SOAR

STATE-OF-THE-ART REPORT (SOAR)
MAY 2018

DSIAC-2018-0849

UNMANNED AERIAL SYSTEMS (UAS) FOR INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE (ISR)

By Matthew Harbaugh

Contract Number: FA8075-14-D-0001
Published By: DSIAC

DISTRIBUTION STATEMENT A
Approved for public release: distribution unlimited.

This Page Intentionally Left Blank

SOAR

STATE-OF-THE-ART REPORT (SOAR)
MAY 2018

UNMANNED AERIAL SYSTEMS (UAS) FOR INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE (ISR)

MATTHEW HARBAUGH

State-of-the-Art Report

ABOUT DSIAC

The Defense Systems Information Analysis Center (DSIAC) is a U.S. Department of Defense (DoD) IAC sponsored by the Defense Technical Information Center (DTIC). DSIAC is operated by SURVICE Engineering Company under contract FA8075-14-D-0001 and is one of the next-generation DoD IACs transforming the IAC program into three consolidated basic centers of operation (BCOs): DSIAC, Homeland Defense Information Analysis Center (HDIAC), and Cyber Security and Information Systems Information Analysis Center (CSIAC). The core management and operational responsibilities for six legacy IACs (AMMTIAC, CPIAC, RIAC, SENSIAC, SURVIAC, and WSTIAC)* were officially transitioned to DSIAC on July 1, 2014. In addition, DSIAC is responsible for supporting the three new technical areas: Autonomous Systems, Directed Energy, and Non-lethal Weapons.

DSIAC serves as the U.S. national clearinghouse for worldwide scientific and technical information for weapon systems; survivability and vulnerability; reliability, maintainability, quality, supportability, interoperability (RMQSI); advanced materials; military sensing; energetics; directed energy; and non-lethal weapons. As such, DSIAC collects, analyzes, synthesizes, and disseminates related technical information and data for each of these focus areas. These efforts facilitate a collaboration between scientists and engineers in the Defense Systems community while promoting improved productivity by fully leveraging this same community's respective knowledge base. DSIAC also uses information obtained to generate scientific and technical products; including databases, technology assessments, training materials, and various technical reports.

State-of-the-Art Reports (SOARs) – one of DSIAC's information products – provide in-depth analysis of current technologies, evaluate and synthesize the latest technical information available, and provide a comprehensive assessment of technologies related to the Defense Systems's technical focus areas. Specific topic areas are established from collaboration with the greater Defense Systems community and vetted with DTIC to ensure the value-added contributions to warfighter needs.

DSIAC's mailing address:

DSIAC
4695 Millennium Drive
Belcamp, MD 21017-1505
Telephone: (443) 360-4600

**AMMTIAC = Advanced Materials and Manufacturing Technical Information Analysis Center*
CPIAC = Chemical Propulsion Information Analysis Center
RIAC = RMQSI Information Analysis Center
SENSIAC = Military Sensing Information Analysis Center
SURVIAC = Survivability Information Analysis Center
WSTIAC = Weapons Systems Technology Information Analysis Center

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

The 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 the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the 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
05-2018

2. REPORT TYPE
State-of-the-Art Report

3. DATES COVERED

4. TITLE AND SUBTITLE
Unmanned Aerial Systems (UAS) for Intelligence, Surveillance, and Reconnaissance (ISR)

5a. CONTRACT NUMBER
FA8075-14-D-0001

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Matthew Harbaugh

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) AND ADRESS(ES)
DSIAC
4695 Millennium Drive
Belcamp, MD 21017-1505

8. PERFORMING ORGANIZATION REPORT NUMBER
DSIAC-2018-0849

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Defense Technical Information Center (DTIC)
8725 John J. Kingman Road
Fort Belvoir, VA 22060

10. SPONSOR/MONITOR'S ACRONYM(S)
DTIC

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/ AVAILABILITY STATEMENT
DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

13. ABSTRACT
This report summarizes information about various unmanned aerial systems (UAS) platforms currently used for intelligence, surveillance, and reconnaissance (ISR). The applicability of various UAS platforms and sensor payloads for specific types of missions is discussed, and an overview of the challenges of using UAS for ISR in specific environments is provided. Finally, some of the emerging capabilities of unmanned systems and how these systems may be used for ISR in the future are considered.

14. SUBJECT TERMS
unmanned systems, UAV, UAS, drones, PED systems, sensor payloads, ISR, data exploitation, defended airspace, GPS-denied, counter-UAS, swarm, manned-unmanned teaming

15. SECURITY CLASSIFICATION OF:

a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED

16. LIMITATION OF ABSTRACT
UU

17. NUMBER OF PAGES
44

18a. NAME OF RESPONSIBLE PERSON
Vincent "Ted" Welsh

18b. TELEPHONE NUMBER *(include area code)*
443-360-4600

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39.18

THE AUTHOR

MATTHEW HARBAUGH

Matt Harbaugh serves as the Executive Director of the West Virginia University Innovation Corporation, an independent, non-profit, applied research corporation that partners with government and industry to develop, test, and commercialize new technologies. Matt's prior experience includes serving as the CEO of a Carnegie-Mellon University software spinout that was acquired by Facebook and spending nearly a decade at Innovation Works, Inc., one of the most active seed-stage venture capital funds in the United States, where he served as Chief Investment Officer.

ABSTRACT

This report summarizes information about various unmanned aerial systems (UAS) platforms currently used for intelligence, surveillance, and reconnaissance (ISR). The applicability of various UAS platforms and sensor payloads for specific types of missions is discussed, and an overview of the challenges of using UAS for ISR in specific environments is provided. Finally, some of the emerging capabilities of unmanned systems and how these systems may be used for ISR in the future are considered.

CONTENTS

CONTENTS, *continued*

FIGURES

CONTENTS, *continued*

TABLES

SECTION 01

Introduction

This state-of-the-art report (SOAR) provides an overview of the use of unmanned aerial systems (UAS) platforms and technologies for intelligence, surveillance, and reconnaissance (ISR).

Recent advancements in information technology and reductions in cost have greatly increased the utility of UAS for ISR and other missions and have presented new opportunities to deploy UAS for missions that were not previously feasible. However, with the increased use of UAS has also come new threats and challenges driven by the growing reliance upon such systems to collect mission-critical information and the increased use of UAS by both friendly forces and enemies.

The challenges presented by the increased use of UAS are both technical and strategic. Technical challenges include the ability to counter cyber threats and the challenge of processing the enormous amount of data produced by UAS; strategic challenges include the question of how best to use UAS in dynamic and contested environments.

To address current challenges and exploit new technical capabilities, several exciting areas of UAS development are currently being pursued by military and civilian innovators. Among these areas is the development of multi-UAS systems, such as the Smart Warfighting Array or Reconfigurable Modules (SWARM), which are quickly becoming a reality, as described further in this report.

This Page Intentionally Left Blank

SECTION 02

Advantages of Using UAS in ISR Missions

Over the past 15 years, the U.S. military has increasingly come to depend on UAS as a primary method of gathering data for ISR missions. The use of UAS for ISR has many advantages: UAS are generally less expensive than manned aircraft; they can be deployed for very long missions without being limited by the endurance of human aircrews; and they can operate without putting a pilot at risk of injury, capture, or death [1].

UAS are used to collect current data on enemy terrain, organization, and infrastructure and also to support adaptive, real-time planning, including monitoring enemy centers of gravity, capabilities, and offensive and defensive positions, as well as assessing battle damage after the fact [2].

UAS are particularly useful as part of ongoing U.S. counterterrorism operations in which they are used to monitor large geographic areas for suspected terrorists, insurgents, and militants. In addition, in higher-intensity operations, the Air Force's unmanned aircraft can increase the rate at which ground targets can be detected and identified [1].

In June 2016, the Defense Science Board released a study on autonomous systems, including UAS, and established the following categories of the factors and circumstances under which autonomy can most benefit DoD missions:

- Rapid decision-making;
- High heterogeneity and/or volume of data;
- Intermittent communications;
- High complexity of coordinated action;
- Danger of mission;
- High persistence or endurance [3].

All of these factors potentially exist in ISR missions, making UAS especially well-suited for ISR. It is no surprise, therefore, that UAS have become some of the military's most valuable tools for gathering and exploiting data.

This Page Intentionally Left Blank

SECTION 03

Types of UAS ISR Missions

3.1 BROAD-AREA MAPPING AND SURVEILLANCE

Because they can loiter for long durations at high altitudes, UAS have proven to be valuable tools for wide-area surveillance over geographic areas of interest. Cruising at extremely high altitudes, a high-altitude long-endurance (HALE) UAS such as the RQ-4 Global Hawk can survey large geographic areas with pinpoint accuracy, giving military decision-makers real-time information regarding enemy location, resources, and personnel [4].

3.2 TARGET TRACKING

Another common use of HALE UAS platforms is for identification and tracking of targets of interest. Using specialized sensors and machine learning software (see Sections 7 and 8), a HALE unmanned system can track targets of interest while loitering overhead during the day or night and in any weather condition.

