December 2019
Report No. 19-010

Charles D. Baker
Governor
Karyn E. Polito
Lieutenant Governor
Stephanie Pollack
MassDOT Secretary & CEO

The Application of Unmanned Aerial Systems In Surface Transportation - Volume II-E: Assessment of Unmanned Aircraft System Situational Awareness Technology to Support Applications in Surface Transportation

Principal Investigator
Dr. Michael Plotnikov
University of Massachusetts Amherst

Research and Technology Transfer Section
MassDOT Office of Transportation Planning

U.S. Department of Transportation
Federal Highway Administration

Technical Report Document Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
19-010	n/a	n/a

4. Title and Subtitle	5. Report Date
The Application of Unmanned Aerial Systems In Surface Transportation – Volume II-E: Assessment of Unmanned Aircraft System Situational Awareness Technology to Support Applications in Surface Transportation	December 2019
	6. Performing Organization Code 19-010
7. Author(s) Michael Plotnikov	8. Performing Organization Report No.
9. Performing Organization Name and Address University of Massachusetts Amherst UMass Transportation Center, 214 Marston Hall 130 Natural Resources Road, Amherst, MA 01003	10. Work Unit No. (TRAIS) n/a
	11. Contract or Grant No.
12. Sponsoring Agency Name and Address Massachusetts Department of Transportation Office of Transportation Planning 10 Park Plaza, Suite 4150, Boston, MA 02116	13. Type of Report and Period Covered Final Report June 2018 – December 2019
	14. Sponsoring Agency Code n/a

15. Supplementary Notes
Project Champion – Jeffrey DeCarlo, MassDOT Aeronautics Division

16. Abstract
Rapid proliferation of drones creates serious challenges to transportation facilities and the traveling public. Designed to expand and update the results of the Phase I Counter-Unmanned Aircraft System (CUAS) study, the Phase II study presented herein was conducted to review the current technologies available to detect, track, and identify small UAS entering restricted airspace, specifically near critical ground transportation infrastructure including within densely populated metropolitan areas. The study included an expanded literature synthesis, the design of a prototype for field testing of select CUAS technologies, and field demonstrations of selected CUAS technologies. On the basis of this study, recommendations have been made regarding counter-drone technologies and testing procedures in order to find the best available solutions to protect transportation infrastructure from potential drone threats.

17. Key Word	18. Distribution Statement
counter-UAS technology, transportation safety, situational awareness, CUAS, air traffic safety, non-cooperating drones	unrestricted

19. Security Classification (of this report)	20. Security Classification (of this page)	21. No. of Pages	22. Price
unclassified	unclassified	44	n/a

Form DOT F 1700.7 (8-72) **Reproduction of completed page authorized**

This page left blank intentionally.

The Application of Unmanned Aerial Systems In Surface Transportation - Volume II-E: Assessment of Unmanned Aircraft System Situational Awareness Technology to Support Applications in Surface Transportation

Prepared By:

Principal Investigator
Michael Plotnikov, Ph.D.
University of Massachusetts Amherst

Prepared For:

Massachusetts Department of Transportation
Office of Transportation Planning
Ten Park Plaza, Suite 4150
Boston, MA 02116

December 2019

This page left blank intentionally.

Acknowledgments

This study was undertaken as part of the Massachusetts Department of Transportation Research Program with funding from the Federal Highway Administration State Planning and Research funds. The authors are solely responsible for the accuracy of the facts and data, the validity of the study, and the views presented herein.

The research team would like to acknowledge the efforts of Dr. Jeffrey DeCarlo and his team from the MassDOT Aeronautics Division for their help and guidance throughout all stages of the project. In addition, we would like to acknowledge the contributions of Gabriel Sherman and Jose Simo from the MassDOT OTP Research Section for providing the research team with valuable feedback. Finally, the research team would like to thank Dr. John Collura from UMass Aviation Center for his help with editing the final draft of the document, as well as Matt Mann and Tracy Zafian from the UMass Transportation Center for their contributions to interagency coordination and review of this report and technical memorandum on the literature synthesis.

Disclaimer

This page left blank intentionally.

Executive Summary

This study of Assessment of Unmanned Aircraft System Situational Awareness Technology to Support Applications in Surface Transportation was conducted as part of the Massachusetts Department of Transportation (MassDOT) Research Program. This program is funded with Federal Highway Administration (FHWA) State Planning and Research (SPR) funds. Through this program, applied research is conducted on topics of importance to the Commonwealth of Massachusetts transportation agencies.

The rapid proliferation of UAS (unmanned aircraft systems also known as drones) creates serious challenges to transportation facilities and traveling public. Designed to expand and update the results of the Phase I Counter-Unmanned Aircraft System (CUAS) study also funded through MassDOT with FHWA monies, the Phase II study presented herein was conducted to review the current technologies available to detect, track, and identify small UAS entering restricted airspace, specifically near critical ground transportation infrastructure, including that located within densely populated metropolitan areas.

The objectives of this research were: (1) to accomplish a UAS-related literature synthesis of commercially available counter-drone technologies; and (2) to design a prototype of a field test to evaluate CUAS products intended to detect, track and identify cooperative and non-cooperative drones in the vicinity of critical transportation facilities; and (3) to validate the prototype and to conduct a field test of select CUAS products and technologies. Due to a number of logistical constraints, rigorous field testing of CUAS technologies was not conducted during this study.

The research found that CUAS systems that integrate multiple technologies to detect, track, and identify UAS are the most promising solutions for protecting critical transportation infrastructure. In addition, the selection of CUAS products should consider all environmental factors around the protected facilities that can dramatically affect the performance of tested products, such as terrain, weather, noise, among others. Finally, the decision to implement a specific CUAS product should take into account the current regulatory framework in the U.S. and restrictions specific to a given state and jurisdiction.

This page left blank intentionally.

Table of Contents

This page left blank intentionally.

List of Tables

This page left blank intentionally.

List of Figures

This page left blank intentionally.

List of Acronyms

Acronym	Expansion
ADS–B	Automatic Dependent Surveillance–Broadcast
ADS–R	Automatic Dependent Surveillance–Receive
AI	Artificial Intelligence
AUDS	Anti-UAS Defense System
COTS	Commercial Off-The-Shelf
CUAS	Counter-Unmanned Aerial System (Technology)
EO	Electro-Optical
FAA	Federal Aviation Administration
FHWA	Federal Highway Administration
FTA	Federal Transit Administration
FRA	Federal Railroad Administration
GPS	Global Positioning System
GNSS	Global Navigation Satellite System
IR	Infra-Red
LiDAR	Light Detection and Ranging
MassDOT	Massachusetts Department of Transportation
NextGen	Next Generation Air Transportation System
RF	Radio Frequency
UAS[*]	Unmanned Aerial System(s) or Unmanned Aircraft System(s)
sUAS[2]	Small Unmanned Aerial System(s) or Small Unmanned Aircraft System(s)

[*] The terms “UAS” and “drone” are used interchangeably.

[2] Per current FAA regulations (Pub. L. 112-95, sec. 331(6)), a sUAS is defined as a small unmanned aircraft (system) with a takeoff weight under 55 pounds.

This page left blank intentionally.

1.0 Introduction

This research project, on the Assessment of Unmanned Aircraft System Situational Awareness Technology to Support Applications in Surface Transportation, was undertaken as part of the Massachusetts Department of Transportation (MassDOT) Research Program. This program is funded with Federal Highway Administration (FHWA) State Planning and Research (SPR) funds. Through this program, applied research is conducted on topics of importance to the Commonwealth of Massachusetts transportation agencies.

1.1 Problem Statement

Cost reductions and innovations in global positioning systems (GPS), cameras, and other advanced sensor-based technologies have led to increased use of small unmanned aircraft systems (sUAS). The Federal Aviation Administration (FAA) estimates that combined hobbyist and commercial sUAS sales will rise from 2.5 million units in 2016 to 7 million units by 2020 (*1*). Another report predicts that there could be more than 2.5 million sUAS in the United States by 2020 with a takeoff weight, over 0.55lbs, for which current FAA regulations require FAA registration (*2*). FAA regulations define a sUAS as a small unmanned aerial aircraft with a takeoff weight under 55 pounds.

