



INSTITUTE FOR DEFENSE ANALYSES

**Technology Trends in Small Unmanned
Aircraft Systems (sUAS) and Counter-UAS:
A Five-Year Outlook**

G. James Herrera
Jason A. Dechant
E.K. Green

November 2017
Approved for public release;
distribution is unlimited.
IDA Paper P-8823
Log: H 17-000624



The Institute for Defense Analyses is a non-profit corporation that operates three federally funded research and development centers to provide objective analyses of national security issues, particularly those requiring scientific and technical expertise, and conduct related research on other national challenges.

About This Publication

This work was conducted by the Institute for Defense Analyses (IDA) under contract HQ0034-14-D-0001, project ER-6-4036, "Evaluating Assessment Methodologies," for the Office of Infrastructure Protection, National Protection and Programs Directorate, U.S. Department of Homeland Security (DHS). The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Acknowledgments

The authors wish to thank Mr. Matthew Barger of the Sector Outreach and Programs Division of DHS for his guidance and direction, reviewers Dr. Robert Zirkle and Ms. Jacqueline Du Bois for their careful review of this paper, Ms. Dana Coppola for editing, and Ms. Amberlee Mabe-Stanberry, who produced this paper. The author would also like to thank the subject matter experts interviewed and comprising review panels whose experience provided the basis for the data and findings in this paper.

For More Information:

Dr. Jason A. Dechant, Project Leader
jdechant@ida.org, 703-845-2495

ADM John C. Harvey, Jr., USN (Ret), Director, SFRD
jharvey@ida.org, 703-575-4530

Copyright Notice

© 2017 Institute for Defense Analyses
4850 Mark Center Drive, Alexandria, Virginia 22311-1882 • (703) 845-2000

This material may be reproduced by or for the U.S. Government pursuant to the copyright license under the clause at DFARS 252.227-7013 (a)(16) [June 2013].

INSTITUTE FOR DEFENSE ANALYSES

IDA Paper P-8823

**Technology Trends in Small Unmanned
Aircraft Systems (sUAS) and Counter-UAS:
A Five-Year Outlook**

G. James Herrera
Jason A. Dechant
E.K. Green

This page is intentionally blank.

Executive Summary

The U.S. Department of Homeland Security (DHS) is responsible for protecting and enhancing the resilience of much of the nation’s critical infrastructure. Presidential Policy Directive 21 (PPD-21) and the supporting National Infrastructure Protection Plan divide critical infrastructure into 16 sectors. DHS is the designated sector-specific agency for 10 of them. PPD-21 also instructs DHS to “coordinate the overall federal effort to promote the security and resilience of the Nation’s critical infrastructure.” In these roles, DHS concerns itself with threats to infrastructure posed across all domains—air, land, sea, and cyber.

Although threats and technologies are rapidly evolving across all domains, the air domain has become increasingly complex in recent years with the proliferation of unmanned aircraft systems (UAS). In particular, consumer demand and benefits from commercial and private interests for small UAS (sUAS), specifically those weighing less than 55 pounds (lbs.) and operate at no more than 400 feet above ground, have caused rapid expansion of both sUAS and counter-UAS markets. With new producers vying for market shares, competition is fostering rapidly decreasing prices and innovative technological features intended to garner a comparative advantage.

Objectives

The objectives of this assessment are to (1) identify current and anticipated advancements in specific sUAS and counter-UAS technologies, and (2) characterize general development trends in the sUAS and counter-UAS industry over the next five years. The assessment and resultant findings and recommendations were based upon a varied set of data comprised of subject matter expert interviews and review panels, secondary sources (e.g., open reporting and extant analyses), and engagement with the UAS community at industry meetings and government wargames. The research benefited from more than two dozen UAS expert interviews across the public and private sectors.

Findings

The following summarize the key findings from the technology trends assessment that are further detailed throughout the paper:

Key Findings from the Survey of sUAS Technology Trends

Over the next five years, trends in sUAS technology will be observed in four general categories:

1. Platform Modification

- **Size** will *continue to decrease* while maintaining and/or increasing capabilities; however, use will be largely for hobbyists.
- Gross **weight** for sUAS platforms will *continue to decrease*; however, with advancements in power supplies and new recharging options, weight will be less of a hindrance to continual use.
- As sUAS decrease in size, they also will *maintain or increase* **payload** capabilities, eventually being able to carry much more than their own weight.

2. Platform Operation

- sUAS will increase **speed** capabilities for rotocopters surpassing 200 mph.
- sUAS will continue to increase their **range and endurance** steadily.
- Most commercial electronic and mechanical **capabilities** available for other mobile platforms will become available for sUAS within the next five years (robotics, sensors, audio/video, etc.).

3. **Autonomy.** Autonomous systems already exist, but the degree of autonomy, and the level of sophistication of communication between units, will continue to expand, allowing sUAS to perform any functionally programmable operation.

4. **Swarming.** Swarming technology will increase rapidly worldwide and in five years, without government interference, easily programmable and purchasable swarming technology will be widely available to the average consumer.

Key Findings from the Survey of Counter-UAS Technology Trends

Over the next five years, trends in counter-UAS technologies will be observed across the three steps of the *Counter-UAS Process*: (1) Detection, Identification, and Tracking, (2) Threat Decision, and (3) Threat Response. These are highlighted below:

1. Detection, Identification, and Tracking

- **Sensors, identification, and tracking systems** for countering UAS will see *steady growth over the next five years*; however, persistent sUAS development trends will create *new capability gaps*.
- A major existing gap is tracking multiple sUAS targets simultaneously; this gap will be filled in five years.

- Technologies developed in isolation and the integration of systems remain a challenge; a human in the loop will still be required to fuse systems for detection, identification, and tracking.
2. Threat Decision
- **Threat decision-making** is not just a technology solution, it requires rules of engagement policies and protocols to be established; this will *continue to be a slow process* that is pieced together over the next five years.
 - Threat decision-making will remain the least developed step in the Counter-UAS Process.
 - The response process must be minimized to less than one minute, and the United States likely won't be able to accomplish this in the next five years.
 - Threat decision making will still require a human in the loop because policies and protocols for automated systems are not being established.
 - Some limited automated response systems may exist for select parties and limited applications.
3. Threat Response
- **Threat response** technologies developed by government and industry to counter domestic UAS threats will *continue to see rapid growth*; however, most solutions will *still be illegal or limited in the United States*.
 - This will continue over the next five years unless significant regulatory changes are made.
 - Most government and industry investments are in active, not passive, counter-UAS technologies.
 - The United States is expected to see a steady increase in the number of vendors producing active systems over the next five years as the threat grows.
 - There is anticipation of the United States relaxing limits on active systems.
 - Currently, commercial vendors largely ignore collateral damage produced by counter-UAS; however, systems that minimize collateral damage will be a focus area in the next five years.
 - Domestic markets will see a growth in systems that minimize collateral damage.

This paper further details the above findings and characterizes anticipated trends in sUAS and counter-UAS technologies with examples and references.

This page is intentionally blank.

Contents

1.	Introduction	1
	A. Objectives	1
	B. Scoping Considerations	1
	C. Organization of Paper	2
2.	Approach	3
	A. Technology Assessment Approach	3
	B. Data Sources	5
	1. Primary Sources	5
	2. Secondary Sources	6
	3. Community Engagement	6
3.	Technology Trends	7
	A. Trends in sUAS Development	7
	1. Platform Modification	7
	2. Platform Operation	11
	3. Autonomy	19
	4. Swarming	21
	B. Trends in Counter-UAS	23
	1. Trends Overview	23
	2. Technology Trends Applied to the Counter-UAS Process	24
4.	Conclusion	31
	A. Key Findings from the Survey of sUAS Technology Trends	31
	1. Platform Modification	31
	2. Platform Operation	31
	3. Autonomy	31
	4. Swarming	32
	B. Key Findings from the Survey of Counter-UAS Technology Trends	32
	1. Detection, Identification, and Tracking	32
	2. Threat Decision	32
	3. Threat Response	32
	C. General Findings in Counter-UAS Development	33
	Appendix A. Illustrations	A-1
	Appendix B. References	B-1
	Appendix C. Abbreviations	C-1

This page is intentionally blank.

1. Introduction

Although threats and technologies are rapidly evolving across all domains, the air domain has become increasingly complex in recent years with the proliferation of unmanned aircraft systems (UAS). In particular, consumer demand and benefits from commercial and private interests for small UAS (sUAS), specifically those weighing less than 55 pounds (lbs.), has caused rapid expansion of both UAS and counter-UAS markets. With new producers vying for market shares, competition is fostering rapidly decreasing prices and innovative technological features intended to garner a comparative advantage.

To assist the Department of Homeland Security (DHS) with understanding the current and near-term state of sUAS and counter-UAS technologies, along with the probable impacts these technologies have on critical infrastructure vulnerability, the DHS Office of Infrastructure Protection (IP) through its Sector Outreach and Programs Division (SOPD) asked the Institute for Defense Analyses (IDA) to assess sUAS and counter-UAS technology trends over the next five years.

This paper describes the approach, sources, and findings of the IDA assessment. This chapter provides an overview of the assessment's objectives, scoping considerations, and provides an organization of the remainder of the paper.

A. Objectives

The objectives of this assessment are to (1) identify current and anticipated advancements in sUAS and counter-UAS technologies, and (2) to characterize general development trends in the sUAS and counter-UAS industry over the next five years. The assessment and resultant findings and recommendations were based on a varied set of data comprised of subject matter expert interviews and review panels, secondary sources (e.g., open reporting and extant analyses), and engagement with the UAS community at industry meetings and government wargames. The research benefited from more than two dozen UAS expert interviews across the public and private sectors.

B. Scoping Considerations

Assessing technology trends for sUAS and counter-UAS is a broad subject; therefore, several scoping determinations were necessary to narrow the topic and make it more tractable.¹ These include the following boundaries:

¹ The scope was developed in coordination with the DHS/SOPD sponsor.

- sUAS are defined as UAS that operate at no more than 400 feet (ft.) above ground level, and weigh no more than 55 lbs. The weight limitations are consistent with the Department of Defense (DOD) Groups 1 and 2 classifications.²
- Developmental technology projections extend out five years from 2017.
- Specific technologies that either advance or are used to counter cyber or electronic warfare attacks were deemed outside the scope of the survey.
- Classified systems were not assessed in this paper.

