9-2019

Current Trends in Small Unmanned Aircraft Systems: Implications for U.S. Special Operations Forces

J. Philip Craiger
Embry-Riddle Aeronautical University, philip.craiger@erau.edu

Diane Maye Zorri
Embry Riddle Aeronautical University, mayed@erau.edu

Joint Special Operations University
Department of Strategic Studies

Current Trends in Small Unmanned Aircraft Systems:

Implications for U.S. Special Operations Forces

by J. Philip Craiger and Diane Maye Zorri

JSOU Press
Occasional Paper
September 2019

On the cover: Dozens of drones swarm a cloudy sky. PHOTO BY ANDY DEAN PHOTOGRAPHY/ SHUTTERSTOCK

JSOU Press Publications are available for download at:
http://jsou.libguides.com/jsoupublications.

ISSN 2572-9020 (print)
ISSN 2572-9039 (online)

About the Authors

Dr. J. Philip Craiger is an associate professor of cybersecurity in the Department of Security Studies and International Affairs at Embry-Riddle Aeronautical University, Daytona Beach, Florida. Philip previously served as professor in the School of Engineering Technology at Daytona State College, where was the principal investigator of the $1.8 million NSF-funded *Advanced Cyberforensics Education Consortium*. From 2004–2010 he served a dual appointment at the University of Central Florida (UCF) as assistant director for digital evidence at the National Center for Forensic Science, and as an assistant professor in the Department of Engineering Technology. At UCF, Dr. Craiger was instrumental in developing the first online master of science in digital forensics in the United States.

Philip started his career as an associate professor in the Department of Computer Science at the University of Nebraska at Omaha. He is a member of the American Academy of Forensic Sciences, and holds numerous professional certifications including Certified Information Systems Security Practitioner (CISSP), Certified Cyber Forensics Practitioner (CCFP) from $(ISC)^2$, SANS GIAC Computer Forensics Analyst, and an EC-Council Certified Ethical Hacker. His research and teaching interests include Small Unmanned Aircraft Systems (sUAS) cybersecurity, cyberforensics, and general aviation cybersecurity.

Dr. Diane Maye Zorri is an assistant professor of security studies at Embry-Riddle Aeronautical University in Daytona Beach, Florida. She also served as a visiting professor at John Cabot University, in Rome, Italy, and was an affiliated scholar with George Mason's School for Conflict Analysis and Resolution (S-CAR). Prior to her work in academia she was an officer in the U.S. Air Force and later worked in the defense industry doing foreign military sales, integrated communications, and proposal development for an Italian defense conglomerate. She is a graduate of the U.S. Air Force Academy and Naval Postgraduate School, and earned a Ph.D. in political science from the Schar School of Policy and Government at George Mason University.

Current Trends in Small Unmanned Aircraft Systems: Implications for U.S. Special Operations Forces

This paper assesses current trends in small unmanned aircraft systems (sUAS) technology and its applications to the Special Operations Forces (SOF) community. Of critical concern to SOF is that commercial-off-the-shelf (COTS) sUAS technologies are relatively inexpensive, improving at a dramatic rate, and widely available throughout the world. Insurgents, terrorists, violent extremist organizations (VEOs) and other nefarious actors have used COTS sUAS to conduct offensive attacks as well as to develop battlefield situation awareness; these technological improvements combined with their widespread availability will require enhanced and rapidly adaptive counter-sUAS measures in the future. To understand the most current trends in the unmanned aircraft systems (UAS) technology and their applicability to SOF, this paper analyzes the definition and classification of sUAS, their major applications, and characteristics. In the military context, UAS are principally used for intelligence, surveillance, and reconnaissance (ISR), border security, counterinsurgency, attack and strike, target identification and designation, communications relay, electronic attack, remote sensing, and aerial mapping. As technology improves, smaller versions of sUAS will be used by both friendly operators and maligned actors (insurgents, terrorists, VEOs, nation states) as force multipliers for military operations. As armed forces around the world continue to invest in research and development of sUAS technologies, there will be tremendous potential to revolutionize warfare, particularly in context of special operations. Consequently, the use of sUAS technology by SOF is likely to escalate over the next decade, as is the likelihood of sUAS countermeasures due to the availability of the technology within nefarious organizations.

