designed to integrate data from multiple sensors and interface with different effectors. The customer's needs dictate the types of sensors and effectors used to complete the system, so cost, coverage, assessment range, and install time all depend on the types of sensors and effectors selected.

Limited or Confidential Information – Some companies have products that have not been marketed for various reasons, so in many cases there is no information on the company website about the CUAS solution. Sometimes it is because the system is still in the prototype stage of development or it was developed specifically for one sensitive customer and not necessarily for mass production. Defense companies may only make product information available to military or government customers on a confidential basis. Some examples of these situations are provided below.

- Alion Science & Technology is developing a device to take control of encroaching drones to avoid collisions with manned aircraft. The latest information found on this system was in 2016 when the company had a patent pending on the system and was reluctant to discuss its

---

[17] https://azgardgroup.com/products/drone-countermeasures.

specific features. No substantial information was found on the company website about this system.[18]

- Mitsubishi – A 2017 article in *UAS Vision* discussed Mitsubishi's first anti-UAV system, but no information on this system was found on the Mitsubishi website or from other sources. When asked about this system, company reps claimed it has only sold this system to "1 undisclosed government client."
- Northrop Grumman's DRAKE solution is a CUAS multi-function electronic warfare (EW) system. While a publicly distributed brochure is available upon request, information on frequency, power and effective distances is classified under the program's Security Classification Guide.
- NEC – A 2015 article appeared in *ComputerWorld* regarding NEC's surveillance system that can spot drones from up to 1 km. The system includes two cameras, acoustic sensors, and a radio detection finder. Currently, the system is still in the prototype stage and has yet to be given a name.

[18] https://www.ainonline.com/aviation-news/business-aviation/2016-05-17/counter-uas-system-horizon.

4. APPLICATION AND PLATFORM CONSIDERATIONS

The key benefit of the market survey and resulting database of products and technologies is that it can inform government agencies on the selection, acquisition, design, and implementation of available CUAS technologies according to their requirements. During these activities several factors must be considered to ensure the final system functions as intended or as required. This section discusses differences in CUAS applications and platforms and their impact on technology selection and deployment to meet user requirements.

4.1. CUAS Threat Engagement Sequence

The product data in the market survey can inform government agencies on the selection, acquisition, design, and implementation of CUAS technologies according to their requirements. However, reviewing this information requires some understanding of the range of activities and operations that are required in countering the UAS threat, and which portion(s) of the CUAS engagement sequence a particular product fulfills. A CUAS engagement sequence, or framework, defines the sequence of major steps needed to execute an effective response to a UAS threat. Figure 4-1 shows an example engagement sequence.

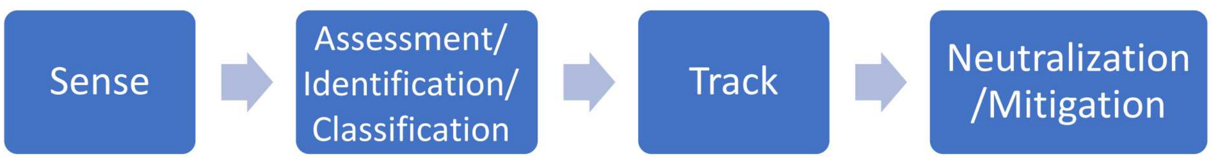


Figure 4-1: Example CUAS Engagement Sequence

The engagement sequence is an abbreviated version of the systems engineering model used for several decades now by physical security system professionals to analyze the performance and effectiveness of a security system, and the timeline associated with responding to a threat,[19] which was developed in the 1960s as a systems engineering approach to physical security. A diagram of the framework is shown in Figure 4-2, and a more comprehensive explanation is contained in This page left blank. But the essential point is that interruption and neutralization of a threat requires that it first be detected, then assessed to determine if it is a true alarm, a response initiated, and arrival of that response in time and with sufficient force/capability to effectively neutralize the threat.

[19] Garcia, Mary Lynn, *The Design and Evaluation of Physical Protection Systems,* 2nd Ed. Boston, Butterworth-Heinemann, 2008.

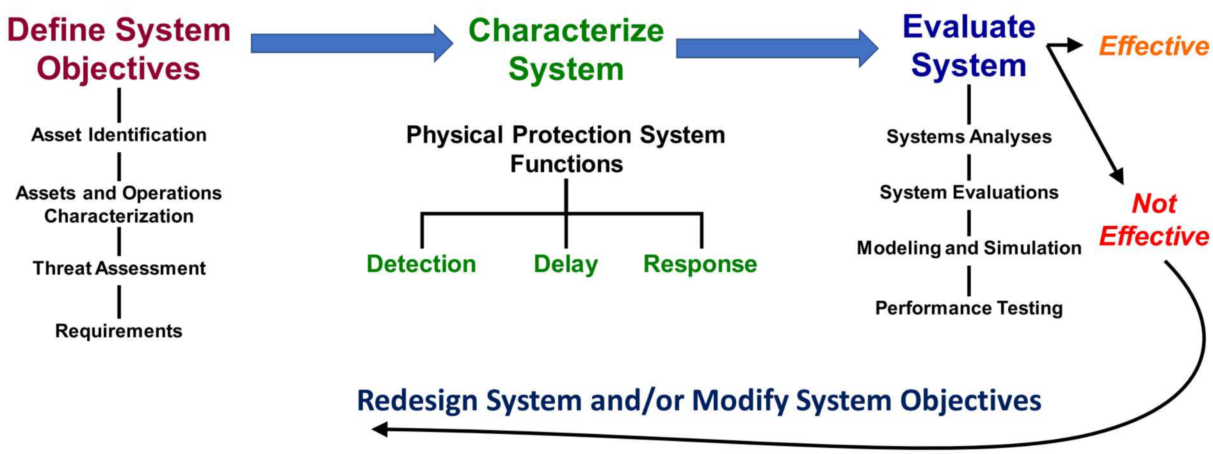


Figure 4-2: Systems Engineering Framework for the Design and Evaluation of Physical Security Systems

Different entities use slightly different terminology when applying the framework to CUAS and labeling the major steps in the engagement sequence; however, the engagement sequence typically contains the following core processes:

Sense: Sensing is the initial discovery and awareness that there is something in the air that the CUAS technology has determined is likely an unauthorized UAS. Some entities may refer to as detection or airspace awareness.

Assessment: Sometimes referred to as identification/classification, assessment is the process of determining whether the UAS alarm reported to the operator is in fact a true alarm requiring a mitigation response, and not a false or nuisance alarm. Often this can be achieved through optical means but many systems do not incorporate an optical assessment capability to facilitate human assessment/confirmation of sensor-reported alarm information. Whether this approach is required is policy dependent, however, this capability is important in situations where frequent pauses in commercial operations or dispatch of security/response personnel for nuisance alarms must be minimized. High nuisance alarm rates (NARs) lead to loss of confidence in the system and a tendency to ignore or turn off the technology altogether. Other forms of UAS assessment include use of additional or complementary sensing technologies in alternate phenomenologies (such as RF, radar, acoustics, optics, and machine learning) to attempt to identify the UAS make/model or to classify the type (multi-rotor, fixed wing, size, etc.). This approach can increase the confidence in the alarm data and provide additional information helpful in determining an appropriate response.

Track: Often a byproduct of or automated as a part of sensing, tracking is the continued monitoring of the UAS position history (track) and typically displaying it to an operator that is assessing UAS incursion alarms. There are multiple UAS sensing and tracking technologies available for consideration. Appendix C provides a summary and comparison of some UAS sensing technologies including their strengths and weaknesses, based on observations from testing and demonstration events.

Mitigate: An organization may need to initiate an appropriate response to counter any threat(s) posed by the target of interest. Mitigation is sometimes referred to as negation, neutralization, defeat, interdiction, or response. There is a wide range of non-kinetic and kinetic mitigation technologies available for consideration. Appendix D provides a summary and comparison of some types of UAS mitigations including their strengths and weaknesses, based on observations from testing and some demonstration events.

Once the UAS has been mitigated or defeated, the final response sequence to the UAS is not over. Any downed or defeated UAS should be treated as a suspicious object until cleared by the proper authorities. After being cleared, the UAS may need to be processed for forensics, used for prosecution, or identified for incident reporting and as such may need to be preserved to the greatest extent possible.[20]

When reviewing a CUAS technology for potential down selection or acquisition decisions, it is important to understand which portions of the engagement sequence the product or technology will fulfill, and how effectively it meets regulations, policy, or requirements related to that step in the sequence. For high risk applications, it may be important to consider whether there is sufficient backup or complementary capability within each step in the engagement sequence. It may be critical to have multiple and complementary means of sensing, assessment, tracking, and mitigation, based on threat characteristics, or physical limitations of any one single technology. For example, radar based sensing and tracking technologies typically have poor performance in inclement weather, due to high NARs, making it extremely difficult to differentiate an actual threat UAS from background clutter (rain). A complementary technology such as an RF sensor that is less affected by inclement weather may be able to sense any RF communications between the UAS and its base station.

The figure below illustrates one way that the mitigation step of the engagement sequence can be decomposed or partitioned further to show a range of potential response options, in order of increasing potential for collateral damage or safety risk. When reviewing a technology for potential down-selection or acquisition, it may be important to understand where the mitigation technology falls on this scale, its potential for collateral damage, and whether it enables or supports multiple forms of response (vs. just one type).

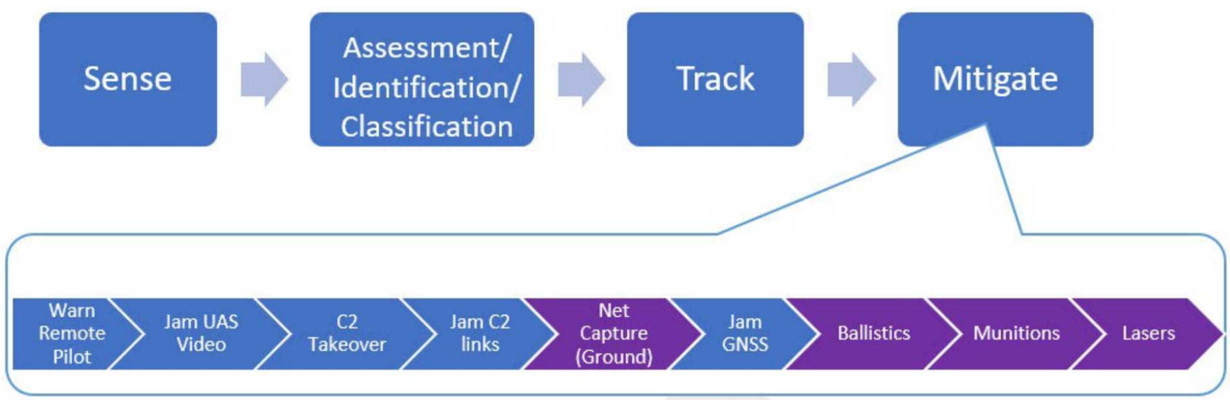


Figure 4-3: Example CUAS Mitigation Sequence

There are advantages and disadvantages to each type of mitigation and specific CONOP and policy implications. Several of the above mitigations may be required to have confidence in the ability to neutralize a UAS threat. Each is described further in SAND2019-0191.[21]

---

[20] National Science and Technology Council, CUAS Technology Fast Action Committee, *Standard Guidelines For Test and Evaluation Of Counter-Unmanned Aircraft Systems Technologies*, January 2019.
[21] Brooks, Watson, Kouhestani, SAND2019-0191, *Near-Term and Turnkey CUAS Solutions for Consideration,* January 2019 (OUO).

4.2. Platform Considerations

4.2.1. Handheld/Wearable Technologies

Technologies in this category span a very wide range of physical forms and transmit/communication capability, but are designed to be either worn on the body, carried in a backpack or in hand, or located inside a response vehicle for immediate deployment when needed (such as by a roving security patrol). They can be detection-only, mitigation-only, or have both features. A popular style are hand-held RF- and GNSS-mitigation systems that resemble a firearm. Examples include the following:

- Smart phone apps. These take advantage of sensors and capabilities in smart phones to provide localized awareness-only UAS sensing and reporting. Examples include apps that utilize the microphone to listen for UAS acoustic noise or apps that utilize the phone's radio/cellular communications antennas to listen for UAS-based Wi-Fi, telemetry, and video signal protocols. These typically provide very short range sensing around the operator depending on line of sight and signal strength. (e.g., DeTect Inc.'s DroneWatcherApp, Northrop Grumman's MAUI acoustic sensing App)

Figure 4-4: Example Smart Phone App from Detect, Inc.

- Body-camera styled units that are worn on a person and provide a simple audible or vibration alert when a UAS is in the area. This can be done via RF sensing within the unit itself, or by a larger site system that notifies the person if a UAS is approaching them. Some products come pre-programmed with automated mitigation features that can be initiated (depending on the UAS sensed, frequency band, and any white-listing features). Figure 4-4 shows the WhiteFox Scorpion battery-powered unit which is worn on a soldier's backpack shoulder strap or in a pocket. A simple on-off button controls operation. The Scorpion provides a small range of automatic UAS takeover/mitigation in the form of triggering RTL or Land behaviors.

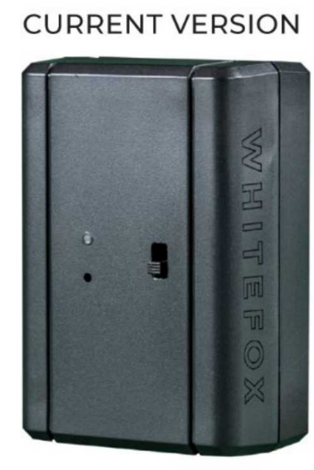


Figure 4-5: WhiteFox Defense Technologies Scorpion Wearable CUAS

- Handheld non-kinetic mitigation systems such as directional RF emitting 'guns' styled after firearms. Typically these are mitigation-only systems designed to jam (overpower) or interfere with C2, telemetry, or GNSS links, but might also some also include sensing features to aid an operator in sensing the UAS direction to aid in situations where the operator cannot see the UAS to understand where to point the RF-mitigation. Figure 4-6 shows examples from DroneShield and Batelle.