C. Organization of Paper

This paper is organized into three chapters following the introduction. Chapter 2, “Approach,” provides an overview of the technology trends assessment approach, including the analytic framework and data sources. Chapter 3, “Technology Trends,” provides the complete trend results for sUAS and counter-UAS capabilities assessed, along with their impacts to critical infrastructure vulnerability. Chapter 4, “Conclusion,” summarizes the key findings from the two technology trends surveys, along with general findings for the commercial counter-UAS market over the next five years.

² Department of Defense, “Unmanned Aircraft System Airspace Integration Plan,” March 2011, D-3, accessed July 2017, http://www.acq.osd.mil/sts/docs/DOD_UAS_Airspace_Integ_Plan_v2_%28signed%29.pdf.

2. Approach

This chapter outlines the technology trends assessment approach applied to survey both sUAS and counter-UAS technologies, as well as the data sources utilized to populate the analytic framework and identify overall development trends in the industry. For each technology trend pertaining to the development of sUAS, the probable impact on critical infrastructure vulnerability is also provided. Subsequent chapters provide categorical data and findings that follow the framework.

A. Technology Assessment Approach

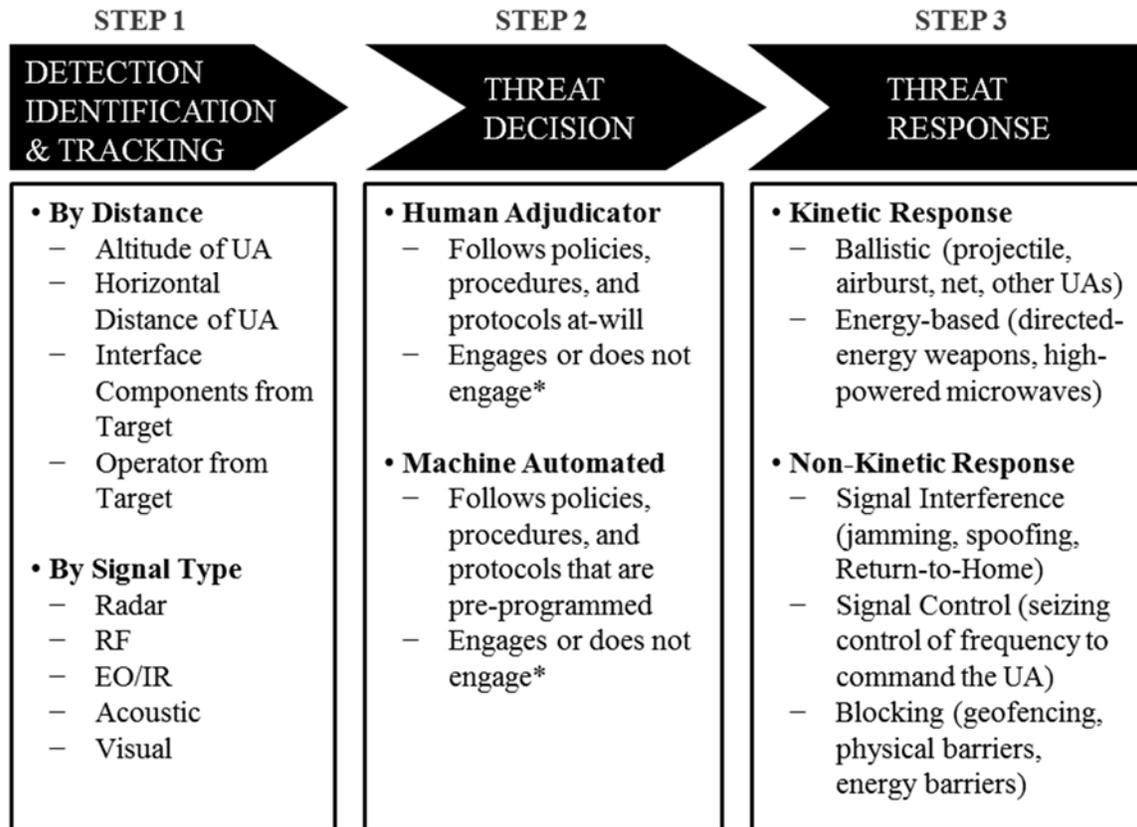
The approach included surveying all publicly available information on the internet, conducting interviews with government subject matter experts, attending conferences and forums to collect commercial product information, and referencing (but not citing) Sensitive But Unclassified documentation to inform open-source analysis. The subsequent section expands upon these data sources. After all available information was collected, the technologies were separated into two basic categories: (1) technologies that advanced the development of sUAS as a platform; and (2) technologies that were intended to counter UAS, and more precisely sUAS. The range of technologies assessed included unclassified, commercially produced domestic and foreign sUAS and counter-UAS products that were either currently available for purchase or were in testing and evaluation (T&E). For those products in T&E, at least one prototype had to appear to function as intended.

Technologies that advance the development of sUAS were first organized into two subcategories: (1) Platform Modification technologies and (2) Platform Operation technologies. Platform Modification technologies include fundamental changes to the base sUAS platform, which could increase sUAS capabilities or add new capabilities. Platform Operation technologies are those that are considered augmenting technologies to existing sUAS platforms, which could also result in increased or new operational capabilities. These groupings had some areas of overlap, but ultimately were used to determine what key technological capabilities were most developed by commercial producers. Through expert interviews, two additional subcategories, autonomy and swarming, were identified as significant and unique to sUAS development and were subsequently studied separately and included in the assessment. A technology trend categorization scheme for sUAS development was created based on these key capability subcategories (provided below).

Categorization of sUAS Development Trends

- **Platform Modification**
 - Technology Trend: Size
 - Technology Trend: Weight
 - Technology Trend: Design
- **Platform Operation**
 - Technology Trend: Speed
 - Technology Trend: Range/Endurance
 - Technology Trend: Functions
- **Autonomy**
 - Technology Trend: Semi-Autonomous Systems
 - Technology Trend: Fully-Autonomous Systems
- **Swarming**
 - Technology Trend: Cooperative Swarming
 - Technology Trend: Coordinated Swarming

Counter-UAS technologies were grouped based on an internally adapted version of a commonly referenced schema for conducting counter-UAS that has been circulated throughout the UAS community. The elements of this process at the top level (i.e., basic steps) typically include detection, identification, and response, though sometimes tracking and decision making are also included. Although this process is widely discussed throughout the UAS community, it has not been officially formalized and referenced in a standard representation. Therefore, the research team constructed its own Counter-UAS Process diagram to organize counter-UAS trend results (Figure 1). Through the expert interviews, additional inputs on general trends in counter-UAS developments were also collected and are presented first as a primer to more specific Counter-UAS technology trends.



*Not engaging could mean that an adequate passive defense system is in place for the threat type (e.g., facility net) or no threat is determined.

Figure 1. The Counter-UAS Process³

B. Data Sources

In addition to the expertise provided by the research team, the analysis relied on data provided by the following sources:

1. Primary Sources

a. Expert interviews

A primary source of data for this assessment came in the form of dozens of individual interviews with subject matter experts across the UAS community on topics such as innovation in sUAS and sUAS related technologies; technological developments in counter-UAS with particular attention to counter-sUAS products; and the impact of evolving sUAS technologies on critical infrastructure. Interviewees came from both

³ The term UA refers to the “unmanned aircraft” portion of a UAS. This may also be referred to as an Unmanned Aircraft Vehicle, or UAV; however, not all UAs transport people or goods, thus the term “vehicle” has been omitted.

government and non-government sources across the public, private, and non-profit sectors. These were structured interviews conducted on a not-for-attribution basis and coordinated with the sponsor.⁴

b. Review panels

An additional primary source of data came from expert review panels convened by the research team to review and provide input into the research on current and forthcoming sUAS technological capabilities. These panels consisted of senior researchers from across IDA. Panelists had decades of collective experience in unmanned systems and related technologies, as well as commensurate experience with DHS planning and programming.

2. Secondary Sources

Secondary sources, including open reporting and previous studies and analyses, comprised a large portion of the information. These were generally related to existing UAS capability and counter capability articles and reports; government reports, documents, and legislation addressing UAS and counter-UAS use and protection authorities; and available UAS threat, vulnerability, and risk assessments. Examples of secondary sources are documented throughout this paper.

3. Community Engagement

As part of the data collection effort, and to get a better sense of stakeholders' opinions regarding the growth of sUAS and counter-UAS capabilities, the research team also engaged in outreach and participation throughout the UAS community. These engagements included several interagency conferences, exercises, and workshops, as well as public events for innovative UAS and counter-UAS technologies across the country.⁵

⁴ Further information regarding interviewed subject matter experts should be requested from the Sector Outreach and Programs Division (SOPD) of the Department of Homeland Security Office of Infrastructure Protection (DHS/IP).

⁵ Further information regarding specific events attended should be requested from the SOPD of the DHS/IP.

3. Technology Trends

This technology trends assessment was not intended to be an in-depth evaluation of specific commercial sUAS technologies, nor to verify or validate any commercial product claims. It only estimates the future state of a relevant technology category out to five years, and provides a brief analysis on the trend's impact on critical infrastructure vulnerability.

A. Trends in sUAS Development

The following section summarizes the results of the technology trends survey for the advancement of sUAS out to five years. It includes the general development trend of a sUAS capability area and the impact of that trend on critical infrastructure vulnerability, and provides an example of a relevant technology product(s).

1. Platform Modification

These technology trends encompass the three key capability areas that commercial vendors are attempting to improve when altering designs for sUAS platforms. The investment by commercial industry is primarily driven by the global hobbyist market, with the majority of the market share held in China by companies such as DJI.⁶

a. Size

In general, sUAS will continue to decrease in size while maintaining or increasing most operational capabilities. sUAS below .55 lbs. (249 grams), often referred to as “nano” or “micro” UAS, are currently available, and flight capabilities for these sUAS are expected to advance. Their commercial purpose is primarily recreational use or audio and video recording.

Impact on Vulnerability – Nano UAS increase the threat to critical infrastructure from the surveillance attack vector by allowing access to locations larger sUAS previously could not enter (e.g., ventilation grates to enter closed facilities). In addition to improved access, the smaller-sized UAS could provide for undetected surveillance for longer periods, as they may be more difficult to detect and respond to with existing counter-UAS technologies. Beyond surveillance advantages, other attack vectors are not significantly impacted by decreases in sUAS size; thus, critical infrastructure vulnerability to those attack vectors does not increase. Further, smaller types of sUAS are highly sensitive to weather conditions, such as strong winds, which can affect precision maneuverability.

⁶ “DJI is Running Away with the Drone Market,” Recode-Vox Media, Inc., accessed July 21, 2017, <https://www.recode.net/2017/4/14/14690576/drone-market-share-growth-charts-dji-forecast>.