3.3 CHEMICAL, BIOLOGICAL, RADIOLOGICAL, NUCLEAR, AND EXPLOSIVES (CBRNE) SENSING

When used for CBRNE detection, a UAS is equipped with specialized CBRNE sensors that can detect explosives, radiation, chemical, and biological hazards from afar. The use of UAS for CBRNE missions enables commanders to reduce risks of human loss and permanent health damages to first responders and soldiers in potentially dangerous or contaminated environments [5].

3.4 OVER-THE-HILL RECONNAISSANCE

At the opposite end of the ISR mission spectrum, UAS are also beginning to be used for short-distance, near-to-earth surveillance to see “over the next hill” or “around the corner,” providing real-time information to troops about conditions and threats in their immediate area.

This Page Intentionally Left Blank

SECTION 04

Overview of Current UAS Technologies

The varying goals and conditions under which ISR missions are performed often dictate specific combinations of (1) UAS platforms; (2) surveillance sensor payloads; and (3) processing, exploitation, and dissemination (PED) methods.

1. **UAS Platforms** range from small (or nano), hand-launched systems that operate only within line-of-sight, to long-range high-altitude systems that can loiter over a specific geographic area and/or track a specific target for an extended period of time.
2. **Sensor Payloads** can include visual, infrared (IR), radio frequency (RF), and other types of signal measurements. The update rate of the surveillance can range from a single snapshot to a high-speed motion picture.
3. **PED Systems** encompass the various methodologies used to distill and communicate actionable intelligence from the vast amount of data collected by the sensors on the UAS. These systems enable collected data to be used in real time, delayed a few minutes or hours, or transmitted after completion of the mission [6].

For any given ISR mission, there is likely an optimal combination of UAS platform, sensor, and PED system that will yield the highest-quality data and most useful intelligence. Some analysts consider the choice of platform-sensor-PED combination as a matter of selecting the right tool for a specific job. While this choice has historically been dictated primarily by considering the size, weight, and power (SWaP) limitations of each UAS platform, the Air Force has recently stated that, as the type and capabilities of platforms and sensor technologies have expanded, the Air Force is now first asking what type of data is desired, and then working backward to identify appropriate sensors, and finally to the choice of UAS platform [7].

The following sections describe the various types of platforms, sensors, and PED systems currently used by the U.S. military.

This Page Intentionally Left Blank

SECTION 05

UAS Group Characterization

The Joint Unmanned Aircraft System (JUAS) Center of Excellence, with the assistance of the Services/U.S. Special Operations Command (USSOCOM), developed UAS categories applicable to all current and future DoD UAS. The categories are based upon weight [2], altitude, and speed, as shown in Table 5-1.

If a UAS has characteristics in multiple classes, it is classified as a member of the largest class in which a characteristic is found. For example, if a UAS has two characteristics in Group 1 and one characteristic in Group 2, it is classified as Group 2 [2].

Group 1 UAS are back-packable and used for "over-the-hill" ISR. With manual operator control or via a preprogrammed route of flight, they use onboard sensors and communications equipment to gather and transmit imagery of the objective area to the operator or ground control station [8]. The advantages of Group 1 UAS are that they are lightweight, man-portable, and have modular sensor payloads and a small logistical footprint [2]. Group 1 UAS limitations are that they need to operate within the operator's line of sight at low altitudes and have limited endurance [2].

Group 2 UAS typically are launched by catapult in support of ISR missions of brigade-level and lower units. They usually do not require an improved runway [2]. The advantages of Group 2 UAS include greater power, endurance, and payload capability than Group 1 UAS. Disadvantages include limited range and endurance and a greater logistical footprint compared to Group 1 UAS [2].

Group 3 UAS operate at medium altitudes and usually have medium to long range and endurance. They typically operate from unimproved areas and may not require an improved runway. Advantages include a broader selection of sensors, as well as the capability of carrying weapons. The Group 3 UAS logistical footprint is larger than that of Groups 1 or 2, and Group 3 UAS typically require ground support equipment [2].

Table 5-1. UAS Categorization

Category	Size	Maximum Gross Takeoff Weight (MGTW) (lb)	Normal Operating Altitude (ft)	Airspeed (kn)
Group 1	Small	0–20	<1,200 AGL	<100
Group 2	Medium	21–55	<3,500	<250
Group 3	Large	<1,320	<18,000 MSL	<250
Group 4	Larger	>1,320	<18,000 MSL	Any airspeed
Group 5	Largest	>1,320	>18,000	Any airspeed

AGL = Above-Ground Level; MSL = Mean Sea Level

Group 4 UAS are relatively large systems, operate at medium to high altitudes, and have extended range and endurance. They normally require improved areas/runways for launch and recovery, and their logistics footprint is similar to that of manned aircraft of similar size [2].

Group 5 UAS are the largest systems, operate in the medium- to high-altitude environment, and typically have the greatest range/endurance and airspeed. They perform specialized missions, including broad area surveillance and target tracking, and can carry a wide range of sensor payloads, weapons, and supplies. Group 5 UAS have stringent airspace requirements, require improved areas for launch and recovery, and have logistics footprints that are similar to those of similarly sized manned aircraft [2].

As of January 2014, the total number of UAS in use by the U.S. military was approximately 10,000, with the vast majority being small UAVs, including 7,362 Ravens; 990 Wasps; 1,137 Pumas; and 306 T-Hawks (Figure 5-1) [9].

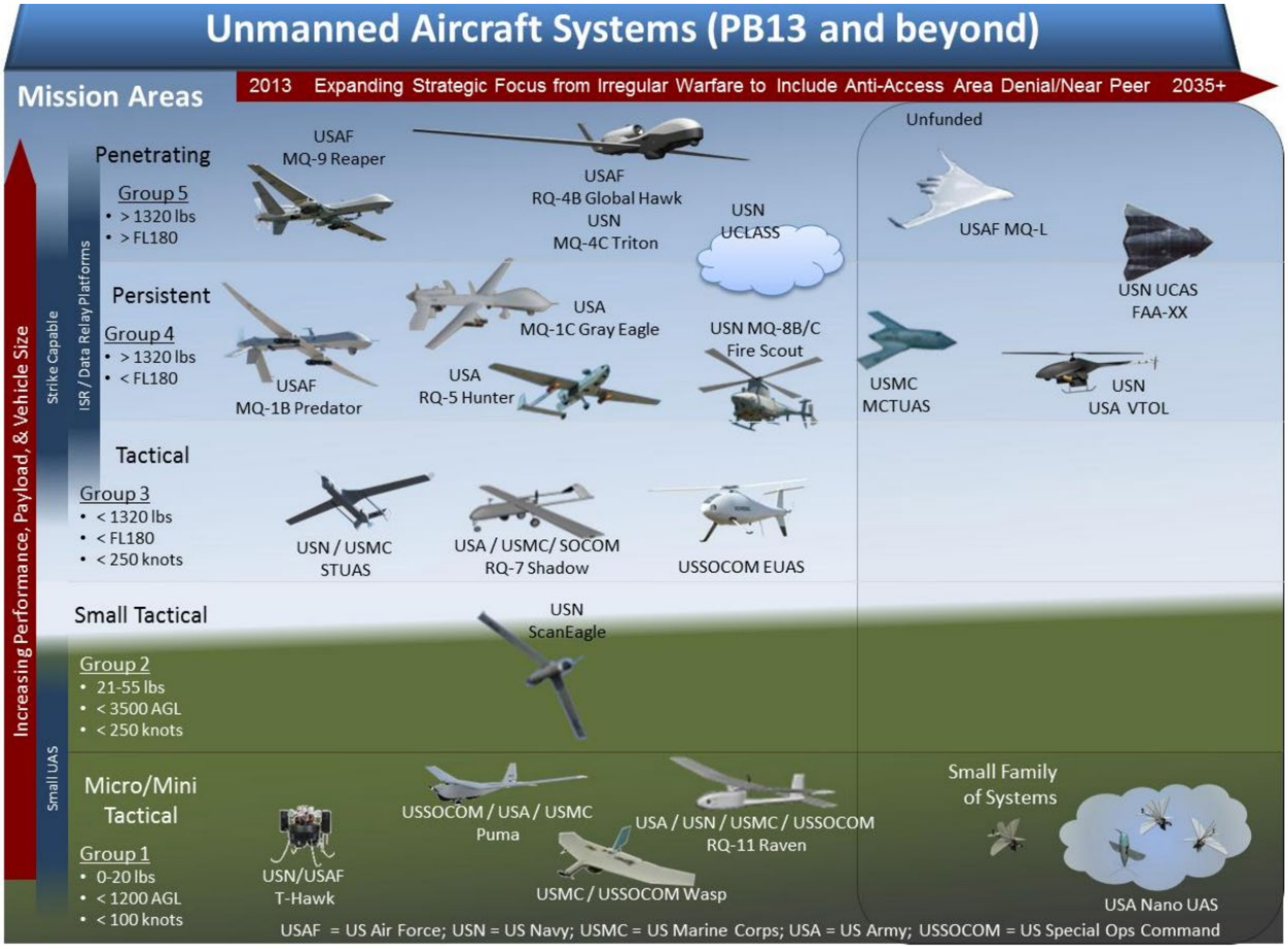

Figure 5-1. Examples of UAS in each performance group *(Source: DoD).*

SECTION 06

UAS Platforms Deployed, by Branch

Figure 6-1. The Raven is a self-contained, rucksack-portable UAS that is remotely operated and used in support of combat battalion-level and below operations and other combat support units *(Source: U.S. Marine Corps)*.