Figure 4-6: RF Emitting 'Gun' from Droneshield (top), and Battelle (bottom)

The handheld DroneKiller from IXI technologies utilizes a different technology than jamming. The DK transmits low-power RF waveforms that are substantially similar to those used by the UAS's ground station to communicate with the UAS. This generates a large number of bit errors in the on-board processor during the time the UAS is receiving both the C2 transmission and the DK transmission, causing the UAS to enter it's default lost link mode which is generally to either land or return-to-launch point. Figure 4-7 shows the DroneKiller.

Figure 4-7: IXI Technologies DroneKiller

- Portable kinetic net-capture systems such as game-capture net-guns, shot-gun bola rounds, and shoulder-fired net projectiles. Generally these systems rely on a person (or other integrated technology) to provide the UAS sensing/tracking/assessment. Range is usually very limited. Some systems can be linked wirelessly to a fixed site's larger sensing and C2 systems to alert and aid the operator in locating the UAS. Figure 4-8 shows the Skywall 100; Figure 4-9 shows the AMTEC Skynet round.

Figure 4-8: Skywall100 Launcher, Projectile, and Stowage Case

Figure 4-9: AMTEC Skynet shotgun rounds

- Firearms. Human tracking and aiming of small caliber firearms has been demonstrated in multiple events to be very ineffective as a kinetic mitigation, even against hovering targets. However, several companies have outfitted firearms with aim-assist and target-tracking/lock-on technologies to improve the probability of hit and probability of kill of a UAS. [e.g., AimLock, Inc., R-M1]. A few companies have developed 25- and 40-mm munitions for improved kinetic performance as well. (For example, General Dynamics AFCAS, Nammo Programmable Ammunition (Norway).) Figure 4-10 shows the Aimlock R-M1 which is meant more as a ground-mobile system, mounted on a vehicle as a remotely operated weapon system (ROWS). These technologies might not have policy support for domestic use.

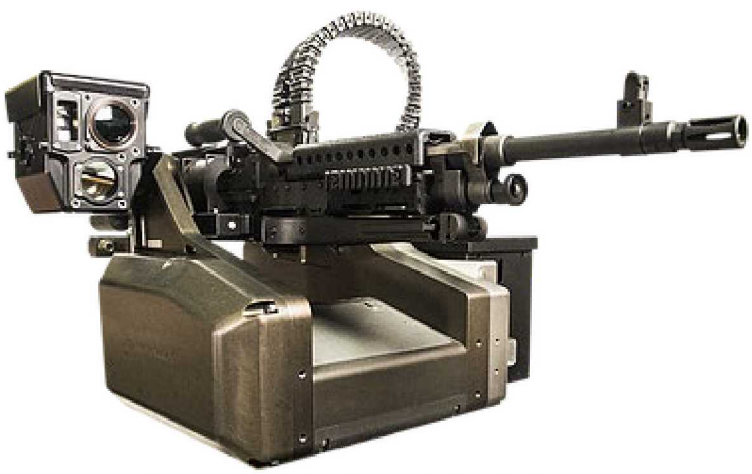


Figure 4-10: AimLock R-M1 CUAS

4.2.2. Portable, Man-packable, and Ground-Mobile Technologies

Some applications may require systems that are more suited for mobile UAS operations. Examples include convoys, land and maritime-based shipments, temporary operations/surveillance, or other moving assets, VIP protection, and operations that transition from fixed site to mobile conditions such as at forward operating bases. Systems meant for mobile operations may or may not be smaller form factor versions of larger fixed-site systems designed to provide on-the-move awareness and mitigation capability around the mobile operation. Typically the mitigations are RF-based only, but tethered intercepting UAS and other mitigation options do exist.

Figure 4-11 shows the AFRL NINJA lineup, which includes an "on the move" RF detect, ID, track and defeat configuration of C2 Links with library-based system fingerprint and soft kill recipes. It is not an RF "jammer" but utilizes RF techniques to take over and defeat the UAS using COTS software-defined radios. With eight independent assignable RF detect/counter channels, it enables crowd sourcing of new capabilities from across US government agencies.

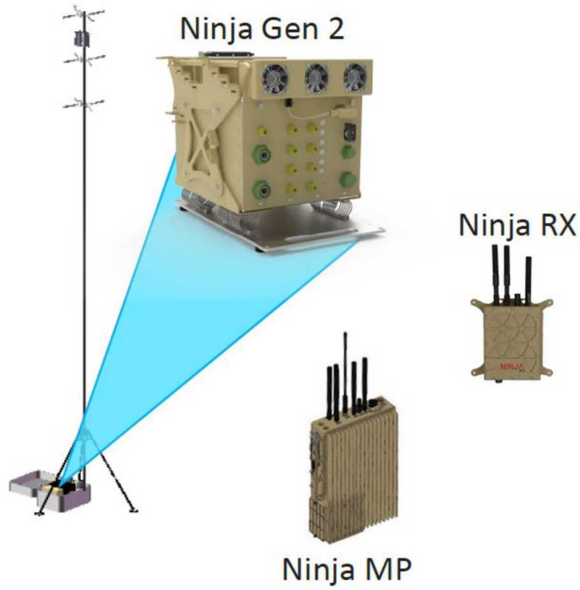


Figure 4-11: AFRL NINJA Product Line, including MP (Man-Packable)

Figure 4-12 similarly shows multiple man-portable products from Elta-North America including the man-portable aerial radar kit (MARS-K), or the more encompassing man-portable anti-drone system kit (MADS-K), which includes the MARS-K Radar with EO/IR optics and a directional jammer with radar slew to cue. Each has been integrated into prototype 'on-the-move' vehicle configurations, and other options include portable long-range RF take-over capability and aim-assist slew-to-cue technology for infantry small arms (smart shooter).

Figure 4-12: Clockwise, from Top left: MARS-K, MADS-K, 'on-the-move' prototypes, and Smart-Shooter (SMASH) from Elta North America

Such products should be ruggedized to support frequent movement, rough conditions, and exposure to the elements. The CUAS may be fixed to and even receive power from the vehicle, and operate either as commanded by an operator or in an autonomous mode (e.g., automatically attempt to block or mitigate any UAS RF signals detected). Testing of these systems prior to acquisition or deployment is recommended first in a static mode, and then in a mobile mode, to identify performance strengths and weaknesses, and to determine how performance is impacted by operational factors, such as vehicle speed, separation (for multi-node systems), background, and threat characteristics.

Geo-location (3D position estimate) of UAS threats can be challenging for 'one-the-move' mobile systems that are unable to read internal telemetry data from the UAS. In some cases, the CUAS might only be capable of providing an azimuth or line-of-bearing (LOB), to indicate the direction of the sensed UAS. Distance and altitude/elevation may not known, but security personnel can look in the indicated direction and determine a course of action. This is already challenging during the day and is more difficult at night. For mobile operations, systems that automatically take over the non-whitelisted aircraft within its sensing volume and command a land or return-to-launch action without knowing the aircraft position/location may be a more suitable and effective concept of operation (CONOP) than trying to determine the aircraft's exact position and track it.

Figure 4-13 shows a larger system set-up in one type of ground-mobile configuration, in which larger generator powered equipment is towed behind a vehicle, and parked in a temporary location. This is one common configuration for fixed-site equipment being brought to a test/demonstration event, to facilitate rapid movement, setup and demonstration of the technology. In a true deployment, the equipment can be set up in a fixed-site configuration described in Section 4.2.3.

Figure 4-13: Example CUAS that can be set up in a towable ground-mobile configuration

4.2.3. Static (Fixed Site) Applications

Though many systems are advertised as ‘easy to setup’ and ‘portable’ to appeal to a broader market base including temporary military or police operations, they might be best operated in a permanently-installed configuration. This allows optimization of the configuration for the area to be protected and any unique conditions such as terrain, line-of-sight, weather, policy constraints, and threats of interest. Primary design concerns include providing clean power and reliable communication connections between system components, in locations that are access-controlled by the site, and in a configuration or placement that provides optimal coverage for security areas of interest and against the threats of concern. This may require balancing or compromises against other constraints. This may require mounting sensors atop towers, buildings, or tall masts, and networking multiple sensing nodes into a complete area/perimeter solution with a C2 system at a protected command center that receives all edge and network device information and commands all mitigation actions (Figure 4-14). Figure 4-14 shows a kinetic technology for a fixed site application.

Figure 4-14: Example of Fixed-Site CUAS (Detect Inc. DroneWatcher LT)

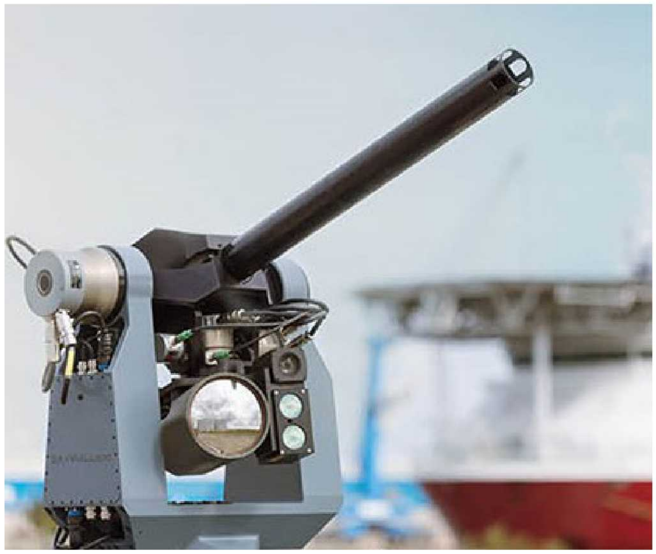


Figure 4-15: Example of a Kinetic Mitigation (net projectile) for Fixed-Site Application (Skywall 300)

Many CUAS technologies can sense and geolocate UAS at very long ranges (12+miles), but capability and accuracy may depend on the type, geometric spacing and height of sensing components, or the ability to directly interpret the telementry data in the RF communication protocol. Expenses associated with providing power or communications to an ideal sensing node location may require compromises in placement, which may impact sensing or tracking performance. Sensing components will typically be located on elevated positions in access-controlled locations such as rooftops of alarmed buildings, water towers, or other tall infrastructure to improve line-of-sight concerns with foliage, skyline, or terrain features that may inhibit performance.

As UAS technology (such as autonomous navigation) evolves, sites should consider the extent to which the technologies that comprise their CUAS are robust to changes in the threat, or how the system can evolve over time to keep pace with the changing threat characteristics. For example, suppose a CUAS product relies completely on RF emissions such as radio control, telemetry, video transmission, or UAS traffic management beacons for sensing and mitigation. If the threats of concern evolve to an alternative form of navigation or control such that they are not transmitting RF (e.g., flying dark) or do not rely on GNSS signals, the system may not be able to sense, track, identify, or mitigate the UAS. A different or complementary phenomenology may be needed to compensate for this condition.

Important design considerations for fixed-site applications may include answers to the following questions. Brackets after each bullet indicate the portion of the physical security system design/evaluation framework it relates to, to help understand the context of the question or issue. For reference, the PSS design/evaluation framework is shown again as Figure 4-16. It is important to keep this framework in mind when considering aspects of CUAS selection, testing, acquisition, deployment, CONOPS/Policy and operations.

- What UAS threats or adversary actions should be sensed and mitigated? What UAS incursion characteristics are important from a security perspective? [Define PSS Requirements, Threat Definition]
- How far away should the CUAS begin to sense and track approaching UAS? What is the range of UAS speeds that can reasonably be expected? [Define PSS Requirements, Detection, Delay, Response, Path Interruption Analysis]

- How will alarms be handled – are all UAS alarms presented to the operator or security professional treated with equal weight and as true alarms? (Note, all CUAS technologies tested to date have a non-zero nuisance/false alarm rate) Or will an independent means of assessing those alarms be provided to allow verification of the alarm condition prior to exercising a mitigation action? (e.g., via camera or an alternative sensing system that relies on separate phenomenology to generate an alarm.) [Detection, Alarm Assessment]
- What legal mitigation authorities are allowed, and what is the CONOP for exercising those mitigations, and the order of escalation (or rules of engagement)? Does the CUAS support these policies? [Regulatory Requirements, Response Planning]
- Can any of the CUAS engagement sequence steps including mitigation be automated, or will a person staff and operate the system 24/7? What decisions are they authorized/required to make? [Define PSS Requirements]
- What are the UAS altitudes of concern directly overhead, and other distances from areas of security interest? (e.g., A UAS may be able to get above a radar with a narrow field of view, or not remain in the field of view long enough to generate a useful track to an operator, and therefore approach undetected.) [Threat Definition, Define PSS Requirements]

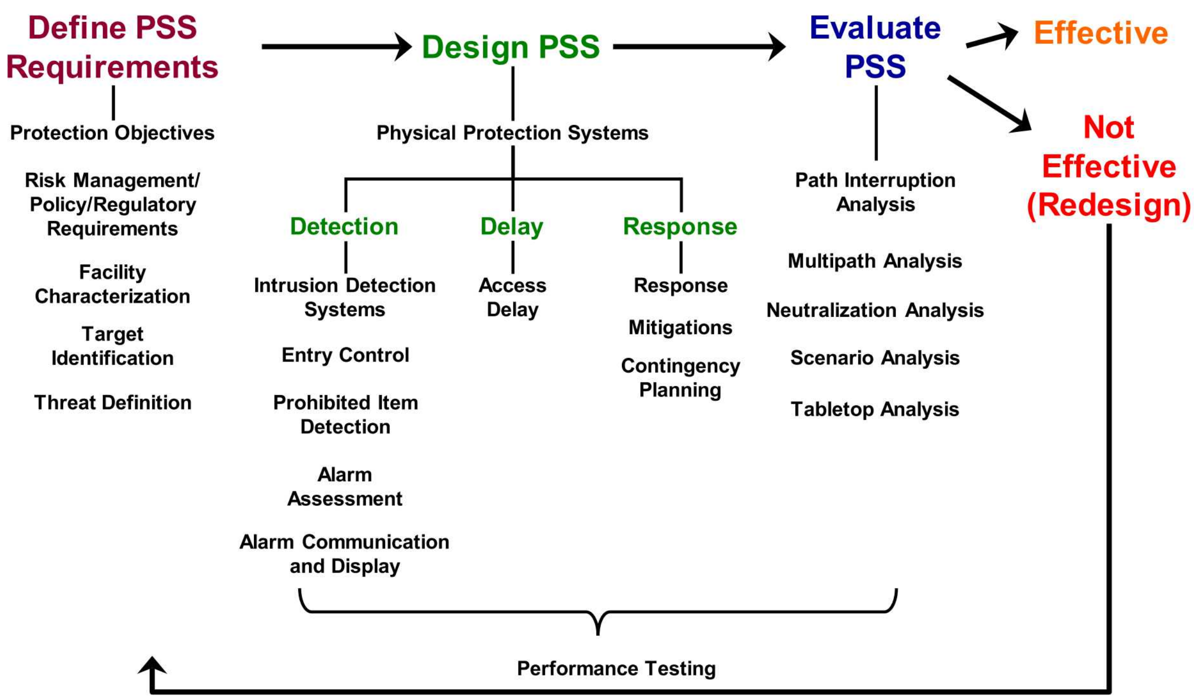


Figure 4-16: Systems Engineering Framework for the Design and Evaluation of Physical Security Systems

4.2.4. Aerial/Intercepting UAS Platforms

Some applications may benefit from use of an intercepting UAS, which can be considered a special form of kinetic mitigation (Figure 4-15). Typically the UAS platform only comprises the mitigation portion of the UAS engagement sequence, with long-range sensing, tracking and assessment/identification provided by other ground-based sensors. Multiple mitigation payload options exist (including RF/electromagnetic interference, or even UAS designed to ram the threat aircraft) but the most common market approach is an autonomous UAS with deployable entanglement capability (nets, streamers, etc.).