Technology Example – The “SKEYE Nano 2 Camera” (Figure 2) weighs approximately 17 grams, fits in the palm of your hand, and can record in high definition (HD) 720p resolution or better, with continuous flight times of five minutes or more. The average cost of these types of sUAS range from \$15-\$100, depending on the features added (e.g., HD camera type, first person view option, etc.). They are readily available from online vendors, such as Amazon.com.



Figure 2. SKEYE Nano 2 Camera sUAS⁷

b. Weight

sUAS will continue to decrease in weight while maintaining or increasing most operational capabilities, including achieving steady gains in carrying capacity (i.e., payload) as excess lift is produced. Typical payloads for commercially available sUAS (e.g., DJI MG-1) range from 20-25 lbs., which is often equal to or just slightly more than what the sUAS weighs.⁸ As lighter and stronger materials are used, the sUAS could take on much heavier payloads while maintaining existing operational standards, especially where complementary design features help to balance out the distribution of weight. Additionally, commercial producers have recognized that the heaviest component on sUAS is typically the fuel source (i.e., the battery). New fuel types, such as hydrogen fuel cells and solar panels, are being tested by commercial producers to further reduce gross weight and increase continuous flight times.

Impact on Vulnerability – Employing a lighter sUAS does not directly increase the vulnerability of critical infrastructure to existing attack vectors; however, indirectly, lighter sUAS do allow for significant increases in payload capacity and longer flight times, assuming no changes are made to the current propulsion systems. This could increase the likelihood of success of surveillance or an impact attack, and potentially, if a payload

⁷ “SKEYE Nano 2 Camera,” TRNDlabs, accessed July 21, 2017, <https://www.trndlabs.com/product/skeye-nano-2-camera/>.

⁸ “MG-1 SPECS,” DJI, accessed July 21, 2017, <http://www.dji.com/mg-1/info#specs>.

capacity was large enough for a given asset, could increase the degree of critical infrastructure vulnerability.

Technology Example – An example of a reduced-weight (but not size) sUAS is the Intelligent Energy Limited modified hydrogen-powered sUAS (Figure 3). This sUAS uses hydrogen fuel cell technology to supply electrical power, which provides a higher energy-to-mass ratio than traditional battery-based systems and can be refueled in a few minutes. The sUAS can also stay in flight for up to two hours before needing to land for refueling.⁹



Figure 3. Intelligent Energy’s Ultra Lightweight Fuel Cell System¹⁰

c. Design

Trends for design include a steady growth in new platform structures to enhance sUAS operations. Generally, the development of multi-modal platforms that can operate in mixed environments (air, land, water surface, underwater) are taking hold among consumers and producers. Within the next five years, there will be a steady increase in sUAS that combine aerial modes with underwater and ground vehicle modes, potentially challenging the definition of sUAS as an aircraft. Innovations in engine technologies and designs for sUAS, such as distributed electric propulsion systems, contribute to multi-modal designs. Another trend is toward environmentally friendly sUAS. This can include anything from technological advances in biodegradable frames and electronic components, to noise reduction technologies that are meant to quiet sUAS to protect wildlife. Signature reduction or stealth designs are also being pioneered for sUAS, largely for military purposes.

⁹ “Hydrogen-Powered Drone takes Flight,” BBC News, accessed July 21, 2017, <http://www.bbc.com/news/av/technology-35890486/hydrogen-powered-drone-takes-flight>.

¹⁰ “Drones Products,” Intelligent Energy, accessed July 21, 2017, <http://www.intelligent-energy.com/our-products/drones/products/>.

Impact on Vulnerability – Multi-modal platform designs do not increase critical infrastructure vulnerability to existing sUAS attack vectors, but instead add new threats to the vulnerability picture through new attack vectors. For example, a critical infrastructure facility such as a dam may now face new vulnerabilities from sUAS employing underwater attacks in combination with aerial ones, whereas before they had to consider only aerial threats.

Design trends that are intended to protect the environment appear to have different impacts on critical infrastructure vulnerability. For instance, decomposable or disposable sUAS do not have an impact on critical infrastructure vulnerability, even though they may make it challenging for law enforcement to identify the cause of disruption after an attack. Conversely, sUAS that are designed to be quiet could thwart counter-UAS systems designed to detect their acoustic signatures. Each new technology would have to be assessed individually.

Technology Example – Oakland University’s “Loon Copter” (Figure 4) is capable of traditional aerial flight, on-water surface operation, and aquatic diving and navigation. It is a prototype vehicle that has not been made commercially available. However, several other universities, laboratories, and companies around the world are developing similar multi-modal sUAS for a variety of purposes, including military operations.



Figure 4. Oakland University’s Loon Copter Multi-Modal sUAS¹¹

¹¹ “Loon Copter: Amphibious Drone Floats, Flies & Dives,” Gajitz, accessed July 20, 2017, <http://gajitz.com/loon-copter-amphibious-drone-floats-flies-dives/>.

2. Platform Operation

These technology trends encompass the three key operational performance areas that commercial vendors are attempting to improve for sUAS platforms. A strong demand for the widespread application of sUAS in multiple commercial industry sectors, such as agriculture and telecommunications, and the presumed high return on investment (or reduction in labor costs), is largely driving industry innovation. Recreational users are also playing a role in advancing certain technology areas, such as the speed of sUAS, to increase performance capabilities for activities such as racing competitions.

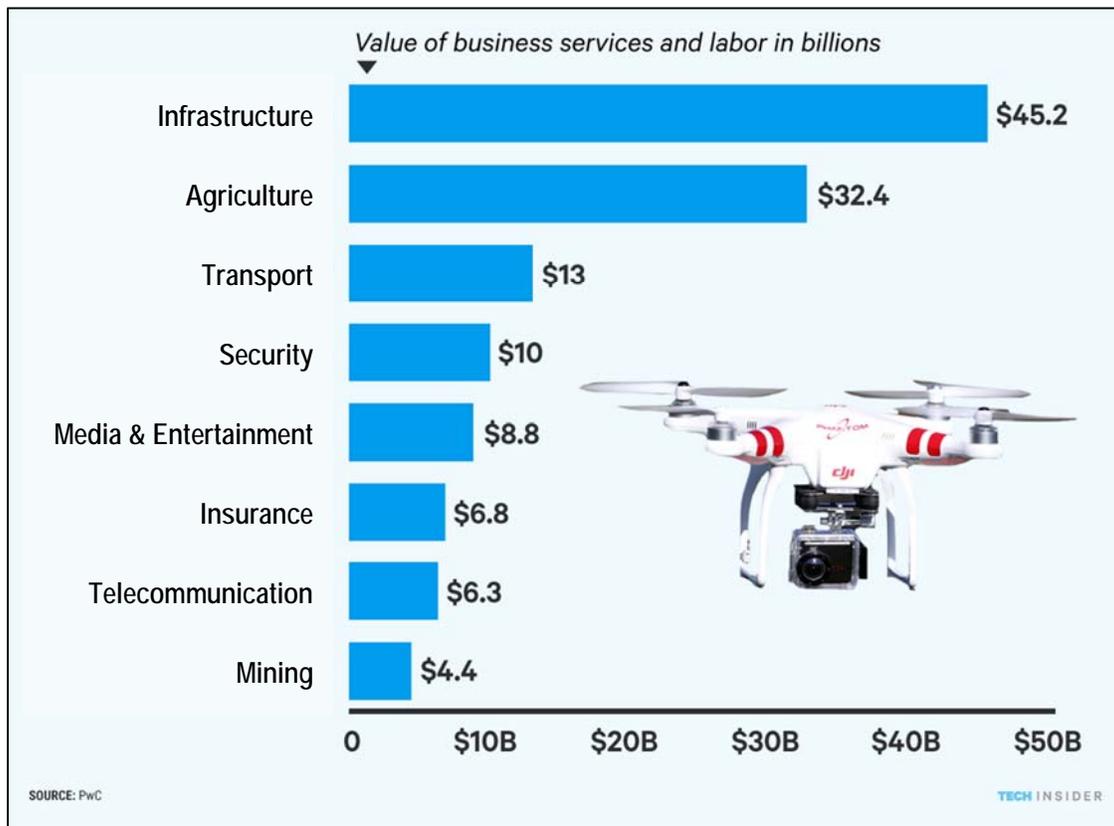


Figure 5. Predicted Value of UAS by Industry¹²

a. Speed

The speed at which sUAS can traverse a particular distance or height will continue to increase. Most improvements are being made with rotary sUAS, where the sUAS racing market is driving the demand. “Drone racing” competitions, where both speed and maneuverability are being judged, are growing in popularity across the world. Enhancing one implies a trade-off in the other, as is currently observed in the industry between fixed-

¹² “Drones Could Replace \$127 Billion Worth of Human Labor,” Tech Insider, accessed July 20, 2017, <http://www.businessinsider.com/drones-could-replace-127-billion-of-human-labor-2016-5>.

wing and rotary designs. Fixed-wing sUAS can fly at speeds more than twice that of rotary, but cannot navigate the obstacles one might find in complex racing courses. The average racing rotary quadcopter speeds range from 80-150 miles per hour (mph), with the fastest currently at 179.6 mph (“Racer X” in June 2017).¹³ Some modified fixed-wing sUAS can fly at speeds of more than 400 mph. While slower than fixed-wing sUAS, quadcopters can perform with precision maneuverability and avoid challenging obstacles. Additionally, with the advent of first-person view (FPV) piloting, rotary sUAS can operate at high speeds in both outdoor and indoor racing environments. All of these factors have led consumers to advance the baseline product platforms themselves through three-dimensional printing (i.e., additive manufacturing) and parts modifications to achieve the fastest rotary speeds possible. Commercial producers have picked up on these cues and are offering faster off-the-shelf models to racers. Within five years, rotary sUAS will surpass the 200 mph mark, and fixed-wing sUAS will see some enhancement in speed through the advancement of miniature (or hobbyist) turbine engines.

Impact on Vulnerability – Faster sUAS can increase weaponization threats by increasing the momentum of direct kinetic impacts and impacts with mounted or fixed weapons. Thus, critical infrastructure vulnerability will increase as a function of the advances in speed, which are tied directly to the type of sUAS used against a critical infrastructure asset. Additionally, increased speed and maneuverability can make sUAS less vulnerable to counter-UAS.

Technology Example – In Germany in 2013, a fixed-wing sUAS was documented as reaching speeds of up to ~440 mph using a Behotec JB-180 turbine engine (Figure 6).¹⁴ Since then, several other sUAS hobbyists have tested similar aircraft reaching comparable speeds. In response to popular interests, domestic markets for miniature turbine engines have expanded noticeably.