Introduction to sUAS

Definition of UAS

UAS—sometimes referred to as unmanned aerial systems, or more colloquially, drones—are defined by the Federal Aviation Administration (FAA) as "an unmanned aircraft and the equipment necessary for the safe and efficient operation of that aircraft. An unmanned aircraft is a component of a UAS. It is defined by statute as an aircraft that is operated without the possibility of direct human intervention from within or on the aircraft."[1] Historically, the Department of Defense (DOD) defined these as unmanned aerial vehicles (UAVs), or when weaponized, unmanned combat aerial vehicles; however, these terms have been supplanted by the term UAS. Their defining characteristic is that they have no onboard pilot-in-command, although most do require a remote pilot-in-command. UASs vary in design and sophistication; the majority of UASs require a manual controller, a communications link between the controller and remote pilot-in-command, and

1. Public Law 112-95, 112th Congress, *FAA Modernization and Reform Act of 2012*, Section 331(8), https://www.congress.gov/112/plaws/publ95/PLAW-112publ95.pdf.

sometimes an observer. Newer and more sophisticated UAS have the capability of autonomous or semi-autonomous flight. Current UAS technologies, and a five-year outlook for future advances, are provided later in this paper.

Classifications of UAS

UAS come in a variety of configurations and sizes. The DOD categorizes UAS into five groups, as demonstrated in table 1.

UAS Category	Max Gross Takeoff Weight (lbs.)	Normal Operating Altitude (ft.)	Speed (KIAS)	Representative UAS
Group 1	0–20	<1200 AGL	100 kts.	Commercial hobby UAS, Buster, WASP III
Group 2	21–55	<3500 AGL	<250	ScanEagle, Silver Fox
Group 3	<1320	<18,000 MSL	<250	RQ-7 shadow, RQ-21 Blackjack
Group 4	>1320	<18,000 MSL	Any Airspeed	MQ-8 Fire Scout, Predator, MQ-1C
Group 5	>1320	>18,000 MSL	Any Airspeed	MQ-9 Reaper, RQ-4 Global Hawk

Table 1. Unmanned Aircraft Systems Categorization Chart. SOURCE: DEPARTMENT OF DEFENSE, JOINT PUBLICATION 3-30, COMMAND AND CONTROL OF JOINT AIRCRAFT OPERATIONS

UAS in groups 3 through 5 are commonly found in military operations for ISR, and offensive operations (e.g., kinetic payloads). The DOD has recently become concerned with UAS in group 1, and their capability for interfering with military operations, or providing maligned actors with intelligence and battlespace awareness. Due to their size, group 1 UAS are typically referred to as UAS. Most sUAS are COTS products, and their development has proliferated over the last decade. The FAA predicts purchases of sUAS will grow from 1.9 million in 2016 to 4.3 million by 2020, and commercial sUAS will increase from 600,000 in 2016 to 2.7 million by 2020.[2] While these COTS sUAS have grown in popularity for hobbyists, the use of commercial UAS has expanded due to their ability to perform work that once required substantial equipment, personnel, time, and money. For instance, commercial sUAS are now used in crop monitoring, law enforcement, infrastructure inspections, cargo transport, storm tracking, geographic mapping, and consumer package delivery.[3]

The growing awareness and concern within the DOD regarding sUAS in active theaters of military operations has occurred for several reasons, notably their widespread availability, relatively low cost, and their rapidly increasing payloads and flight times. This concern is underscored by several instances where sUAS were used by insurgents and terrorists for offensive operations—including payload delivery of kinetic devices, as well as non-offensive operations, such as creating battlespace awareness. Compounding the issue for the future is the fact that the number of commercial sUAS companies is growing each year, therefore widespread availability of sUAS for both

2. Federal Aviation Administration, "FAA and ASSURE Announce Results of Air-to-Air Collision Study," 28 November 2017, https://pr.cirlot.com/faa-and-assure-announce-results-of-air-to-air-collision-study.

3. Diyva Joshi, "Exploring the latest drone technology for commercial, industrial, and military drone uses," *Business Insider*, 13 July 2017, https://www.businessinsider.com/drone-technology-uses-2017-7.

good and maligned actors alike is guaranteed for the foreseeable future. Additionally, companies are adding new high-end technological features to these sUAS and increasing their capabilities while maintaining a relatively low cost (in contrast to larger, military-grade UAS).

Most, if not all, COTS sUAS are commercially available from a small number of companies from various countries, including DJI (Chinese), Yuneec (Chinese), Parrot (French), Hubsan (Chinese), 3D Robotics (U.S.), and Autel (U.S.), among others. As of November 2018, DJI holds over 70 percent of the market share for commercially available sUAS, making the Chinese the world's largest supplier of sUAS.[4]

Compounding the issue for the future is the fact that the number of commercial sUAS companies is growing each year, therefore widespread availability of sUAS for both good and maligned actors alike is guaranteed for the foreseeable future.