Though it promises new opportunities, the rapid proliferation of sUAS also has the potential to lead to activities that may harm people and destroy or damage property. In order to ensure public safety and security, there is a need to evaluate technologies that can detect, track, and identify cooperating and non-cooperating sUAS, specifically those operating near sensitive areas such as transportation infrastructure.

1.2 Research Objectives

The objectives of this research were:

1. To create a literature synthesis which focuses on CUAS technologies capable of detecting, tracking, and identifying sUAS near critical surface transportation infrastructure.
2. To develop a prototype of a pilot study for field testing CUAS technologies.
3. To conduct a field test to evaluate selected CUAS products, and to provide recommendations to MassDOT regarding potential CUAS solutions to address problems related to non-cooperative UAS near critical transportation infrastructure.

1.3 Report Outline

The remaining sections of this report are organized as follows. Chapter 2 describes the research methodology for this project. Chapter 3 describes the results of the literature synthesis and the initial COTS (commercial off-the-shelf) product selection, provides an outline of the prototype for a field test to evaluate select CUAS technologies, and discusses the observations made during the field demonstration of selected CUAS. Chapter 4 gives conclusions and recommendations. Chapter 5 provides the list of references used in this study. Chapter 6 contains appendices with detailed data collected during the literature synthesis, as well as other reference material, including details on the COTS CUAS technologies and products considered during this research.

2.0 Research Methodology

The first task of this project was to conduct a literature synthesis to identify the CUAS technologies available worldwide. The results of this task were presented in the Technical Memorandum on Literature Synthesis.

The second task of the project was to perform a preliminary selection of CUAS technologies based on both technical parameters and some non-technical characteristics that were also found to be important during the literature synthesis.

The third task of this project was to develop a prototype of a pilot study for a field evaluation of select CUAS technologies.

The fourth task of the project was to execute field testing of the selected CUAS technologies.

The first two tasks cover the first research objective presented in Section 1.2; the third task covers the second research objective; and the last task covers the third research objective.

2.1 Literature Synthesis and Preliminary Evaluation

The purpose of the literature synthesis was to collect preliminary information about technologies, trends, manufacturers, and products that can help to detect, track, and identify both cooperative and non-cooperative UAS in the proximity of critical transportation infrastructure. The information was collected from professional literature, internet publications, the Transportation Research International Documentation (TRID) database, conference proceedings, manufacturer brochures, and other sources. The information gathered through the literature study was also used to perform an initial selection of the commercial off-the-shelf (COTS) CUAS products.

The evaluation of CUAS technologies included three steps as described below:

- Step 1: Initial selection of CUAS products on the basis of: (a) U.S. market availability; and (b) compliance with U.S. civilian regulations.
- Step 2: Evaluation of selected CUAS in terms of technical parameters and capabilities.
- Step 3: Field testing of select CUAS products identified during the technical evaluation in Step 2.

The literature synthesis covers Task 1 while the evaluation of CUAS covers Tasks 2 and 4.

2.2 Design of the Prototype of the Field Test

A prototype for the field testing of CUAS technologies was developed on the basis of the literature synthesis. The field test was intended to evaluate selected COTS CUAS technologies capable of detecting, tracking, and identifying cooperating and non-cooperating UAS, including 1) assessing their performance, capabilities, and reliability, as well as 2) evaluating their practical utility for protecting critical surface transportation infrastructure.

The research team designed the prototype of the field test to be similar to experiments conducted by the military *(3)* and cross-government research organizations *(4)*, with the major differences related to the special focus on protection of ground transportation infrastructure, limited scope (detection, tracking and identification technologies only) timeframe (a few days) and budget.

The exercise can be roughly described as a "war game" between the individual or a group of counter-UAS manufacturers who will try to protect a designated facility ("defenders") and an individual or a joint group of MassDOT/UMass UAS pilots, equipped with a variety of different airframes, who will try to access the designated facility ("attackers").

The field tests have been designed to allow maximum flexibility to vendors, MassDOT, and the research team. This means, for example, that the test may be conducted at different times and different locations for different vendors or products.

The design for the field testing includes six distinct options. Those options include the following:

1. Each selected CUAS product will be tested at a single location;
2. All selected products that utilize the same type of technology (e.g. radar) will be tested at a single location;
3. All selected products with different technologies will be tested at a single location;
4. Each selected CUAS product will be tested at multiple locations;
5. All selected products that utilize the same technology (e.g. radar) will be tested at multiple locations;
6. All selected products with different technologies will be tested at multiple locations.

3.0 Results

3.1 Literature Synthesis

During the literature synthesis, the research team identified 49 different COTS CUAS products from 30 manufacturers. Twenty-four of these products are available on domestic market, the rest are sold only outside the U.S.

A number of CUAS technologies that detect, track, and identify cooperating and non-cooperating sUAS have emerged in recent years to help protect public safety and critical transportation infrastructure. Some technologies initially developed for military applications may not be suitable for civil applications due to their high costs or because they may introduce additional hazards, disrupt the normal operation of critical communication and navigation equipment, or raise privacy and health-related concerns. Both MassDOT and FHWA are interested in finding the most appropriate technological solutions to address potential sUAS-related threats to critical transportation infrastructure while minimizing potential negative impacts associated with the use of CUAS technology The literature synthesis presented in this section is intended to assist MassDOT and the FHWA in better understanding the current state of the practice of CUAS technology.

Building on the 2016 Phase I review of the commercial off-the-shelf (COTS) CUAS products and survey of a diverse group of decision makers (*5*), the research team conducted a literature synthesis to identify currently available technologies that can detect, track, and identify UAS entering restricted airspace, specifically near critical transportation infrastructure. This study is wider in scope than the Phase I project, and focused on protecting a wider variety of surface transportation facilities beyond airports. Therefore, the literature synthesis was expanded to include technologies that can protect smaller yet equally important ground transportation infrastructure including within densely populated urban areas.

There has been a dramatic change in the landscape of CUAS technologies since the Phase I study. The numbers of both manufacturers and available products have quadrupled. As the market has become more saturated, some less competitive products and manufacturers have left the market, while others have merged efforts with former competitors or large, diverse electronics and defense industry consortia.

While the research team tried to examine all existing technologies, the Phase II synthesis focused on civilian off-the-shelf CUAS products commercially available worldwide. UAS detection and tracking technology solutions can be divided into two groups. The first group consists of devices that utilize active detection methods. The second group includes devices that utilize passive detection methods. The most common active detection method is radar, which emits signals in the radio frequency (RF) spectrum and then captures the signal reflection from the aircraft and other moving or static objects. Passive detection methods utilize electro-optical, acoustic, and RF sensors to capture signals emitted by the aircraft itself.

Both passive and active systems have proven to be effective in detecting and tracking UAS at both long (radar and RF-spectrum scanning) and medium to short distances (electro-optical, acoustic) (*5*). A brief summary of the advantages and drawbacks associated with different detection, tracking, and identification technologies is presented in Table 3.1.

Table 3.1. UAS detection, tracking, and identification technologies

	Active	**Passive**		
	Radar	**Radio Frequency**	**Electro-Optical**	**Acoustic**
Advantages	Long-range; all-weather	Long-range; all-weather; ability to track pilot and UAS	High accuracy of tracking and identification, including the payload	Low cost; high accuracy of tracking
Drawbacks	Affected by terrain; limited UAS identification capabilities	Can't "see" UAS flying in a fully autonomous mode	Limited range; affected by elements and terrain	Limited range; affected by noisy environment

As shown in Table 3.1, there is no single universal solution for UAS-imposed threats. There are a number of reasons for this. The primary one is that UAS are typically small targets that may have a wide variety of physical characteristics and that are usually moving at low altitudes. Also, sUAS are usually made of composite materials that decrease the probability of stable and reliable detection, tracking, and identification with radar technology. In addition, sUAS do not carry a transponder such as the one used in the Automatic Dependent Surveillance-Broadcast (ADS–B) systems proposed in the Next Generation Air Transportation System (NextGen) for aircraft in controlled airspace. Moreover, there is currently no single standard for sUAS communication protocol or a specific frequency band. However, there is hope that this will soon change. DJI, the largest manufacturer of commercial UAS, just announced that all its drones that require FAA registration are going to be equipped with the ADS-R receiver starting in 2020; this is seen as a first step toward integrating sUAS into the national airspace (*6*). Finally, there is a growing trend of utilizing a wide group of stakeholders in the establishing up of standards on sUAS electronic communication and identification procedures (*7*). The push towards active ID mechanisms could establish a common feature that would enable a fairly universal detection, tracking, and identification approach. The effectiveness of potential solutions depends on how the standard ID is implemented. However, challenges still remain with UAS that operate in radio-silent mode.