To meet the variety of requirements, missions, and operations of the United States military, more than 20 UAS platforms are currently in service, with new platforms currently under development and testing. The following sections and Table 2 provide a brief overview of this diverse portfolio.

6.1 U.S. ARMY

The Army employs UAS for Joint ISR missions and for reconnaissance, surveillance, and target acquisition (RSTA) missions. Army operations require continuous surveillance and reconnaissance to provide situational awareness and timely warning of an imminent or impending threat, making unmanned aerial vehicles (UAVs) an ideal tool [2]. As of September 2013, the Army had a fleet of more than 6,200 UAS (55 percent of the Army's total fleet of aircraft), primarily in the Group 1 UAS category – Ravens (Figure 6-1), Wasps, Pumas, and T-Hawks. At the time, this number was expected to grow to approximately 10,000 UAS, representing more than 75 percent of the Army's total aviation assets [6].

In January 2017, the Army issued a Request for Information (RFI) for industry and academia to submit information related to very small/nano, portable, unmanned air vehicles that could be used as Soldier-Borne Sensors (SBS) to collect over-the-hill ISR data for use at the squad level, as seen in Figure 6-2. Through this SBS program, the Army is currently evaluating a variety of solutions for such applica-

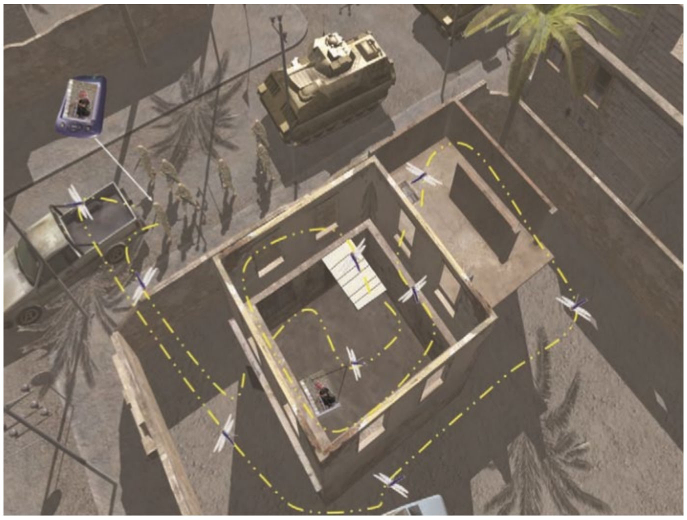

Figure 6-2. The Army wants to use nano-UAS to reconnoiter the interior of structures prior to soldiers entering them. The nano-UAS will be controlled by small handheld or soldier-worn devices *(Source: U.S. Army Roadmap for UAS 2010-2035)*.

Figure 6-3. The MQ-9 Reaper is larger and more heavily armed than the MQ-1 Predator and is used for attack and IRS missions *(Source: U.S. Air Force Photo / Lt. Col. Leslie Pratt)*.

tions. Requirements include weight of 150 grams (about 5 ounces), 15-minute flight time, and wind tolerance of up to 15 knots [10].

6.2 U.S. AIR FORCE

In contrast to the Army's preference for small UAS, the Air Force tends to employ larger, longer-duration, high-altitude UAS, with a goal of collecting a large amount of data over a broader geography, and for tracking specific targets over a longer period of time. The Air Force's first widely used UAV, the MQ-1 Predator, was deployed in response to the need for high-quality ISR data. As technology has progressed, the Air Force has shifted to the MQ-9 Reaper (Figure 6-3), a more advanced version of the Predator with longer endurance and better sensors [7].

According to the Congressional Budget Office, in 2017 the Air Force fielded 75 UAS squadrons, consisting of 110 MQ-1 Predators, 36 RQ-4 Global Hawks, and 279 MQ-9 Reapers. The number of Air Force UAS squadrons is projected to decline from 75 to 30 by 2021 as the fleet of MQ-1 Predators is retired. In addition to those aircraft, the Air Force has acknowledged that it also operates at least one other type of UAS, a stealth platform called the RQ-170 Sentinel, the quantities and characteristics of which remain classified [1].

6.3 U.S. NAVY AND MARINE CORPS

The Navy currently employs small UAS Carrier-Launched Airborne Surveillance and Strike System (UCLASS) shipboard tactical vehicles for surveillance and weapons ordinance delivery. These vehicles include Boeing's ScanEagle and RQ-21A Blackjack, both of which are launched from ships using a rail system and are recovered using a sky hook.

The Navy also uses Northrop Grumman's larger Group 5 MQ-4C Triton long-range, long-endurance UAS (Figure 6-4) for real-time ISR missions over vast ocean and coastal regions. In December 2017, the U.S. Navy ordered its seventh, eighth, and ninth Tritons, with plans to eventually deploy 68 such aircraft. These plans demonstrate that the Navy expects the Triton to be a crucial component of its strategy for conducting surveillance of surface ship and submarine traffic around the globe [11].

The Navy and Marine Corps also both use a portfolio of smaller, hand-launched UAS vehicles consisting of the RQ-11B Raven, RQ-12A Wasp, and

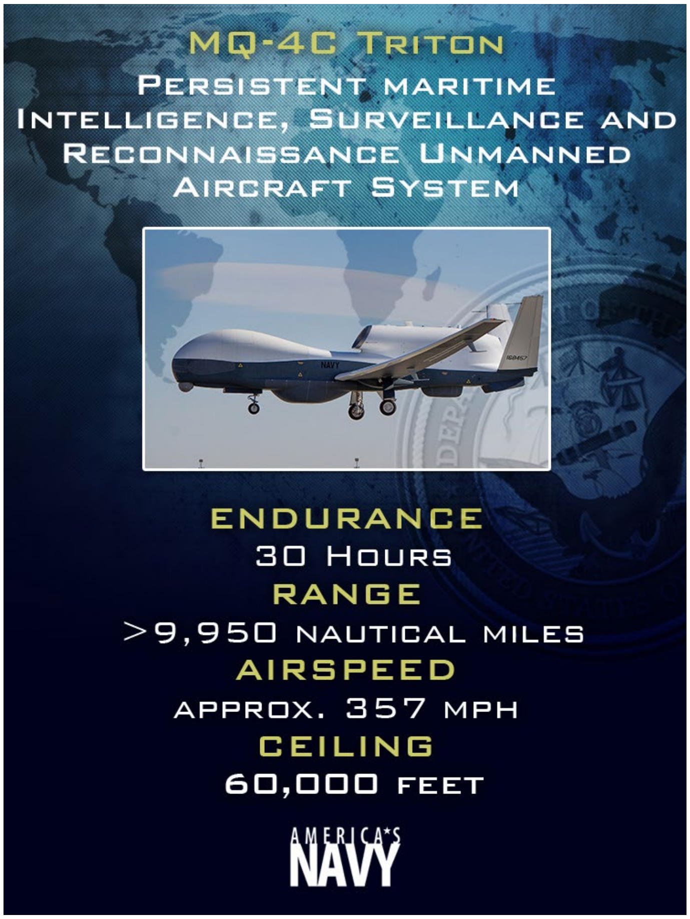

Figure 6-4. MQ-4C Triton system capabilities *(Source: U.S. Navy).*

RQ-20A Puma (Figure 6-5). Together, they form the Small Unit Remote Scouting System (SURSS) program of record. Non-program-of-record systems within the portfolio consist of SkyRanger and InstantEye vertical take-off and lift systems as well as the PD-100 Black Hornet micro UAS [8].

Figure 6-5. A Puma AE UAS is hand-launched from a Riverine Command Boat (RCB) at sea *(Source: U.S. Navy photo by Mass Communication Specialist 1st Class Peter Lewis).*

It is expected that both the Navy and Marines will increasingly shift their aircraft assets toward optionally manned and unmanned aircraft for ISR in coming years, resulting in a projected increase in naval and marine aircraft from 3,700 vehicles in 2013 to 4,800 by 2035, including up to 2,500 UAS [6]. Table 6-1 shows the U.S. military's currently deployed UAS and those being tested. Note that additional non-program-of-record and commercial-off-the-shelf (COTS) UAS platforms are likely under evaluation by the DoD. Table 6-1 is not intended to be an exhaustive list of non-program-of-record or COTS UAS systems.