Characteristics of sUAS

Aeronautical Design Types

There are two primary aeronautical design types for sUAS: fixed-wing and rotary. Fixed-wing sUAS are similar to traditional fixed-wing aircraft, and depend on thrust from one or more propellers, airspeed, and wing shape, to afford lift. A primary limitation of fixed-wing sUAS is that they cannot hover; however, fixed-wing types can fly twice as fast as rotary-type sUAS. Drone racing competitions, where both maneuverability and speed are judged, has been the big driver in promoting increases in speed. Currently, the average racing speed for rotary-types range from 80-150 mph, whereas some fixed-wing types can fly at speeds over 400 mph.[5] Rotary-wing sUAS are by far the most common sUAS, and these are typically called "copters" (after helicopters) and have the additional capability of vertical takeoff and landing. Common rotary configurations include four (quadcopter) and eight (octocopter) rotors, although the quadcopter represents the lion's share of sUAS. There exists a hybrid type that includes both fixed-wing and rotary capability, but they are in limited production and will not be described here.

Operational Modes

The majority of current sUAS provide line-of-sight (LOS) remote control. These sUAS require a flight controller, which can be a dedicated hardware controller or an application running on a smart device. A direct, LOS communications link is required between the controller and sUAS, which can be either radio frequency (RF) communications link, or an Institute of Electronic and Electrical Engineers (IEEE) 802.11 Wi-Fi link.

4. Fiona Lau and Julie Zhu, "Chinese drone maker DJI seeking at least $500 million in funds," *Reuters*, 21 March 2018, https://www.reuters.com/article/us-dji-tech-fundraising/chinese-drone-maker-dji-seeking-at-least-500-million-in-funds-sources-idUSKBN1GY0A7.

5. G. James Herrera, Jason A. Dechant, and E.K. Green, "Technology Trends in Small Unmanned Aircraft System (sUAS) and Counter-UAS: A Five-Year Outlook," Institute for Defense Analyses, November 2017, https://apps.dtic.mil/dtic/tr/fulltext/u2/1047506.pdf.

Senior Airman Madelyne Kowalczyk, the 11th Security Forces Squadron counter small unmanned aircraft systems NCO-in-charge, operates a sUAS on Joint Base Andrews, Maryland, on 1 March 2019. The aircraft in use was modified to comply with Air Force standards. PHOTO BY U.S. AIR FORCE AIRMAN FIRST CLASS MICHAEL S. MURPHY

The majority of current COTS sUAS require that the pilot-in-command fly the sUAS, thus they contain limited autonomous capabilities. However, more sophisticated—and more expensive—rotor-type sUAS include advanced features that provide additional capabilities, such as auto-takeoff, auto-return home, waypoints, points of interest, and follow-me. "Auto-takeoff" allows the sUAS to rise to a pre-set height and hover until piloted. For GPS-enabled sUAS, "auto-return home" remembers the exact location from which it took off, and can automatically return to that location if, for example, the battery on the UAS is running low or if the communications link is lost. sUAS flight can be pre-determined with the use of "way points," allowing the sUAS to self-fly via the way points without direction from a pilot. For camera-equipped sUAS, "points of interest" can be designated by the pilot, allowing the sUAS to focus its camera on a particular location or object continuously, regardless of the sUAS flight plan. Finally, "follow me" allows the sUAS to follow the pilot or other moving object.

sUAS Military Applications

A May 2018 report published by the Defense Systems Information Analysis Center offered a detailed description of the UAS platforms and payloads that are used for ISR by the U.S. military.[6] Platforms included exemplars from groups 1–5 in UAS types (see table 1). The report identified four types of UAS ISR missions including: broad-area mapping and surveillance performed by high-altitude long endurance (HALE) UAS; target tracking; chemical, biological, radiological, nuclear, and explosives (CBRNE) sensing; and over-the-hill reconnaissance (using class 1 or class 2 UAS).

Operational objectives and operating conditions under which missions are performed dictate combinations of UAS platforms, sensor payloads, and processing, exploitation, and dissemination (PED) methods.[7] Platforms range from small hand-held launch systems to HALE systems with

6. Matthew Harbaugh, "Unmanned Aerial Systems (UAS) for Intelligence, Surveillance, and Reconnaissance (ISR): State-of-the-Art Report (SOAR)," Defense Systems Information Analysis Center, May 2018.

7. Harbaugh, "Unmanned Aerial Systems," 8–1.

the ability to loiter over a geographic region and/or track a target. Sensor payloads include visual, infrared, radio frequency, and other sensors. PED systems include methodologies to extract and communicate actionable intelligence from the totality of raw data collected by the UAS sensors, with processing times ranging from immediate, to hours, through the completion of the mission.