In order to achieve the most reliable performance, the majority of sUAS detection and tracking systems must integrate multiple types of sensor technologies, both active and passive. Examples of such comprehensive solutions are currently offered by SRC, Inc. (Gryphon Skylight, ACR Hawk) and by Dedrone (DroneTracker Multi-Sensor). The smaller DroneTracker system offers a range of UAS detection and tracking of up to 500 meters (1,640 ft.), while the larger Gryphon Skylight claims the capability to detect UAS as far away as 10 kilometers (6.1 mi.) with radar, and up to 3 kilometers (1.9 mi.) with its spectrum sensing and slew-to-cue camera (*8, 9*).

Another notable comprehensive sUAS detection and tracking system is offered by DeTect Inc. The DeTect DroneWatcher equipped with HARRIER Drone Surveillance Radar provides a comprehensive, layered solution for detection, tracking, alerting, and interdiction of DJI Phantom-size UAS at distances of up to 4 kilometers (3.1 mi.). Advanced technology combines

Signals Intelligence (SIGINT) which gathers information by intercepting transmitted signals, and radar for detection and tracking (*10*). Often, higher-end drone detection and tracking systems can also integrate and control third-party devices including signal jammers to intercept non-cooperative intruder sUAS. However, the price of such systems is often outside the budgets of smaller transportation facilities and operators. In addition, there are legal restrictions which limit wider implementation of such devices in the U.S.

It is worth noting that on the low end of the CUAS market, there are a number of innovative products that are either free or very inexpensive. Such products include apps that can turn a WiFi-capable consumer electronic device - such as a smartphone, tablet, or computer - into a personal UAS detector.

3.2 Preliminary Evaluation of CUAS Products

Evaluation and selection of sUAS detection, tracking and identification systems is not a trivial task for a number of reasons. First, there are numerous variables to consider related to operational environment, potential vulnerabilities, types of target sUAS, capital and operational costs, among others. Operational environment-related variables may include the landscape, prevailing weather, and population density near a protected facility, among others. Potential vulnerabilities will vary with the type of the facility. The type of UAS as well as its size will greatly impact a CUAS system's ability to detect, track and identify intruders. Capital and operational costs will affect the ability of the transportation facility managers to provide sufficient level of protection for their facilities. Degree of compliance with federal, state, and local laws and regulations will greatly affect potential level of implementation of CUAS technology. Finally, concerns associated with potential collateral damage may significantly restrict CUAS adoption under certain conditions.

The evaluation of CUAS technologies was completed in the following three steps.

Step 1: Initial selection of CUAS products on the basis of: (a) U.S. market availability; and (b) compliance with U.S. civilian regulations.

Step 2: Evaluation of selected CUAS in terms of technical parameters and capabilities.

Step 3: The study proposed field testing of select CUAS products chosen on the basis of the evaluation in Step 2. It was expected that the field testing will be conducted by MassDOT and the UMass research team at a location and using a testing format selected by MassDOT. Due to a number of logistical constraints, rigorous field testing of CUAS technologies was not conducted during this study. The constraints against field testing included the regulatory restrictions in the U.S., lack of time to finalize the format of the field tests, limited funding, and the challenges of trying to have multiple vendors participate in a single field test. In lieu of field testing, there were a number of field demonstrations conducted by individual CUAS vendors and attended by MassDOT staff and others. Those demonstrations did not include rigorous testing of CUAS products under a variety of conditions, but the results of the demonstrations were still

informative. MassDOT may consider incorporating field testing into a future round of CUAS research.

On the basis of the findings of the Phase 1 study and the past UAS experiences of MassDOT staff and the UMass research team, a decision was made to group the CUAS evaluation parameters into three categories: 1) primary performance-related; 2) secondary performance-related; 3) other important parameters such as capital and operating costs as well as regulatory constraints. As suggested by the panel of experts who contributed to the Phase I CUAS review and by the feedback from MassDOT on the draft Phase II literature synthesis, each category of parameters was evaluated independently.

The primary performance-related parameters include detection, tracking, and identification ranges. Those parameters are paramount for the successful protection of transportation facilities as they directly affect amount of time available for authorities responsible for the facility operations to select and apply appropriate countermeasures. The secondary performance parameters include the ability to detect and identify payload, operate in adverse conditions, and detect rogue drones that operate in a fully-automated, radio-silent mode. The last category includes other important non-performance related parameters such as system capital and operational cost; regulatory compliance; as well as parameters related to collateral damage or potential environmental impacts. Figure 3.1 demonstrates the importance of the detection, tracking and identification ranges for the successful protection of critical infrastructure, and also provides a glimpse of challenges associated with such tasks.

The horizontal axis of the graph presented in Figure 3.1 indicates the distance from the drone to the protected area. The icons below the horizontal axis provide the typical detection ranges for a radar-based system (approximately 7.5 mi. or 12km.), an electro-optical (EO) system (approximately 2.5 mi. or 4 km.) and acoustic detectors (approximately 0.5 mi. or 0.8 km.). The vertical axis of the graph indicates travel time to protected area. Inclined lines originating from the point of the axes' origin (0,0) represent two types of sUAS approaching the restricted area: 1) a typical quadcopter of the DJI Phantom-class drone (with a cross-section approximately 0.25-0.3 square meters) traveling at the maximum speed of 45 mph (73 km/h); and 2) a faster fixed-wing type drone with the same reflective surface as DJI Phantom travelling at a speed of 100 mph (160 km/h), the maximum speed for sUAS allowed per FAA regulations. The ranges are shown under ideal conditions: flat terrain; no direct obstructions; overcast light conditions without precipitation; and typical ambient noise.) Figure 3.1 allows one to make a quick estimate of the available reaction time to implement countermeasures after the intruder drone is detected by a CUAS system.

As shown in Figure 3.1, typical radar systems have an advantage over electro-optical and acoustic sensors in term of detection and tracking ranges. Note that the typical ranges of RF systems are not shown on the graphics. There are two reasons for such exclusion. The first reason is that the typical detection range of the RF systems can vary considerably depending on the transmitter power output, radio frequency and communication protocol between the sUAS and its ground controller. The second reason relates to performance variability related to of the types of antenna and amplifier used in different RF CUAS systems. For example, while the detection range of the popular DJI portable RF CUAS device equipped with a simple omni-

directional antenna is similar to a typical control range of DJI Phantom IV drone (about 5 km., or 3 mi.), the detection range of the stationary system from the same manufacturer with a complex array of directional antennae and a high sensitivity amplifier can increase the detection range to up to 10 times as far (*11*).