Most, if not all net-capture-based intercepting UAS companies have moved away from human-piloted net-capture strategies. Instead they incorporate machine learning and processing of data received from sensor payloads/technologies adapted from self-driving automobile industry to automate navigation, threat-UAS tracking/following, and timing of entanglement deployment. Though currently the maturity is low, autonomous UAS-on-UAS technology already exceeds the ability of human pilots to manually track, follow, and capture an evading UAS.[22] This capability requires integration with other ground-based sensing and tracking technologies so that the intercepting UAS can be directed to the general response area first. Depending on where it is used, this technology may require temporary halting of some fixed site operations while the intercepting UAS is in use.

Figure 4-17 shows the Dronehunter UAS from Fortem Technologies, and the Airspace Galaxy system which inclues an autonomous UAS as a mitigation option. Both systems must receive general threat location data to determine a general intercept course. The DroneHunter uses an onboard radar for local target tracking and net deployment determination. The Airspace system uses onboard optical sensing and machine learning for local target tracking and streamer entanglement deployment.

[22] Brooks, Watson, Kouhestani, SAND2019-0191, *Near-Term and Turnkey CUAS Solutions for Consideration,* January 2019, page 12 (OUO).

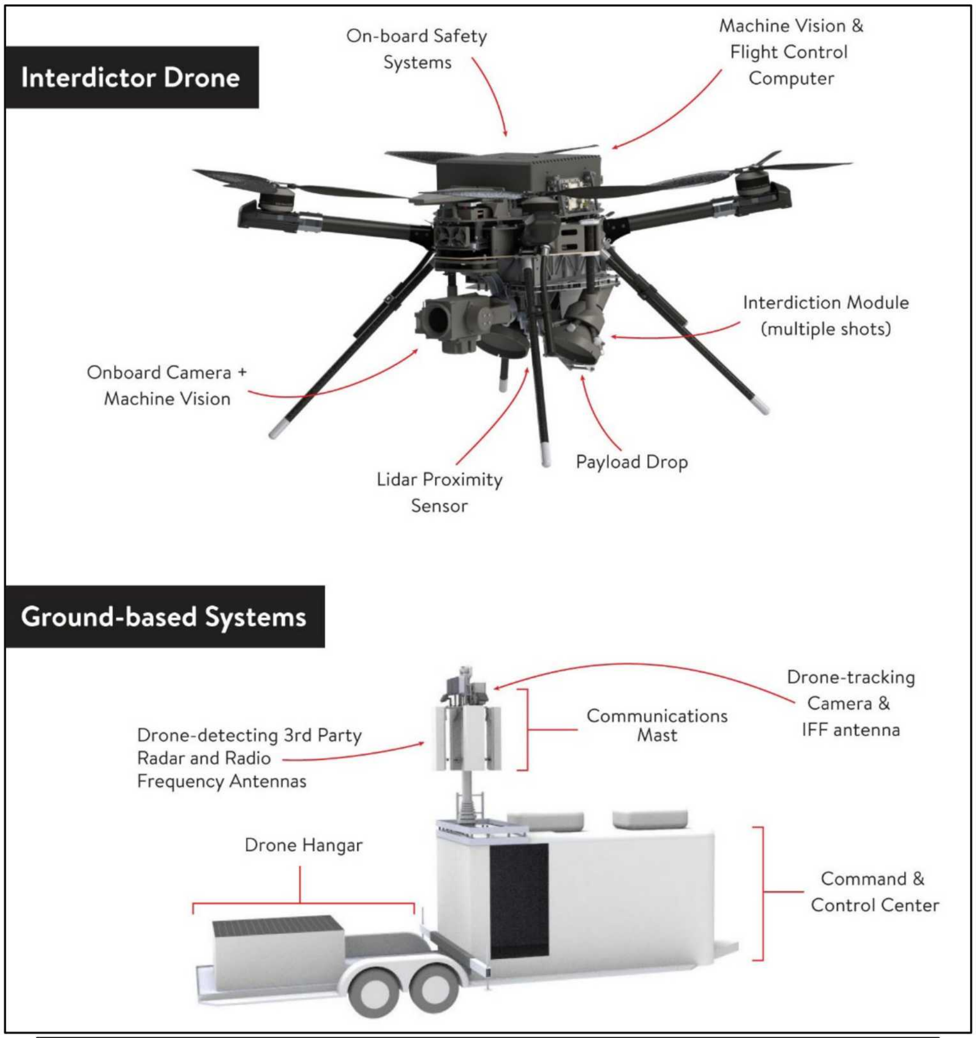


Figure 4-17: Airspace (top) and FORTEM DroneHunter-UAS (bottom)

4.3. Temporary Measures

A large, full-featured ground-fixed system covering the entire area of interest may take several months or more to design (following an onsite survey to determine suitable/optimal installation locations), deliver, provide infrastructure for, install, integrate with existing security or C2 systems, and certify (receive all required authorities to operate). However, many manufacturers offer turnkey ground-mobile or portable solutions. These may be suitable temporary measures. Often these are portable or scaled versions of their larger systems, and sometimes designed for minimal or no input from an operator. Alternatively, many of the ground-fixed platform products identified through the market survey can be deployed in a rapid, stand-alone and temporary configuration. Although such a configuration may not be optimal, it may provide an acceptable level of performance until more permanent means are established.

4.4. CUAS Performance Requirements

CUAS technologies will require a variety of capabilities (e.g., sensing, assessment, and neutralization) to effectively mitigate a UAS threat, due to the range of UAS capabilities, potential CUAS deployment locations/environments (e.g., urban versus rural), and use cases. Initially, the majority of CUAS technologies offer a single sensing phenomenology, single assessment phenomenology (or no assessment means), and single neutralization phenomenology (with particular emphasis on RF techniques). As the UAS threat evolves, an enduring CUAS sensing, assessment, and neutralization capability is needed. This could be achieved by utilizing complementary sensing, assessment, and neutralization phenomenologies.

The CUAS products identified through this survey should not be thought of as having static capabilities or features, or that their performance is limited to the stated specifications (e.g., RF mitigation power levels that can easily be modified to meet requirements). It is important to remember that many manufacturers generally want to deliver the best product or configuration of their product that they can, to meet the users' needs. Many are willing to customize certain aspects or the configuration, including integration of additional sensors or components to meet any requirements. Depending on the requirements, multiple systems or component types may have to be utilized and integrated. It is important to establish performance requirements in terms of the following topics:

- Vendor maturity, stability, and support. For example, evidence that the vendor is financially stable and will be around long-term to support and update the product over time. Evidence the vendor has support programs in place for existing customers
- How the CUAS should integrate with existing CONOPS including whether it will need to integrate with any existing systems/C2 software or whether it will operate in a stand-alone mode
- Number of operators required, and level of training required
- Power and communication infrastructure requirements
- Required ranges for sensing, assessment, and mitigation capabilities based on UAS threat characteristics (size, altitudes, speeds, distances, and navigation methods)
- Frequency bands for sensing, tracking and mitigation of UAS control, telemetry, and video transmissions and GNSS signals
- Mitigation characteristics including types of mitigations desired (considering policy, potential for collateral damage, and ongoing evolution in UAS navigation technology) and the number of simultaneous or successive UAS that can be mitigated
- Maximum NARs

- Product technical maturity. Depending on the level of acceptable risks, it may be important to obtain evidence of a product or technology's readiness level
- Acquisition costs vs. deployment/installation costs vs. annual operation and support costs

5. CONCLUSIONS AND PATH FORWARD

The past few years have seen a significant rise in the global number of CUAS products and technologies. This market survey identified over 300 such products, then collected technical data on more than 225 of the products. A significant number of these have international sales and many have been demonstrated in test events, making down-selection challenging given the number of choices. New products are continually being discovered.

Identified products span all possible platforms, including wearable, hand-held, man-portable, mobile, fixed site, and aerial. Common means of sensing and tracking are RF triangulation of UAS communications and radar based detection of moving objects in the airspace. A wide range of non-kinetic and kinetic mitigations exist, including aerial payload and handheld versions of each. Lower maturity but developing technologies include lasers, EMP, optical EO/IR sensing, and machine learning. Because machine learning has the potential to greatly improve optical sensing as well as kinetic capture/kill capability, several companies are incorporating the technology.

The market survey culminated in the creation of an accompanying database of technical and proprietary data on most of the identified products. This information is considered OUO and is exempt from public release under the Freedome of Information Act.

5.1. Next Steps

Because this survey represents a snapshot in time, and the CUAS and UAS markets are evolving, it is recommended that the market survey be repeated on a periodic basis to maintain currency. This will enable improvements in data quality and accuracy, and identification of technical trends over time.

5.2. Lessons Learned

Several lessons were learned in the market survey process that, if implemented can improve the quality and efficiency of future surveys.

- Effective range of RF-based mitigation systems was not collected because this value will depend on many factors. However, in future surveys RF antenna power and gain specifications should be collected, so effective ranges can be estimated automatically using a standardized set of analysis assumptions to normalize the results. This way it will be clear what the performance estimate is based on system specifications. These data and calculations were outside of the scope of this work, given the short duration and importance of balancing data collection against time it takes to respond to the market survey.
- The use of the FBO.gov website in support of an RFI was very helpful, however, RFI responses were submitted via email to the RFI owner. For future surveys, responders will be directed to a secure website allowing them to register an account, set up a username/password, and enter technical data/responses into the web interface. This will allow population of the database to be an automated process, allow users to update and revise their information at any time, and enable upload of supporting information such as whitepapers, marketing brochures, spec sheets, videos, photos, etc. This will also improve responders' confidence in the security of their proprietary information.
- Specific use cases and requirements were unknown at the time the survey questionnaire was developed. In the future, the survey can more easily address focused interagency needs by ensuring nomenclature, questions, and allowable responses/choices are standardized and directly tie back to requirements.

- Down selection of a CUAS may require information on the vendor characteristics (size of company, years in business, quality program, certifications, financial stability, etc.). This information may enable down-selection criteria focused on risks associated with the manufacturer.
- It was observed that installation time may not be a great differentiator between products; this is largely because the time required to unpack, place, connect, and turn on or configure equipment is quick for nearly all products. The question on installation time may need to be adjusted to reflect other concerns such as-pre- and post-install activities required to actually finalize the deployment.

REFERENCES

2014-2018 BlackDart event reports and participant lists.

2015-2016 Desert Chance I, II, III event reports and participant lists.

2016 and 2017 National Nuclear Security Administration (NNSA) CUAS test event reports and participant lists.

2017 Adaptive Red Team/Technical Support and Operational Analysis 17-4 event participant list.

2017-2018 Hard Kill I, II event reports and participant lists.

2017 Department of Homeland Security TACTIC II event participant list.

9AB0-16, *Global Defense Counter-UAS Technologies Market, Forecast to 2022*, Frost & Sullivan, October 2017.

9AB0-22, *Global Commercial Counter-UAS Technologies Market, Forecast to 2022*, Frost & Sullivan, October 2017.

"Anti-Drone Market Analysis and Segment Forecasts to 2024," Grand View Research, 2018.

Arthur Holland Michel, COUNTER-DRONE SYSTEMS, Bard College Center for the Study of the Drone, February 2018.

Birch, et. al., *UAS Detection, Classification, and Neutralization: Market Survey 2015,* SAND2015-6365, Sandia National Laboratories, February 2015 (UUR).

Brooks, et. al., *Counter-Unmanned Aircraft Systems Market Survey*, SAND2019-1468, Sandia National Laboratories, February 2015 (OUO).

"Counter UAS industry directory," March 2018.V1, www.unmannedairspace.info.

DF0152SR, "Global Military UAV Market 2018-2028," Strategic Defence Intelligence, May 2018 PowerPoint presentation.

Homeland Security Systems Engineering and Development Institute Assessment of Current Kinetic/Non-Kinetic Options, June 30 2016.

Huw Williams, Derrick Maple, Chris Hawkins, MN Wasif, Scott Johnson, Geoff Fein, "Technical Outlook For Global C-UAS Capabilities," Jane's by IHS Markit, April 2017 PowerPoint presentation.

NI-BRIS-004/01, *BRISTOW 18 Final Report,* Nexus Imaging Ltd., funded by the UK Centre for the Protection of National Infrastructure and the Defence Science and technology Laboratory, June 2018.