Table 6-1. UAS Platforms Currently Deployed or Being Tested by the U.S. Military [12]

Name	Company	Used by	Group	Specifications	Range	Ceiling	Endurance
PD-100 Black Hornet Nano	Prox Dynamics	Navy, USMC, SOCOM	1	100-mm length; 120-mm rotor span; 16 gm	1 km	Close-to-Earth	25 min
Snipe Nano	AeroVironment	N/A	1	140 gm	1 km	Close-to-Earth	15 min
InstantEye	PSI Tactical Robotics	Army, USMC (testing)	1	249.5 gm	1 km	Close-to-Earth	15 min
Perdix	MIT Lincoln Labs	Navy (testing)	1	2.6-in. length; 11.8-in. wingspan; 290 gm	N/A	Close-to-Earth	20 min

Name	Company	Used by	Group	Specifications	Range	Ceiling	Endurance
RQ-12 Wasp	AeroVironment	Army, USAF, USMC	1	2.5-ft length; 3.3-ft wingspan; 2.85 lb	5 km	500 ft	50 min
RQ-20 Puma	AeroVironment	Army, USMC, USAF, SOCOM	1	4-ft 7-in. length; 9-ft 2-in. wingspan; 14 lb	20 km	500 ft	3 h
SkyRanger	Aeron Labs	Navy, USMC	1	20-in. length folded; 5.3 lb	5 km	1,500 ft	50 min
RQ-16 T-Hawk	Honeywell	Army, Navy	1	20 lb; vertical take-off and landing	6 NM	10,500 ft	40 min
RQ-11 Raven	AeroVironment	Army, USMC, SOCOM	1	4-ft 7-in. length; 4-ft 6-in. wingspan; 4.2 lb	10 km	14,760 ft	90 min
Stalker	Lockheed Martin	SOCOM	1	10-ft wingspan; 14.5 lb	20 km	15,000 ft	2 h
MQ-19 Aerosonde	AAI	Navy, USMC, USAF, SOCOM	2	5-ft 8-in. length; 9-ft 8-in. wingspan; 22 lb	150 km	15,000 ft	14 h
ScanEagle	Boeing (In-situ)	Navy, USMC	2	4-ft 6-in. length; 10.2-ft wingspan; 44 lb	100 km	19,500 ft	28 h
RQ-7 Shadow	AAI	Army & USMC	3	11-ft length; 13-ft wingspan; 185.2 lb	109 km	14,000 ft	7 h
RQ-21A Blackjack	Boeing (In-situ)	Navy, USMC	3	8.2-ft length; 15.7-ft wingspan; 135 lb	102 km	20,000 ft	16 h
MQ-1 Predator	General Atomics	USAF	4	27-ft length; 55-ft wingspan; 1,130 lb	770 NM	25,000 ft	26 h
MQ-8B Fire Scout unmanned helicopter	Northrop Grumman	Navy	4	23.95-ft length; 27.5-ft rotor diameter; 3,150 lb	596 NM	12,500 ft	7.75 h
MQ-8C Fire Scout unmanned helicopter	Northrop Grumman	Navy	4	41.4-ft length; 35-ft rotor diameter; 6,000 lb	1,227 NM	16,000 ft	12 h
MQ-1C Gray Eagle	General Atomics	Army	4	28-ft length; 56-ft wingspan; 3,600 lb	2,500 NM	29,000 ft	27 h
Coyote	Raytheon	Army, USAF	5	36-in. length; 58-in. wingspan; 13 lb	50 NM	30,000 ft	60 min
MQ-9 Reaper	General Atomics	USAF	5	36-ft length; 66-ft wingspan; 4,900 lb	1,500 NM	50,000 ft	30 h

Name	Company	Used by	Group	Specifications	Range	Ceiling	Endurance
MQ-4C Triton	Northrop Grumman	Navy	5	47.6-ft length; 131-ft wingspan; 32,250 lb	8,200 NM	55,000 ft	24 h
RQ-4 Global Hawk	Northrop Grumman	USAF	5	47.6-ft length; 131-ft wingspan; 14,950 lb	12,300 NM	60,000 ft	33 h
RQ-170 Sentinel	Lockheed Martin	USAF	N/A	N/A	N/A	N/A	N/A
RQ-180	Northrop Grumman	USAF	N/A	N/A	N/A	N/A	N/A

This Page Intentionally Left Blank

SECTION 07

UAS Sensor Payloads

7.1 ELECTRO-OPTICAL (EO) VIDEO CAMERAS

The primary data collection instruments used for UAS ISR are imaging sensors, including EO cameras for capturing still images and full motion video (FMV) in daylight [13]. FMV provides an on-demand, close-up view of the combat zone that would not otherwise be possible. It provides the military with "pattern of life" imagery of the battle scene, tracking high-value targets in real time while reducing collateral damage and enabling commanders to make decisions and execute missions from a safe distance without endangering the lives of their troops [14].

7.2 INFRARED (IR) IMAGING SENSORS

To capture FMV or still images in low-light conditions or darkness, UAS employ IR sensors that can record images that cannot be seen using visible light, but are visible in the IR spectrum.

7.3 SYNTHETIC APERTURE RADAR (SAR) IMAGING SENSORS

When visibility levels prohibit the use of either EO cameras or IR sensors, SAR provides an all-weather sensor capable of supplying photographic-like images in daylight or at night and in all weather conditions. Compared to real aperture radar, SAR increases image resolution by synthetically increasing the antenna's size or aperture [13]. SAR complements EO cameras and other optical imaging capabilities because it is not constrained by the time of day or atmospheric conditions [2].

7.4 MULTISPECTRAL IMAGERY (MSI) AND HYPERSPECTRAL IMAGERY (HSI) SENSORS

To complement the EO and IR sensors of UAS, MSI and HSI sensors are also available. Historically associated with satellites, advancements in MSI and HSI technology have made terrain analysis, high-resolution map imagery, and three-dimensional topographic models from UAVs possible [13]. Figure 7-1 shows a U.S. Department of Agriculture (USDA) UAS equipped with an MSI camera.

Figure 7-1. Onyxstar HYDRA-12 UAV with embedded hyperspectral camera for agricultural research *(Source: Cargyrak [CC BY-SA 4.0], from Wikimedia Commons).*

7.5 MOVING TARGET INDICATOR (MTI)

An MTI is a radar presentation that shows only targets that are in motion. With an MTI, signals from stationary objects are subtracted from the return signal, thus isolating only the moving targets [2].

7.6 LIGHT DETECTION AND RANGING (LIDAR)

LIDAR may be used for explosive hazards detection and for weather prediction. For example, Doppler LIDAR provides data such as cloud density, wind speed, and real-time vertical wind profiles. In addition, a multispectral LIDAR payload can detect chemical effluents that are associated with chemical and biological warfare agents [2].

7.7 LASER RADAR (LADAR)

LADAR performs three-dimensional imaging and can look through cover such as trees, foliage, and camouflage. It produces a virtual picture that can reliably identify targets that would otherwise be hidden, such as vehicles, air defense systems, and explosive hazards [2].

7.8 CHEMICAL, BIOLOGICAL, RADIOLOGICAL, NUCLEAR, AND EXPLOSIVES (CBRNE) DETECTION

Compact, active, multispectral chemical sensors are enabling the remote detection of chemicals associated with weapons [2].

7.9 SIGNALS INTELLIGENCE (SIGINT) SENSORS

Signals intelligence (SIGINT) sensors provide situational awareness and intelligence on an adversary's capabilities, status, and intentions by detecting and intercepting signals from communications and other electronic systems. Due to the classified nature of the communications, SIGINT data are often processed at a secure facility that is physically separated from the unit that is operating the UAS [2].

SECTION 08

PED Systems

With recent improvements in sensor technologies, UAS are now able to collect vast quantities of data from still-image and video cameras, radar, SIGINT, EO sensors, and other kinds of surveillance and reconnaissance equipment. The resulting massive amount of data has created new challenges for efficient data PED, i.e., the process of deriving actionable information from the data and communicating it clearly and credibly to senior leaders so that they can make command decisions [15].

Until recently, PED processes required either storing the data onboard the UAS and physically downloading it for review at the end of the mission or downloading the data files in-mission through a data link and then fusing and analyzing the data via systems on the ground. Both methods present challenges.

Onboard data storage is typically restricted by the SWaP limitations of a particular UAS, which, in turn, limits the mission duration when the UAS's onboard storage capacity is reached. Furthermore, stored data also create significant latency between data collection and analysis since operators must wait for the UAS to return to base before they can review time-sensitive data [16].

Although in-mission data transfers provide on-ground analysts with faster access to data, this method requires more power and sufficient available bandwidth to send data to the on-ground analysis team. Bandwidth limitations or intermittent communications signals may result in slow downloads of large data files, broken communications links, and increased latency that could create potential inaccuracies in intelligence between data collection and analysis [16].

In addition to the issue of how to store and transmit such a large quantity of data, the massive amount of data itself also presents a needle-in-a-haystack problem for analysts seeking actionable information; therefore, it may be desirable to use automated data analysis tools with a degree of artificial intelligence [16]. These problems are increasingly being addressed through a combination of onboard, real-time PED technology and machine learning systems. See Section 8.2 for further discussion of the use of artificial intelligence and machine learning for data analysis.