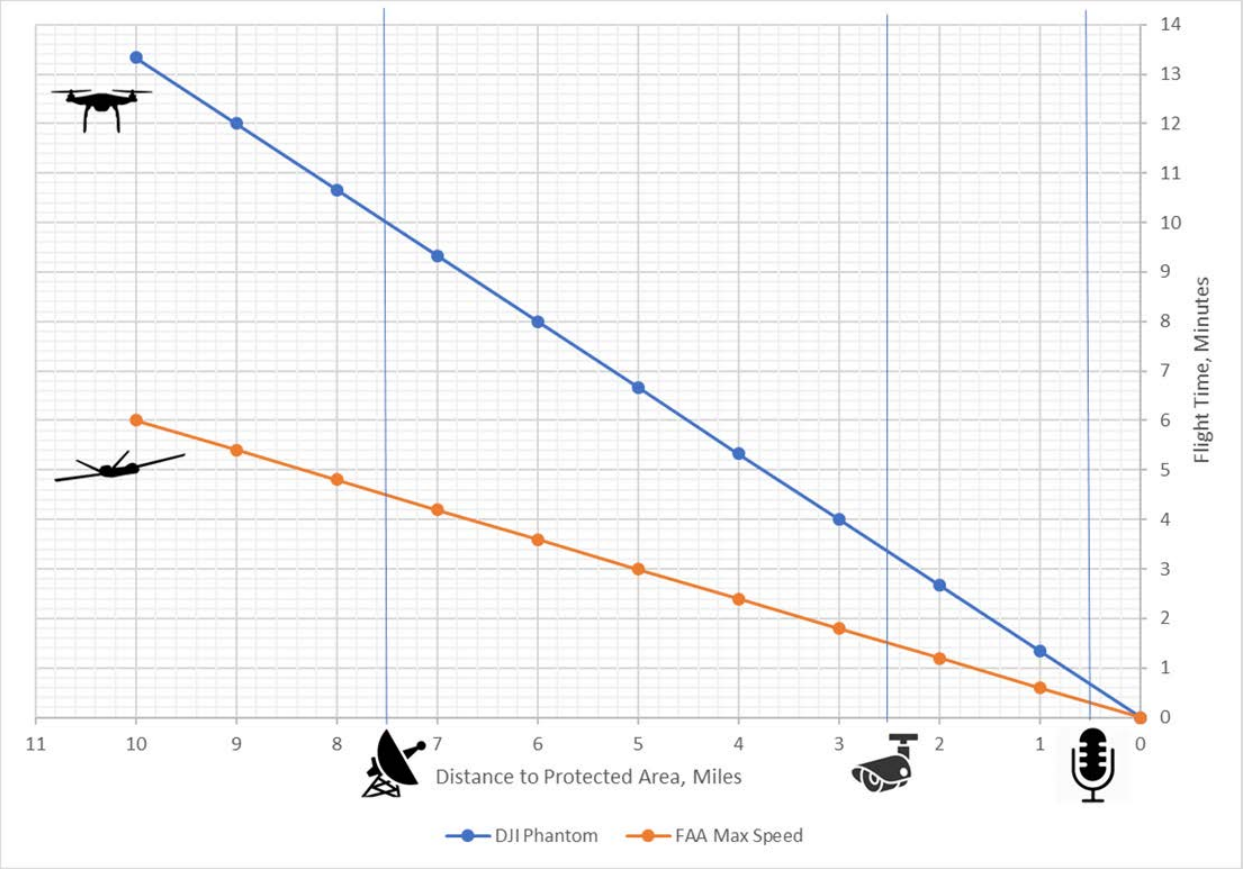

Figure 3.1. Typical detection ranges of various CUAS technologies vs. UAS flight time

Figure 3.1 also provides a display of challenges associated with the short time to engage CUAS mitigation strategies once an intruder UAS has been detected. The problem becomes more significant due to the fact that under current regulations only a few federal agencies (the Department of Homeland Security, Department of Justice, U.S. Coast Guard, Department of Energy, and Department of Defense) are authorized to deploy and implement effective drone interdiction technologies (*12*). The majority of transportation facilities do not have such technologies available at the time of a UAS attack and as a result mitigation will most likely be limited to less effective passive countermeasures, such as notification of the proper authorities and creation of a record of the incident. Another challenge is associated with accurately identifying the potential level of threat from a sUAS. For example, in some situations, such as near a busy airport, the physical presence of any sUAS can raise a red alert. In other cases, such as in the proximity of facilities with large numbers of people and limited emergency evacuation abilities, such as bridges, tunnels, or large transit hubs, the presence of an intruder drone may be considered a serious threat only when such a drone is carrying an unidentifiable suspicious payload.

Of the 49 CUAS detection and tracking systems identified in Step 1 (see Appendix A, Tables 6.1 and Table 6.2), 24 systems available on U.S. market were evaluated in Step 2 based on a number of performance metrics and other factors (see Appendix A, Table 6.3) From the results of this evaluation, 7 systems were recommended for field testing in Step 3 (Table 3.2). More details on the systems evaluated in Step 2 are available in the *Technical Memo on Literature Synthesis* produced for that evaluation.

Table 3.2. sUAS detection, tracking and identification systems recommended for field test

Manufacturer	**Model**	**Detection Technology***	**Detection Range*, km (mi)**	**Final Score**
Adsys Controls Inc.	SATS2 Aerial Surveillance	EO/LiDAR, Acoustic	10	87.5
AeroDefence	AirWarden	RF	7	72
DJI	Aeroscope (Stationary)	RF	Up to 50 (30)	75.5
SRC	Gryphon Skylight, Gryphon Mobile Skylight	Radar, RF, EO, IR	10 (6) 4.8 (3) 3 (1.8)	87.5
Liteye	ADIS	Radar, EO, IR	3–8 (1.8–5)	75.5
Sensofusion USA	Airfence	RF	Up to 10 (6)	78

Notes: *Detection range is shown for DJI Phantom-size target, the most common sUAS on U.S. market.

3.3 Design of the Prototype of the Field Test

The field test can be briefly described as a “war game” between the individual or a group of CUAS manufacturers who will try to protect a designated facility (“defenders”) and an individual or a joint group of MassDOT or UMass UAS pilots, equipped with a variety of different airframes who will try to access the designated facility (“attackers”).

The field testing has been designed to allow maximum flexibility to vendors, MassDOT, and the UMass research team. This means that the test may be conducted at different times and different locations for different vendors or products.

In order to provide the required flexibility, the field testing design includes six distinct options. Those options include the following:

1. Each selected CUAS product will be tested at a single location;
2. All selected products that utilize the same technology (e.g. radar) will be tested at a single location;
3. All selected products representing all technologies will be tested at a single location;
4. Each selected CUAS product will be tested at multiple locations;

5. All selected products that utilize the same technology (e.g. radar) will be tested at multiple locations;
6. All selected products representing all technologies will be tested at multiple locations.

Each design option has distinct benefits and drawbacks that can be presented with a help of five major evaluation criteria. The evaluation criteria include the following:

1. Convenience to vendors, including flexibility of time and location as well as the level of exposure of the product to potential competition;
2. Convenience to the research team, including factors related to level of effort associated with organizing, and conducting the event, and data processing;
3. Total time needed to conduct the test;
4. Total costs associated with conducting the tests; and
5. Quality and reliability of collected data.

The major benefits and challenges associated with the six different design options presented in Table 3.3.

Table 3.3. Major benefits and challenges of CUAS field test options

	One Vendor, One Location	**One Tech, One Location**	**All Tech, One Location**	**One Vendor, Multiple Locations**	**One Tech, Multiple Locations**	**All Tech, Multiple Locations**
Convenience to Vendor	Excellent	Very Good	Good	Fair	Poor	Very Poor
Convenience to Researcher	Good	Very Good	Excellent	Very Poor	Poor	Fair
Total Time	Average	Low	Very Low	Extremely High	Very High	High
Total Cost	Average	Low	Very Low	Extremely High	Very High	High
Data Reliability	Poor	Fair	Good	Very Good	Very Good	Excellent

In the proposed field testing, the test site(s) and the facilities to be protected during the tests will be selected by MassDOT. The vendor(s) will be granted the opportunity to survey the area designated for protection and to install, test, adjust their equipment as needed prior to the actual field test. Similarly, the UAS pilots will be granted the opportunity to access the test site prior to the test flights to plan the mission and to familiarize themselves with the landscape.

3.3.1 Test Site Selection

In coordination with MassDOT, the UMass research team considered four potential test sites and the advantages and challenges of each.

1. Gillette Stadium at Foxborough, Massachusetts
2. Joint Base Cape Cod at Bourne, Massachusetts
3. University of Massachusetts, Amherst, Massachusetts
4. Fort Devens Reserve Force Training Area at Devens, Massachusetts

3.3.1.1 Gillette Stadium

Advantages: Gillette Stadium has the advantage of being a facility with major public events that should be considered for protection against non-authorized, non-cooperative UAS. Also, as the stadium is a well-known landmark, a test conducted at this facility could increase the vendors' interest in participating in the field test.

Challenges: The major challenges are related to the requirement to obtain permits to conduct the proposed test, potential delays associated with obtaining such permits, and possible limitations on the scope of the test due to the nature of the facility. Other challenges may be associated with the need to handle the installation of larger and heavier UAS detection products, such as the large radar, which should be placed high over the ground in order to achieve optimal performance. Finally, compared to the other potential sites, this location probably has the highest travel and accommodation costs for the research team and vendors.

3.3.1.2 Joint Base Cape Cod

Advantages: The Joint Base Cape Cod has the advantage of being an already established UAS test site and a military location that may have fewer restrictions associated with both the conducting of UAS flights and on-site testing of CUAS technologies.