This page left blank

APPENDIX A. REQUEST FOR INFORMATION FORM

Department of Homeland Security Counter Unmanned Aircraft System Request for Information (RFI)		
Field Name	**Field Description**	**Enter Information in Fields below**
General Product/Company Information		
Product Name	*What is your counter-UAS product name?*	Click or tap here to enter text.
Manufacturer	*What is your Company's name?*	Click or tap here to enter text.
Country of Origin	*Enter your product's country of origin?*	Click or tap here to enter text.
Website	*Enter company's website address*	Click or tap here to enter text.
POC1_Name	*Best person to contact?*	Click or tap here to enter text.
POC1_Title	*Contact's title?*	Click or tap here to enter text.
POC1_Phone	*Phone number to reach you?*	Click or tap here to enter text.
POC1_Email	*Email address?*	Click or tap here to enter text.
POC2_Name	*Contact's name?*	Click or tap here to enter text.
POC2_Title	*Contact's title?*	Click or tap here to enter text.
POC2_Phone	*Phone number to reach you?*	Click or tap here to enter text.
POC2_Email	*Email address?*	Click or tap here to enter text.
Number of Customers	*How many customers have purchased this product?*	Click or tap here to enter text.
Customer List	*Please provide a sample listing of customers who have purchased this product.*	Click or tap here to enter text.
Number of Systems Deployed	*How many units of your product have been deployed/ or are operational worldwide?*	Click or tap here to enter text.
Status	*What is the maturity or level of development of your product?* *(Please use one of the following choices: prototype, in development, production/operational, no longer offered.)*	Click or tap here to enter text.

Department of Homeland Security Counter Unmanned Aircraft System Request for Information (RFI)		
Field Name	**Field Description**	**Enter Information in Fields below**
Cost Information		
Unit Cost *($ USD)*	*What is the cost of the complete/full system with all typical components?*	Click or tap here to enter text.
Area Coverage *(Please use km^2)*	*What size area can be protected by one unit?*	Click or tap here to enter text.
Install Time	*Typically, how long does it take to install the above quoted system at a fixed facility? Assume all required power and communications infrastructure exist at all required locations.*	Click or tap here to enter text.
Annual Cost *(in thousands, $ USD)*	*Although annual support costs might vary with the implementation, what are the typical total annual maintenance, support, and update costs (e.g., full service contract)*	Click or tap here to enter text.
Number of Persons	*How many people does it take to operate all aspects of your CUAS product? That is, alarm monitoring, alarm assessment, tracking, response/mitigation, troubleshooting, etc.*	Click or tap here to enter text.
Technical Characteristics		
Platform 1 (select one)	*What is the platform type of your CUAS product? If multiple platforms are applicable, please list each type separately below.* *(Please select Aerial, Ground Fixed, Ground Mobile, Handheld/Person, other-please specify)*	Click or tap here to enter text.
Platform 2 (select one)		Click or tap here to enter text.
Platform 3 (select one)		Click or tap here to enter text.

Department of Homeland Security Counter Unmanned Aircraft System Request for Information (RFI)		
Field Name	**Field Description**	**Enter Information in Fields below**
Sensing Technical Characteristics		
UAS Sense Technology 1	*What technologies do you utilize to sense or track the UAS threat? List all that apply, using a single entry per row. Leave blank if N/A.* *(Please select Electro-optical, infrared, radar, RF signal emissions, acoustic/ seismic, human, other-please specify)*	Click or tap here to enter text.
UAS Sense Technology 2		Click or tap here to enter text.
UAS Sense Technology 3		Click or tap here to enter text.
UAS Sense Technology 4		Click or tap here to enter text.
UAS Sense Technology 5		Click or tap here to enter text.
RF Sensing Type 1	*If sensing is based on detection of RF transmissions, what specifically about the UAS is being sensed by your product? List all that apply but only one per row; leave blank if N/A.* *(Please enter: Controller/handset, telemetry/data link, video, Wi-Fi, cellular communications, other-please specify)*	Click or tap here to enter text.
RF Sensing Type 2		Click or tap here to enter text.
RF Sensing Type 3		Click or tap here to enter text.
RF Sensing Type 4		Click or tap here to enter text.
RF Sensing Type 5		Click or tap here to enter text.
Signal Decode	*If sensing is RF-based, does the system decode the RF transmissions to gather additional UAS information? (Please enter Yes or, No)*	Click or tap here to enter text.
Sense Track Range *(km)*	*What is the typical maximum horizontal sensing/tracking distance (km) for a small (Group 1, <10lbs, or ~0.01m²) UAS?*	Click or tap here to enter text.
Assessment Camera	*Does it include an integrated camera to allow an operator to optically verify the cause of an alarm? (Please enter Yes or, No)*	Click or tap here to enter text.
Assessment Range *(Please use km)*	*If so, what is the typical maximum effective range for optical assessment of a small UAS?*	Click or tap here to enter text.
UAS Identification	*Does your product identify the type of UAS (fixed vs. rotary wing) or the make/model? (Please enter Yes or, No)*	Click or tap here to enter text.
Identification Method	*If your product is capable of identifying the UAS make/model, is an exact match against an internal library required to generate a UAS alarm? (Please enter Yes or, No)*	Click or tap here to enter text.
Number of Simultaneous Sense-Track	*What is the number of UAS that can be simultaneously sensed/tracked without degrading system performance/latency*	Click or tap here to enter text.

Department of Homeland Security Counter Unmanned Aircraft System Request for Information (RFI)		
Field Name	**Field Description**	**Enter Information in Fields below**
Provides UAS Track	*Does the system provide UAS Track history?* *(Please enter Yes, No, or N/A)*	Click or tap here to enter text.
Provides Position	*What kind of position information on the threat UAS is provided?* *(LOB, 2D geolocation, 3D location, alarm only [no position], N/A)*	Click or tap here to enter text.
Mitigation Technical Characteristics		
Mitigation Type	*What type of mitigation is used?* *(Non-kinetic, kinetic, intercepting UAS, multiple, N/A)*	Click or tap here to enter text.
Non-kinetic 1	*If your product has non-kinetic capabilities, please list all that apply; list each in a separate row.* *(Please enter: RF interference, GNSS interference, RF deception/control, GNSS deception, acoustic, EMP, or other-specify)*	Click or tap here to enter text.
Non-kinetic 2		Click or tap here to enter text.
Non-kinetic 3		Click or tap here to enter text.
Non-kinetic 4		Click or tap here to enter text.
RF Shape	*If an RF mitigations are used, are the antennas: omni-directional, directional or both?* *(Please enter: Omni-directional, directional, both, or other-specify)*	Click or tap here to enter text.
GNSS Bands	*Which GNSS bands do you mitigate?* *List all that apply: GPS: L1, L2, L5, GLONASS: G1, G2, G3, Galileo: E1, E5, E6, other-specify. Leave blank if N/A.*	Click or tap here to enter text.
Kinetic 1	*If your product uses kinetic mitigation(s), please List all that apply; list each in a separate row.* *(Laser, ballistic, net capture, entanglement, ballistic munition, guided munition, other-specify)*	Click or tap here to enter text.
Kinetic 2		Click or tap here to enter text.

Department of Homeland Security Counter Unmanned Aircraft System Request for Information (RFI)		
Field Name	**Field Description**	**Enter Information in Fields below**
Intercepting UAS 1	*If your product uses an intercepting UAS (hunter-killer UAS) what mitigation payload capability is utilized? If more than one type is provided, please list each in a separate row.* *(Please use net capture, entanglement, projectile/munition, RF, EMP, other-specify)*	Click or tap here to enter text.
Intercepting UAS 2		Click or tap here to enter text.
Kinetic Range *(km)*	*What is the typical maximum range of your kinetic mitigation capability? For example, net capture, claimed effective distance.*	Click or tap here to enter text.
Number of Simultaneous Mitigated	*How many UAS can be mitigated simultaneously, including cases where the UAS are on separate frequency control bands?*	Click or tap here to enter text.
Test/Demo History		
Event 1	*If you have participated in any CUAS Test/demonstration events in the past three years, please list the event name and date (year). Please list each one in a separate row.*	Click or tap here to enter text.
Event 2		Click or tap here to enter text.
Event 3		Click or tap here to enter text.
Event 4		Click or tap here to enter text.
Event 5		Click or tap here to enter text.
Event 6		Click or tap here to enter text.
Event 7		Click or tap here to enter text.
Event 8		Click or tap here to enter text.
Event 9		Click or tap here to enter text.
Event 10		Click or tap here to enter text.
Product Description		
System Description	*Please describe your product? How is it operated? What are the components? What are its capabilities?*	Click or tap here to enter text.

Department of Homeland Security Counter Unmanned Aircraft System Request for Information (RFI)		
Field Name	**Field Description**	**Enter Information in Fields below**
Interoperability 1	*Describe the your product's "interoperability." For example, does it have an open software architecture so it can be connected to an existing C2 system? Can other components communicate with it? Do you provide an API? Is it compliant with any sensor communication standards like CoT, TCUT or SEIWG-ICD-0101B?*	Click or tap here to enter text.
Interoperability 2 *(Yes, No)*	*Do any of the descriptions listed for Interoperability 1 (or similar) apply?*	Click or tap here to enter text.
Tech Support	*Please describe any training, operations, maintenance, and troubleshooting support you provide post-sale. (For example, Is the support offered onsite or by phone? Is the support free for a given duration? Is a service/subscription contract required for ongoing support? Is there an annual fee for support?)*	Click or tap here to enter text.
References		
Reference 1	*If your product has been assessed or evaluated in any US government agency reports, please provide the report reference information (if known) (e.g., author, title, and date).*	Click or tap here to enter text.
Reference 2		Click or tap here to enter text.
Reference 3		Click or tap here to enter text.
Reference 4		Click or tap here to enter text.
Reference 5		Click or tap here to enter text.
Reference 6		Click or tap here to enter text.
Reference 7		Click or tap here to enter text.
Reference 8		Click or tap here to enter text.
Reference 9		Click or tap here to enter text.
Reference 10		Click or tap here to enter text.

APPENDIX B. MARKET SURVEY RESULTS

B.1. Summary Table

Table B-1 lists all known CUAS products identified or confirmed through the research and review of information in Section 2.1. This is the master list of known products. CUAS technologies are listed in alphabetical order by manufacturer name. Only a few of the database headings are shown to keep the table very high-level and suitable for reprinting in this report. (The completed Request for Information forms as well as the spreadsheet of the master list will be available on Sandia National Laboratories' External Collaboration Network for download by DHS S&T.)

The table indicates which products are components versus 'systems' or combinations of multiple technologies/products, and products for which the team was able to collect additional technical information. In all, the database lists about 316 products.

Table B-1: CUAS Product Summary Table

#	Manufacturer	Product_Name	Country	Platform	Detection	Mitigation_Type	Mitigation Method	URL
1	911 Security (reseller)	AirGuard 911 (DJI Aeroscope)	China	Ground-Based	RF	Non-Kinetic	RF	Link
2	ALX Systems	Sentinel	Belgium	UAV	EO, IR	N/A		Link
3	ALX Systems	Spartiath	Belgium	Ground-Based, UAV	Radar	N/A		Link
4	AMTEC Less Lethal Systems	Skynet	USA	Handheld		Kinetic	Shotgun Net Ammunition	Link
5	Accenture Federal Services	THORIUM REACTOR	USA	Handheld	RF	Non-Kinetic	Deception, RF	Link
6	Accipiter	NM1-8A Drone Radar System	Canada	Ground-Fixed	Radar	Kinetic		Link
7	Accipiter	NM1-KHSxV Security Radar System	Canada	Ground-Fixed	Radar, EO, IR	Kinetic		Link
8	Advanced Protection Systems SA	Ctrl+Sky	Poland	Ground-Fixed, Ground-Mobile, Ground-Portable	Radar, Acoustic, EO, IR, RF	Non-Kinetic	GNSS Interference, RF Interference, RF Spoofing, Killer UAS	Link
9	Advanced Radar Technologies	Drone Sentinel	Spain	Ground-Based	Radar, EO, IR	N/A		Link
10	Aerial Armor (reseller)	DJI Aeroscope, Dedrone RF100/RF300	China	Ground-Fixed, Ground-Mobile	RF	N/A		Link
11	AeroDefense, formerly Drone Go Home	AirWarden	USA	Ground-Fixed, Ground-Mobile, Handheld	RF	Non-Kinetic	RF Deception/Control, RF Interference	Link
12	AimLock, Inc.	R-M1	USA	Aerial, Ground-Fixed, Ground-Mobile	Acoustic, EO, IR, RF, Radar	Kinetic	Airburst Munitions, Chaff, Ballistic	Link
13	Air Force Research Laboratory	NINJA	USA	Aerial, Ground-Fixed, Ground-Mobile	RF	Non-Kinetic	C2 Hijack, Modify RTL Position, RF Deception/Control, RF Interference	N/A
14	Airbus Group SE	Counter UAV System	France	Ground-Fixed	Radar, IR,	Non-Kinetic	GNSS Interference, RF Interference	Link
15	Airfence Solutions Ltd	ApolloShield Counter Drone System	Israel	Aerial, Ground-Fixed, Ground-Mobile	RF	Non-Kinetic	RF Interference	Link
16	Airspace Systems, Inc.	Airspace Systems Mitigation Solution	USA	Aerial, Ground-Fixed		Intercepting UAS	RF Interference	Link
17	Alion Science & Technology	CUAS	USA	Ground-Mobile		Non-Kinetic	RF Deception/Control	Link
18	Allen Vanguard	ANCILE	Canada	Ground-Fixed, Ground-Mobile		Non-Kinetic	GNSS Interference, RF Interference	Link