The report also identified nine disparate UAS ISR sensor payloads (see table 2). Much like the advances in capability the sUAS have experienced over the past decade, UAS sensor payloads are showing a remarkable shift in capability. For instance, over the past decade UAS payloads have been operating for longer amounts of time, in more extreme weather and temperatures, using less power, and now have the ability to network with other sensors.[8] Furthermore, as sensor size decreases, sUAS platforms are able to carry more sensors and integrate operations across several disparate systems.[9]

UAS ISR Sensor Payload	Purpose
1. Electro-optical video cameras	Capturing still images and full motion video (FMV)
2. IR imaging sensors	Capturing photographic imgaes or FMV in low lt conditions or darkness
3. Synthetic Aperture Radar	All-weather capabilities for supplying photographic-like images
4. Multispectral imagery and Hyperspectral Imagery	Terrain analysis, high-resolution map imagery, and three-dimensional topographic models
5. Moving target indicator	Isolation of moving targets using radar
6. Light detection and Ranging (LIDAR)	Explosives hazards detection, weather prediction (using Doppler LIDAR), and detection of chemical effluents (using multispectral LIDAR)
7. Laser Radar	Three-dimensional imaging: can see through tree canopies, camouflage, etc.
8. CBRNE sensors	Remote detection of chemical, biological, radiological, nuclear and other explosive devices
9. Signals Intelligence	Situational awareness and intelligence on an adversary by detecting signals from electronic communication

Table 2. sUAS ISR Sensor Payloads. SOURCE: MATTHEW HARBAUGH, "UNMANNED AERIAL SYSTEMS (UAS) FOR INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE (ISR): STATE-OF-THE-ART REPORT (SOAR)," DEFENSE SYSTEMS INFORMATION ANALYSIS CENTER

sUAS Threats

As sUAS see increases in speed, battery capacity, new sensors, and availability, along with decreases in weight, they are likely to be used by maligned actors for offensive attacks, as well as defensive tactics. These threats have a precedent. For instance, in 2014, the Islamic State of Iraq and Syria (ISIS) posted Syrian military target videos taken with a DJI quadcopter.[10] In 2017, ISIS used a

8. John Kelly, "Sensor Payloads for Unmanned Vehicles," *Military and Aerospace Electronics*, 1 August 2018, https://www.militaryaerospace.com/articles/print/volume-29/issue-8/technology-focus/sensor-payloads-for-unmanned-vehicles.html.

9. Suraj Gupta, Mangesh Ghonge, and P.M. Jawandhiya, "Review of Unmanned Aircraft System (UAS)," *International Journal of Advanced Research in Computer Engineering and Technology* 2:4 (April 2013): 1646-1658.

10. Jamie Conliffe, "ISIS Militants Use Same Drones as Ordinary Folks," *Gizmodo*, 29 August 2014, http://gizmodo.com/isis-militants-use-the-same-drones-as-ordinary-folks-1628376186.

COTS sUAS to attack Iraqi military vehicles while filming the attacks. ISIS leaders even created a distinct military unit known as the "Unmanned Aircraft of the *Mujahadeen*."[11]

The ability to carry a significantly destructive explosive payload currently exists. Palmer and Geis noted that the (no longer available) DJI S1000+ eight-bladed octocopter has a 15-minute flight endurance with a payload of almost 15 pounds and costs $1,500.[12] To put this in perspective, a 15-pound payload can equate to six explosives or Thermite grenades, while also carrying a camera for first-person view (FPV). As of November 2018, the Chinese replaced the S1000+ with the DJI Spreading Wings S1000+ Professional Octocopter, which now has a 24-pound payload capacity and a 15-minute fly time. As technology improves, the capability of carrying even larger payloads with concomitant longer flight times will increase—thus creating more lethality at a cheaper cost.

Current and Future Threat Scenarios

Utilizing a red-teaming approach to UAS, a 2015 U.S. Army War College report identified three threat scenarios for consideration by the U.S. military: single human controlled UAS, human controlled or semi-autonomous groups of UAS, and autonomous swarms of UAS.[13] Table 3 outlines the three scenarios, their use in the present day or future, a description of the threat, and finally their significance (being at the tactical, operational, or strategic level of warfare). The report suggests the most significant threat scenario is only a few decades away, where swarms of UAS could have strategic significance in warfare.

Threat Scenario	Time Period	Description	Significance
1. Single UAS: Human Controlled	Present Day	Tactical action to create a terrorism incident. Scenerio variants: Drone-up shooting, Improvised Explosive Devices (IEDs), Crowd Targeting, and Aircraft Takedown.	Tactical (+Terrorism Disruptive Potentials)
2. Group of UAS: Human Controller or Semi-autonomous	Present Day, Near Futures (Some Years)	Force-on-force engagement in insurgency environment. Scenerio variants: Squad-sized Virtual Martyrs Unit and Semi-autonomous Drone Squadron.	Operational
3. Swarm of UAS: Autonomous	Futures (A Few Decades)	Robotic targeting of human personnel, materiel, vehicles, aircraft, and vessels in conflict and war. Scenerio variants: Swarms and Micro-Swarms.	Strategic

Table 3. UAS Threat Scenarios. SOURCE: ADAPTED FROM ROBERT J. BUNKER, TERRORIST AND INSURGENT UNMANNED AERIAL VEHICLES: USE POTENTIALS, AND MILITARY APPLICATIONS

11. Joby Warrick, "Use of 'Weaponized' Drones by Islamic State Spurs Terrorism Fears," *Washington Post*, 21 February 2017, https://www.washingtonpost.com/world/national-security/use-of-weaponized-drones-by-isis-spurs-terrorism-fears/2017/02/21/9d83d51e-f382-11e6-8d72-263470bf0401_story.html?noredirect=on&utm_term=.cccf0316d2ff.