Challenges: The major challenges could be associated with having to obtain permits to allow access to the base for certain individuals from both the research team and vendor representatives, and the timeframe needed to obtain such permits.

3.3.1.3 University of Massachusetts Amherst

Advantages: The University of Massachusetts Amherst campus has the advantage of being a home of the UMass research team and the UMTC administrative team. This could help simplify the process of getting sUAS flight permits. Also, the campus is familiar ground for the research team pilots, who will, therefore, require less time and preparation for the test flights. Finally, the process of setting up and conducting the experiment as well as costs associated with travel and accommodations on campus during the testing are expected to be the lowest if this test site is selected.

Challenges: Due to the large number of people working and/or living on the UMass Amherst campus, more time and effort for planning, scheduling, and safety considerations may be required.

3.3.1.4 Devens Reserve Forces Training Area (RFTA)

Advantages: The Devens RFTA has the advantage of being an already established UAS test location which may eventually become a part of a large proposed UAS test corridor between Massachusetts and New York. It is also a long-time military installation that may have fewer restrictions associated with both the conducting of sUAS flights and on-site testing of CUAS technologies.

Challenges: Major challenges could be associated with obtaining permits to get access to the base for certain individuals from both the research team and vendor representatives, and the timeframe needed to obtain such permits.

3.3.2 Additional Details for Consideration

It is desirable that the design of the field tests include both common challenges and technology-specific challenges to evaluate CUAS products. Common challenges include ones to help evaluate the ability of CUAS to detect and track multiple drones representing various platforms approaching the protected facility at different directions, speed, and altitude. Technology-specific challenges access and evaluate each product's vulnerabilities as described in the literature synthesis. Such technology-specific challenges may include: a low-altitude terrain-following approach to test radar capabilities; an autonomous flight in a near radio-silent mode to test RF-intelligence CUAS systems; an approach during the poor visibility to test EO systems; and an approach conducted in a noisy environment to test acoustic sensors. It is also desirable to conduct a test of multiple technologies working together under a combination of unfavorable conditions. Table 3.4 provides a brief summary of the strengths and limitations of CUAS technologies, as evaluated by the researchers based on performance criteria. The summary could serve as a guide for designing various CUAS challenges.

Table 3.4. CUAS technology performance indicators

Performance Indicators	**Counter-UAS Technology Solution**			
	Radar	**RF Intelligence**	**Electro-Optical**	**Acoustic**
Range	Excellent	Excellent	Fair	Poor
Target Tracking	Good	Good	Good	Fair
Target Identification	Fair	Excellent	Excellent	Good
Payload Identification	None	Fair	Excellent	None
Low Light	Excellent	Excellent	Fair	Excellent
Urban Landscape	Fair	Good	Fair	Good
Noisy Environment	Excellent	Excellent	Excellent	Poor
Weather Precipitation	Excellent	Excellent	Poor	Fair
Rogue Drone	Excellent	None	Excellent	Excellent
Ability to Locate Pilot	None	Excellent	Fair	Poor
Difficulty of Installation	High	Medium	Low	Low
Difficulty of Maintenance	Low	Low	High	Average

3.4 Field Testing and Demonstrations

As was discussed earlier, due to a number of logistical constraints, rigorous field testing of CUAS technologies was unable to be conducted during this study. The constraints against field testing included the regulatory restrictions (see Appendix D for details), lack of time to finalize the format of the field tests due to project evolution based on MassDOT priority needs, the challenges of selecting the best format and location for the testing, and of coordinating with multiple vendors, and limited funding for conducting the tests. (only a few thousand dollars in total were allocated for field testing in the project budget).

In lieu of field testing, there were a number of field demonstrations conducted by individual CUAS vendors and attended by MassDOT staff and others. Those demonstrations did not include rigorous testing of CUAS products under a variety of conditions, but the results of the demonstrations were still informative.

One such CUAS demonstration was conducted in June 2019, in Foxborough, Massachusetts near Gillette Stadium, and attended by MassDOT staff, UMass research team members, as well as by various public officials and researchers. The demo, conducted by an invited CUAS vendor, included an "invasive" drone and a "defender" CUAS drone. The demonstration was conducted in a closed parking lot, and a safety perimeter was established around the demonstration area. The demonstration provided effective detection, identification, tracking and capture of the non-cooperative "invasive" drone flying in a "silent" autonomous mode without radio communication. At the beginning of the demo, the vendor's personnel described the CUAS technology and the demo procedures. During the demonstration, the CUAS "defender" rapidly detected and tracked the invasive drone using radar. After tracking the invasive drone, the CUAS drone sent a message to the ground operator asking for permission to launch the CUAS drone. During the demo flight, both the defender and invasive drones operated autonomously using GPS, with pilots standing by ready to intervene in case of emergency. As the defender drone approached within striking distance of the invasive drone, it asked the ground operator for permission to capture. Once permission was granted, the defender drone quickly captured the invasive drone. Finally, the defender drone brought the captured invasive drone back to the launch area, so that the invasive drone and the disabling technology on board the CUAS drone could be examined.

MassDOT may consider incorporating rigorous field testing into a future round of CUAS research.

4.0 Conclusions and Recommendations

Designed to expand and update the results of the Phase I study on CUAS technologies for protecting airports, the Phase II study was conducted to review technologies available to detect, track, and identify sUAS near critical ground transportation infrastructure, including that located near or within densely populated metropolitan areas.

Consistent with the findings from Phase I, as well as similar reviews and field tests conducted by others (*13, 14, 15, 16*), this study have found that there is no CUAS product that utilizes any single type of sensing technology while at the same time being capable to address all challenges associated with sUAS detection, tracking, and identification. The most promising technologies include RF signal intelligence, EO systems, acoustic signature techniques, and surveillance radar. Each technology has distinctive advantages and drawbacks related to its capabilities, reliability, and capital and operating costs. Hence, the research team recommends to select products that combine multiple UAS detection, identification and tracking technologies that would provide the most robust protection for critical transportation facilities.

Based on a preliminary evaluation carried out by the research team, seven commercially available CUAS products have been identified for field testing. The evaluation of selected CUAS products was based on parameters and capabilities provided by the manufacturers. The evaluation parameters included: detection, tracking, and identification ranges; the ability to detect and identify payload, operate in adverse conditions, and detect rogue drones that operate in a fully-automated, radio-silent mode; and some non-technical parameters such as capital and operational costs, regulatory compliance, potential collateral damage and environmental impacts.

The prototype of the field test was designed to evaluate CUAS products that represent the most promising CUAS technologies for detecting, tracking, and identifying cooperative and non-cooperative sUAS. The field test would assess the selected CUAS products for their performance, capabilities, and reliability for protecting critical surface transportation infrastructure. It is recommended that a prototype for the field test be conducted upon the final approval of the testing design and location(s) by MassDOT during the next phase of UAS research.

It is expected that the results of this study will be of interest to a variety stakeholders including State DOT officials; FHWA, FAA, the Federal Transit Administration (FTA), the Federal Railroad Administration (FRA), and other federal agencies; transportation security and law enforcement agencies; university researchers; transportation facility operators, contractors, and consultants.

This page left blank intentionally.