#	Manufacturer	Product_Name	Country	Platform	Detection	Mitigation_Type	Mitigation Method	URL
19	Anduril Industries	The Lattice Platform	USA	Aerial, Ground-Fixed, Ground-Mobile	Radar, EO, IR	Optional	Optional	Link
20	Aquila Defense Group Counter UAS	Aquila Defense Group Counter UAS	Switzerland	Ground-Fixed, Ground-Mobile, Handheld	RF, Radar, Acoustic, IR	Non-Kinetic	GNSS Interference, RF Interference	Link
21	Aquila International	Beam 250	USA	Ground-Fixed, Ground-Mobile, Handheld	Radar	N/A		Link
22	ArtSYS360	RS500	Israel	Ground-Based	RF	Non-Kinetic	RF Jamming, GNSS Jamming	Link
23	Ascent Vision	CM202U	USA	Ground-Fixed	EO, IR	N/A		Link
24	Ascent Vision	X-Madis	USA	Ground-Mobile	Radar, EO, IR	Non-Kinetic	RF Interference	Link
25	Aselsan Corporation	IHASAVAR	Turkey	Handheld		Non-Kinetic	RF Jamming, GNSS Jamming	Link
26	Aselsan Corporation	IHTAR	Turkey	Ground-Based	Radar, RF	Non-Kinetic	RF Jamming, GNSS Jamming	Link
27	Aveillant	Gamekeeper 16U	UK	Ground-Based	Radar	N/A		Link
28	Azgard Group LLC (reseller)	DroneTracker (Dedrone), Mesmer (Dept 13)	USA	Ground-Fixed, Ground-Mobile, Ground-Portable	Acoustic, EO, IR, RF, Radar	N/A	RF	Link
29	BATS	Drone Guard	Belgium	Ground-Fixed	Radar, EO, IR	Non-Kinetic	GNSS Interference, RF Interference	Link
30	BYLBOS/Roboost	SPID	France	Ground-Based	EO, IR, RF	Non-Kinetic	RF Jamming, GNSS Jamming	Link
31	Babcock	LDEW-CD	USA	Ground-Based	Radar, EO, IR	Kinetic	Laser, Gatling Gun	Link
32	Battelle	Drone Defender	USA	Ground-Fixed, Ground-Mobile		Non-Kinetic	GNSS Interference, RF Interference	Link
33	Battelle	Drone Defender V2	USA	Handheld		Non-Kinetic	GNSS Interference, RF Interference	Link
34	Black Sage/IEC Infrared	Counter UAVX	USA	Ground-Fixed, Ground-Mobile, Handheld	Radar, EO, IR	Non-Kinetic	GNSS Deception, RF Deception/Control, RF Interference	Link
35	Blighter, Chess Dynamics, Enterprise Control Systems	Blighter AUDS	UK	Ground-Fixed	Radar, EO, IR	Non-Kinetic	RF Interference	Link
36	Blind Tiger	WIDDS (Wireless Intrusion Detection and Defeat System)	USA	Ground-Fixed	RF	Non-Kinetic	RF Interference	Link
37	Boeing	Laser Avenger	USA	Ground-Based	Radar	Kinetic	Laser	Link
38	Boeing/General Dynamics	MEHEL 2.0	USA	Ground-Based		Kinetic	Laser	Link
39	Booz Allen Hamilton	Enforce Field	USA	Ground-Fixed	Acoustic, EO, IR, RF, Radar	N/A		Link

#	Manufacturer	Product_Name	Country	Platform	Detection	Mitigation_Type	Mitigation Method	URL
40	Broadfield Security Services	Drone Blocker	Netherlands	Ground-Fixed		Non-Kinetic	RF Interference	Link
41	Broadfield Security Services	UAS Detection and Verification System	Netherlands	Ground-Fixed, Ground-Mobile	Radar, EO, IR, Acoustic	N/A		Link
42	C Speed, LLC	LightWave CUAS Surveillance Suite	USA	Aerial, Ground-Fixed, Ground-Mobile	Radar, RF	Non-Kinetic	RF Interference	Link
43	CACI	SkyTracker-AWAIR	USA	Ground-Fixed	RF	Non-Kinetic	GNSS Interference, RF Deception/Control, RF Interference	Link
44	CACI	SkyTracker-BAM	USA	Handheld	RF	Non-Kinetic	GNSS Interference, RF Deception/Control, RF Interference	Link
45	CACI	SkyTracker-CORIAN	USA	Ground-Fixed	RF	Non-Kinetic	GNSS Interference, RF Deception/Control, RF Interference	Link
46	CRFS Inc.	RFeye Site with 3D TDOA module	UK	Ground-Fixed, Ground-Mobile	RF	N/A		Link
47	CRFS Inc.	RFeye Site with AOA RF emitter geolocation	UK	Ground-Fixed, Ground-Mobile	RF	N/A		Link
48	CS Communication & Systems Canada Inc.	Boreades	Canada	Ground-Fixed, Ground-Mobile	Radar, EO, RF, Acoustic	Multiple	GNSS Interference, RF Interference, Net Capture	Link
49	CTS	Drone Jammer	China	Handheld		Non-Kinetic	RF Jamming, GNSS Jamming	Link
50	CerbAir	CerbAir Fixed	France	Ground-Fixed	RF, EO,IR	Multiple	RF Interference, Net Capture	Link
51	CerbAir	CerbAir Mobile	France	Ground-Mobile	RF, EO,IR	Multiple	RF Interference, Net Capture	Link
52	Chenega Europe	dronecollider	Ireland	UAV		Intercepting UAS	Sacrificial collision drone	Link
53	Chenega Europe	dronesnarer	Ireland	Handheld		Kinetic	Net	Link
54	Chenega Europe	dronesoaker	Ireland	Handheld		Kinetic	Water projector	Link
55	Chenega Europe	dronetaker	Ireland	UAV		Non-Kinetic	Spoofing	Link
56	Chenega Europe	dronetracker	Ireland	Ground-Based	Acoustic, Motion Detection	N/A		Link
57	Chenega Europe	dronevigil Array	Ireland	Ground-Based	Radar	N/A		Link
58	Chenega Europe	dronevigil Defender	Ireland	Handheld		Non-Kinetic	RF Jamming	Link
59	Chenega Europe	dronevigil Field Mobile	Ireland	Ground-Based	Radar	N/A		Link
60	Chenega Europe	dronevigil Holographic	Ireland	Ground-Based	Radar	N/A		Link
61	Cintel	C-UAS (unknown name)	USA	UAV		Non-Kinetic	RF Interference	Link

#	Manufacturer	Product_Name	Country	Platform	Detection	Mitigation_Type	Mitigation Method	URL
62	Citadel	Titan V3	USA	Ground-Fixed, Handheld	RF	Non-Kinetic	Targeted Interference, RF Deception/Control, RF Interference	Link
63	Cobham Antenna Systems	Directional Flat Panel Antenna	UK	(other-specify) Antenna	RF	Non-Kinetic	RF Jamming, GNSS Jamming	Link
64	Cobham Antenna Systems	Directional Helix Antenna	USA	(other-specify) Antenna	RF	Non-Kinetic	RF Jamming, GNSS Jamming	Link
65	Cobham Antenna Systems	High Power Ultra-Wideband Directional Antenna	UK	(other-specify) Antenna	RF	Non-Kinetic	RF Jamming, GNSS Jamming	Link
66	Cobham Antenna Systems	Wideband Omni-Directional	UK	(other-specify) Antenna	RF	Non-Kinetic	RF Jamming, GNSS Jamming	Link
67	Cogniac Corporation	Universal Imagery Recognition Platform (UIRP)	USA	Ground-Fixed (Software), Ground-Mobile (Software)	EO, IR	N/A		Link
68	Colorado Engineering, Inc. (CEI)	Skyline Radar	USA	Aerial, Ground-Fixed, Ground-Mobile	Radar	N/A		Link
69	Controp	SPEED-BIRD	Israel	Ground-Fixed	EO, IR	N/A		Link
70	Controp	Tornado	Israel	Ground-Based	EO, IR	N/A		Link
71	Convexum	Convexum Platform	Israel	Ground-Based	RF	Non-Kinetic	RF Jamming, Spoofing	Link
72	Copious Imaging	WISP	USA	Ground-Fixed, Ground-Mobile, Maritime-Mobile	IR	N/A		Link
73	D-Fend Solutions	N/A	Israel	Ground-Based	RF	Non-Kinetic	RF Jamming, Spoofing	Link
74	DJI	AeroScope	China	Ground-Fixed, Ground-Mobile	RF	N/A		Link
75	DRS/Moog	Mobile Low, Slow Unmanned Aerial Vehicle Integrated Defense Systems	USA	Ground-Fixed, Ground-Mobile	Radar	Multiple	RF Interference, Ballistic Munitions, High Energy Laser	Link
76	DeDrone, Inc.	DroneTracker	USA	Ground-Fixed, Ground-Mobile, Ground-Portable	Acoustic, EO, IR, RF, Radar	N/A		Link
77	DeTect, Inc.	DroneWatcherAPP	USA, UK	Handheld	Mobile App	N/A		Link
78	DeTect, Inc.	DroneWatcherLT	USA, UK	Ground-Fixed	RF	N/A		Link
79	DeTect, Inc.	DroneWatcherRF	USA, UK	Aerial, Ground-Fixed, Ground-Mobile	RF	Non-Kinetic	GNSS Interference, RF Deception/Control	Link
80	DeTect, Inc.	Harrier Drone Surveillance Radar (DSR)	USA, UK	Ground-Fixed, Ground-Mobile	Radar	N/A		Link

#	Manufacturer	Product_Name	Country	Platform	Detection	Mitigation_Type	Mitigation Method	URL
81	Delft Dynamics	Drone Catcher	Netherlands	UAV		Intercepting UAS	Net Capture	Link
82	Department 13 International	MESMER	USA	Ground-Fixed	RF	Non-Kinetic	RF Deception/Control	Link
83	Diehl Defence	HPEMcounterUAS	Germany	Ground-Fixed		Non-Kinetic	Electromagnetic pulse	Link
84	Digitech Info Technology	JAM-1000	China	Ground-Based		Non-Kinetic	RF Jamming, GNSS Jamming	Link
85	Digitech Info Technology	JAM-2000	China	Handheld		Non-Kinetic	RF Jamming, GNSS Jamming	Link
86	Digitech Info Technology	JAM-3000	China	Ground-Based		Non-Kinetic	RF Jamming, GNSS Jamming	Link
~~87~~	Dragonfly Pictures Inc. (DPI) UAV Systems	Tethered Unmanned Aerial Vehicle (TUAV)	USA	UAV	Payload dependent	Optional	Payload Dependent	Link
88	Drone Defence	Dynopis E1000MP	UK	Ground-Mobile		Non-Kinetic	GNSS Interference, RF Interference	Link
89	Drone Defence	NetGun X1	UK	Handheld		Kinetic	Net	Link
90	Drone Defence	SkyFence	UK	Ground-Fixed		Non-Kinetic	RF Interference	Link
91	Drone Labs	Drone Detector	USA	Ground-Based	RF	N/A		Link
92	Drone Security Defence		UK	Ground-Based	Unknown	Unknown	Unknown	Link
93	DroneShield	DroneBeam	Australia	Ground-Fixed		Non-Kinetic	Optical Blinding	Link
94	DroneShield	DroneCannon	Australia	Ground-Fixed		Non-Kinetic	GNSS Interference, RF Interference	Link
95	DroneShield	DroneCannon RW	Australia	Ground-Mobile		Non-Kinetic	RF Interference	Link
96	DroneShield	DroneGun MKII	Australia	Handheld		Non-Kinetic	GNSS Interference, RF Interference	Link
97	DroneShield	DroneGun Tactical	Australia	Handheld		Non-Kinetic	GNSS Interference, RF Interference	Link
98	DroneShield	DroneHeat	Australia	Ground-Fixed	IR	N/A		Link
99	DroneShield	DroneOpt	Australia	Ground-Fixed	EO	N/A		Link
100	DroneShield	DroneSentinel	Australia	Ground-Fixed	Radar, RF, Acoustic, EO, IR	N/A		Link
101	DroneShield	DroneSentry	Australia	Ground-Fixed	Radar, RF, Acoustic, EO, IR	Non-Kinetic	GNSS Interference, RF Interference	Link
102	DroneShield	Faralert Sensor	Australia	Ground-Fixed	RF	N/A		Link
103	DroneShield	RadarOne	Australia	Ground-Fixed	Radar	N/A		Link
104	DroneShield	RadarZero	Australia	Ground-Fixed	Radar	N/A		Link
105	DroneShield	RfOne	Australia	Ground-Fixed	RF	N/A		Link

#	Manufacturer	Product_Name	Country	Platform	Detection	Mitigation_Type	Mitigation Method	URL
106	DroneShield	Wide Alert Sensor	Australia	Ground-Fixed	Acoustic	N/A		Link
107	Dronefence	UAV Tracker	Germany	Ground-Mobile	RF, Acoustic, EO, IR	Non-Kinetic	RF Interference	Link
108	Dynetics, Inc.	GroundAware GA1360	USA	Ground-Fixed, Ground-Mobile	Radar	N/A		Link
109	Dynetics, Inc.	GroundAware GA4120	USA	Ground-Fixed, Ground-Mobile	Radar	N/A		Link
110	Dynetics, Inc.	GroundAware GA9000	USA	Ground-Fixed, Ground-Mobile	Radar	N/A		Link
111	Dynetics, Inc.	SoundAware	USA	Ground-Fixed	Acoustic	N/A		Link
112	Dzyne Technologies Incorporated	CURES (Counter Unmanned Rapid Engagement System)	USA	UAV	EO	Intercepting UAS	Entanglement	Link
113	ECA Group	EC-180	France	Aerial, Ground-Fixed	Acoustic, EO, IR, RF, Radar	N/A		Link
114	EIDOS (reseller, Tech Integrator)	DroneTracker (Dedrone)	USA	Ground-Based	RF	Non-Kinetic	RF	Link
115	ELTA (Israel Aerospace Industries)	Drone Guard	Israel	Ground-Fixed, Handheld	Radar, EO	Non-Kinetic	GNSS Interference, RF Interference	Link
116	ELTA North America	Man-Portable Anti-Drone System – Kit (MADS-K)	USA	Handheld	Radar, EO, IR	Non-Kinetic	GNSS Interference, RF Interference	Link
117	ELTA North America	Man-Portable Anti-Drone System – Kit Version 4 (MADS-K V4) Static	USA	Ground-Fixed	Radar, EO, IR	Multiple	GNSS Deception, RF Deception/Control, Ballistic Munitions	Link
118	ELTA North America	Man-Portable Anti-Drone System – Kit Version 4 On The Move (MADS-K V4 OTM)	USA	Ground-Mobile, Handheld	Radar, EO, IR	Multiple	GNSS Deception, RF Deception/Control, Ballistic Munitions	Link
119	EWA Government Systems Inc.	EWA Counter UAS System	USA	Ground-Fixed, Ground-Mobile, Handheld	Radar, IR	Non-Kinetic	GNSS Interference, RF Interference	Link
120	Echodyne	EchoGuard MESA Radar	USA	Aerial, Ground-Fixed, Ground-Mobile	Radar	N/A		Link
121	Elbit Systems of America	ReDrone	Israel	Ground-Fixed, Ground-Mobile	RF	Multiple	GNSS Interference, RF Interference, Entanglement	Link
122	Elbit Systems of America	SupervisIR	Israel	Ground-Fixed	IR	N/A		Link
123	Elettronica (ELT) Roma	ADRIAN	Italy	Ground-Fixed, Ground-Mobile, Handheld	RF, EO, IR	Non-Kinetic	GNSS Interference, RF Deception/Control, RF Interference	Link