12. Thomas Palmer and John Geis, "Defeating Small Civilian Unmanned Aerial System to Maintain Air Superiority," *Air & Space Power Journal* (Summer 2017): 102–118.

13. Robert J. Bunker, *Terrorist and Insurgent Unmanned Aerial Vehicles: Use Potentials, and Military Applications* (Carlisle Barracks, PA: U.S. Army War College Strategic Studies Institute Press), August 2015.

Threat Scenario 1: Human Controlled Single UAS

The U.S. Army War College report identified this scenario as a tactical operation to instill terrorism and panic. Being at the tactical level of warfare, this scenario is highly plausible for special operators. This scenario is a current threat as al-Qaeda, its successors, and its affiliates have perpetrated, or attempted to perpetrate, these types of events. Furthermore, these scenarios are highly achievable with COTS sUAS. Within this scenario are three variants: drone-up shooting, IED crowd targeting, and aircraft takedown.

"Drone-up shooting" involves a low and slow flying drone used to assassinate a political leader, military person, or other person(s) of significance. This is easily achievable as current, advanced COTS sUAS are outfitted with high-resolution video cameras that provide the pilot-in-command with a FPV of the sUAS flight. sUAS have demonstrated the ability to fly weapons, including a firearm and a flamethrower.[14] Current sUAS technologies include the ability to set and self-fly via way points, focus on a point of interest while the sUAS navigates, and follow me technology (all described previously), providing additional capabilities of stalking potential targets. This capability poses an imminent threat to both U.S. forces and political leaders. In 2017, an Iranian drone dropped a weapon near U.S. SOF operating in Syria,[15] and on 4 August 2018, when two sUAS outfitted with four pounds of plastic explosives were used in an attempted assassination of Venezuelan President Nicolás Maduro during a speech at a military parade in Caracas. Although the attempts were unsuccessful, the events underscore the fact that this type of threat is real and current.[16]

The second variant involves "IED crowd targeting." Rather than a single point of attack with the drone-up shooting, this variant seeks to cause damage across a wide area, targeting crowds at political rallies or sporting events, in order to generate panic and chaos, potentially leading to crowd stampedes.[17] The final variant of the human-controlled, single sUAS threat involves the takedown of a commercial aircraft, where the sUAS pilot uses the speed and kinetic effects of an sUAS to simulate a bird strike. In reality, the potential effects of such a strike would be much worse given the added size, weight, and materials with which sUAS are made.[18] Currently, there are issues with drones interfering with commercial aircraft. Researchers from the University of Dayton Research Institute Impact Physics lab partnered with Sinclair College National UAS Training and Certification Center identified the potential effects of a purposeful sUAS strike against a commercial aircraft. They used two DJI Phantom 2 Quadcopters and the right wing of a Mooney M20, a small general aviation

14. Cyrus Farivar, "Man Who Built Gun Drone, Flamethrower Drone Argues FAA Can't Regulate Him," *ARS Technica*, 9 June 2016, https://arstechnica.com/tech-policy/2016/06/man-who-built-gun-drone-flamethrower-drone-argues-faa-cant-regulate-him.

15. Paul McCleary, "SOCOM Looks to Field New Drones, Upgrade Comms, Fast," *Breaking Defense*, 22 May 2018, https://breakingdefense.com/2018/05/socom-looks-to-field-new-drones-upgrade-comms-fast.

16. Erin Kelly, "Venezuela Drone Attack: Here's What Happened with Nicolas Maduro," *USA Today*, 6 August 2018, https://www.usatoday.com/story/news/politics/2018/08/06/venezuela-drone-attack-nicolas-maduro-assassination-attempt-what-happened/913096002/.