¹³ “Drone Racing League Sets World Record for Fastest Quadcopter,” ZDNet, accessed July 21, 2017, <http://www.zdnet.com/article/drone-racing-league-sets-world-record-for-fastest-quadcopter/>.

¹⁴ “Fastest Remote-Controlled Jet-Powered Model Aircraft (RC),” Guinness World Records, accessed July 21, 2017, [http://www.guinnessworldrecords.com/world-records/fastest-remote-controlled-jet-powered-model-aircraft-\(rc\)?fb_comment_id=701907789916475_1110755145698402](http://www.guinnessworldrecords.com/world-records/fastest-remote-controlled-jet-powered-model-aircraft-(rc)?fb_comment_id=701907789916475_1110755145698402). Live test viewable at: <https://www.youtube.com/watch?v=sa-TSNeTK-A&spfreload=10>.



Figure 6. sUAS powered by a Behotec JB-180 turbine engine

Technology Example – Racing quadcopters are continuously being compared to determine current leaders in the speed category. Many are built by consumers or small businesses, who then offer similar builds for sale online to other racing enthusiasts. Figure 7 provides a snapshot of the current rotary FPV sUAS leaders and their key specifications.

	DESIGN	SPEED (MPH)	VERIFIED	THRUST WEIGHT	THRUST (G)	WEIGHT (G)	MOTORS	BATTERY	ASSEMBLY	RTF PRICE
	VXR-190	166	GPS	15	7400	479	2450kv	5S	MATERIALS PARTS	\$738
	RACER X	164	TIMER	>9	>7550	800	2500kv	10S	3D-PRINT PARTS	>\$1000
	VX1	152	GPS	15	7400	485	2450kv	5S	MATERIALS PARTS	\$720
	SPEEDY GONZALAS	145	GPS	12	6800	570	2750kv	6S	PARTS	\$544
	STIGG 195	128	RADAR	10	5400	560	2500kv	4S	PARTS	\$738
	MORPHEUSX 195	125	RADAR	13	7100	557	2400kv	4S	PARTS	\$568
	GT2 200 2017	99	RADAR	12	6644	554	2450kv	4S	PNP	\$396
	DARKMAX 220	99	RADAR	11	5180	487	2550kv	5S	PNP	\$322
	GT2 200	89	RADAR	10	5200	504	2300kv	4S	PNP	\$459
	X215 PRO	81	RADAR	9	4600	510	2600kv	4S	PNP	\$283
	LIZARD 95	76	RADAR	6	648	111	6000kv	3S	BNF	\$235
	ARC 200	75	EST.	9	4000	458	2600kv	4S	PARTS	\$434
	LISAM 210	75	EST.	9	3800	416	2300kv	4S	PARTS	\$233
	WIZARD X220	68	RADAR	6	3100	535	2300kv	3S	RTF	\$245

Note: Assembly Codes: Plug-&-Play (PNP), Bind-&-Fly (BNF), Ready-To-Fly (RTF)

Figure 7. Fastest First-Person View (FPV) sUAS – August 2017¹⁵

¹⁵ “Fastest FPV Racing Drones 2017” FPV Drone Reviews, accessed November 2, 2017, <http://fpvdronereviews.com/guides/fastest-racing-drones/>.

b. Range/endurance

sUAS will continue to increase in operational range while maintaining and/or increasing endurance capabilities. New platform designs, such as multi-modal sUAS, are contributors to improved range capabilities. Advancements in power supplies, such as solar-powered sUAS, will also allow operation for longer periods. Another approach to increasing endurance is to add autonomous battery replacement/charging stations in key operating locations for sUAS, which could provide nearly continuous flight operations. Several companies are pursuing these technologies, asserting that infrastructure is the missing component, not advanced battery options.¹⁶ Overall, the commercial industry is heavily invested in improving how far and for how long sUAS can operate.

Impact on Vulnerability – Longer flight times increase the threat from surveillance to critical infrastructure by allowing sUAS to loiter longer. It may also increase the chances of a successful attack by allowing them to loiter until the best opportunity arises (e.g., until a door opens). Increased ranges could also allow sUAS to target critical infrastructure that would otherwise be out of range, for example, offshore oil drilling rigs.

Technology Example – Solar electric propulsion systems are not only being applied to large UAS; sUAS, such as the Silent Falcon (Figure 8), are also adapting the technology. With a carbon fiber body, the Silent Falcon can stay in the air for up to five hours, depending on weather conditions. The Silent Falcon is also extremely quiet. The manufacturer claims that it is audibly undetectable 100 meters off the ground.¹⁷ The manufacturer also states that the product is designed for commercial, public safety, security, and military applications.



Figure 8. Solar-powered Silent Falcon sUAS¹⁸

¹⁶ “DroneHome,” Asylon, accessed July 20, 2017, <http://www.flyasylon.com/product/>.

¹⁷ “Silent Falcon,” Silent Falcon, accessed July 23, 2017, <http://www.silentfalconuas.com/silent-falcon>.

¹⁸ “Solar-Powered Silent Falcon UAV Unveiled,” New Atlas, accessed July 19, 2017, <http://newatlas.com/silent-falcon-uav/23641/>.

Technology Example – Tethered sUAS can operate without charging and have uninterrupted video streams. However, their range is limited/fixed to their base unit. AT&T’s Flying Cell on Wings (Flying COW) (Figure 9) platform for disaster emergency response is an example of a tethered sUAS for the Emergency Services Sector. It is designed to provide Long Term Evolution (LTE) network coverage from the sky to customers on the ground during disasters or major events.¹⁹



Figure 9. AT&T Flying Cell on Wings (Flying COW)²⁰

c. Functions

New commercial functions for sUAS will continue to emerge. Existing functions will also continue to improve incrementally as mountable hardware systems become more stable, durable, and reliable and associated management software is improved. Functions making the greatest gains include simple and complex mechanical systems, high-fidelity and streaming audio/video systems, and onboard sensors and data processing units. Market demand is growing for these types of products, which are designed to be fixed to any type of commercial sUAS and can operate at range.

Impact on Vulnerability – The impact of new capabilities and functions for sUAS vary and should be assessed on an individual basis. For the following types of technologies, the impact on critical infrastructure vulnerability from an increased or new sUAS capability has been assessed.

¹⁹ “When COWs Fly: AT&T Sending LTE Signals from Drones,” AT&T, accessed July 21, 2017, http://about.att.com/innovationblog/cows_fly.

²⁰ “AT&T Tests COW Flying Over Georgia,” GAFollowers, accessed July 21, 2017, <http://www.gafollowers.com/att-tests-cow-flying-georgia/>.

- *Mechanical Systems*: New mechanical systems have varied effects on critical infrastructure vulnerability, in some cases enhancing existing threats and in others creating new attack vectors. For example, a precision mechanical arm attached to a sUAS creates a new, non-kinetic direct attack vector. This type of sUAS capability can disrupt or damage critical infrastructure by means not previously available (e.g., cutting cables). Even simple mechanical systems, such as external servo release systems are being adapted to sUAS, and can be purchased online for less than \$50.²¹ These systems have their own internal power sources, are easy to operate, and can mount to commercially available sUAS (e.g., DJI Phantom 4). sUAS equipped with advanced or simple mechanical systems can be used to release harmful payloads from high altitudes above targets.
- *High Fidelity, Streaming, and Augmented Reality Audio/Video*: Due to consumer demand for greater fidelity in sUAS audio and video, companies are now offering sUAS that can stream live video anywhere in the world at extremely high resolutions, up to and including 6K (or 6144x3072). Some companies are starting to offer video streaming as a type of “rent-from-home” service, where the user can fly sUAS in real time, and stream video online from their home.²² Augmented Reality (AR) platforms for sUAS are also being developed to enhance FPV experiences, aid law enforcement personnel, and for gaming and racing recreational users. Consequently, the cost for past years’ technologies are also decreasingly rapidly. sUAS with 4K resolution streaming now sell for less than \$1,000. Higher fidelity audio/video for sUAS increases the threat from remote surveillance while retaining quality resolution and signal transmission. Augmented reality technology for sUAS is also developing quickly for both racing and gaming sUAS consumers. Although it does not have a direct impact on critical infrastructure vulnerability, this type of technology could aid in the targeting of critical infrastructure assets, thus improving the likelihood of successful attacks.
- *Sensors and Processing*: There is a desire for greater capability in onboard sensors and processors for sUAS, so that analytics can be delivered to users in real time. Outputs can then be viewed on mobile phones or tablet controllers, allowing for real time decision-making. The push for enhanced sensor capacity is also driving innovations leading to reductions in size, weight, and cost of sUAS sensors. For example, the demand for light detection and ranging (LiDAR) sensors on sUAS has brought costs down to within a few hundred dollars. These

²¹ See example at FlyingTech.co.uk. “Remote Control Servo Driven Payload Release Mechanism,” FlyingTech, accessed August 1, 2017, <http://www.flyingtech.co.uk/electronics/drone-remote-control-payload-release-mechanism>.

²² “CAPE,” Cape Productions, Inc., accessed August 15, 2017, <https://www.cape.com/>.

higher quality sensors could increase the threat from surveillance to critical infrastructure by providing real-time measurements and geo-locational data to threat actors, who could then act upon that information. However, critical infrastructure vulnerability does not inherently change.

Technology Example – PRODRONE’s PD6B-AW-ARM mechanical arm sUAS (Figure 10) has a maximum payload of 44 lbs. and a pair of 5-axis robotic arms, equipped with a variety of motions and tilts that can lift up to about 22 lbs. for approximately 30 minutes.²³ This sUAS can be used to perform specific “hands-on” operations, such as cutting cables or wires, turning dials, and transporting or retrieving hazardous materials at high altitudes.



Figure 10. PRODRONE PD6B-AW-ARM²⁴

Technology Example – AR applications are now being developed and sold to sUAS pilots who can use the technology to train and master aerial skills, as well as for recreational purposes. Edgybees, an augmented reality technology company, developed the first AR gaming application for DJI sUAS pilots using the Epson Moverio BT-300 Drone Edition smart glasses (Figure 11).²⁵ The game layers a virtual picture onto an FPV view of the real world through the smart glasses. Pilots can then navigate their sUAS through a virtual obstacle course. The game also offers track guiding, training for obstacle avoidance, and

²³ “PRODRONE Unveils the World’s First Dual Robot Arm Large-Format Drone,” PRODRONE, accessed July 23, 2017, <https://www.prodrone.jp/en/archives/1420/>.

²⁴ Ibid.