5.0 References

1. Department of Homeland Security. *Unmanned Aircraft Systems Addressing Critical Infrastructure Security Challenges.* n.d. https://www.dhs.gov/sites/default/files/publications/uas-ci-challenges-fact-sheet-508.pdf. Accessed June 9, 2018.
2. Federal Aviation Administration. *FAA Forecast, Fiscal Years 2016–2036*. 2016. https://www.faa.gov/data_research/aviation/aerospace_forecasts/media/FY2016-36_FAA_Aerospace_Forecast.pdf. Accessed June 9, 2018.
3. Rader, J. Army Air Defenders Participate in Black Dart 2018. U.S. Army. 2018. https://www.army.mil/article/211603/army_air_defenders_participate_in_black_dart_2018. Accessed Dec. 12, 2018.
4. MITRE Corporation. The MITRE Challenge: Countering Unauthorized Unmanned Aircraft Systems. 2016. https://www.mitre.org/research/mitre-challenge/mitre-challenge-uas. Accessed Dec. 12, 2018.
5. Looze, D., M. Plotnikov, and R. Wicks. *Current Counter-Drone Technology Solutions to Shield Airports and Approach and Departure Corridors*. Massachusetts Department of Transportation, Boston, MA, 2016.
6. Murphy, K. DJI To Install ADS-B Sensors in All New Drones Starting Next Year. 2019. https://www.interdrone.com/news/dji-to-install-ads-b-sensors-in-all-new-drones-starting-next-year/?utm_source=SilverpopMailing&utm_medium=email&utm_campaign=InterDrone%20News%20-%20DJI%20ADS-B%20Standard%2005-23-19%20(1)&utm_content= Accessed May 25, 2019.
7. Federal Aviation Administration. *UAS Identification and Tracking (UAS ID) Aviation Rulemaking Committee (ARC). ARC Recommendations: Final Report*. 2017. https://www.faa.gov/regulations_policies/rulemaking/committees/documents/media/UAS%20ID%20ARC%20Final%20Report%20with%20Appendices.pdf. Accessed Nov. 1, 2018.
8. Dedrone. Drone Detection Sensors. n.d. https://www.dedrone.com/products/hardware. Accessed July 19, 2018.
9. SRC Inc. Gryphon Skylight UTM System. Detect, Track and Classify Moving Objects in Your Airspace. n.d. http://www.gryphonsensors.com/drone-detection.html. Accessed July 19, 2018.
10. DeTect, Inc. Drone Detection & Defense Systems. https://detect-inc.com/drone-detection-defense-systems/. n.d. Accessed July 19, 2018.
11. DJI Corporation. DJI Aeroscope. https://www.dji.com/aeroscope. Accessed Aug. 1, 2018.
12. Federal Aviation Administration. *Updated Information on UAS-Detection and Countermeasures Technology (Counter-UAS) at Airports, May 2019. Attachment 2, Frequently Asked Questions and Answers Concerning UAS Detection Systems.* https://www.faa.gov/airports/airport_safety/media/Attachment-2-FAQS-UAS-Detection-Systems.pdf. Accessed Nov.11, 2019.
13. Center for the Study of the Drone at Bard College. Counter-Drone Systems 2018. http://dronecenter.bard.edu/publications/counter-drone-systems/. Accessed Aug. 8, 2018.

14. Unmanned Airspace. *The Counter UAS Directory.* 2018. https://www.unmannedairspace.info/wp-content/uploads/2018/05/Counter-UAS-directory.-May-2018.-v1.docx.pdf. Accessed Aug. 8, 2018.
15. Black Dart: DOD's Largest Live-fly, Live-fire Joint Counter-Drone Technology. *SOFREP (Special Operations Forces Report) Online*. https://sofrep.com/gear/black-dart-dods-largest-live-fly-live-fire-joint-counter-drone-technology/. Accessed Feb. 23, 2020.
16. MITRE Inc. MITRE Names C-UAS Challenge Winners. 2016. https://www.mitre.org/news/press-releases/mitre-names-c-uas-challenge-winners. Accessed Aug. 8, 2018.
17. DroneShield. *Counterdrone Handbook. 3rd Edition.* https://www.droneshield.com/counterdrone-handbook. Accessed Feb. 23, 2020.
18. Snead, J., J.-M. Seibler, and D. Inserr. *Establishing a Legal Framework for Counter-Drone Technologies*. Backgrounder #3305. The Heritage Foundation. Washington, D.C., 2018.

6.0 Appendices

Appendix A: UAS Detection and Tracking Systems

Table 6.1. UAS detection and tracking systems: U.S. manufacturers

Manufacturer	Product Name	Type(s) of Sensor(s)*	Detection Range, km (mi)	Web Page Link
Adsys Controls Inc.	SATS2 Aerial Surveillance	EO/LiDar, Acoustic	Up to 10 (6)	1
AeroDefence	AirWarden	RF	Up to 7 (4.4)	2
C Speed LLC	LightWave Radar	Radar	Up to 10 (6)	3
Dedrone	RF-100	RF	2 (1.3)	4
	RF-300	RF	1.5 (1)	
DeTect	DroneWatcherRF Mini	RF	0.5–0.8 (0.3–0.5)	5
	DroneWatcherRF	RF	3.2+ (2+)	
	DroneWatcher DSR	Radar	3.2+ (2+)	
Drone Labs	DD610AR Stationary Drone Detector	RF	1 (0.6)	7
	DM610R Portable Drone Detector	RF	1 (0.6)	
DroneShield	DroneSentinel	Radar, RF, EO, IR	5 (3)	8
Dynetics	GA 9000	Radar	5 (3)	9
SRC	Gryphon Skylight	Radar, RF, EO, IR	10 (6)	10
	Gryphon Mobile Skylight	Radar, RF, EO, IR	10 (6)	
Liteye	ADIS	Radar, EO, IR	8 (5)	11
Sensofusion USA	Airfence	RF	10 (6)	12
SpotterRF	A150 A-Series Counter-Drone Radar	Radar	0.2 (0.13)	13
	A600 A-Series Counter-Drone Radar	Radar	0.6 (0.4)	
	A3000 A-Series Counter-Drone Radar	Radar	0.7 (0.5)	
	A2000 A-Series Counter-Drone Radar	Radar	1 (0.6)	
TCI	Blackbird	RF	N/D	14
UMass/Raytheon	CASA Radar	Radar	1 (0.6)	15

Table 5.2. UAS detection and tracking systems: Manufacturers outside U.S.

Manufacturer	Product Name	Type(s) of Sensor(s)	Detection Range, km	Country of Origin	Web Page Link
Exponent	DroneHunter	EO, IR	N/D	U.A.E.	1
DJI	AeroScope (Stationary)	RF	Up to 50 (30)	China	2
	Aeroscope (Portable)	RF	Up to 5 (3)	China	2
Groupe ADP/DSNA Services	Hologarde	Radar, RF, EO	5 (3)	France	3
HGH Infrared Systems	Spynel M	IR/EO	1.5 (1)	France	4
Kelvin Hughes	SharpEye	Radar	N/D	U.K.	5
Squarehead	Discovair	Acoustic	0.5 (0.3)	Norway	6
Meritis	ADS-2000	Acoustic	N/D	Switzerland	7
	SC-1000T	EO, IR	N/D		
	SC-1500T	EO, IR	N/D		
	SR-9000S	Radar	N/D		
Microflown AVISA	SKYSENTRY	Acoustic	0.4 (0.25)	Netherlands	8
Miltronix	Drone Detection Radar	Radar	4 (2.5)	U.K.	9
Mydefence	EAGLE	Radar	1 (0.6)	Denmark	10
	WINGMAN 100	RF	1 (0.6)		
	WATCHDOG	RF	1 (0.6)		
	WOLFPACK	RF	1 (0.6)		
NEC		EO, IR, RF, Acoustic	1 (0.6)	Japan	11
Quantum Aviation	TUNGSTEN	Radar	Up to 12 (7.5)	U.K.	12
	V3 Radar	Radar	1.6 (1)		
	TITANIUM	RF	N/D		
	CHROMIUM	EO, IR	4 (2.5)		
Rinicom	Sky Patriot	EO	0.8 (0.5)	U.K.	13
Robin Radar Systems	Elvira	Radar	3 (2)	Netherlands	14
TeleRadio Engineering	SkyDroner 1000	EO, Other	0.5 (0.3)	Singapore	15
	SkyDroner 500	EO, Other	1 (0.6)		
TRD Consultancy	Orion-D	RF	4 (2.5)	Singapore	16