17. Bunker, *Terrorist and Insurgent*, 26.

18. Bunker, *Terrorist and Insurgent*, 26.

plane.[19] The researchers used a 2,800 lb. air cannon and compressed air to shoot the quadcopter at the wing with a velocity of 238 mph, mimicking the combined speed of a small general aviation aircraft and a COTS sUAS. The sUAS punctured a hole in the wing, going deep into the wing and denting a spar—an important structural element for aircraft stability. There are obvious drawbacks of this study that limit the generalizability of the test to real-world conditions. First, small aviation aircraft wings are not as sturdy as larger commercial and military aircraft wings. Second, the velocity provided was much less than what would occur with sUAS capable of speeds of 200 mph, and a military or commercial aircraft flying at 400 mph or higher. Having said that, in December 2018, a Boeing 737-800 reportedly struck a drone during a descent into Tijuana, Mexico, creating extensive damage to the aircraft's nose cone and radome.[20] Likewise, in December of the same year, the United Kingdom's Gatwick Airport shut down due to the disruption caused by multiple sUAS flying over the airfield.[21] While British officials have suggested the disruption was not terror-related, VEOs and small terrorist cells could replicate the act and create a much wider disturbance to international air travel.

Threat Scenario 2: Human Controlled or Semi-Autonomous sUAS Groups

The Army War College report notes there have been no documented events where insurgents or terrorists have used sUAS groups for an attack. Regardless, this variant is predicted on current trends in increases, improvements, and refinements in sUAS technology. Prone to operational-level effects, this scenario includes two variants: a squad-sized virtual martyrs' unit, and semi-autonomous sUAS squadron.

The squad-sized virtual martyrs scenario is comprised of multiple racing sUAS outfitted with IEDs. The goal of this sUAS squad is to detonate an IED once they come into proximity with the target (essentially becoming a martyr by blowing themselves up). The second variant involves a squadron of semi-autonomous sUAS launched simultaneously, which includes previously described scenarios of the drone-up shooting and the IED crowd targeting variants, with the addition of autonomous capabilities. According to the report, the squadron could be sent to particular GPS coordinates, or use Geofencing capabilities to patrol a particular area, autonomously identifying potential targets using various sensors (e.g., forwarding looking infrared and heat signatures). The report notes that this scenario is not about causing terror and panic directly, but rather a focus on combat power in force-on-force engagements with insurgency environments.

19. Alex Davies, "A Drone-Flinging Cannon Proves UAVs Can Mangle Planes," *Wired*, 11 October 2018, https://www.wired.com/story/drone-plane-collision-damage-study.

20. *El Universal*, "Aeromexico investiga daños a punta de avion que aterrizo en Tijuana," 13 December 2018, https://www.eluniversal.com.mx/cartera/negocios/aeromexico-investiga-danos-punta-de-avion-que-aterrizo-en-tijuana.

21. "Gatwick Airport, Drones Ground Flights," BBC News, 20 December 2018, https://www.bbc.com/news/uk-england-sussex-46623754.

Threat Scenario 3: Swarms of Autonomous sUAS

The final threat scenario is forward looking and involves swarms of autonomous sUAS. These technologies are being researched and developed by the U.S. military including the Army, Navy, as well in other countries, most notably China, but also Russia to a lesser extent.[22] Swarms are discussed in more detail below.

sUAS Swarms

A single, or even a handful of sUAS can pose serious threats to ongoing military operations. However, as sUAS technology expands, an even greater threat involves multiple sUAS acting in concert and without human input. The term for massive collections of sUAS is a swarm. The U.S. Army defines a swarm as:

> Swarming is a method of operations where large numbers of autonomous systems actively coordinate their actions to achieve operational outcomes. Swarming overwhelms targets by using mass and attrition in combination with decentralized maneuvers or combined fires from multiple directions.[23]

Colloquially, a swarm has been defined as a collection (40 or more) entities, such as fish, birds, etc., that use similar behavioral rules to achieve a common objective.[24] With respect to sUAS, a swarm consists of multiple (tens, hundreds, or thousands) of sUAS with the capability of self-organizing and autonomous behavior through underlying artificial intelligence (AI) technologies. Swarms bring advantages over single or small groups of human-piloted sUAS. For instance, if a few sUAS malfunction (e.g., due to engine failure), in theory a swarm would have the ability to autonomously share data, communicate, synchronize, and adapt, allowing the remaining sUAS to adapt to a dynamic situation, such as reassigning mission tasks which are then communicated to the remaining, functioning sUAS.[25]

---

22. See: U.S. Army UAS Center of Excellence, "Eyes of the Army" U.S. Army Unmanned Aircraft Systems Roadmap 2010-2035. U. S. Army UAS Center of Excellence (ATZQ-CDI-C), 2010; Kelsey Atherton, "Navy Office Awards $30 Million Contract for Drone Swarms," C4ISRNET, 27 June 2018, https://www.c4isrnet.com/unmanned/2018/06/27/office-of-naval-research-awards-raytheon-30-million-to-develop-locust-swarm.

23. See: "The U.S. Army Robotic and Autonomous Systems Strategy," (Fort Eustis, VA: Maneuver, Aviation, and Soldier Division, Army Capabilities Integration Center) March 2017, http://www.arcic.army.mil/App_Documents/RAS_Strategy.pdf.