²⁵ “Augmented Reality Drone Game Launches on Smart Glasses,” DRONELIFE, accessed July 21, 2017, <http://dronelife.com/2017/06/02/edgybees-augmented-reality-drone-game/>.

social media data sharing. Gamers can link their user ID to their Facebook account and share their achievements with top performing pilots appearing on a leaderboard.²⁶

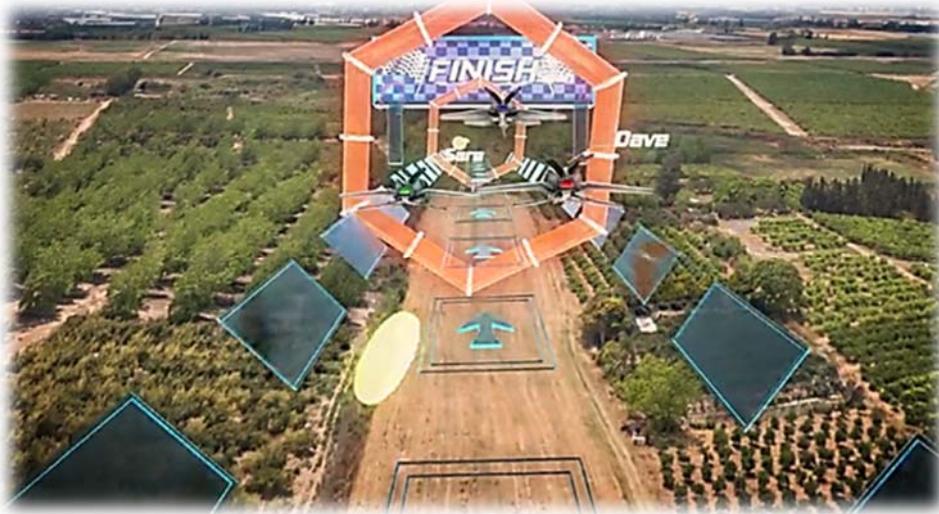


Figure 11. Augmented Reality for sUAS

Technology Example – FLIR has released a compact, lightweight, dual-sensor thermal and visible light imager designed for sUAS. The FLIR Duo lets you view thermal or visible imagery alone, or combined in Multi-Spectral Dynamic Imaging or Picture-in-Picture format (Figure 12).²⁷ It also features onboard recording and real-time remote control of camera functions over Bluetooth.



Figure 12. FLIR® Duo™ R Thermal Camera for sUAS

²⁶ Ibid.

²⁷ “FLIRDuo™,” FLIR, accessed July 26, 2017, <http://www.flir.com/suas/duo/>.

3. **Autonomy**

Developing autonomous UAS is a cumulative process, requiring the constant addition of new technologies and supporting systems to move from a semi-autonomous capability toward a fully autonomous one. However, what makes a unit fully autonomous is not agreed upon by public or private UAS producers and consumers. At a minimum, the aviation community agrees that UAS must be able to navigate through the air without direct human piloting to be considered autonomous. Yet, several commercial manufacturers suggest that additional capabilities are necessary to create full autonomy. The typical features they assign to fully autonomous UAS are adaptive flying, object sense-and-avoidance, object tracking, waypoint navigation, and safe return-to-home.

a. Semi-autonomous systems

Most advertised commercially available “autonomous” sUAS are viewed as semi-autonomous systems, with immature or limited capabilities.²⁸ The individual technologies that comprise a semi-autonomous sUAS will continue to develop, increasing in capability. However, it is unclear what immediate additional technologies will be adapted for sUAS to increase autonomy. It is likely that as swarming technology develops, autonomy will become intertwined with smart communication systems that allow sUAS to communicate with one another independently during swarm operations. This could include sensing when another sUAS is not able to continue the mission, filling in a gap, or providing additional lift capability to underperforming cargo-transport sUAS.

Impact on Vulnerability – Despite the capabilities acquired through semi-autonomous systems, critical infrastructure vulnerability is not affected. However, once a flight path has been established and the sUAS is set to autonomous mode, disruption of the flight path is nearly impossible without direct intervention (e.g., kinetic countermeasure).

Technology Example – The DJI Inspire 2 (Figure 13) is advertised as one of the most advanced “autonomous” sUAS commercially available for purchase. Its capabilities include obstacle avoidance, object tracking, and the use of pre-programmed waypoints to navigate, including a return to home feature. However, the sense and avoid systems that support obstacle avoidance are limited in range and direction: it can only detect forward/downward at a 25° angle out to 98 feet (ft.), and directly upward to 16 ft.²⁹ This leaves the sides, rear, and undercarriage of the sUAS vulnerable. Additionally, there is the problem of the detection system operating more slowly than available flight speeds. The sense and avoid systems function at 34 mph or slower, yet the sUAS is capable of flying at up to 58 mph. These systems would not be able to protect the sUAS from other sUAS, birds, or manned aircraft traveling at higher speeds or approaching from unprotected directions.

²⁸ Personal interviews, March–July 2017.

²⁹ “INSPIRE 2,” DJI, accessed July 27, 2017, <https://www.dji.com/inspire-2>.

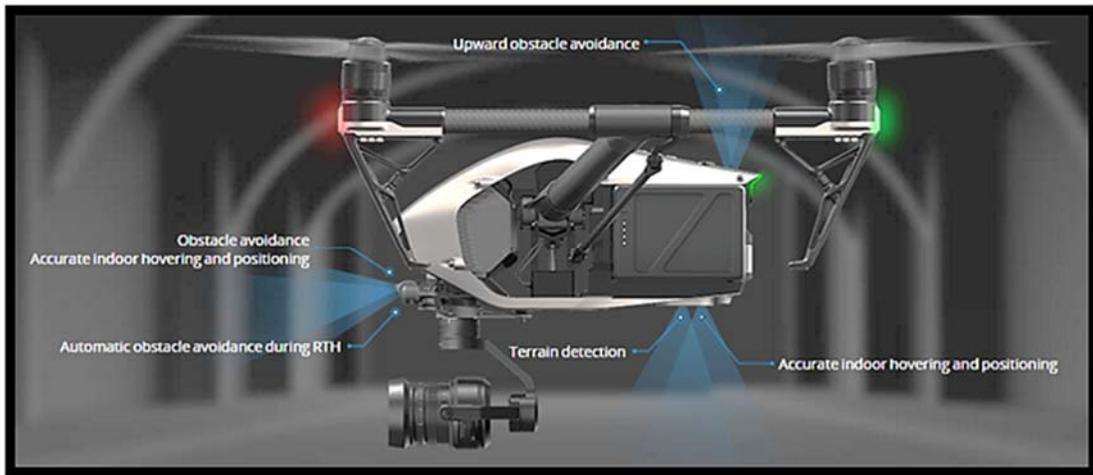


Figure 13. DJI Inspire 2³⁰

b. Fully autonomous systems

As mentioned earlier, there is no formal agreed-upon concept for “fully autonomous UAS,” but commercial manufacturers are striving to realize their own visions of this amorphous goal. The United States is one of the most advanced countries developing technologies for autonomous UAS. Another country leading the way in UAS autonomy is Israel. It recently authorized a company, Airobotics Ltd., to fly fully unmanned autonomous UAS within its borders for business purposes.³¹ No other country has authorized such activity. It is unclear what designs and functional attributes Airobotics will build into these deployable UAS.

Impact on Vulnerability – With the exception of unanticipated advancements in decision-making capability, critical infrastructure vulnerability would not be affected by fully autonomous UAS. However, once a flight path has been established and the sUAS is set to autonomous mode, disruption of the flight path is nearly impossible without direct intervention (e.g., kinetic countermeasure). Additionally, advanced sense and avoid systems for UAS might thwart some counter-UAS technologies (e.g., evading aerial nets).

Technology Example – The Perdix swarm demo at China Lake, California, featured a series of sUAS missions launched off F/A-18s that demonstrated collective decision making, adaptive formation flying and self-healing (Figure 14).³² DOD officials described

³⁰ Ibid.

³¹ “Airobotics Scores Authorization to Fly Autonomous Drones in Israel,” TechCrunch, accessed August 2, 2017, <https://techcrunch.com/2017/03/27/airobotics-scores-authorization-to-fly-autonomous-drones-in-israel/>.

³² “DOD Achieves Largest Drone-Swarm Demo,” C4ISRNET, accessed July 21, 2017, <http://www.c4isrnet.com/unmanned/uas/2017/01/10/DOD-achieves-largest-drone-swarm-demo/>.

the demonstration as “one of the most significant tests of autonomous systems.”³³ The DOD stated: “Perdix are not pre-programmed synchronized individuals, they are a collective organism, sharing one distributed brain for decision-making and adapting to each other like swarms in nature. Because every Perdix communicates and collaborates with every other Perdix, the swarm has no leader and can gracefully adapt to drones entering or exiting the team.”³⁴



Figure 14. Perdix Swarm Demo

4. Swarming

Swarming technology will continue to develop rapidly and is being driven by the military, academia, and commercial sectors. Many commercial uses exist, such as mapping oil spills from the air, agricultural spraying, or search and rescue operations. The U.S. government has an interest in swarming technology to enable sUAS to perform military operations, conduct infrastructure inspections, and support law enforcement personnel. This has led to several partnerships with academia and industry, and the establishment of centers of excellence to support swarm research, development, test, and evaluation. Worldwide, other countries are investing heavily in swarming technology as well, most noticeably China, Russia, Israel, and the United Kingdom.

There are several aspects to sUAS swarming, including how many users are required to operate the swarm (one operator controlling multiple UAS or multiple operators needed to control multiple UAS); whether the operation must be pre-programmed, or if it can be

³³ Ibid.

³⁴ “DOD Ramps Micro-Drones after Successful ‘Swarm’ Test,” Defense Systems, accessed July 23, 2017, <https://defensesystems.com/articles/2017/01/13/swarmleopold.aspx>.

managed in real-time; and if sUAS swarms operate as a single body to perform a single function (cooperative swarming) or if they can perform separate distinct tasks in coordination with each other (coordinated swarming). The capability for a single operator to control multiple sUAS simultaneously in real time (not pre-programmed) is increasing, and is being enabled by the use of LTE networks and mobile phone applications.

a. Cooperative swarming

There is continuous development in cooperative swarming technologies, and within five years, sUAS will be able to perform a wide variety of complex functions en masse, such as land surveying and mapping, more complex entertainment performances, and effective manned-unmanned teaming for military operations.

Impact on Vulnerability – Generally, cooperative swarms do not directly increase critical infrastructure vulnerability to sUAS attack, but can increase consequences. In principle, if you are vulnerable to one sUAS, then you are vulnerable to many.