#	Manufacturer	Product_Name	Country	Platform	Detection	Mitigation_Type	Mitigation Method	URL
124	Epirus, Inc.	Leonidas	USA	Aerial, Ground-Fixed, Ground-Mobile	EO, IR	Non-Kinetic	EMP	Link
125	Exponent	Drone Hunter	UAE	UAV	EO, IR	N/A		Link
126	FLIR Systems Inc.	Argus-3D	USA	Ground-Fixed, Ground-Mobile, Handheld	EO, IR, Radar	Non-Kinetic	GNSS Interference, RF Interference	Link
127	FLIR Systems Inc.	FLIR 280HDEP with Moving Target Radar	USA	Ground-Fixed, Ground-Mobile	EO, IR, Radar	N/A		Link
128	FLYMOTION	AeroScope	USA	Ground-Fixed, Ground-Mobile	RF	N/A	N/A	Link
129	Fortem Technologies	Drone Hunter	USA	Aerial, Ground-Fixed	Radar	Intercepting UAS	Net Capture	Link
130	Fortem Technologies	SkyDome (Drone Hunter + TrueView R30)	USA	Ground-Fixed, UAV	Radar	Intercepting UAS	Net	Link
131	Fortem Technologies	TrueView R30 Radar	USA	Ground-Mobile, UAV	Radar	N/A		Link
132	Fovea Aero	CCOD	USA	UAV		Intercepting UAS	Net Capture	Link
133	Fu Yu Electronics (Fuyuda)	Portable Anti-UAV Defence System	China	Ground-Mobile		Non-Kinetic	GNSS Interference, RF Interference	Link
134	GEW Technologies	SkyScan7	South Africa	Ground-Fixed, Ground-Mobile	RF	Non-Kinetic	GNSS Interference, RF Interference	Link
135	General Atomics	Fencepost	USA	Ground-Fixed, Ground-Mobile	Acoustic	N/A		Link
136	General Dynamics Ordnance & Tactical Systems (GD-OTS)	Advanced Fire Control Augmentation System (AFCAS) for C-UAS	USA	Ground-Fixed, Ground-Mobile	Radar, EO, IR	Kinetic	Ballistic Munitions	Link
137	Gewerbegebiet Aaronia AG	AARTOS Drone Detection System	Germany	Ground-Fixed	RF	Non-Kinetic	GNSS Interference, RF Interference	Link
138	Gresco Technology Solutions	Aeroscope G-16	USA	Ground-Fixed	RF	N/A		Link
139	Gresco Technology Solutions	Aeroscope G-8	USA	Ground-Fixed, Ground-Mobile	RF	N/A		Link
140	Gresco Technology Solutions	Aeroscope Mobile	USA	Ground-Mobile	RF	N/A		Link
141	Groupe Assman	MTX-8	France	UAV		Kinetic	Net	Link
142	Gryphon Sensors	Skylight	USA	Ground-Based	Radar, RF, EO, IR	N/A		Link
143	Gryphon Sensors	Skylight Mobile	USA	Ground-Based	Radar, RF, EO, IR	N/A		Link
144	HGH Infrared Systems	Spynel-M	France	Ground-Fixed, Ground-Mobile	IR	N/A		Link

#	Manufacturer	Product_Name	Country	Platform	Detection	Mitigation_Type	Mitigation Method	URL
145	HGH Infrared Systems	Spynel-S	France	Ground-Fixed, Ground-Mobile		N/A		Link
146	HGH Infrared Systems	Spynel-X	France	Ground-Fixed, Ground-Mobile		N/A		Link
147	HP Marketing and Consulting	HP 3962H	Germany	Handheld		Non-Kinetic	GNSS Interference, RF Interference	Link
148	HP Marketing and Consulting	HP 47	Germany	Handheld		Non-Kinetic	GNSS Interference, RF Interference	Link
149	Harp Arge	Drone Savar	Turkey	Handheld		Non-Kinetic	RF Jamming	Link
150	Hensoldt GmBH/Kelvin Hughes Inc./Hensoldt Inc.	Xpeller SPEXER 2000 Radar	UK	Ground-Fixed, Ground-Mobile	EO, Radar	Non-Kinetic	GNSS Interference, RF Interference	Link
151	Hensoldt GmBH/Kelvin Hughes Inc./Hensoldt Inc.	Xpeller SPEXER 500 Radar	UK	Ground-Fixed, Ground-Mobile	EO, Radar	Non-Kinetic	GNSS Interference, RF Interference	Link
152	Hensoldt GmBH/Kelvin Hughes Inc./Hensoldt Inc.	Xpeller SXv Radar	UK	Ground-Fixed, Ground-Mobile	EO, Radar	Non-Kinetic	GNSS Interference, RF Interference	Link
153	HiGH + MiGHTY	SKYNET	Taiwan	Handheld		Non-Kinetic	RF Jamming, GNSS Jamming	Link
154	Hikvision	Defender Series UAV-D04JA	China	Handheld		Non-Kinetic	RF Jamming, GNSS Jamming	Link
155	IACIT	DRONEBlocker 0100	Brazil	Ground-Fixed	Acoustic, EO, IR, RF, Radar	Non-Kinetic	RF Interference	Link
156	IACIT	DRONEBlocker 0200	Brazil	Ground-Fixed	Acoustic, EO, IR, RF, Radar	Non-Kinetic	RF Interference	Link
157	IDS (Ingegneria dei Sistemi SPA)	Black Knight	Italy	Ground-Fixed	Radar, EO, IR	Non-Kinetic	GNSS Interference, RF Interference	Link
158	IEC Infrared Systems LLC	Lycan CUAS	USA	Ground-Fixed, Ground-Mobile, Maritime-Mobile	EO, IR, Radar, RF	Multiple	GNSS Interference, RF Interference, Net Capture	Link
159	IMI Systems	Red Sky 2 Directional Drone Defender System (RSk-DD)	Israel	Ground-Mobile	Radar	Non-Kinetic	GNSS Interference, RF Interference	Link
160	IMI Systems	Red Sky 2 Multi-Directional Unit (RSK-MD)	Israel	Ground-Mobile	RF	Non-Kinetic	GNSS Interference, RF Interference	Link
161	IXI Technology	Drone Killer	USA	Handheld		Non-Kinetic	GNSS Interference, RF Deception/Control (Bit Error Rate Saturation), RF Interference	Link

#	Manufacturer	Product_Name	Country	Platform	Detection	Mitigation_Type	Mitigation Method	URL
162	Invisible Interdiction Inc.	Ghoul Tool Full-Spectrum (GTFS)	USA	Ground-Fixed, Ground-Mobile, Handheld		Non-Kinetic	GNSS Interference, RF Interference	Link
163	Invisible Interdiction Inc.	Ghoul Tool Medium-range Module (GTMM)	USA	Ground-Fixed, Ground-Mobile, Handheld		Non-Kinetic	GNSS Interference, RF Interference	Link
164	Invisible Interdiction Inc.	Ghoul Tool Short-range Module (GTSM)	USA	Ground-Fixed, Ground-Mobile, Handheld		Non-Kinetic	GNSS Interference, RF Interference	Link
165	Invisible Interdiction Inc.	Ghoul Tool Shotgun (GTShotgun)	USA	Handheld		Non-Kinetic	GNSS Interference, RF Interference	Link
166	JCPX Development/DSNA Services/Aveillant	UWAS	Monaco	Ground-Based	Radar, EO, IR	Unknown	Unknown	Link
167	Jiun An Technology	Raysun MD1	Taiwan	Handheld		Non-Kinetic	RF Jamming, GNSS Jamming	Link
168	KB Radar Design Bureau	Groza-R	Belarus	Handheld		Non-Kinetic	RF Interference	Link
169	KB Radar Design Bureau	Groza-S	Belarus	Ground-Fixed	RF	Non-Kinetic	GNSS Deception, GNSS Interference, RF Interference	Link
170	KB Radar Design Bureau	Groza-Z	Belarus	Ground-Fixed	RF	Non-Kinetic	GNSS Interference, RF Deception/Control, RF Interference	Link
171	Kalashnikov/ZALA Aero Group	REX 1	Russia	Handheld		Non-Kinetic	RF Jamming, GNSS Jamming	Link
172	Kelvin Hughes	SharpEye	UK	Ground-Based	Radar	N/A		Link
173	Kirintec	Recurve Max	UK	Handheld		Non-Kinetic	GNSS Interference, Other - Removes control and video links, RF Interference	Link
174	Kirintec	SkyNet Longbow	UK	Ground-Mobile		Non-Kinetic	GNSS Interference, Other - Removes control and video links, RF Interference	Link
175	Kratos Defense & Rocket Support Services, Inc. (KDRSS)	Kratos Tethered UAS	USA	Aerial, Ground-Fixed, Ground-Mobile	EO, RF	N/A		Link
176	L3 Technologies (L3 Communications ASA Ltd)	Drone Guardian	USA	Ground-Fixed, Ground-Mobile	Acoustic, EO, IR, RF, Radar	Multiple	GNSS Interference, RF Interference, Net Capture	Link
177	LGS Innovations	Spectral Wraith	USA	Aerial, Ground-Fixed, Ground-Mobile	RF	N/A		Link
178	Leidos	Drone Dome	USA	Ground-Fixed, Ground-Mobile	Acoustic, EO, IR, RF, Radar	Multiple	Acoustic, GNSS Interference, RF Interference, Ballistic Munition, High Energy Laser	Link

#	Manufacturer	Product_Name	Country	Platform	Detection	Mitigation_Type	Mitigation Method	URL
179	Leonardo DRS	Multi-Mission Hemispheric Radar (MHR)	USA	Ground-Fixed, Ground-Mobile, Portable	Radar	Multiple	GNSS Interference, RF Deception/Control	Link
180	Leonardo DRS	Surveillance and Battlefield Reconnaissance Equipment (SABRE)	USA	Ground-Fixed, Ground-Mobile	Radar	N/A	Machine Gun	Link
181	Leonardo MW Ltd	Falcon Shield	UK	Ground-Fixed	RF, Radar, EO	Non-Kinetic	GNSS Interference, RF Interference	Link
182	Liteye	ADIS	USA	Ground-Based	Radar, EO, IR	N/A		Link
183	Liteye/Orbital ATK	T-REX	USA	Ground-Fixed	Radar, EO, IR	Non-Kinetic	RF Interference	Link
184	LocMas	STUPOR	Russia	Handheld		Non-Kinetic	RF Jamming, GNSS Jamming	Link
185	Lockheed Martin Corp.	ADAM	USA	Ground-Based	EO, IR	Kinetic	Laser	Link
186	Lockheed Martin Corp.	ATHENA	USA	Ground-Based	EO, IR	Kinetic	Laser	Link
187	Lockheed Martin Corp.	ICARUS	USA	Ground-Fixed	Acoustic, EO, IR, RF, Radar	Non-Kinetic	GNSS Interference, RF Deception/Control, RF Interference	Link
188	Lockheed Martin Corp.	MoRFIUS-TL (Tube-Launched) and MATADOR (Quadcopter)	USA	UAV		Non-Kinetic	High Power Microwave	Link
189	MACOM	SPAR Radar Tiles and Appertures	USA	Ground-Fixed, Ground-Mobile	RF	N/A		Link
190	MBDA Deutschland	High Energy Laser Weapon System	Germany	Ground-Based		Kinetic	Laser	Link
191	MC-CLIC	Anti-UAV Rifle	Monaco	Handheld		Non-Kinetic	RF Gun	Link
192	MC2Technologies	Nerod F5	France	Handheld		Non-Kinetic	RF Gun	Link
193	MC2Technologies	Scrambler 1000	France	Ground-Fixed		Non-Kinetic	RF Gun	Link
194	Marduk Technologies	Shark	Estonia	Ground-Based	EO	Kinetic	Laser	Link
195	Meritis	ADS-2000	Switzerland	Ground-Based	Acoustic	N/A		Link
196	Meritis	P6	Switzerland	Handheld		Non-Kinetic	RF Jamming, GNSS Jamming	Link
197	Meritis	RTX-2000M6	Switzerland	Ground-Based		Non-Kinetic	RF Jamming, GNSS Jamming	Link
198	Meritis	RTX-3000X	Switzerland	Ground-Based		Non-Kinetic	RF Jamming, GNSS Jamming	Link
199	Meritis	RTX-300P2	Switzerland	Handheld		Non-Kinetic	RF Jamming, GNSS Jamming	Link
200	Meritis	SC-1000T	Switzerland	Ground-Based	EO, IR	N/A		Link

#	Manufacturer	Product_Name	Country	Platform	Detection	Mitigation_Type	Mitigation Method	URL
201	Meritis	SC-1500T	Switzerland	Ground-Based	EO, IR	N/A		Link
202	Meritis	SR-9000S	Switzerland	Ground-Based	Radar	N/A		Link
203	Meritis	SkyCleaner	Switzerland	Handheld		Non-Kinetic	RF Jamming, GNSS Jamming	Link
204	Microflown AVISA	SKYSENTRY	Netherlands	Ground-Fixed, Ground-Mobile	Acoustic	N/A		Link
205	Miltronix	Drone Detection Radar	UK	Ground-Based	Radar	N/A		Link
206	Mitsubishi Electric Corporation	Drone Deterrence System	Japan	Ground-Fixed	RF	Non-Kinetic	RF Interference	Link
207	Moog Inc.	Gauntlet Counter Unmanned Aerial System	USA	Ground-Fixed, Ground-Mobile	Radar, RF	Non-Kinetic		Link
208	MyDefence Communication ApS	EAGLE	Denmark	Ground-Fixed	Radar	N/A		Link
209	MyDefence Communication ApS	KNOX	Denmark	Ground-Fixed, Ground-Mobile	Multi-sensor Server Solution	Non-Kinetic	RF Interference	Link
210	MyDefence Communication ApS	WATCHDOG	Denmark	Ground-Fixed	RF	N/A		Link
211	MyDefence Communication ApS	WOLFPACK	Denmark	Ground-Fixed	RF	N/A		Link
212	MySky Technoligies		Australia	Ground-Based	Unspecified	N/A		Link
213	NEC	TBD	Japan	Ground-Fixed	EO, IR	N/A		Link
214	NNIIRT	1L121-E	Russia	Ground-Based	Radar	N/A		Link
215	Nammo	Nammo Programmable Ammunition	Norway			Kinetic	Programmable ammunition	Link
216	Netline Communications	C-GUARD DRONENET	Israel	Ground-Fixed		Non-Kinetic	RF Interference	Link
217	Netline Communications	WOODPECKER LIGHT	Israel	Ground-Fixed	RF	N/A		Link
218	Northrop Grumman	AUDS Anti-UAV Defence System	USA	Ground-Fixed, Ground-Mobile, Ground-Portable	Radar, EO, IR	Multiple	GNSS Interference, RF Interference, LW30 Link Fed cannon firing proximity airburst ammunition. Ammunition is currently under development.	Link
219	Northrop Grumman	C-AUDS (Containerized – Anti UAS Defense System)	USA	Ground-Fixed, Ground-Mobile, Ground-Portable	Radar, EO, IR	Multiple	GNSS Interference, RF Interference, LW30 Link Fed cannon firing proximity airburst ammunition. Ammunition is currently under development.	Link