24. See: Andreas Huth and Christian Wissel, "The Simulation of the Movement of Fish Schools," *Journal of Theoretical Biology* 153 (6) 1992: 365–85; Craig Reynolds, "Flocks, Herds, and Schools: A Distributed Behavioral Model," *Computer Graphics 21*(4), July 1987: 25–34.

25. National Academy of Sciences, Engineering, and Medicine, *Counter-Unmanned Aircraft System (CUAS) Capability for Battalion-and-Below Operations: Abbreviated Version of a Restricted Report* (Washington, D.C.: The National Academies Press, 2018).

Current State of Swarming Technology: U.S. and China

The U.S. military has long been a leader in swarming technology.[26] In October 2016, the DOD Strategic Capabilities Office and Naval Air Systems Command tested swarm technology in China Lake, California, where 103 Perdix sUAS were launched from three F/A-18 Super Hornets.[27] The Perdix sUAS demonstrated swarming behaviors, including adaptive formation flying. The DOD aims to create sUAS swarms with more advanced and adaptive capabilities, including collective decision-making and self-healing, as well as increasing swarm size to over 1,000 sUAS.[28]

As of 2018, China holds the world record on the largest sUAS swarm. On 7 December 2017, for nine minutes 1,180 sUAS ($1500/each) performed an aerial display in Guangzhou, China, including autonomously creating formations including a kapok tree flow and a ship.[29] If any of the sUAS in the formation could not fulfill its orders it would land autonomously. Although these maneuvers were nowhere near as complex as those required on an operational battlefield, it does suggest that technology allowing autonomous behavior of a swarm consisting of thousands of individual sUAS currently exists.

In April 2018, in the spirit of innovation and public-private partnership, the Chinese People's Liberation Army (PLA) Air Force announced a competition called "Unmanned Warfront" Intelligent UAV Swarm System Challenge. The competition is open to military scientific research institutes, academic institutions, private enterprises, and sUAS hobbyists. The competition involves autonomous swarms performing tasks such as cooperative reconnaissance and target identification. The technologies employed by the winners of the competition will be given priority for future PLA Air Force projects.[30]

Counter sUAS

In 2015, researchers conducted a study to identify unique UAS countermeasures, identifying 39 unique defense concepts across government reports, academic studies, and news articles.[31] They noted that some defense strategies, while available, were less practical than others. Of more importance is the author's application of the concept of defense-in-depth, a long-standing concept in the field

26. National Academy of Sciences, Engineering, and Medicine, *Counter-Unmanned*.

27. Department of Defense, "Department of Defense Announces Successful Micro-Drone Demonstration," 9 January 2017, https://dod.defense.gov/News/News-Releases/News-Release-View/Article/1044811/department-of-defense-announces-successful-micro-drone-demonstration.

28. Department of Defense, "Department of Defense Announces."

29. Jeffrey Lin and P.W. Singer, "China is Making 1,000-UAV Drone Swarms Now," *Popular Science*, 8 January 2018, https://www.popsci.com/china-drone-swarms. This aerial display can be also be found on YouTube at: https://www.youtube.com/watch?v=Jnei1md-Ia0.

30. Samuel Bendett and Elsa B. Kania, "Chinese and Russian Defense Innovation, with American Characteristics? Military Innovation, Commercial Technologies, and Great Power Competition," *The Strategy Bridge*, 2 August 2018, https://thestrategybridge.org/the-bridge/2018/8/2/chinese-and-russian-defense-innovation-with-american-characteristics-military-innovation-commercial-technologies-and-great-power-competition.

31. Ryan Wallace and Jon Loffi, "Examining Unmanned Aerial System Threats & Defenses: A Conceptual Analysis," *International Journal of Aviation, Aeronautics, and Aerospace*, 2(4):1–33.

of cybersecurity. Defense-in-depth suggests that no single countermeasure to a threat is foolproof; consequently, it is critical that multiple layers of defense be in place to mitigate any threats. They identified a five-layer model that included broad defense strategies, including prevention, deterrence, denial, and detection. Figure 1 displays this defense-in-depth strategy.