8.1 ONBOARD, REAL-TIME PED

In the past, SIGINT has been ground-based because of the sheer volume, weight, and power needed to accommodate the information systems that would otherwise be required for onboard computing in the aircraft. However, the latest CPUs, with high transistor counts in a miniaturized form factor, have been able to deliver a larger number of processing cores, expanded memory, and a host of additional functionality in a single package, enabling increased onboard processing of data [17].

Current solutions enable analysts to access information onboard the UAS itself with data from multiple sensors fused together to create actionable intelligence. Such capabilities enable analysts to tap the most important and relevant events, investigate the signature of objects in different spectral bands, and map results geographically to explore relevant events in the present as well as the past, thereby providing actionable information for intelligence gathering and time-sensitive targeting processes [18].

An example of an onboard, real-time, multisensor PED system is the General Atomics Lynx multimode radar system, which enables advanced ISR in a radar sensor. Lynx is used to conduct ISR by the U.S. Air Force on Reaper and Predator UAS, and by the U.S. Army on Gray Eagle UAS. Lynx employs full-motion "VideoSAR" technology developed by the Sandia National Laboratory, which offers continuous collection and processing of phase history data, allowing observation of slow-moving targets day or night and during inclement weather or atmospheric conditions [19]. The system also enables automatic Ground Moving Target Indication (GMTI) with very low minimum detectable velocity and precise SAR geolocation, enabling Lynx to detect both stationary and moving objects while maintaining nonstop, uninterrupted eyes on the target [20, 21].

8.2 DATA EXPLOITATION USING ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

To rapidly analyze the massive amounts of images and data collected by UAS, military and civilian analysts are increasingly using machine learning, a type of artificial intelligence that spots patterns in massive data sets, to identify trends and derive meaning from raw information. Such software incrementally enriches its database to describe relevant context, environment, threats, user inputs, and mission objectives. It records new input, then integrates and generalizes past experience to make decisions that are informed by the accumulated data and experience. With machine-learning algorithms, more data are usually better, and the learning algorithms are adept at finding useful data and ignoring that which is irrelevant [3].

In April 2017, the Pentagon announced the creation of an Algorithmic Warfare Cross-Functional Team (AWCFT), called "Project Maven," through which it will use machine-learning algorithms to hunt for Islamic State militants in Iraq and Syria by turning countless hours of aerial surveillance video into actionable intelligence [22]. The Pentagon determined that due to the large amount of data collected by UAS, analysts have been forced to spend too much time on basic tasks such as sorting, labeling, and describing. Project Maven is intended to allow these analysts to instead focus on higher value tasks, such as contextualization and red teaming [23].

According to the memorandum announcing the creation of Project Maven, this new team will accomplish the following:

- Organize a data-labeling effort, and develop, acquire, and/or modify algorithms to accomplish key tasks;
- Identify required computational resources and identify a path to fielding that infrastructure; and
- Integrate algorithmic-based technology with programs of record in 90-day sprints [24].

The effort currently focuses on object detection, classification, and alerts from FMV sensor data from the MQ-9 Reaper and MQ-19 Aerosonde UAS platforms [23]. It is expected that soon artificial intelligence will increasingly be integrated into PED systems using algorithms to help users select details or spot trends in the imagery being collected by UAS. In so doing, the algorithms will help operators better understand what they are seeing, why it is there, and what it is likely to do [7].

09

Challenges of Using UAS for ISR

Whereas there has been a dramatic increase in the use of UAS for ISR in the past 15 years, the increased reliance on unmanned systems has also brought new challenges. These challenges are both strategic and technical, including the vulnerability of UAS to cyber attacks, combatting an adversary's counter-UAS air defenses, and operating in GPS-denied environments.

9.1 VULNERABILITY TO CYBER ATTACK

UAS are highly exposed, linked, complex pieces of hardware with high strategic and economic value [25]. Furthermore, because UAS are dominated by software and rely on communications networks, ensuring the security of electronics and communications in UAS systems is of paramount importance for their safe and reliable use in ISR missions.

Cyber attacks can disrupt the command and control of the UAS and prevent the UAS from observing specific ground-based locations by changing navigation waypoints, embedding errors in the GPS, or altering a UAS camera direction. Alternatively, cyber attacks can disrupt data being sent to the ground for PED, thereby disabling ground-based interpretation of streaming video [26]. Such potential vulnerabilities of UAS platforms have led to significant research into methods of defending UAS against cyber attacks and have created an urgency to develop standards and frameworks for assurance of reliability and resilience to malicious interference [27].

In response, the Defense Advanced Research Projects Agency (DARPA) in 2012 created a program to develop High Assurance Cyber Military Systems (HACMS), intended to protect systems from cyber hacking and hijacking [28]. Rather than patching systems after a vulnerability is discovered, DARPA created the HACMS program to develop a clean-slate, mathematically based approach for building secure software for network-enabled embedded systems such as the command-and-control and ISR systems on UAS [28, 29].

Recently, under DARPA's HACMS program, a team led by Rockwell Collins demonstrated new tools for building UAS software that is provably secure against many classes of cyber attack. The team developed system architecture models, software components for mission and control functions, and operating system software, all of which are mathematically analyzed to ensure key security properties. In 2017, the prototype system was tested on a research quadcopter and then transitioned to Boeing's Unmanned Little Bird (ULB) helicopter for demonstration [30].

In addition, in 2014, a team of researchers from the University of Virginia and the Georgia Tech Research Institute demonstrated effective defense against cyber attacks on UAS using a novel "system-aware" approach that they developed. Using this approach, the team could defend against embedded Trojan horses within the UAS and from third-party locations using the aircraft's air-ground communication system to access onboard electronic systems. Technical results from the flight tests were positive, demonstrating that the system-aware concept can significantly improve the cybersecurity of physical systems [26].

However, despite these cybersecurity projects, cyber threats continue to remain a challenge for the use of UAS in the field, especially with respect to low-cost COTS UAV systems that warfighters may use as quick-and-easy ISR solutions. For example, in August 2017, the Army issued a memorandum ordering that soldiers discontinue the use of UAS manufactured by DJI Unmanned Aircraft Systems due to "cyber vulnerabilities." The directive stated the following:

> *DJI Unmanned Aircraft Systems (UAS) products are the most widely used non-program of record commercial off-the-shelf UAS employed by the Army. The Army Aviation Engineering Directorate has issued over 300 separate Airworthiness Releases for DJI products in support of multiple organizations with a variety of mission sets. Due to increased awareness of cyber vulnerabilities associated with DJI products, it is directed that the U.S. Army halt use of all DJI products. This guidance applies to all DJI UAS and any system that employs DJI electrical components or software including, but not limited to, flight computers, cameras, radios, batteries, speed controllers, GPS units, handheld control stations, or devices with DJI software applications installed [31].*

After the Army directive, DJI released an enhanced privacy mode to address the Army's concerns [32]. Despite the enhancement, however, as of January 2018, the Army's ban remained, and the episode continues to serve as a clear example of the Department of Defense's (DoD's) recognition of the difficulty and importance of cybersecurity challenges when using UAS for ISR.

9.2 OPERATING IN DEFENDED AIRSPACE

Because UAS were designed to be relatively low-cost surveillance systems, most of the current fleet of UAS have corresponding limitations in that their airframes were designed for fairly low-performance, undemanding flight. They are not generally expected to have high speed and maneuverability or to operate in defended airspace [1]. As a result, UAS conducting ISR are vulnerable to interception and/or destruction by adversaries using a variety of methods.

For example, shoulder-launched missiles pose a significant threat to relatively slow-flying UAS conducting ISR missions. In October 2017, Houthi fighters shot down a U.S. Air Force MQ-9 Reaper drone over Yemen. While the specific method used has not been disclosed, analysts have speculated that the rebels may have employed a man-portable surface-to-air missile system [33].

In addition to the risk posed by shoulder-launched missiles, in November 2014, China highlighted its ability to destroy surveillance drones using lasers. According to an official statement from the China Academy of Engineering Physics, the Chinese-developed system has a 1.2-mile range and can bring down a UAS traveling as fast as 112 miles per hour at an altitude of up to 1,640 feet, incapacitating a drone within 5 seconds. The system can be installed on vehicles, and it reportedly had a 100% success rate in a test that involved shooting down more than 30 drones [34].

9.3 INTERFERENCE WITH CONTROL AND COMMUNICATIONS SYSTEMS

Beyond the risks posed by conventional and advanced weapons, UAS conducting ISR are also vulnerable to electronic counter-UAS technologies due to UAS reliance on sophisticated electronic systems. These technologies can disrupt a UAS platform's controls and communications system.

In November 2017, the Russian Defense Ministry revealed that it had formed at least 20 units to combat unmanned aircraft. Russian anti-drone units are equipped with automated radio interference systems that are reportedly able to detect and jam radio signals and interfere with UAV mission systems within a radius of up to 18 miles [35].

According to a press release from the Russian Defense Ministry, the Russian system is being used in training exercises to determine the frequency of control and transmission of information from UAVs and suppress communication channels by radio interference. In addition, these training exercises also involved intercepting control of and landing UAVs to seize reconnaissance information [35].