#	Manufacturer	Product_Name	Country	Platform	Detection	Mitigation_Type	Mitigation Method	URL
220	Northrop Grumman	Drone Restricted Access Using Known EW (DRAKE)	USA	Ground-Fixed		Non-Kinetic	RF Interference	Link
221	Northrop Grumman	M-AUDS (M-ATV AUDS)	USA	Ground-Fixed, Ground-Mobile, Ground-Portable	Radar, EO, IR	Multiple	GNSS Interference, RF Interference, LW30 Link Fed cannon firing proximity airburst ammunition. Ammunition is currently under development.	Link
222	Northrop Grumman	Mobile Application for UAS Identification	USA	Handheld	Acoustic	N/A		Link
223	Northrop Grumman	Venom	USA	Ground-Based	Laser Designator	N/A		Link
224	OIS-AT	3D Air Surveillance UAV Detection Radar	India	Ground-Based	Radar	N/A		Link
225	Open Works Engineering	Skywall 100	UK	Handheld		Kinetic	Ballistic Munitions, Net Capture	Link
226	Open Works Engineering	Skywall 300	UK	Ground-Fixed, Ground-Mobile		Kinetic	Net Capture	Link
227	Optix	Anti-Drone System	Bulgaria	Ground-Fixed		Non-Kinetic	GNSS Interference, RF Interference	Link
228	Orad	DROM Drone Defense System	Israel	Ground-Fixed, Ground-Mobile	RF	Non-Kinetic	RF Interference	Link
229	Orelia	Drone Detector	France	Ground-Fixed	Acoustic	Non-Kinetic	RF Interference	Link
230	PDA Electronics	Repulse 24	UK	Any		Non-Kinetic	RF Interference	Link
231	PDA Electronics	Repulse 2458E	UK	Ground-Fixed, Handheld		Non-Kinetic	RF Interference	Link
232	PDA Electronics	Repulse 2458H	UK	Handheld		Non-Kinetic	RF Interference	Link
233	PDA Electronics	Repulse 360/320	UK	Any		Non-Kinetic	RF Interference	Link
234	Panasonic	Drone Finder	Japan	Ground-Fixed	Acoustic, EO	N/A		Link
235	Phantom Technologies	Eagle108 Tactial Drone Jammer	Israel	Ground-Based	RF?	Non-Kinetic	RF Jamming, GNSS Jamming	Link
236	Poly Technologies	Silent Hunter	China	Ground-Based	EO, IR	Kinetic	Laser	Link
237	Prime Consulting & Technologies	GROK Jammer	Denmark	Ground-Fixed		Non-Kinetic	GNSS Interference, RF Interference	Link
238	Prime Consulting & Technologies	GROK Mobile Gun	Denmark	Handheld		Non-Kinetic	GNSS Interference, RF Interference	Link
239	Prime Consulting & Technologies	Mini-range counter-UAV system	Denmark	Ground-Based	EO, IR	N/A		Link

#	Manufacturer	Product_Name	Country	Platform	Detection	Mitigation_Type	Mitigation Method	URL
240	Prime Consulting & Technologies	Small-range counter-UAV system	Denmark	Ground-Based	Radar, EO, IR	N/A		Link
241	QRCtech	Passive CUAS detection system	USA	Ground-Mobile	RF	N/A		Link
242	QinetiQ	OBSIDIAN	UK	Ground-Based	Radar	N/A		Link
243	Quantum Aviation	Titanium	UK	Ground-Fixed	RF, EO, IR, Radar	Non-Kinetic		Link
244	RADA Electronic Industries	All-Threat Air Surveillance Radars	Israel		Radar	N/A		Link
245	Radio Hill Technologies Inc.	ASP with Dronebuster Block 3B	USA	Ground-Fixed, Ground-Mobile		Multiple	GNSS Interference, RF Interference, Ballistic Munitions, High Energy Laser	Link
246	Radio Hill Technologies Inc.	Dronebuster	USA	Handheld		Non-Kinetic	GNSS Interference, RF Interference	Link
247	Radio Hill Technologies Inc.	Dronebuster Block 3	USA	Handheld		Non-Kinetic	GNSS Interference, RF Interference	Link
248	Radio Hill Technologies Inc.	Dronebuster Block 3B	USA	Handheld		Non-Kinetic	GNSS Interference, None (UAS nearby alert only), RF Interference	Link
249	Rafael Advanced Defense Systems	Drone Dome	Israel	Ground-Fixed	Radar, EO, IR	Multiple	RF Interference, High Energy Laser	Link
250	Rajant Corp	MANET	USA	UAV		Intercepting UAS	Swarming	Link
251	Raytheon	Acoustic CUAS System (ACUAS)	USA	Ground-Mobile	Acoustic	N/A		Link
252	Raytheon	HELWS MRZR	USA	Ground-Mobile	EO, IR	Kinetic	High Energy Laser	Link
253	Raytheon	Low-power (10kW) High Energy Laser Weapons System (HELWS)	USA	Ground-Mobile		Non-Kinetic	High Energy Laser	Link
254	Raytheon	Phaser (High Power Microwave (HPM))	USA	Ground-Fixed, Ground-Mobile	EO, IR, Radar	Non-Kinetic	High Power Microwave	Link
255	Raytheon	Skyler - Advanced 3D AESA Netted Radar with Dual Pol Weather, targeting low Radar Cross Section Low Altitude Aircraft	USA	Ground-Fixed, Ground-Mobile	Radar	Non-Kinetic	RF Deception/Control, RF Interference, RF Spoofing – Deploy cyber payload, High Energy Laser, High Power Microwave	Link

#	Manufacturer	Product_Name	Country	Platform	Detection	Mitigation_Type	Mitigation Method	URL
256	Raytheon	Windshear Counter-UAS Integration Platform	USA	Ground-Fixed, Ground-Mobile	Acoustic, EO, IR, RF, Radar	Multiple	GNSS Interference, RF Deception/Control, RF Interference, High Energy Laser, High Power Microwave	Link
257	Rheinmetall AG	HEL Effector Wheel XX	Germany	Ground-Based	Radar	Kinetic	Laser	Link
258	Rinicom	Sky Patriot	UK	Ground-Fixed	EO,IR	N/A		Link
259	Robin Radar Systems	ELVIRA	Netherlands	Ground-Fixed, Ground-Mobile, Maritime-Mobile	Radar	N/A		Link
260	Rohde & Schwarz	Ardronis-D	Germany	Ground-Fixed	RF	N/A		Link
261	Rohde & Schwarz	Ardronis-I	Germany	Ground-Fixed	RF	N/A		Link
262	Rohde & Schwarz	Ardronis-P	Germany	Ground-Fixed	RF	Non-Kinetic	RF Interference	Link
263	Rohde & Schwarz	Ardronis-R	Germany	Ground-Fixed	RF	Non-Kinetic	RF Interference	Link
264	Rostec	Shipovnik-Aero	Russia	Ground-Based	RF, Unknown	Non-Kinetic	RF Jamming, GNSS Jamming	Link
265	SC Scientific and Technical Center of Electronic Warfare	Repellent-1	Russia	Ground-Based	RF	Non-Kinetic	RF Jamming	Link
266	SCG, LLC & DMT Radar, US Rep is Van Cleve & Associates	DroneRANGER	Spain, Switzerland	Ground-Fixed, Ground-Mobile	Acoustic, EO, IR, RF, Radar	Non-Kinetic	GNSS Interference, RF Interference	Link
267	SCI Technology, Inc.	AeroGuard	USA	Aerial, Ground-Fixed, Ground-Mobile		Intercepting UAS	Entanglement, Net Capture	Link
268	SESP Group	Drone Defeater	UK	Ground-Fixed, Ground-Mobile	EO, IR, RF	Non-Kinetic	RF Interference	Link
269	ST Engineering Electronics and VT Miltope	Sky Archer	USA	Ground-Fixed, Handheld	RF, EO	Non-Kinetic	RF Interference	Link
270	ST Kinetics	C-UAS Grenade	Singapore			Kinetic	Projectile	Link
271	Saab Defense and Security, USA, LLC	Saab C-sUAS System	Sweden	Ground-Fixed, Ground-Mobile	Radar	Multiple	RF Deception/Control	Link
272	Search Systems	Sparrowhawk	UK	UAV		Intercepting UAS	Net	Link
273	Selex	Falcon Shield	UK	Ground-Fixed	EO, IR, Radar	Non-Kinetic	RF Deception/Control, RF Interference	Link
274	Sensofusion	Airfence	Finland	Ground-Based	RF	N/A		Link
275	Sierra Nevada Corp.	SkyCAP	USA	Ground-Fixed		Non-Kinetic	RF Interference	Link

#	Manufacturer	Product_Name	Country	Platform	Detection	Mitigation_Type	Mitigation Method	URL
276	Signal Systems Corp.	Three Dimensional Acoustic Sensing Unit (3DASU)	USA	Ground-Fixed	Acoustic	N/A		Link
277	SkySafe	SkySafe	USA	Ground-Fixed, Ground-Mobile	RF	Non-Kinetic	GNSS Interference, RF Deception/Control, RF Interference	Link
278	SkySec	CDS-LS Sentinel Catch	Switzerland	Aerial, Handheld		Intercepting UAS	Net	Link
279	SkySec	CDS-LS Sentinel Catch and Carry	Switzerland	Aerial, Ground-Fixed		Intercepting UAS	Net	Link
280	Sohgo Security Services		Japan	Ground-Based	Acoustic	N/A		Link
281	Space Dynamics Laboratory	SHIELD (Shotgun Interdiction of Enemy Low-flying Drones), and SHIELD Optic	USA	Aerial, Ground-Fixed, Handheld	EO, IR, radar	Kinetic	Machine Gun Airburst 40mm, Shotgun	Link
282	Space Sciences Corp.	RAMROD (Risk Avoidance Multi-purpose Ramming Operations Drone)	USA	UAV	Radar, acoustic, LIDAR, RF	Multiple	Acoustic, EMP, GNSS Interference, RF Interference, Laser, Ballistic, Net capture, Munitions	Link
283	SpotterRF	A-Series Counter-Drone Radar	USA	Ground-Fixed	Radar	N/A		Link
284	SpotterRF	SpotterRF 3D-500 CUAS Radar	USA	Ground-Fixed, Ground-Fixed	Radar	N/A		Link
285	Squarehead Technology	Discovair G2	Norway	Ground-Fixed	Acoustic	N/A		Link
286	SteelRock Technologies	NightFighter Man-Portable CUAS	UK	Handheld		Non-Kinetic	RF Interference	Link
287	SteelRock Technologies	Odin	UK	Ground-Fixed, Ground-Mobile	RF	Non-Kinetic	GNSS Deception/Control, GNSS Interference, RF Deception/Control, RF Interference	Link
288	Syracuse Research Corp (SRC), Inc.	Silent Archer® Counter-UAS Technology	USA	Ground-Fixed, Ground-Mobile	Acoustic, EO, IR, RF, Radar	Multiple	GNSS Interference, RF Deception/Control, RF Interference, HPM, Net Capture	Link
289	TCI International, Inc.	Blackird Drone Detection 240	USA	Ground-Fixed, Ground-Mobile	RF	N/A		Link
290	TCI International, Inc.	Blackird Drone Detection 280	USA	Ground-Fixed, Ground-Mobile	RF	N/A		Link
291	TCI International, Inc.	Blackird Drone Detection 903	USA	Ground-Fixed, Ground-Mobile	RF	N/A		Link

#	Manufacturer	Product_Name	Country	Platform	Detection	Mitigation_Type	Mitigation Method	URL
292	TRD Consultancy	Orion-7 MP Drone Slayer	Singapore	Handheld		Non-Kinetic	RF Jamming, GNSS Jamming	Link
293	TRD Consultancy	Orion-D	Singapore	Ground-Based	RF	Non-Kinetic	RF Jamming, GNSS Jamming	Link
294	TRD Consultancy	Orion-H Drone Slayer	Singapore	Handheld		Non-Kinetic	RF Jamming, GNSS Jamming	Link
295	Technology Service Corp.	Aquila Seeker	USA	Aerial, Ground-Fixed, Ground-Mobile	RF	Intercepting UAS	Intercepting UAS	Link
296	Technology Service Corp.	TEMPR CUAS RADAR	USA	Aerial, Ground-Fixed, Ground-Mobile	Radar	N/A		Link
297	Telaforce		USA	Ground-Based	RF	N/A		Link
298	TeleRadio Engineering	SkyDroner 1000	Singapore	Ground-Based	EO, Other	N/A		Link
299	TeleRadio Engineering	SkyDroner 500	Singapore	Ground-Based	EO, Other	N/A		Link
300	Terra Hexen	Droneblocker System-Omnidirectional	Poland	Ground-Based		Non-Kinetic	RF Jamming, GNSS Jamming	Link
301	Terra Hexen	SAFESKY	Poland	Ground-Based	Radar, EO, Acoustic	Non-Kinetic	RF Jamming, GNSS Jamming	Link
302	Terra Hexen	Unidirectional Neutralizer	Poland	Handheld		Non-Kinetic	RF Jamming, GNSS Jamming	Link
303	Textron Systems	StrongArm – Handheld, Fixed Site/ Vehicular	USA	Ground-Fixed, Ground-Mobile, Handheld		Non-Kinetic	GNSS Interference, RF Deception/Control, RF Interference	Link
304	Thales	SQUIRE Radar	France	Ground-Fixed, Ground-Mobile	Radar	N/A		Link
305	Thales	Hologarde Integrated Drone Defense System	France	Ground-Fixed	Radar, RF, EO, IR	Non-Kinetic	RF Deception/Control, RF Interference	Link
306	Thales-Raytheon Systems	AN/MPQ-64F1 Improved Sentinel	France	Ground-Based	Radar	N/A		Link
307	Theiss UAV Solutions, LLC	Excipio Aerial Netting System and Excipio Reaper System	USA	UAV		Intercepting UAS	Net Capture, Projectile	Link
308	Torrey Pines Logic	Beam220	USA		Optical	N/A		Link
309	TrustComs	Drone Blocker	France	Ground-Fixed	TBA	Non-Kinetic	RF Deception/Control, RF Interference	Link
310	Veth Systems	Drone Hunter	Hungary	Ground-Based		Non-Kinetic	RF Jamming, GNSS Jamming	Link
311	Vigilant Drone Defense	Vigilant Drone Denial System	USA	Aerial, Ground-Fixed, Handheld	RF	Non-Kinetic	RF Interference	Link
312	Vorpal Ltd.	VigilAir	Israel	Aerial, Ground-Fixed, Ground-Mobile	RF	Non-Kinetic	RF Deception/Control	Link