Technology Example – A record number of 1,000 Chinese sUAS performed aerial formations in Guangzhou, China, in February 2017 (Figure 15). According to local news portal ycw.com, the sUAS formed six different formations during a 15-minute performance, controlled by one computer.³⁵



Figure 15. Chinese Lunar New Year sUAS Swarm³⁶

³⁵ “1,000 Drones Perform Spectacular Formations in Guangzhou,” CRIENGLISH.com, accessed July 21, 2017, <http://english.cri.cn/12394/2017/02/13/2021s951725.htm>.

³⁶ “1,000 drones perform stunning formations in S #China's #Guangzhou on Sat to celebrate the #LanternFestival, setting a new world record,” People's Daily China Twitter account, accessed July 23, 2017, <https://twitter.com/PDChina/status/831010744015548417>.

b. Coordinated swarming

The technology for coordinated swarming exists today and has been demonstrated by universities and industry. Within five years, individual users will be able to perform a wide variety of separate tasks with multiple sUAS at the same time. A future scenario might include a team of four sUAS tasked with transmission line repair, where one sUAS is used for line observation and situational awareness, a separate sUAS is used for line testing and data relay, and the remaining two are conducting repairs using remotely controlled technologies, such as robotic arms with cable cutters. These four sUAS could all be controlled by the same operator.

Impact on Vulnerability – Generally, coordinated swarms do not directly increase critical infrastructure vulnerability, but can increase the consequences. Coordinated swarms can also support follow-on operations by threat actors, increasing the likelihood of success of second-order attacks. Additionally, as sUAS functions become more complex and new attack vectors are introduced, vulnerability could increase.

B. Trends in Counter-UAS

The following section summarizes the results of the technology trends assessment for counter-UAS for domestic purposes out to five years. It first provides general trends in the global development of counter-UAS commercial technologies, and then more specific trends for technologies that support steps in the aforementioned Counter-UAS Process. Where available, examples of promising technologies that are still being developed, and appear to address a wide range of stakeholder concerns, have been included.

1. Trends Overview

Counter-UAS is a rapidly growing global market, where most product development and testing is occurring overseas in foreign countries. Due to legal restrictions in the United States, counter-UAS technologies that are developed domestically are generally not being tested outside of controlled laboratory environments or remote rural locations. Thus, their actual capabilities and effectiveness in different settings, such as urban locations, are not known. Foreign countries have ongoing and extensive testing being performed without any restrictions and as a result, U.S. companies are going abroad to test products. Furthermore, due to the current legal restrictions on technology types that can be employed to counter UAS in the United States, many products developed domestically are marketed for foreign commercial markets or for military use overseas (U.S. and foreign militaries).

In general, most commercial counter-UAS products developed throughout the world are designed to oppose commercial off-the-shelf (COTS) sUAS that are widely marketed and studied, whereas custom-built sUAS can easily defeat counter-UAS products currently available. Customization is occurring more frequently and modifications to existing platforms could include a variety of changes, such as altering communications channels,

adding blocking equipment, employing quiet or stealth designs, improving sense and avoid systems, or installing onboard countermeasures. Additionally, most counter-UAS products are designed to address only a single sUAS threat; thus, swarming technology can easily defeat these products. This trend is expected to remain constant for the next five years.

2. Technology Trends Applied to the Counter-UAS Process

Counter-UAS are typically marketed as distinct technological capabilities, providing support to either Step 1, Step 2, or Step 3 of the previously described Counter-UAS Process (Figure 1). Most do not provide support to more than one step at a time; however, more complex systems are beginning to emerge. Step 1 and Step 3 technologies are currently the largest focal area for commercial manufacturers developing combined systems. Within the next five years, manufacturers will likely produce several products that offer mixed-sensor arrays for detection, identification, and tracking, linked to third-party threat response capabilities. User interfaces for these types of combined systems will maintain a human in the loop for decision making because automated decision-making systems are not being developed.

a. Detection, identification, and tracking

There is wide community consensus that detection and tracking are essential components of countering a sUAS threat, and yet they are viewed as the least mature technologies being developed by commercial vendors. Legal restrictions are not the source of this problem, as testing these technologies is legal in United States. The challenge lies in developing new sensor products that can distinguish different small-sized flying objects in both simple and complex environments. The U.S. government has been working to implement mandatory electronic identification and tracking devices for UAS that operate on existing communications and navigation networks (e.g., 4G/5G LTE, Global Positioning System (GPS), etc.) to partially solve the problem, but full implementation is still at least two to three years out. This effort would address only compliant sUAS; non-compliant sUAS would still require more advanced technologies and products that combine sensor types to detect, identify, and track sUAS.

The following are identified technology trends for the detection, identification, and tracking of sUAS carried out to five years:

- New sensors, ID tagging technology, and tracking software will see steady growth, eventually filling the technology gap that currently exists; however, as sUAS decrease in size, new gaps will arise.
- Detection technologies will become mixed systems, combining sensor types such as audio with visual, electro-optical/infrared systems (EO/IR), radio frequency (RF), and GPS.

- There will be slow growth in technologies that minimize false detections and maximize reliability. The problem will compound as the current need to differentiate between sUAS and birds morphs into a need to distinguish between sUAS and insects in the future.
- Tracking multiple objects simultaneously will be required for an effective counter-UAS. Commercial producers understand this. An increase in technology is expected, with the commercial market beginning to fill this gap over the next five years.
- Within five years, we will see many semi-autonomous counter-UAS products that detect, identify, track (Step 1), and respond to sUAS threats (Step 3), but retaining a human in the loop for decision making will persist (Step 2).

Promising Technology. 5D Robotics’ positioning and navigation node (i.e., PulsON® sensor, Figure 16) is able to track any vehicle type by virtue of its patented fusion of GPS, inertial sensing, optics-based localization, and ultra-wideband ranging technologies.³⁷ These sensors can be mounted to traffic lights and posts to create a smart grid for tracking vehicles, including sUAS. When arranged in a constellation (at least three sensors), the network created can offer up to 15-centimeter accuracy for object tracking. 5D Robotics claims that their product is more reliable than GPS and can function in rain, dust, snow, and fog.



Figure 16. PulsON® 440 smart sensor³⁸

³⁷ “Products,” 5D Robotics, accessed July 21, 2017, <http://5drobotics.com/products/>.

³⁸ “P440 Smart Sensor,” 5D Robotics, accessed July 21, 2017, <http://5drobotics.com/wp-content/uploads/2016/06/p440-cut-sheet.pdf>.

b. Threat decision

The threat decision step (Step 2) encompasses both the decision-making process that must be formally developed (protocols, procedures, approvals, etc.), and the response element, whether it be a human being or an automated system, that carries out the decision-making process. This step is the least developed in the counter-UAS process, yet it is becoming increasingly important to threat-response personnel. Following response time estimates (see example 1) for sUAS attacks, a need to expedite the threat decision step has been recognized. Automated response systems could lessen the burden of response personnel and place it on technology or the sUAS operator.

Example 1:

Threat: A store-bought \$1,500 DJI Phantom 4, traveling at a max speed of 20 m/s (or ~45 mph) with an explosive payload equal to that of the weight of its camera (~.75lbs), will traverse one kilometer in just under 50 seconds (depending on weather conditions) to reach its target.

Response: Security personnel would have to be notified of the pending sUAS attack by detection, identification, and tracking systems (often operated separately from response systems), and then proceed to an available open line-of-sight location to mitigate the threat (utilizing currently permissible counter-UAS technologies). All of these steps would have to occur within 50 seconds to be effective.

Precondition for Success: Protocols/procedures would need to be well developed to allow security personnel to respond in time; automated decision-making could reduce this step to seconds.

The following are identified technology trends for threat decision making carried out to five years:

- Commercial markets are not incentivized to develop automated response systems, nor is the demand for such systems by government and commercial stakeholders strong; within five years, some automated response systems may exist for select interested parties.
- Counter-UAS stakeholders at all levels of government are still in the early stages of developing necessary rules of engagement for countering UAS. Most of these assume human-in-the-loop decision-making and response procedures. Very little attention has been dedicated to protocols that an automated response system could follow. This will hinder the rate at which automated systems come online.

Promising Technology. Dedrone’s “automatic” anti-drone platform includes their DroneTracker web-based software (Figure 17) and several required and optional hardware components, such as RF sensors, detection radar, a modular jamming system, etc. The system claims to automatically classify UAS, issue alerts, and record evidence to identify

and assess potential threats. It can also “automatically” trigger offensive or defensive countermeasures. Additionally, the system allows integration with third-party mitigation technologies, which will need to be assessed for legal use in the United States (Dedrone is a German-based company).³⁹

The Dedrone system is marketed as “a future-proof software platform that mitigates all drone threats” and is scalable and customizable.⁴⁰ Despite such declarations by its makers, the system still currently requires human input to activate/decide applicable mitigation measures to respond to incoming threats. With some software interface customization and a well-developed automated response protocol, the Dedrone system could be transformed into a fully automated counter-UAS system. Legal considerations for the United States would also have to be incorporated into any automated mitigation measure chosen.

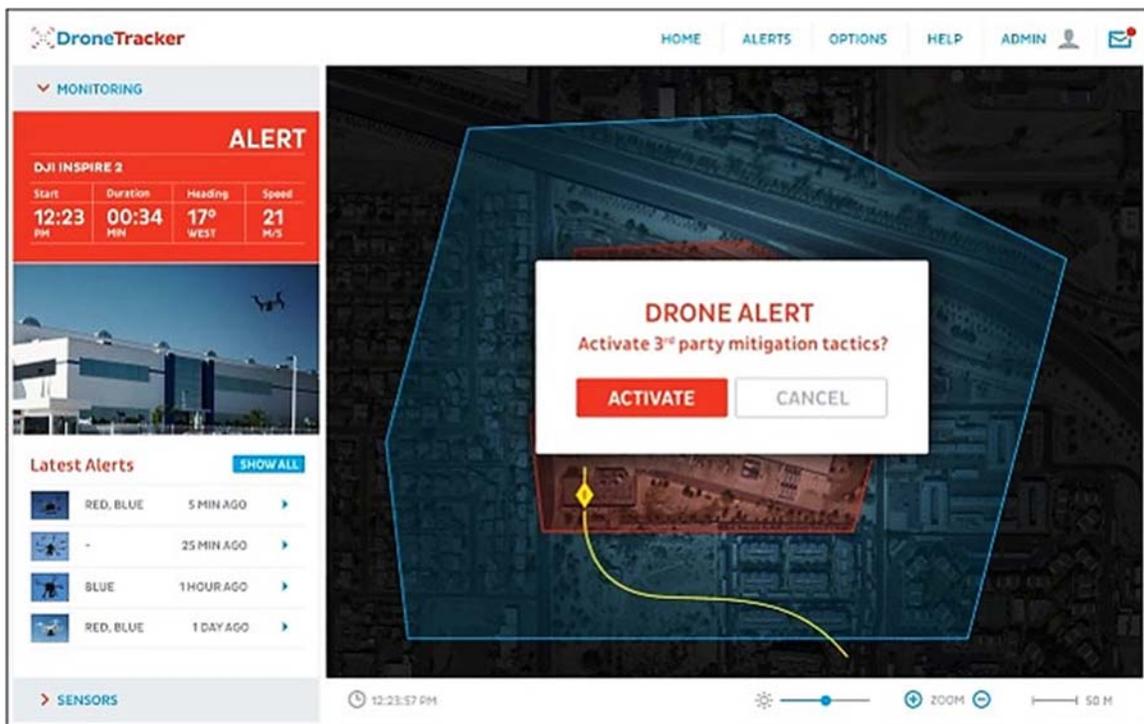


Figure 17. Dedrone System

c. Threat response

Threat response includes the technologies required to counter UAS threats, and can be kinetic or non-kinetic. Threat response products are the most developed and largest area

³⁹ “Product,” Dedrone, accessed July 23, 2017, <https://www.dedrone.com/en/dronetracker/drone-protection-software>.