Table 6.3. CUAS detection, tracking and identification product evaluation

Product		Primary Performance Parameters			Secondary Performance Parameters					Non-Performance Parameters		
Manufacturer	**Model**	**Detection**	**Tracking**	**Identification**	**Payload ID**	**Landscape**	**Weather**	**Rogue Drone**	**Pilot Locate**	**Cost**	**Compliance**	**Env. Concerns**
Adsys Controls Inc.*	SATS2*	10	10	10	H	A	A	H	A	P	H	H
AeroDefence*	AirWarden*	7	7	7	A	H	H	P	H	A	H	H
C Speed LLC	LightWave Radar	10	7	3	P	A	H	H	P	P	H	P
Dedrone	RF-100	2	7	7	A	H	H	P	H	H	A	H
	RF-300	1.5	7	7	A	H	H	P	H	H	A	H
DeTect	DroneWatcherRF Mini	0.8	7	7	A	H	H	P	H	A	A	H
	DroneWatcherRF	3.2	7	7	A	H	H	P	H	A	A	H
	DroneWatcher DSR	3.2	7	3	P	A	H	H	P	P	H	A
DJI*	AeroScope (Stationary)*	10	7	7	A	H	H	P	H	A	A	H
	Aeroscope (Portable)	5	7	7	A	H	H	P	H	H	A	H
Drone Labs	DD610AR	1	7	7	A	H	H	P	H	H	A	H
	DM610R	1	7	7	A	H	H	P	H	H	A	H
DroneShield	DroneSentinel	5	7	7	H	A	H	H	H	P	A	P
Dynetics	GA 9000	5	7	3	P	H	H	H	P	A	H	P
SRC*	Gryphon Skylight*	10	10	10	H	H	H	H	H	P	A	P
	Mobile Skylight *	10	10	10	H	H	H	H	H	P	A	P
Liteye*	ADIS*	8	8	8	H	A	H	H	H	P	H	P
Sensofusion USA*	Airfence*	10	7	7	A	H	H	P	H	H	A	H
SpotterRF	A150	0.2	7	3	P	A	H	H	P	A	H	A
	A600	0.6	7	3	P	A	H	H	P	A	H	A
	A3000	0.7	7	3	P	A	H	H	P	A	H	A
	A2000	1	7	3	P	A	H	H	P	A	H	A
TCI	Blackbird	7	7	7	A	H	H	P	H	H	A	H
UMass/Raytheon	CASA Radar	1	7	3	P	A	H	H	P	P	H	P

Notes: These ratings were assigned by the research team. The primary performance parameters were rated on a scale 1 to 10 with 10 being the best. ("Detection" column displays product detection range in miles as reported by the manufacturer.) The secondary performance parameters and non-performance parameters are rated as poor (P), average (A) or high (H). CUAS products recommended for further evaluation in the prototype of the field tests are marked with an asterisk in the first two columns (Manufacturer, Model).

Appendix B: UAS Interception and Interdiction Systems

Currently, several methods have been considered to deter, immobilize, or destroy invasive drones in flight-restricted areas. Such methods include the following (*17*):

- RF or GPS signal jamming (can be either wide-area or targeted)
- GPS spoofing
- RF hacking
- Flight disruption by use of electromagnetic or laser impulse
- Flight disruption by use of kinetic means (either destructive or non-destructive)

The first method, RF or GPS signal jamming, utilizes two different approaches. The first approach uses a broad-spectrum, wide-area signal jamming. The second approach uses narrow-beam/narrow-RF spectrum antennae to disrupt a drone's operation and bring it down to the ground.

The second method, GPS spoofing, deceives a GPS receiver by broadcasting a signal with incorrect GPS coordinates and forces a UAS to change its initial path and landing point.

The third method, UAS RF or communication link hacking, hijacks an operator's control over their drone and, for example, sends a command for immediate landing as the UAS enters a restricted area.

The fourth method disrupts a UAS flight using electromagnetic or laser impulse by either damaging the electronic components on the UAS circuit board or the drone itself to bring down invasive UAS. Finally, the fifth method, flight disruption by physical means, implements physical objects to bring down invasive UAS, either without destruction (such as Drone SkyWall, a net and parachute combination) or destructive (such as guns or other weapons).

There are also non-technology-based methods—such as the use of predator birds—which, though considered exotic, have proven to work well on small- to medium-sized drones (*16*). Such solutions are beyond the scope of this research due to the lack of testing or reliability records in the United States.

6.4 provides a brief summary of the advantages and drawbacks of various drone deterrence and interception methods.

Table 6.4. UAS deterrence and interception methods: Pros and cons

	RF Signal Jamming	GPS Spoofing	RF Hacking	El-mag or Laser	Kinetic	
					Destructive	Non-Destructive
Advantages	Wide area of coverage; not labor-intensive	Wide area of coverage; not labor-intensive	Low interference and collateral damage	Effective against all UAS	Effective against all UAS	Effective against all UAS
Drawbacks	Potential interference; ineffective against fully auto UAS	Potential interference; ineffective against fully auto UAS	Ineffective against fully auto UAS	Collateral damage; legal limitations	Collateral damage; legal limitations	Short range; labor intensive

The research team identified 54 interception and interdiction system available either in the U.S. or internationally. Brief details of selected UAS interception and interdiction systems, embedded technology, and their major technical parameters are presented in Table 6.5 (U.S. manufacturers) and Table 6.6 (non-U.S. manufacturers).

Table 6.5. UAS interdiction systems: U.S. manufacturers

Manufacturer	Product Name	Interdiction Method(s)*	Interception Range, km (mi)	Web Page Link
Battelle	Drone Defender V2 C-UAS	RF/GNSS jamming	0.4 (0.25)	1
CACI	Small Form Factor	RF jamming	N/D	2
Dedrone	RF and GPS Jammer	RF/GNSS jamming	N/D	3
DroneShield	DroneGun MKII	RF/GNSS jamming	2 (1.3)	4
	DroneGun Tactical	RF/GNSS jamming	1 (0.6)	
IXI Technology	Drone Killer	RF/GNSS jamming	0.8 (0.5)	5
NASA Langley Research Center	Safeguard System	Net capture	0.4 (0.25)	6
Radio Hill Technologies	Dronebuster Block 3	RF/GNSS jamming	N/D	7
	Dronebuster FS	RF/GNSS jamming	N/D	
Repulse	Repulse 24	RF jamming	1 (0.6)	8
	Repulse 2458E	RF jamming	1 (0.6)	
	Repulse 2458H Handheld	RF jamming	1 (0.6)	
	Repulse 360	RF jamming	2 (1.3)	
SCI Technology	AeroGuard	Net capture	N/D	9
Sierra Nevada Corporation	SkyCAP	RF jamming	N/D	10
Theiss UAV Solutions	Excipio Aerial Netting System	Net capture	N/D	11

Table 6.6. UAS interdiction systems: Manufacturers outside U.S.

Manufacturer	Product Name	Interdiction Method(s)	Interception Range, km (mi)	Country of Origin	Web Page Link
CTS	Drone Jammer	RF/GNSS jamming	No data	China	1
Delft Dynamics	DroneCatcher	Net capture	No data	Netherlands	2
Digitech InfoTech	JAM-1000	RF/GNSS jamming	0.3 (0.2)	China	3
	JAM-2000	RF/GNSS jamming	1.2–2.1 (0.7–1.5)		
	JAM-3000	RF/GNSS jamming	No data		
Drone Defence	Dynopis E1000MP	RF/GNSS jamming	1 (0.6)	U.K.	4
	SkyFence	RF jamming	0.5 (0.3)		
Groupe Assman	MTX-8	Net capture	No data	France	5
Harp Arge	Drone Savar	RF jamming	No data	Turkey	6
HiGH + MiGHTY	SKYNET	RF/GNSS jamming	No data	Taiwan	7
Hikvision	Defender Series UAV-D04JA	RF/GNSS jamming	No data	China	8
H.P. M&C	HP 3962 H	RF/GNSS jamming	No data	Germany	9
	HP 47	RF/GNSS jamming	No data		
Jiun An Technology	Raysun MD1	RF/GNSS jamming	1.1 (0.7)	Taiwan	10
Kirintec	Recurve	RF/GNSS jamming	No data	U.K.	11
	Sky Net Longbow	RF/GNSS jamming	No data		
Meritis	P6	RF/GNSS jamming	No data	Switzerland	12
	RTX-2000M6	RF/GNSS jamming	No data		
	RTX-3000X	RF/GNSS jamming	No data		
	RTX-300P2	RF/GNSS jamming	No data		
	SkyCleaner	RF/GNSS jamming	No data		
Open Works Eng.	Skywall 100	Net capture	No data	U.K.	13
	Skywall 300	Net capture	No data		
Optix	Anti-Drone	RF/GNSS jamming	Up to 2 (1.3)	Bulgaria	14
Prime C & T	GROK Jammer	RF/GNSS jamming	2–4 (1.2–2.5)	U.K.	15
	GROK Mobile Gun	RF/GNSS jamming	1 (0.6)		
	Meritis Jammer	RF/GNSS jamming	No data		
	Phantom Jammer	RF/GNSS jamming	2 (1.3)		
Quantum Aviation	VANQUISH 1	RF jamming	No data	U.K.	16
	VANQUISH 3	Net capture	No data		
Search Systems	Sparrowhawk	Net capture	No data	U.K.	17
Skysec	Sentinel Catch	Net, parachute	5 (3)	Switzerland	18
	Sentinel Catch &-Carry	Net, hook	2 (1.3)		
SteelRock Technologies	NightFighter	RF/GNSS jamming	No data	U.K.	19
Terra Hexen	Omnidirectional Jammer	RF/GNSS jamming	No data	Poland	20
	Neutralizer	RF/GNSS jamming	No data		
TRD Consultancy	Orion	RF/GNSS jamming	1.5 (1)	Singapore	21