#	Manufacturer	Product_Name	Country	Platform	Detection	Mitigation_Type	Mitigation Method	URL
313	WhiteFox	Dronefox Fortify	USA	Ground-Fixed	RF	Non-Kinetic	RF Deception/Control	Link
314	WhiteFox	Dronefox Mobile	USA	Ground-Fixed, Ground-Mobile	RF	Non-Kinetic	RF Deception/Control	Link
315	WhiteFox	Scorpion	USA	Aerial, Ground-Fixed, Handheld	RF	Non-Kinetic	RF Deception/Control	Link
316	esc Aerospace	CUAS	Germany	Ground-Fixed	RF, Radar, Acoustic, EO	Non-Kinetic	EMP, GNSS Interference, RF Interference	Link

APPENDIX C. GENERAL CHARACTERISTICS OF COMMON UAS SENSING AND TRACKING TECHNOLOGIES

Table C-1 lists some typical characteristics of various UAS sensing and tracking technologies. Performance can vary depending on the specific sensing component and its integration into the CUAS.

Table C-1: UAS Sensing and Tracking Technology General Characteristics

	Acoustic/ Seismic	Passive RF (spectrum analysis)	Active RF (radar)	Optical Imaging
Sensing Mode	Microphone arrays sense UAS sound waves	Reception and analysis of UAS RF transmissions (video, control, telemetry, Wi-Fi)	Active detection of reflected radio signals	Reflections or emissions of visible to infrared (IR) light wavelengths
Sensor Field of View	90-360°	360°	90-360° (horizontal) 3-90° (vertical)	variable, very small to 360° (WAMI), imager dependent
Weather	Susceptible; wind increases background noise level	Small effect (attenuation of signals)	Susceptible; moisture/rain causes high NAR	Susceptible (depending on wavelength; IR is much less susceptible)
Range (5 lb. UAS)	Low	Very High	Variable, typically Medium to High	Low to High
Geolocation Accuracy	Low, line of bearing (LOB) only	Medium, LOB to 2D geolocation	High, 3D location	LOB (no distance information)
Tracking Accuracy	Medium	High	Very High	High
Night Operation	Same as day	Same as day	Same as day	No degradation for IR wavelength systems
Autonomous UAS Sensing?	Yes	No	Yes	Yes
Typical Weaknesses	Limited range	Multiple targets can cause unacceptable latency	Birds and weather cause high NAR	Generally, requires integration with additional technologies; expense
Typical Strengths	Does not require line of sight	Ability to recognize communication protocols, intercept video, ID UAS make/model/controller	High accuracy multi-target tracking with almost no latency	Generates useful, easily interpretable data for human decision-making

This page left blank

APPENDIX D. GENERAL CHARACTERISTICS OF COMMON UAS MITIGATION TECHNOLOGIES

Table D-2 lists some typical characteristics of common unmanned aircraft system (UAS) mitigation technologies. Performance can vary depending on the specific mitigation component, maturity, UAS threat, operational environment, and other factors.

Table D-2: General Characteristics of UAS Mitigation Technologies

	Electromagnetic/Radio Frequency (RF) Countermeasures	Global Navigation Satellite System Countermeasures	Net Capture (ground-platform)	Net-Capture (aerial platform)	Ballistic Projectiles	Directed Energy
Mitigation Mode	Interference, commands, and takeover (radio control (RC)/navigation)	Interference (prevent waypoint navigation), location spoof (exploit waypoint navigation)	Net is launched or deployed to intercept and entangle the UAS (typically via propellers)	Entanglements fired from or dragged underneath an intercepting UAS	Projectiles or munitions fired from the ground	Damage to airframe or electronics via deposition of laser, microwave, acoustic or other energy
Weather	Minimal effect	Minimal effect	Susceptible	Susceptible, UAS-dependent	Minimal effect	Susceptible – rain/clouds can attenuate/reflect
Range	Variable, depends on many factors	High to Very High, depending on power levels	Low	Low-Medium, UAS dependent	Low, depending on targeting method	Variable depending on many factors, generally low-medium
Multi-shot/ targets	Yes	Yes	Limited	Limited	Yes	Yes
Night Operation	Same as day	Same as day	Reduced range	Reduced range	Depends on targeting technology, operator	Same as day
Mitigates Dark UAS?	No (for non-RC navigation)	No (for non-GNSS navigation)	Yes, if in range and can be targeted/ tracked	Yes, if in range and can be targeted/ tracked	Yes, if in range and can be targeted/ tracked	Yes, if in range and can be targeted/ tracked
Weakness	Must know which RF band to mitigate, lower RC bands are harder to mitigate, dark UAS	Potential collateral damage, does not immediately stop fixed-wing UAS, dark UAS	Range, speed of target, limited rounds, human operated	Fast-moving or evading UAS, autonomous operation still developing	Policy, collateral damage, safety/liability, ineffective on moving UAS unless using smart-aim technology	Policy, collateral damage, safety/liability, evading UAS are a challenge

This page left blank

APPENDIX E. SYSTEMS ENGINEERING FRAMEWORK FOR PHYSICAL SECURITY SYSTEMS DESIGN AND EVALUATION

Sandia National Laboratories (Sandia) began in 1945 as Z Division, the engineering arm of Los Alamos Scientific Laboratory (LASL). Ultimately, its growth prompted its separation from LASL in 1949, and Bell Laboratories was tasked with managing Sandia. As an engineering laboratory, Sandia implemented the rapidly evolving principles of systems engineering, a term and concepts initially developed at Bell Telephone Laboratories in the early 1940s.

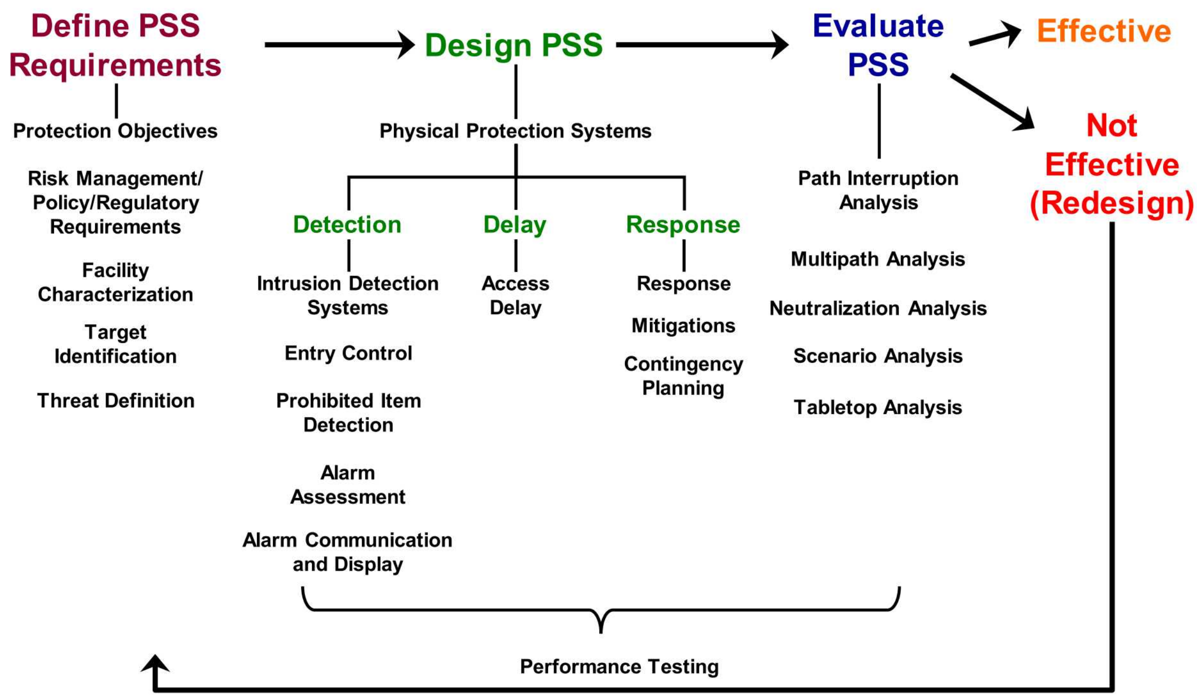
In the 1970s, Sandia's work supporting national security was broadened to include development of physical protection principles and technologies to protect some of the nation's most critical assets. Up to that point the physical security of critical U.S. assets followed a military model, relying heavily on armed personnel to protect critical assets. Sandia pioneered the concept of treating security like an engineering problem, and that combining technology with people could increase effectiveness of physical protection in a system designed to achieve specific performance objectives.

Although systems engineering has many forms, at a high level, the design of a system requires developing clear system objectives, designing a system to meet the objectives, and then testing the design to determine if it sufficiently meets those objectives. If the system does not meet the objectives, it can be redesigned in an iterative process until the objectives are met. In some cases, if a design does not meet the defined objectives the objectives can be revisited to ensure they are accurate and realistic.

This high-level concept of systems engineering was adapted to physical protection. In security, the objective is to protect something—facilities, assets, people, a capability, or the environment—from someone attempting to cause harm. In contrast, the objective of safety is to protect facilities, assets, people, or the environment from natural disasters, equipment failures, or human errors.

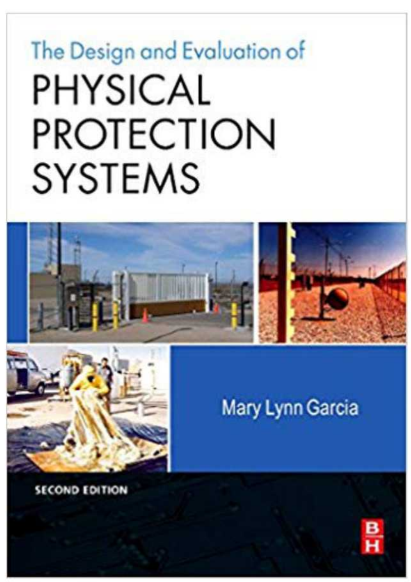
A physical protection framework based on systems engineering concepts was developed by Sandia. It was termed the Design and Evaluation Process Outline, or DEPO illustrated below. In the DEPO framework, the first phase, defining system objectives, consists of identifying what needs to be protected and the threat or threats it needs to be protected from. This phase includes identifying any regulatory or policy-based requirements as well as functional or performance requirements.

The second phase consists of designing physical protection systems (PPS) with measures that achieve three core functions: Detection, Delay, and Response. Detection is sensing that a potential threat is attempting to do something, assessing the threat/alarm to determine if it is an an actual threat, and if so, initiating a response to that threat. The role of barriers (Delay) in the design is to make the adversary tasks after the initial detection point difficult and to increase the time necessary for the threat to cause harm. This allows sufficient time to respond and prevent the threat. Response is the process of interrupting the threat and neutralizing it prior to the threat causing harm to the protected asset. The last phase of the DEPO process is to test the system to determine whether it meets the defined objectives. If so, the design is good, and if not, the system can be redesigned, or the objectives modified until a final PPS design is achieved.



In Counter-Unmanned Aircraft Systems (CUAS) applications, there is a tendency to skip directly to the 'kill chain', or 'detect, delay, response' portion of the model above, without complete context of the requirements or performance testing/evaluation methods that will enable a determination as to whether the component or technology will meet defined objectives. This broader context and systems engineering approach to CUAS is critical to identifying, acquiring, and deploying solutions, and to conducting standardized testing and evaluation.

For additional information on the above framework, and the process for designing and assessing security systems in general, please see Garcia, Mary Lynn, *The Design and Evaluation of Physical Protection Systems*, 2nd Ed. Boston, Butterworth-Heinemann, 2008.



DISTRIBUTION

Email—External (encrypt for OUO)

Name	Company Email Address	Company Name
Timothy Bennett	timothy.bennett@hq.dhs.gov	DHS S&T
Jeff Randorf	Jeffrey.Randorf@hq.dhs.gov	DHS S&T
John Vehmeyer	John.Vehmeyer@hq.dhs.gov	DHS S&T
Curtis Austin	curtis.austin@associates.hq.dhs.gov	DHS S&T
Brian Davis	brian.davis@associates.hq.dhs.gov	DHS S&T
Shane Cullen	Shane.Cullen@hq.dhs.gov	DHS S&T

Email—Internal

Name	Org.	Sandia Email Address
Carol Jacobus	1182	cjacobu@sandia.gov
Daniel Barton	6520	bartondl@sandia.gov
Scott Brooks	6524	shbrook@sandia.gov
Camron Kouhestani	6524	cgkouhe@sandia.gov
Chad Monthan	6524	cwmonth@sandia.gov
Erik Faye	6621	ejfaye@sandia.gov
John Stikar	6621	jastika@sandia.gov
Sharon Del Prete	10665	stdelpr@sandia.gov
Technical Library	9536	libref@sandia.gov

Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.