⁴⁰ Ibid.

of commercial investment for counter-UAS. Threat response technologies are often developed as individual systems, separate from the rest of the Counter-UAS Process, to be integrated later as one of many countermeasure options. Incongruously, most mitigation technologies developed are illegal for use in the United States. Additionally, mitigation technologies are largely tested in rural environments or laboratories in the United States, with some urban testing occurring overseas. This has resulted in a lack of confidence in the effectiveness of countermeasure systems in urban settings.

The following are identified technology trends for sUAS threat response carried out to five years:

- DOD will continue to be viewed as the federal leader in developing and employing counter-UAS mitigation technologies; new countermeasures will continue to be developed for overseas threats.
- DOD is working to finalize a technology roadmap for counter-sUAS, per congressional direction; this could spur further commercial growth in threat response technologies.
- Most counter-UAS mitigation technology investments are in active systems that employ either kinetic or non-kinetic technologies to interfere with sUAS flight directly. Over the next five years, there will be a large increase in counter-UAS vendors developing active systems as sUAS incidents increase, threat types are hyped up, and authorities to counter UAS are exercised.
- There is anticipation of a change in federal restrictions for the use of active systems in the United States. This is supporting the continued development of active countermeasures.
- Collateral damage is largely unaccounted for by commercial vendors. This will change as customers seek products that will leave them less liable.

Promising Technology. The Robotic Falconry drone-catcher system is a non-destructive aerial net system that can be mounted to a variety of sUAS to capture other sUAS and transport them to a desired location (i.e., a “capture and relocate” system).⁴¹ It was developed by Michigan Tech’s Human-Interactive Robotics Lab (HIROLab). When a threat sUAS has been identified, a friendly sUAS with the Robotic Falconry system mounted can be used to intercept the threat sUAS. Upon reaching the target, the friendly sUAS fires a net when commanded and ensnares the target. The Robotic Falconry system

⁴¹ “Drone Catcher: ‘Robotic Falcon’ Can Capture, Retrieve Renegade Drones,” MichiganTech, accessed July 23, 2017, <http://www.mtu.edu/news/stories/2016/january/drone-catcher-robotic-falcon-can-capture-retrieve-renegade-drones.html>.

is not automated, and requires an operator to sight and fire the device while also operating the sUAS. Another limit is that there is only one net cartridge per flight.

Many in the counter-UAS community have voiced strong support for these types of capture and relocate systems. They can potentially limit collateral damage to threat sUAS and reduce secondary effects to local populations from threat payloads.



Figure 18. Robotic Falconry Prototype Drone-Catcher System⁴²

⁴² "Robotic Falconry - Drone Catcher System for Removing the Intruding Drones," TheHiroLab, accessed July 4, 2017, <https://www.youtube.com/watch?v=jvdKNBSWPYU>.

This page is intentionally blank.

4. Conclusion

The proliferation of sUAS for both benign and nefarious use will continue into the foreseeable future, along with sUAS technology advances that permit greater capability in payload, ranges, and functionality. Counter-UAS capabilities will also continue to develop, but in competition with commercial sUAS improvements. To better inform DHS/IP decision makers on the current and projected state of sUAS and counter-UAS technologies, this assessment looked at trends out to five years, and briefly examined the impact of sUAS capabilities on critical infrastructure vulnerability. The following are the summarized key findings from the two categories of the assessment, along with overall findings in counter-UAS development.

A. Key Findings from the Survey of sUAS Technology Trends

Over the next five years, trends in sUAS technology will be observed in four general categories. These are listed below.

1. Platform Modification

- **Size** will *continue to decrease* while maintaining or increasing capabilities; however, use will be largely for hobbyists.
- Gross **weight** for sUAS platforms will *continue to decrease*; however, with advancements in power supplies and new recharging options, weight will be less of a hindrance to continual use.
- As sUAS decrease in size, they also will *maintain or increase* **payload** capabilities, eventually being able to carry much more than their own weight.

2. Platform Operation

- sUAS will increase **speed** capabilities for rotocopters surpassing 200 mph.
- sUAS will continue to increase their **range and endurance** steadily.
- Most commercial **electronic and mechanical capabilities** available for other mobile platforms will become available for sUAS within the next five years (robotics, sensors, audio/video, etc.).

3. Autonomy

- Autonomous systems already exist, but the degree of autonomy and the level of sophistication of communication between units will continue to expand, allowing sUAS to perform any functionally programmable operation.

4. Swarming

- Swarming technology will increase rapidly worldwide and in five years, without government interference, easily programmable and purchasable swarming technology will be widely available to the average consumer.

B. Key Findings from the Survey of Counter-UAS Technology Trends

Over the next five years, trends in counter-UAS technologies will be observed across the three steps of the Counter-UAS Process: (1) detection, identification, and tracking, (2) threat decision, and (3) threat response. These are listed below.

1. Detection, Identification, and Tracking

- Sensors, identification, and tracking systems for countering UAS will see *steady growth over the next five years*; however, persistent sUAS development trends will create *new capability gaps*.
- A major existing gap is tracking multiple sUAS targets simultaneously; this gap will be filled in five years.
- Technologies developed in isolation and the integration of systems remain a challenge; a human in the loop will still be required to fuse detection, identification, and tracking systems.

2. Threat Decision

- Threat decision making is not just a technology solution, it requires rules of engagement policies and protocols to be established; this will *continue to be a slow process* that is pieced together over the next five years.
- Threat decision making will remain the least developed step in the Counter-UAS Process.
- The response process must be minimized to less than one minute, and the U.S. likely won't be able to accomplish this in the next five years.
- Threat decision making will still require a human in the loop because policies and protocols for automated systems are not being established.
 - Some limited automated response systems may exist for select parties and limited applications.

3. Threat Response

- Threat response technologies developed by government and industry to counter domestic UAS threats will *continue to see rapid growth*; however, most solutions will *still be illegal or limited in the United States*.

- This will continue over the next five years, unless significant regulatory changes are made.
- Most government and industry investments are in active, not passive counter-UAS technologies.
 - The United States is expected to see a steady increase in the number of vendors producing active systems over the next five years as the threat grows.
 - There is anticipation of the United States relaxing limits on active systems.
- Currently, commercial vendors largely ignore collateral damage produced by counter-UAS; however, systems that minimize collateral damage will be a focus area in the next five years.
 - Domestic markets will see growth in systems that minimize collateral damage.

C. General Findings in Counter-UAS Development

In general, counter-UAS technology development is a rapidly growing global market where several commercial and government stakeholders have expressed a high interest in developing systems that accurately and efficiently protect people and infrastructure assets, while minimizing potential collateral damage. From the survey, and in particular the interviews and review panels, several general findings in counter-UAS development have been collected. These findings pertain to larger issues across the counter-UAS industry that affect all steps in the Counter-UAS Process, and impact the ability to accurately and efficiently protect people and infrastructure assets in the United States. These are listed below.

- As a result of a rapid growth market and existing legal restrictions for product testing in the United States, counter-UAS product development is occurring largely in foreign countries.
 - Most counter-UAS technologies developed in the United States are not tested outside of a controlled laboratory environment or remote rural locations, making their capabilities in urban environments unknown.
 - Foreign countries have ongoing and extensive testing being performed without any restrictions, and U.S. companies are going overseas to test their products.
- Most counter-UAS systems are based off countering COTS sUAS that are widely known or studied, whereas custom built sUAS can easily defeat currently available systems

- Customized sUAS could include altered communications channels, blocking equipment, stealth designs, etc.
- Counter-UAS technologies currently cannot address more than one or two sUAS threats at a time; therefore, swarming technology can easily defeat existing counter-UAS products.
- Most counter-UAS technologies are built and marketed as individual components of the Counter-UAS Process (Step 1 or Step 2 or Step 3), though more complex systems are beginning to emerge
 - Steps 1 and 3 are the largest focus areas for commercial manufacturers for combined systems, but Step 2 needs significant advancement if sUAS threats are to be addressed in time to prevent an incident.

Appendix A. Illustrations

Figures

Figure 1. The Counter-UAS Process	5
Figure 2. SKEYE Nano 2 Camera sUAS.....	8
Figure 3. Intelligent Energy’s Ultra Lightweight Fuel Cell System.....	9
Figure 4. Oakland University’s Loon Copter Multi-Modal sUAS	10
Figure 5. Predicted Value of UAS by Industry.....	11
Figure 6. sUAS powered by a Behotec JB-180 turbine engine	13
Figure 7. Fastest First-Person View (FPV) sUAS – August 2017.....	13
Figure 8. Solar-powered Silent Falcon sUAS.....	14
Figure 9. AT&T Flying Cell on Wings(Flying COW)	15
Figure 10. PRODRONE PD6B-AW-ARM	17
Figure 11. Augmented Reality for sUAS.....	18
Figure 12. FLIR® Duo™ R Thermal Camera for sUAS.....	18
Figure 13. DJI Inspire 2	20
Figure 14. Perdix Swarm Demo.....	21
Figure 15. Chinese Lunar New Year sUAS Swarm	22
Figure 16. PulsON® 440 smart sensor	25
Figure 17. Dedrone System.....	27
Figure 18. Robotic Falconry Prototype Drone-Catcher System.....	29

This page is intentionally blank.

