INSTITUTE FOR DEFENSE ANALYSES

# Critical Infrastructure Vulnerabilities To Small Unmanned Aircraft Systems

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

January 2018
Approved for public release;
distribution is unlimited.
IDA Document NS D-8907
Log: H 18-000002

INSTITUTE FOR DEFENSE ANALYSES
4850 Mark Center Drive
Alexandria, Virginia 22311-1882

*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.

**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

INSTITUTE FOR DEFENSE ANALYSES

IDA Document NS D-8907

# Critical Infrastructure Vulnerabilities To Small Unmanned Aircraft Systems

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

This page is intentionally blank.

Homeland Security

# CRITICAL INFRASTRUCTURE VULNERABILITIES TO SMALL UNMANNED AIRCRAFT SYSTEMS

## CONCERN

Small unmanned aircraft systems (sUAS) use has increased as a cost-effective, versatile, and convenient business and national security tool, as well as a popular recreational hobby. As a result, intended and unintended threats to critical infrastructure associated with sUAS use may increase in volume in the coming years.

Current trends demonstrate sUAS as an integrated tool for homeland security, defense, commercial business operations, and media applications.

- Advancements in autonomous technologies are increasing, with better drone-to-drone communications reducing the need for human pilots.

## TECHNOLOGY TRENDS†

### Trends in sUAS Development

*5-YEAR OUTLOOK*

**General Trends:** sUAS will be able to travel at greater speeds (200 mph+), carry heavier payloads, and engage multiple flight control modes that enhance operational flexibility, battery life, and flight time.

**Swarming:** The technology required for multiple sUAS to work together in concert will be widely available to the average consumer, rather than only to militaries and major commercial entities.

**Technology and Functions:** Continual transfer of mobile innovations in sensors and robotics to sUAS platform

**Multi-Modal Designs:** Flight capabilities combined with maritime surface, underwater, and ground vehicle modes will be widely available to consumers.

## Trends in Counter-UAS

Industry research and development of counter-UAS capabilities continue to increase and adapt to changes from emerging sUAS threats. However, many counter-UAS technologies are bound by current U.S. regulation and policy, and legal implementation of products in the U.S. will evolve as policy permits. The following trends are grouped according to the three steps of the "Counter-UAS Process" and extend out to five years.

### Detection, Identification, and Tracking

**Sensors and Tracking**

- Capabilities will continue to improve using an array of multiple sensors and microprocessors
- New challenges will emerge from smaller sUAS
- Cost-effective systems will depend on integration into current critical infrastructure security electronic and physical platforms

**ID Tagging**

- Development and implementation will occur over the next five years, and is a priority initiative for the federal government

### Threat Decision

- Due to the short time available to employ a threat response mechanism, human-based threat decision-making will continue to be insufficient for addressing most sUAS threats
- Counter-UAS with automated response protocols have not garnered wide investment, but could reduce delays in sUAS threat response

### Threat Response

- Threat response products will continue to develop rapidly to meet demand

**Passive Systems**

Domestic markets will see growth in passive counter-UAS that are legal and minimize collateral damage

- Ex: facility nets
- Ex: geo-fencing
- Ex: sensor-based smart blinds
- Ex.: police notification systems

## COUNTER-UAS CHALLENGES

Largely, counter-UAS products are built to oppose commercial off-the-shelf sUAS that are widely available and known; however, custom built sUAS can defeat most counter-UAS technologies

Policies, protocols, and rules of engagement for countering UAS threats are not fully developed across government or industry

Damaging or interfering with hostile or threat UAS is illegal, as they're considered aircraft by definition

## VULNERABILITIES

**Vulnerability across selected critical infrastructure sectors to sUAS attack vectors are presented below. The vulnerability for each sector to each attack vector was assessed at the subsector level (see DHS Infrastructure Data Taxonomy), and included an additional measure of threat *uniqueness*.* For each subsector, these assessments were assigned 0, 1, and 2 valuations (Low, Moderate, and High respectively), then averaged for each sector. These averages are the basis for the shading and labeling below.**

| Threats | Surveillance | Impact | Impact with Mounted Weapon | Impact with Explosive | Ballistic and Projectile Weapons | Directed Energy Weapons | Chemical, Biological, Radiological |
|---|---|---|---|---|---|---|---|
| Dams Sector | L | L | L | L | L | L | L |
| Nuclear Reactors, Materials, and Waste Sector | H | M | H | H | H | L | H |
| Chemical Sector | M | M | M | M | L | L | H |
| Critical Manufacturing Sector | L | L | L | L | L | L | L |
| Emergency Services Sector | L | L | L | L | L | L | M |
| Commercial Facilities Sector | M | L | L | L | L | L | H |

* ***Uniqueness:*** **The extent to which sUAS present a vulnerability to an infrastructure asset (or group of assets) that is not presented by traditional ground-based attack vectors.**

| Key | Low | Moderate | High |
|---|---|---|---|
| Vulnerability to Threat | | | |
| Uniqueness of Threat | L | M | H |

## INFRASTRUCTURE PROTECTION CHALLENGES

- Across infrastructure sectors, there is limited knowledge of the risks sUAS pose to infrastructure assets
- Consequences for sUAS attacks have not been fully assessed within each sector
- Where vulnerability and threat assessments have been performed, those assessments have not been revised to include emerging sUAS threats
- There is not widespread awareness of existing options for restricting critical infrastructure airspace
- Best practices and response options are variable from state to state (jurisdiction to jurisdiction)
- Currently, protection of critical infrastructure assets lies principally with industry owners/operators, who have limited knowledge of the available and legal protective measures that could be employed
- sUAS threat response options are limited under existing federal policy, leaving state and local governments with only civil or criminal penalties after the fact

† **See IDA paper:** ***Technology Trends in Small Unmanned Aircraft Systems (sUAS) and Counter-UAS: A Five-Year Outlook,*** **https://www.ida.org/HS/HSResearch**

This page is intentionally blank.

| REPORT DOCUMENTATION PAGE | | *Form Approved OMB No. 0704-0188* |
|---|---|---|



| 1. REPORT DATE (DD-MM-YYYY) | 2. REPORT TYPE | 3. DATES COVERED (From – To) |
|---|---|---|
| xx-01-2018 | Final | |

| 4. TITLE AND SUBTITLE | 5a. CONTRACT NO. |
|---|---|
| *Critical Infrastructure Vulnerabilities To Small Unmanned Aircraft Systems* | HQ0034-14-0001 |
| | 5b. GRANT NO. |
| | 5c. PROGRAM ELEMENT NO(S). |

| 6. AUTHOR(S) | 5d. PROJECT NO. |
|---|---|
| E.K. Green<br>Jason A. Dechant<br>G. James Herrera | ER-6-4036 |
| | 5e. TASK NO. |
| | 5f. WORK UNIT NO. |

| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) | 8. PERFORMING ORGANIZATION REPORT NO. |
|---|---|
| Institute for Defense Analyses<br>4850 Mark Center Drive<br>Alexandria, VA 22311-1882 | IDA Document NS D-8907<br>Log: H 18-000002 |

| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR'S/ MONITOR'S ACRONYM(S) |
|---|---|
| Department of Homeland Security<br>2451 Crystal Drive<br>Arlington, VA 22202 | 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**

**15. SUBJECT TERMS**

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NO. OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | Matthew Barger |
| U | U | U | U | 8 | 19b. TELEPHONE NUMBER (Include Area Code) (703) 603-5086 |

This page is intentionally blank.