9.4 NAVIGATING IN GPS-DENIED ENVIRONMENTS

A further challenge for UAS conducting ISR missions is the difficulty of operating in Global Positioning System (GPS)- and communications-denied environments, such as inside a building, in urban canyons, underground, or under the forest canopy. GPS and communications can also become denied by weather events or by jamming or spoofing tactics by the enemy. In these situations, the UAS must use other sensors to navigate, such as machine vision systems, which may, in turn, generate uncertainty about its exact location. As a result, the U.S. military is pursuing a range of initiatives to bolster wayfinding for UAS that become cut off from the usual means of guidance [36].

DARPA is exploring high-resolution, GPS-independent positioning, navigation, and precision timing systems that will allow for continued operations in a GPS-jammed environment [37]. One accepted industry standard for precision timing is the Institute of Electrical and Electronics Engineers (IEEE) 1588 precision time protocol (PTP), which helps synchronize clocks throughout a computer network. It is designed for systems that require a higher degree of accuracy beyond that which is attainable using Network Time Protocol (NTP), as well as for situations in which GPS signals are inaccessible. Consequently, IEEE 1588/PTP is an increasing requirement for unmanned vehicle navigation in areas where signals from GPS satellites are jammed or otherwise denied [38].

To further address navigation issues in GPS- and communications-denied environments, DARPA's Fast Lightweight Autonomy (FLA) program seeks to develop and test algorithms that will increase the autonomy of UAS navigation. The algorithms developed through the FLA program will reduce the amount of processing power, communications, and human intervention needed for UAVs to navigate around obstacles and accomplish other low-level tasks in a GPS- and communications-denied environment [39].

The FLA program is leading to the development of systems to enable small UAS to quickly navigate rooms, stairways, corridors, and other obstacle-filled environments without a remote pilot. The program will develop and demonstrate systems for the autonomous navigation of UAS that fly at high speeds, fit through open windows, and avoid objects within complex indoor spaces, all without communication links to outside operators and without reliance on GPS [39].

As an outcome of the DARPA FLA program, a team from the Charles Stark Draper Laboratory and the Massachusetts Institute of Technology has developed advanced vision-aided navigation techniques for UAS that do not rely on GPS, maps, or motion capture systems. The team developed and implemented unique sensor and algorithm configurations and has conducted time-trials and performance evaluations in indoor and outdoor venues. The result is a UAS system that can fly autonomously in cluttered indoor and outdoor environments without the use of GPS or any communication, at speeds of up to 45 miles per hour [40].

9.4.1 Distributed Battle Management in Communications-Denied Environments

In addition to developing non-GPS-based navigation systems, DARPA is also pursuing development of advanced Distributed Battle Management (DBM) systems to ensure the reliability of complex, coordinated operations, guided by automated decision tools in a communications-denied environment [28, 29]. In 2014, DARPA announced the DBM program to develop systems that would use automated aids to adapt to unique situations, such as coordinating multiple autonomous and/or human-directed assets in complex and contested airspace without reliable communications [41].

The development of such systems will enable the teaming of human operators with autonomous UAS squadrons that can perform complex missions without reliable communications and will enable missions in denied environments or when stealth requires a communications blackout.

After an initial phase of the DBM program in 2014–2015, which focused on developing algorithms and human-machine interfaces, DARPA awarded a Phase 2 contract to Lockheed Martin in 2016, with the goal of developing and implementing a prototype of an integrated end-to-end DBM system and to test and evaluate the system in large-scale simulations and in live-fly demonstrations [42].

10

Emerging Capabilities for UAS

Trends in UAS platforms and sensors toward smaller, more efficient systems are enabling new use cases that were previously only imagined as science fiction. Military and civilian researchers are currently working toward a vision of coordinating large groups of UAS that can work in "swarms," as well as combining the capabilities of manned and unmanned systems to accomplish tasks more effectively. Some of these efforts are described in the following sections.

10.1 SWARM

As UAS have become increasingly affordable, capable, and available, the ability of multiple small UAS to carry out swarm tactics holds tremendous promise to extend the advantages that U.S. warfighters have in ISR and other field operations [43].

A compelling ISR use case for UAS swarms is for real-time mapping of a nearby contested environment. In such an operation, using software, a swarm of inexpensive, small, low-flying drones (such as a swarm of SBS described in Section 6.1) would collectively construct a dynamic map of the nearby environment within seconds by splicing together a mosaic of images, as seen in Figure 6-1 The swarm instantaneously provides the map and/or other relevant images back to the warfighters on the ground, providing real-time situational intelligence of their immediate vicinity, as seen in Figure 10-1.

Figure 10-1. It is hoped that by 2025, nano-UAVs will collaborate to form swarms that can cover large indoor and outdoor areas *(Source: U.S. Army Roadmap for UAS 2010-2035).*

A successful January 2017 test of 100 microdrones has been the most advanced swarming demonstration to date [44]. The UAS platform used in the test was specifically produced for demonstration purposes by Massachusetts Institute of Technology's (MIT's) Lincoln Laboratory. Furthermore, according to a DoD fact sheet produced at the time of the test, the Defense Industrial Unit-Experimental (DIUx) was seeking companies capable of producing 1,000 units by the end of 2017 [45].

For swarms of slightly larger (but still "small") UAS platforms, the Office of Naval Research has developed the Low-Cost UAS Swarming Technology (LOCUST) program, which fires small UAS from a tube-based launcher. In response to this program, Raytheon developed the Coyote UAS system—a small, expendable system that is deployed from a launch tube to perform ISR missions while a host aircraft remains in safe airspace. In a series of 2016 demonstrations, more than two dozen Coyote systems successfully launched in a swarm and moved in formation, demonstrating the effectiveness of autonomous networking. The swarming capability of this platform can be applicable in multiple missions, from ISR activity to strikes against moving targets in a battlefield environment [46, 47].

10.1.1 Command and Control Systems for Swarms

As the number of UAS in a swarm increases, a persistent challenge has been the scalability of controls, i.e., enabling one operator to oversee multiple UAS and have them perform highly autonomous behaviors without direct intervention from a human operator [43].

With many UAS acting together as a swarm, the location and frequency characteristics of each UAV must be accurately tracked continuously to provide relative positioning and situational awareness. The swarm should be able to act autonomously while searching for targets and relaying the information to all swarm members [48].

Distributed Adaptive Real-Time (DART) systems are key to the safe execution of autonomous, multi-UAS missions. The software controlling these systems must be engineered for high-assurance and must satisfy guaranteed and highly critical safety requirements, such as collision avoidance, while adapting to changing conditions in dynamic and uncertain environments [49].

A team of researchers from MIT has developed a control system that uses decentralized algorithms to manage a swarm of UAS. The MIT team asserts that decentralized control algorithms are more resilient than centralized control algorithms because they do not have a single point of failure. Furthermore, their decentralized algorithms reportedly require less communications bandwidth and have lower computation costs due to the distributed way in which each UAS only needs to understand and share information on obstacle-free regions in its immediate vicinity, rather than having a centralized control algorithm that must understand the entire geography [50].

In January 2017, DARPA detailed its own future vision of a control system for large swarms of UAS through its OFFensive Swarm-Enabled Tactics (OFFSET) program. The program seeks to leverage gaming technologies such as augmented and virtual reality, as well as the use of hand gestures, touch, or haptic interfaces to command swarms. OFFSET focuses on developing complex swarm tactics and human-machine teaming for swarms that could operate in dense, urban environments in the air and on the ground [51].

10.2 MANNED-UNMANNED TEAMING (MUMT)

Another emerging UAS capability is MUMT. It is intended to combine the strengths of manned and unmanned platforms, including dismounted warfighters, manned vehicles, unmanned vehicles, sensors and robotics to achieve improved situational awareness, as well as greater lethality and improved survivability. In addition, MUMT extends sensor coverage and provides additional target acquisition and engagement capabilities [2]. A schematic of how this method can be used in the field is shown in Figure 10-2.

The Air Force's human-UAS teaming effort, "Loyal Wingman," is a project to pair unmanned Lockheed F-16s with F-35s in future battles. In April 2017, Lockheed Martin, the Air Force Research Laboratory (AFRL), U.S. Air Force Test Pilot School, and Calspan Corporation successfully conducted a 2-week demonstration of the Loyal Wingman concept that included having an F-16 autonomously leave its manned lead aircraft, conduct an air strike, then return to flying formation [52].