Appendix B. References

- “1,000 Drones Perform Spectacular Formations in Guangzhou,” *CRIEnglish.com*, February 13, 2017, accessed July 21, 2017, <http://english.cri.cn/12394/2017/02/13/2021s951725.htm>.
- “1,000 drones perform stunning formations in S #China's #Guangzhou on Sat to celebrate the #LanternFestival, setting a new world record,” *People's Daily China* Twitter account, accessed July 23, 2017, <https://twitter.com/PDChina/status/831010744015548417>.
- “Fastest Remote-Controlled Jet-Powered Model Aircraft (RC),” *Guinness World Records*, accessed July 21, 2017, [http://www.guinnessworldrecords.com/world-records/fastest-remote-controlled-jet-powered-model-aircraft-\(rc\)?fb_comment_id=701907789916475_1110755145698402](http://www.guinnessworldrecords.com/world-records/fastest-remote-controlled-jet-powered-model-aircraft-(rc)?fb_comment_id=701907789916475_1110755145698402).
- 5D Robotics. “P440 Smart Sensor,” accessed July 21, 2017, <http://5drobotics.com/wp-content/uploads/2016/06/p440-cut-sheet.pdf>.
- 5D Robotics. “Products,” accessed July 21, 2017, <http://5drobotics.com/products/>.
- Asylon. “DroneHome,” accessed July 20, 2017, <http://www.flyasylon.com/product>.
- Cape Productions, Inc. “CAPE,” accessed August 15, 2017, <https://www.cape.com/>.
- Copestake, Jen. “Hydrogen-Powered Drone Takes Flight,” *BBC News*, March 25, 2016, accessed July 21, 2017, <http://www.bbc.com/news/av/technology-35890486/hydrogen-powered-drone-takes-flight>.
- Dedrone. “Product,” accessed July 23, 2017, <https://www.dedrone.com/en/dronetracker/drone-protection-software>.
- Department of Defense. “Unmanned Aircraft System Airspace Integration Plan,” March 2011, accessed July 2017, http://www.acq.osd.mil/sts/docs/DOD_UAS_Airspace_Integ_Plan_v2_%28signed%29.pdf.
- DJI, “AGRAS MG-1,” accessed August 16, 2017, <https://www.dji.com/mg-1>.
- DJI. “MG-1 SPECS,” accessed July 21, 2017, <http://www.dji.com/mg-1/info#specs>.
- DJI. “INSPIRE 2,” accessed July 27, 2017, <https://www.dji.com/inspire-2>.
- FLIR. “FLIR Duo™,” accessed July 26, 2017, <http://www.flir.com/suas/duo/>.
- FlyingTech. “Remote Control Servo Driven Payload Release Mechanism,” accessed August 1, 2017, <http://www.flyingtech.co.uk/electronics/drone-remote-control-payload-release-mechanism>.
- Gagliardi, Natalie. “Drone Racing League Sets World Record for Fastest Quadcopter,” *ZDNet*, July 14, 2017, accessed July 21, 2017, <http://www.zdnet.com/article/drone-racing-league-sets-world-record-for-fastest-quadcopter/>.

- Gajitz. "Loon Copter: Amphibious Drone Floats, Flies & Dives," accessed July 20, 2017, <http://gajitz.com/loon-copter-amphibious-drone-floats-flies-dives/>.
- Glaser, April. "DJI is Running Away with the Drone Market," *Recode*, April 14, 2017, accessed July 21, 2017, <https://www.recode.net/2017/4/14/14690576/drone-market-share-growth-charts-dji-forecast>.
- Goodrich, Marcia. "Drone Catcher: 'Robotic Falcon' Can Capture, Retrieve Renegade Drones," *MichiganTech*, January 7, 2016, accessed July 23, 2017, <http://www.mtu.edu/news/stories/2016/january/drone-catcher-robotic-falcon-can-capture-retrieve-renegade-drones.html>.
- Intelligent Energy. "Drones Products," accessed July 21, 2017, <http://www.intelligent-energy.com/our-products/drones/products/>.
- James. "Fastest FPV Racing Drones 2017," *FPV Drone Reviews*, August 13, 2017, accessed November 2, 2017, <http://fpvdronereviews.com/guides/fastest-racing-drones/>.
- Kolodny, Lora. "Airobotics Scores Authorization to fly Autonomous Drones in Israel," *TechCrunch*, March 27, 2017, accessed August 2, 2017, <https://techcrunch.com/2017/03/27/airobotics-scores-authorization-to-fly-autonomous-drones-in-israel/>.
- Leopold, George. "DOD Ramps Micro-Drones After Successful 'Swarm' Test," *Defense Systems*, January 13, 2017, accessed July 23, 2017, <https://defensesystems.com/articles/2017/01/13/swarmleopold.aspx>.
- Limpert, Rick. "AT&T Tests COW Flying Over Georgia," *GAFollowers*, February 16, 2017, accessed July 21, 2017, <http://www.gafollowers.com/att-tests-cow-flying-georgia/>.
- Malek Murison, "Augmented Reality Drone Game Launches on Smart Glasses," *Drone Life*, June 2, 2017, accessed July 21, 2017, <http://dronelife.com/2017/06/02/edgybees-augmented-reality-drone-game/>.
- New Atlas. "Solar-Powered Silent Falcon UAV Unveiled," accessed July 19, 2017, <http://newatlas.com/silent-falcon-uav/23641/>.
- Pomerleau, Mark. "DOD Achieves Largest Drone-Swarm Demo," *C4ISRNET*, January 10, 2017, accessed July 21, 2017, <http://www.c4isrnet.com/unmanned/uas/2017/01/10/dod-achieves-largest-drone-swarm-demo/>.
- Pregler, Art. "When COWs Fly: AT&T Sending Cell Signals from Drones," *AT&T*, February 21, 2017, accessed July 23, 2017, http://about.att.com/innovationblog/cows_fly.
- PRODRONE. "PRODRONE Unveils the World's First Dual Robot Arm Large-Format Drone," accessed July 23, 2017, <https://www.prodrone.jp/en/archives/1420/>.
- RC Media World. "Very Very Very Fast Turbine Powered RC Jet 440 MPH Speed Guinness World Record 2013," accessed July 21, 2017, <https://www.youtube.com/watch?v=sa-TSNeTK-A&spfreload=10>.
- Silent Falcon. "Silent Falcon," accessed July 23, 2017, <http://www.silentfalconuas.com/silent-falcon>.

TheHiroLab. "Robotic Falconry - Drone Catcher System for Removing the Intruding Drones," accessed July 4, 2017, <https://www.youtube.com/watch?v=jvdKNBSWPYU>.

TRNDlabs. "SKEYE Nano 2 Camera," accessed July 21, 2017, <https://www.trndlabs.com/product/skeye-nano-2-camera/>.

Weller, Chris. "Drones Could Replace \$127 Billion Worth of Human Labor," *Tech Insider*, May 11, 2016, accessed July 21, 2017, <http://www.businessinsider.com/drones-could-replace-127-billion-of-human-labor-2016-5>.

White House. "Presidential Policy Directive/PPD-21: Critical Infrastructure Security and Resilience, February 12, 2013," accessed July 2017, <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.

This page is intentionally blank.

Appendix C. Abbreviations

AR	Augmented Reality
CBR	chemical/biological/radiological
COTS	commercial off-the-shelf
COW	Cell on Wings
DHS	Department of Homeland Security
DOD	Department of Defense
EO/IR	electro-optical/infrared
FPV	First-Person View
GPS	Global Positioning System
HD	high definition
HIRoLab	Human-Interactive Robotics Lab
IDA	Institute for Defense Analyses
IP	Infrastructure Protection
LiDAR	light detection and ranging
LTE	Long Term Evolution
PPD	Presidential Policy Directive
RC	remote-controlled
RF	radio frequency
SOPD	Sector Outreach and Programs Division
sUAS	small unmanned aircraft systems
T&E	Testing and Evaluation
UA	unmanned aircraft
UAS	unmanned aircraft systems
UAV	unmanned air vehicle

This page is intentionally blank.

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188		
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YYYY) xx-11-2017		2. REPORT TYPE Final		3. DATES COVERED (From – To)	
4. TITLE AND SUBTITLE <i>Technology Trends in Small Unmanned Aircraft Systems (sUAS) and Counter-UAS: A Five-Year Outlook</i>			5a. CONTRACT NO. HQ0034-14-0001		
			5b. GRANT NO.		
			5c. PROGRAM ELEMENT NO(S).		
6. AUTHOR(S) G. James Herrera Jason A. Dechant E.K. Green Ethan A. Klein			5d. PROJECT NO. ER-6-4036		
			5e. TASK NO.		
			5f. WORK UNIT NO.		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Institute for Defense Analyses 4850 Mark Center Drive Alexandria, VA 22311-1882			8. PERFORMING ORGANIZATION REPORT NO. IDA Paper P-8823 Log: H 17-000624		
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Department of Homeland Security 2451 Crystal Drive Arlington, VA 22202			10. SPONSOR'S/ MONITOR'S ACRONYM(S) DHS		
			11. SPONSOR'S/MONITOR'S REPORT NO(S).		
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT The air domain has become increasingly complex in recent years because of the proliferation of unmanned aircraft systems (UAS). In particular, the growing demand for small UAS (under 55 lbs.) by personal enthusiasts and commercial applications has caused rapid expansion of the commercial small UAS markets. With new producers vying for market shares, competition is fostering rapidly decreasing prices, and new innovative technological features intended to garner a comparative advantage. The spread of small UAS for non-governmental applications brings the danger of accidental or even nefarious use of UAS for criminal or terrorist operations. As the sectors specific agency (SSA) for a majority of critical infrastructure sectors, the Department of Homeland Security (DHS) is responsible for understanding trends in small UAS development. To assist DHS with understanding these technology trends, the Office of Infrastructure Protection Sector Outreach and Programs Division asked the Institute for Defense Analyses (IDA) to conduct an assessment of the trends small UAS technology development over the next five years to reduce it. This paper documents the results of the assessment and provides indications of sUAS technology development.					
15. SUBJECT TERMS Unmanned Aircraft Systems, Department of Homeland Security, Vulnerability, Critical Infrastructure					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT U	18. NO. OF PAGES 56	19a. NAME OF RESPONSIBLE PERSON Matthew Barger
a. REPORT U	b. ABSTRACT U	c. THIS PAGE U			19b. TELEPHONE NUMBER (Include Area Code) (703) 603-5086

This page is intentionally blank.