Appendix C: UAS Detection, Tracking and Interdiction Hybrid Systems

UAS Detection, Tracking, and Interception Systems

Today, more and more UAS detection and tracking equipment manufacturers are offering a UAS interception and control system as a part of their purchase package, as there is a clear demand for such all-in-one systems due to increasing awareness about the potential threats presented by non-cooperative UAS to important facilities and infrastructure. The research team identified 57 counter-UAS detection, tracking, identification, interception and interdiction hybrid system available either in the U.S. or internationally. Brief details on these CUAS hybrid systems are presented in Table 6.7 (U.S. manufacturers) and Table 6.8 (non-U.S. manufacturers).

Table 6.76. UAS detection, tracking, and interdiction hybrid systems: U.S. manufacturers

Manufacturer	Product Name	Detection Method(s)	Interdiction Method(s)	Web Page Link
Airspace Systems	Airspace	EO	Net capture	1
Black Sage/IEC Infrared	UAVX	Radar, EO, IR	RF jamming, GNSS jamming	2
Blind Tiger Communication	Wireless Intrusion Detection and Defeat System	RF	GNSS Spoofing	3
CACI	SkyTracker	RF	RF jamming, GNSS jamming and spoofing	4
CellAntenna	D3T	RF	RF jamming, GNSS jamming	5
CITADEL	DFU3000	RF	GNSS Spoofing	6
Department 13 International	MESMER	RF	GNSS Spoofing	7
Dedrone	DroneTracker Multi-Sensor	RF, EO, IR, Acoustic	RF jamming, GNSS jamming	8
DroneShield	DroneSentry	Radar, RF, Acoustic, EO, IR	RF jamming, GNSS jamming	9
Fortem	Drone Hunter	Radar	Net capture	10
Liteye/Blighter/ Chess Dynamics/ECS	AUDS	Radar, EO, IR	RF jamming	11
Lockheed Martin	ICARUS	RF, EO, Acoustic	RF jamming,	12
Orbital ATK	T-REX	Radar, EO, IR	RF jamming, kinetic	13
Rohde & Schwarz	ARDRONIS	RF	RF jamming, GNSS jamming	14
SESP	Drone Defeater	EO, IR, RF	RF jamming	15
SRC	Silent Archer	Radar, EO, IR	RF jamming, GNSS jamming	16
Van Cleve & Associates	DroneRANGER	Radar, IR, EO	RF jamming	17
Whitefox	Dronefox Fortify	RF	GNSS spoofing	18

Table 6.87. UAS detection, tracking, and interdiction hybrid systems: Manufacturers outside U.S.

Manufacturer	Product Name	Detection Method(s)	Interdiction Method(s)	Country of Origin	Web Page Link
Airbus Group SE	Counter UAV System	Radar, IR	RF/GNSS jamming	France	1
ArtSYS360	RS500	RF	RF/GNSS jamming	Israel	2
Aveillant	UWAS	Radar, EO, IR	RF jamming	U.K.	3
Broadfield Security Services	Drone Blocker	RF	RF jamming	Netherlands	4
BYLBOS/Roboost	SPID	EO, IR, RF, Acoustic	RF/GNSS jamming	France	5
CerbAir	CerbAir	RF, EO, IR	RF jamming, net capture	France	6
D-Fend Solutions		RF	RF jamming, spoofing	Israel	7
Dronefence		RF, Acoustic, EO, IR	GNSS Spoofing	Germany	8
Elbit	ReDrone	RF	RF/GNSS jamming	Israel	9
ELTA (Israel Aerospace Industries)	Drone Guard	Radar, EO	GNSS jamming	Israel	10
ELT-Roma	ADRIAN	RF, Radar, EO, IR, Acoustic	RF/GNSS jamming	Italy	11
Gradiant	Counter UAS	RF, EO	RF jamming	Spain	12
Hensoldt	Xpeller	Radar, EO, IR	RF/GNSS jamming	Germany	13
IACIT	DRONEBlocker 0200	EO, RF, Acoustic, Radar	RF jamming	Brazil	14
IMI Systems	Red Sky 2 Drone Defender System	Radar, EO, IR	RF jamming	Israel	15
KB Radar	Groza-Z	RF	RF/GNSS jamming	Belarus	16
L3 Technologies	Drone Guardian	Radar, EO, IR, RF	RF/GNSS jamming	U.K.	17
Mitsubishi Electric Corporation	Drone Deterrence System	RF	RF jamming	Japan	18
Netline Communications	C-Guard Dronenet	RF	RF jamming	Israel	19
Orad	DROM	RF	RF jamming	Israel	20
Orelia	Drone Detector	Acoustic	RF jamming	France	21
Phantom Technologies	Eagle108	RF, Radar, EO, IR	RF/GNSS jamming	Israel	22
Prime Consulting & Technologies	Anti-Drone	Radar, IR, EO, Acoustic	RF/GNSS jamming	Denmark	23
Rafael Defense Systems	Drone Dome	Radar, EO, IR	RF/GNSS jamming, laser	Israel	24
Rohde & Schwarz	ARDRONIS	RF	RF/GNSS jamming	Germany	25
R&S/Diehl Defence/ESG	Guardion	Radar, RF, EO, Acoustic	RF/GNSS jamming	Germany	26
Selex	Falcon Shield	Radar, IR, EO	RF jamming	U.K.	27
SteelRock Technologies	ODIN	RF, IR, Radar, EO	RF/GNSS jamming	U.K.	28
Terra Hexen	SAFESKY	Radar, EO, Acoustic	RF/GNSS jamming	Poland	29

Appendix D: Legal Barriers to CUAS Operations

There are several Federally-mandated legal barriers to CUAS operations. They include the following (*18*):

- 18 U.S. Code § 32: prohibits damaging or destroying an aircraft.
- 18 U.S. Code § 1362: prohibits willful or malicious interference with U.S. government communications.
- 18 U.S. Code § 1367(a): prohibits intentional or malicious interference with satellite communications.
- Title 47: requires radio transmitter operators to be licensed or authorized; prohibits willful interference with radio communications of any station licensed, authorized, or operated by the U.S. government; and prohibits using or generally dealing in (except by the U.S. government) any signal "jamming" devices.
- 49 U.S. Code § 46502: prohibits "seizing or exercising control of an aircraft...by force, violence, threat of force or violence, or any form of intimidation, and with wrongful intent."
- The Computer Fraud and Abuse Act: Creates a long list of crimes prohibiting conduct that affects a computer that is "used in or affecting interstate or foreign commerce," including threatening to damage a computer with the intent to extort anything of value; "knowingly causing the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causing damage without authorization"; unauthorized access with intent to defraud or in combination with destroying, damaging, or altering information; and trafficking in "any password or similar information."
- The Wiretap Act: prohibits the use of "any electronic, mechanical, or other device" to intentionally intercept, attempt, or have someone else intercept the contents of any electronic, wire, or oral communication; disclosing (or attempting to disclose) the contents of any such communication obtained by unlawful interception; and intentionally using or attempting to use the contents of any such communication.
- The Pen Register Act: prohibits the installation or use, without a court order, of pen registers, including any device that "records or decodes" signaling and other information transmitted by electronic communication, or a trap and trace device, including any device capable of identifying information that reveals the source of an electronic communication by capturing an incoming impulse.

There are also FAA regulations that raise the possibility of additional restrictions of CUAS operations. For example, 14 CFR § 107.12 and § 107.19(a) require anyone controlling a drone to have a remote pilot certificate with a sUAS rating or to be under the direct supervision of a remote pilot in command who has the ability to immediately take direct control of the sUAS. This suggests that a CUAS operator might also have to be a licensed UAS pilot.