The Army uses manned AH-64 Apache helicopters teamed with the surveillance capabilities of either

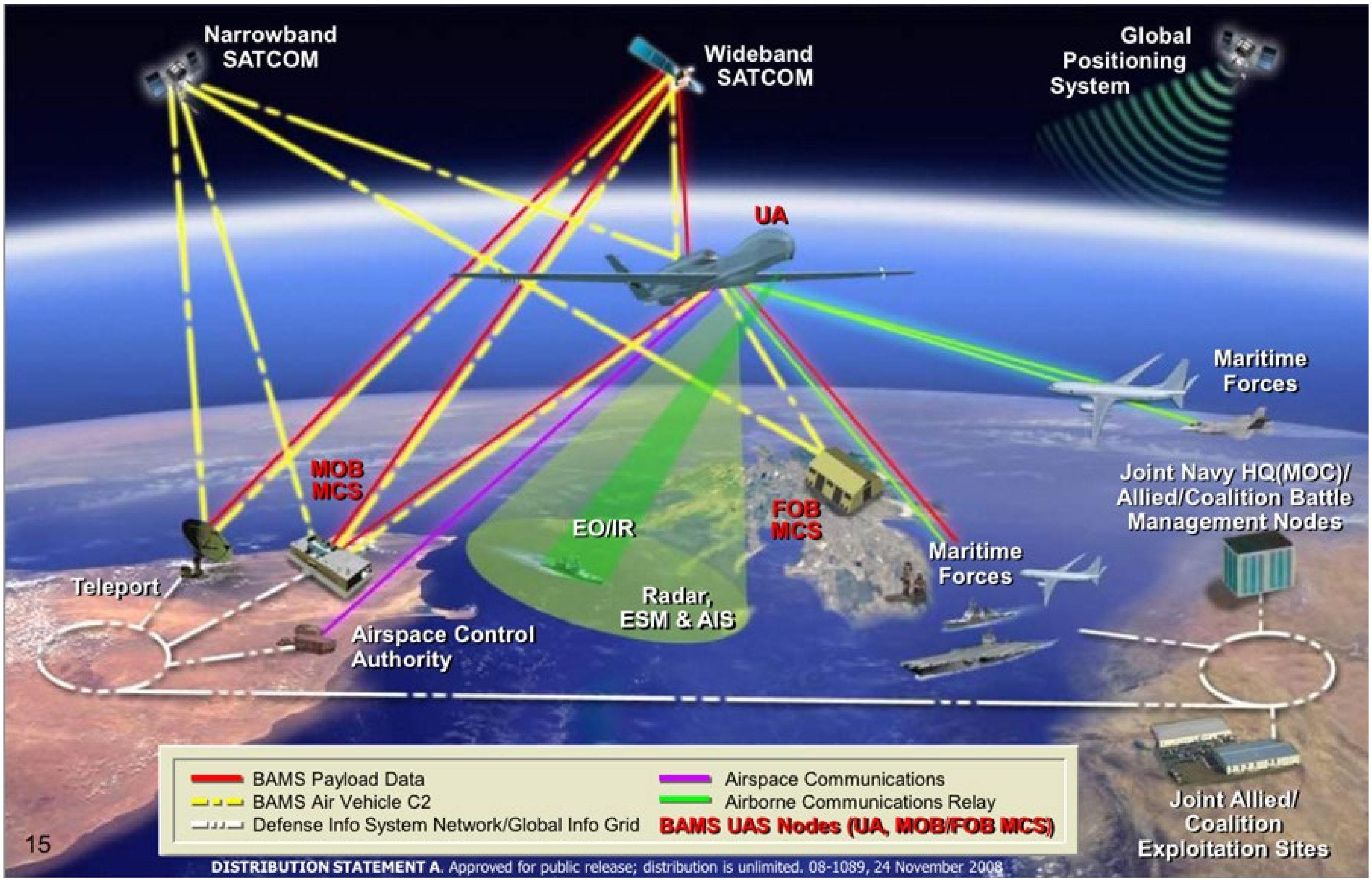

Figure 10-2. In this schematic of MUMT, the transfer of information can be received by either the manned land base or the manned aerial system, which then sends the data to ground forces. In addition, the manned aerial system pilot can use the UAS sensor even if the UAS is up to 80 km away *(Source: U.S. Navy/Naval Air Systems Command)*.

the RQ-7 Shadow or MQ-1C Gray Eagle UAS to take advantage of the UAS ISR payloads to enhance decision-making and mission effectiveness. Such teaming provides an enhanced level of safety for the manned platform. While the UAS provides the forward scouting, the warfighter remains in a protected, non-hostile area until targets are identified and enemy positions are known [53]. Furthermore, these systems enable unit commanders to increase their economy of force while expanding battlefield situational awareness and reducing operating costs [54].

This Page Intentionally Left Blank

11

Summary

Over the past 15 years, the use of UAS of all types and sizes has dramatically increased, and unmanned systems have become an indispensable component of military ISR. With an ever-expanding variety of new platforms, sensors, and information technology (IT) systems, it is likely that the ISR capabilities of UAS will only continue to grow.

Ongoing innovation is enabling the use of multiple, smaller unmanned systems and is bringing immediately actionable information closer to the warfighter. In addition, the use of artificial intelligence is allowing ISR analysts to more quickly identify and act upon the most important data.

As the use of UAS for ISR has grown, the cybersecurity of unmanned systems has emerged as an important concern that will require continual diligence to address. In addition, GPS-denied navigation, communications, and other IT systems-related challenges will continue to require military and civilian researchers to rapidly develop and deploy new technologies to ensure the safety and reliability of the growing fleet of UAS.

Despite these technical challenges, UAS are an increasingly reliable method of collecting valuable information while keeping U.S. warfighters out of harm's way. Consequently, it should be expected that UAS will likely play an increasing role in ISR operations over the coming years and decades.

This Page Intentionally Left Blank

REFERENCES

1. Congressional Budget Office, The U.S. Military's Force Structure: A Primer, https://www.cbo.gov/publication/51535, July 2016, accessed 2 April 2018.
2. U.S. Army UAS Center of Excellence, Eyes of the Army. U.S. Army Roadmap for Unmanned Aircraft Systems, 2010–2035, http://www.rucker.army.mil/usaace/uas/US%20Army%20UAS%20RoadMap%202010%202035.pdf, accessed 27 March 2018.
3. Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, Defense Science Board Summer Study on Autonomy, June 2016, https://www.hsdl.org/?view&did=794641, accessed 27 March 2018.
4. Northrop Grumman, HALE Fact Sheet, http://www.northropgrumman.com/capabilities/rq4block20globalhawk/documents/hale_factsheet.pdf, May 2008, accessed 28 March 2018.
5. Paternnosto, A., Game of Drones: The Unmanned Revolution in CBRNE Security, CBRNE Portal, http://www.cbrneportal.com/game-of-drones-the-unmanned-revolution-in-cbrne-security/, February 2016, accessed 28 March 2018.
6. John A., Volpe National Transportation Systems Center, Unmanned Aircraft System (UAS) Service Demand 2015–2035, page 64, https://fas.org/irp/program/collect/service.pdf, September 2013, accessed 28 March 2018.
7. Insinna, V., U.S. Air Force's Next Drone to be Driven by Data, Defense News, https://www.defensenews.com/smr/defense-news-conference/2017/09/06/air-forces-next-uav-to-be-driven-by-data/, September 2017, accessed 28 March 2018.
8. Navy and Marine Corps Small Tactical Unmanned Aircraft Systems Program Office, http://www.navair.navy.mil/index.cfm/index.cfm?fuseaction=home.displayPlatform&key=4A7F6EC6-C427-4C1E-9F8C-5EB5E9F65C4C, accessed 28 March 2018.
9. Osborn, K., Pentagon Plans for Cuts to Drone Budgets, https://www.military.com/dodbuzz.com/2014/01/02/pentagon-plans-for-cuts-to-drone-budgets/, January 2014, accessed 28 March 2018.
10. Eshel, T., Soldier Borne Sensors, Defense Update, http://defense-update.com/20171027_soldier_borne_sensors.html, October 2017, accessed 28 March 2018.
11. Keller, J., Navy Continues to Beef-Up Wide-Area Ocean Surveillance and ISR with Orders for More Triton UAVs, Military & Aerospace Electronics, http://www.military-aerospace.com/articles/2018/01/uavs-isr-ocean.html, 3 January 2018, accessed 28 March 2018.
12. ISR Unmanned Aerial Vehicles, https://www.militaryfactory.com/aircraft/uav-intelligence-surveillance-reconnaissance.asp, accessed 2 April 2018.
13. Chen, F., UAVs for ISR: Capabilities and Limitations, https://figshare.com/articles/UAVs_for_ISR_Capabilities_and_Limitations/1450805/3, 2015, accessed 28 March 2018.
14. Stone, A., How Full-Motion Video is Changing ISR, C4ISRNet, https://www.c4isrnet.com/intel-geoint/isr/2016/03/23/how-full-motion-video-is-changing-isr/, March 2016, accessed 23 March 2018.
15. Yuruts, A., The Ins and Outs of Drone Data Processing, https://intetics.com/blog/the-ins-and-outs-of-drone-data-processing/, September 2016, accessed 28 March 2018.
16. UAS Vision, On-Board HPEC Processing of Big Data in a Pod, https://www.uasvision.com/2016/09/22/on-board-hpec-processing-of-big-data-in-a-pod/, September 2016, accessed 28 March 2018.
17. Harvey, A., UAV ISR Payloads Demand Lighter Weight, Faster Processing, Military Embedded Systems, http://mil-embedded.com/articles/uav-weight-faster-processing/#, April 2014, accessed 28 March 2018.
18. Eshel T., Future Drones: Mission Systems' Automation. Defense-Update, http://defense-update.com/20171025_mission_autonomy.html, October 2017, accessed 28 March 2018.
19. Sandia National Laboratories, VideoSAR, http://www.sandia.gov/radar/video/index.html, accessed 28 March 2018.
20. General Atomics Aeronautical, Lynx Multi-mode Radar, http://www.ga-asi.com/lynx-multi-mode-radar, accessed 28 March 2018.
21. General Atomics Aeronautical, GA-ASI Revolutionizes SAR Full-Motion Video, http://www.ga-asi.com/ga-asi-revolutionizes-sar-full-motion-video, June 2013, accessed 28 March 2018.
22. Weisgerber, M., The Pentagon's New Algorithmic Warfare Cell Gets Its First Mission: Hunt ISIS, Defense One, http://www.defenseone.com/technology/2017/05/pentagons-new-algorithmic-warfare-cell-gets-its-first-mission-hunt-isis/137833/, May 2017, accessed 28 March 2018.
23. Dobkin, A., DOD Maven AI Project Develops First Algorithms, Starts Testing, Defense Systems, https://defensesystems.com/articles/2017/11/03/maven-dod.aspx, November 2017, accessed 28 March 2018.

REFERENCES, *continued*

24. Deputy Secretary of Defense, Memorandum – Establishment of AWCFT Project Maven, http://www.govexec.com/media/gbc/docs/pdfs_edit/establishment_of_the_awcft_project_maven.pdf, April 2017, accessed 28 March 2018.
25. Hartmann K. and Steup, C., The Vulnerability of UAVs to Cyber Attacks – An Approach to the Risk Assessment, 2013 5th International Conference on Cyber Conflict, K. Podins, J. Stinissen, M. Maybaum (Eds.), © NATO CCD COE Publications, 2013.
26. Horowitz, B., Cybersecurity for Unmanned Aerial Vehicle Missions, The CyberEdge, https://www.afcea.org/content/Article-cybersecurity-unmanned-aerial-vehicle-missions, April 2016, accessed 28 March 2018.
27. Behzadan, V., Cyber-Physical Attacks on UAS Networks-Challenges and Open Research Problems (February 2017), University of Nevada Reno, arXiv:1702.01251v1 [cs.CR], 4 February 2017.
28. Lawrence, C., Distributed Battle Management (DBM), https://www.darpa.mil/ program/distributed-battle-management, accessed 28 March 2018.
29. Osborn, K., DARPA Unveils Hack-Proof Drone, DefenseTech.org, http://defensetech. org/2014/05/21/darpa-unveils-hack-proof-drone/, 21 May 2014, accessed 28 March 2018.
30. Cofer, D., et al., High-Assurance Cyber Military Systems (HACMS), https://insights.rockwellcollins.com/2017/07/06/video-high-assurance-cyber-military-systems-hacms/, July 2017, accessed 28 March 2018.
31. The Robotics Law Journal, US Army Discontinues Use of DJI Drones, http://www.roboticslawjournal.com/news/us-army-discontinues-use-of-dji-drones-78881530, 8 August 2017, accessed 28 March 2018.
32. South China Morning Post, Dronemaker DJI Introduces Privacy Mode After US Army Ban, http://www.scmp.com/tech/china-tech/article/2113799/dronemaker-dji-introduces-privacy-mode-after-us-army-bans, 3 October 2017, accessed 23 March 2018.
33. Trevithick, J., Houthi Rebels Shoot Down U.S. Air Force MQ-9 Reaper Over Yemen, http://www.thedrive.com/the-war-zone/14806/houthi-rebels-shoot-down-u-s-air-force-mq-9-reaper-over-yemen, 3 October 2017, accessed 23 March 2018.
34. The Guardian, China Unveils Laser Drone Defence System, https://www.theguardian.com/world/2014/nov/03/china-unveils-laser-drone-defence-system, 3 November 2014, accessed 23 March 2018.
35. Unmanned Airspace, Russia Forms First Battlefield Tactical Counter-UAV Unit Kursk, http://www.unmannedairspace.info/counter-uas-systems-and-policies/russia-forms-first-battlefield-tactical-counter-uav-unit-kursk/, November 2017, accessed 28 March 2018.
36. Stone, A., The Army is Developing Navigation Tech to Help the GPS-Denied Soldier, https://www.c4isrnet.com/intel-geoint/2017/10/16/the-army-is-developing-navigation-tech-to-help-the-gps-denied-soldier/, October 2017, accessed 28 March 2018.
37. Beyond GPS: 5 Next-Generation Technologies for Positioning, Navigation, and Timing (PNT), https://www.darpa.mil/news-events/2014-07-24, July 2014, accessed 28 March 2018.
38. Keller, J., Micro Data Centers for Military Drones, http://www.militaryaerospace.com/articles/print/volume-28/issue-10/technology-focus/micro-data-centers-for-military-drones.html, October 2017, accessed 28 March 2018.
39. DARPA, FLA Program Takes Flight, https://www.darpa.mil/news-events/2016-02-12, February 2016, accessed 28 March 2018.
40. GPS World, Draper Equips UAVs with Vision for GPS-Denied Navigation, http://gpsworld.com/draper-equips-uavs-with-vision-for-gps-denied-navigation/, August 2017, accessed 28 March 2018.
41. DARPA Seeking Automated Decision Aids for Pilots and Battle Managers in Contested Environments, https://www.darpa.mil/news-events/2014-02-21, February 2014, accessed 29 March 2018.
42. Keller, J., Lockheed Martin to Design Full-Up Prototype Decision Aids to Plan Complex Aerial Warfare, Military & Aerospace Electronics, http://www.militaryaerospace.com/articles/2016/05/decision-aids-aerial-warfare.html, May 2016, accessed 29 March 2018.
43. DARPA, Service Academies Swarm Challenge Live-Fly Competition Begins, https://www.darpa.mil/news-events/2017-04-23, April 2017, accessed 29 March 2018.
44. Beall, A., Pentagon Tests the World's Largest Hive-Minded-Controlled Drone Swarm that Can Jam Weapons, Spy on the Enemy and Launch Deadly Attacks, Daily Mail, http://www.dailymail.co.uk/sciencetech/article-4105554/Pentagon-tests-world-s-largest-hive-mind-controlled-drone-swarm-jam-weapons-spy-enemy-launch-deadly-attacks.html, 10 January 2017, accessed 29 March 2018.
45. Office of the Secretary of Defense, Strategic Capabilities Office, Perdix Fact Sheet, https://www.defense.gov/Portals/1/Documents/pubs/Perdix%20Fact%20Sheet.pdf, accessed 29 March 2018.

REFERENCES, *continued*

46. Richardson, J., The Coming Drone Swarm: Swarming UAVs Demonstrate Enormous Attack Potential. But the Technology Still Needs to be Proved and Trusted, Defense Procurement International, https://www.defenceprocurementinternational.com/features/air/drone-swarms, 16 February 2017, accessed 29 March 2018.
47. Raytheon, Flight into the Future: Raytheon Helps Shape the Next Generation of Unmanned Aerial Vehicles, https://www.raytheon.com/news/feature/uav_future.html, 9 March 2018.
48. Frantz, N., Swarm Intelligence for Autonomous UAV Control, Naval Postgraduate School, https://calhoun.nps.edu/bitstream/handle/10945/2152/05Jun_Frantz.pdf?sequence=1, June 2005, accessed 29 March 2018.
49. Edmondson, J., Verifying Distributed Adaptive Real-Time Systems – SEI Blog, https://insights.sei.cmu.edu/sei_blog/2016/10/verifying-distributed-adaptive-real-time-systems.html, October 2016, accessed 29 March 2018.
50. Lomas, N., MIT Creates a Control Algorithm for Drone Swarms, TechCrunch, https://techcrunch.com/2016/04/22/mit-creates-a-control-algorithm-for-drone-swarms/, April 2016, accessed 29 March 2018.
51. Giangreco, L., DARPA Details OFFSET Swarming UAVs, Flight Global, https://www.flightglobal.com/news/articles/darpa-details-offset-swarming-uavs-433784/, February 2017, accessed 29 March 2018.
52. Lockheed Martin, U.S. Air Force, Lockheed Martin Demonstrate Manned/Unmanned Teaming, http://news.lockheedmartin.com/2017-04-10-U-S-Air-Force-Lockheed-Martin-Demonstrate-Manned-Unmanned-Teaming, April 2017, accessed 29 March 2018.
53. Iriarte, M., MUM-T Operations on the U.S. Army's UAS Roadmap, Military Embedded Systems, http://mil-embedded.com/articles/mum-t-armys-uas-roadmap/, April 2016, accessed 29 March 2018.
54. Van Riper, S., Apache Manned-Unmanned Teaming Capability, https://www.ausa.org/sites/default/files/apache-manned-unmanned-teaming.pdf, September 2014, accessed 29 March 2018.

UNMANNED AERIAL SYSTEMS (UAS) FOR INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE (ISR)

By Matthew Harbaugh

DSIAC-2018-0849