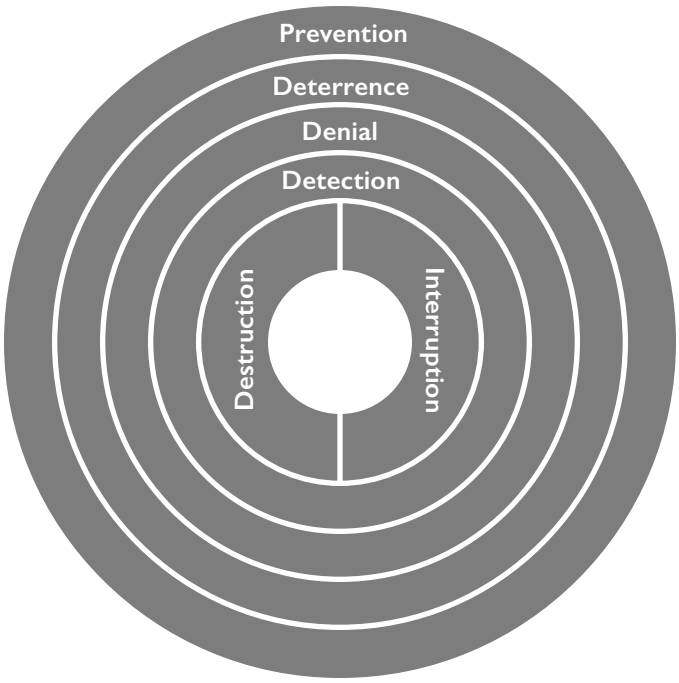

Figure 1. Five-layer defense UAS defense strategies. SOURCE: USED WITH PERMISSION FROM RYAN WALLACE AND JON LOFFI'S "EXAMINING UNMANNED AERIAL SYSTEM THREATS & DEFENSES: A CONCEPTUAL ANALYSIS," INTERNATIONAL JOURNAL OF AVIATION, AERONAUTICS, AND AEROSPACE,2(4), 13.

The outer layer, prevention, is perhaps the most critical defense strategy and is normally achieved through capturing actionable intelligence through the intelligence community and/or law enforcement organizations. Deterrence, the next layer, is primarily achieved through legislation (two remedies). The first is legislation to create and fund counter UAS defenses. The second is the establishment of civil and criminal penalties to prevent the illegal or unethical use of UAS, with associated penalties sufficient to deter this activity. The middle layer, denial, includes passive, (normally) physical barriers that present hazards or obstructions to UAS, such as nets, trees, or other obstacles, precluding the UAS to access vital resources. Detection incorporates active defense mechanisms should prevention, deterrence, and denial defense strategies fail to deter the UAS. Detection mechanisms can be either passive or active. Active detection mechanisms include the use of radar; unfortunately, due to the small size of sUAS it is often difficult or impossible to determine whether a radar blip is a sUAS, bird, kite, or other small flying object. Passive detection mechanisms use sensors to identify UAS signatures. Sensors include visual, acoustic, thermal/infrared, and UAS communications/control frequencies.

An unmanned aircraft system is seen on the flightline at Naval Base Ventura County and Sea Range, Point Mugu, California, on 31 July 2015. The UAS was part of Black Dart 2015, a DOD-sponsored demonstration that included industry personnel and participants from four military branches to assess and improve technologies, tactics, and techniques used by the DOD and its partners in countering the threat of UAS. PHOTO BY OFFICE OF THE SECRETARY OF DEFENSE PUBLIC AFFAIRS LISA FERDINAND

Active defenses are the final layer of defense-in-depth and include two defense measures; interruption or destruction. Interruption can be conducted in several ways, including operator interruption, signal spoofing, signal jamming, malicious code insertion, packet spoofing, and network protocol exploits.[32] Operation interruption involves identifying the sUAS operator, and either requesting or compelling the operator to cease operations. Signal jamming involves overwhelming command and control (C2) signals of the sUAS. Most sUAS are controlled via RF or IEEE 802.11 Wi-Fi signals, the latter of which operate on known frequencies of 2.4GHz or 5GHz. Signal jamming is similar to the cybersecurity concept of denial-of-service (DOS); overwhelm an adversary's capability of sending and receiving signals. Signal spoofing involves sending the sUAS "bogus" geolocation signals, resulting in the degradation of the flight, and the capability of communicating accurate geolocation information, etc. The signals to be spoofed can include the GPS signal, resulting in the sUAS "thinking" it's in one location, when in actuality it's at another. Spoofed C2 signals can cause the sUAS to behave erratically, or cause it to be diverted from its intended target.

Current Military Counter-UAS

Although the U.S. military currently has a multitude of counter sUAS methods; the primary issues are ones of: asymmetry, efficiency, and cost effectiveness. What type of counter-systems are appropriate for swarms of sUAS each of which may cost no more than $1,500? One of the first was a military exercise called "Black Dart," which tested non-kinetic and kinetic methods of countering rogue UAS. Kinetic methods ranged from large caliber guns to Hellfire missiles.[33] The exercise was designed to test counter UAS systems against UAS systems encompassing a broad range of sizes and capabilities. The exercise focuses on sUAS due to the incidents of sUAS flying

32. See: Wallace and Loffi, "Examining Unmanned," 18–21; Iseok Hwang and Cheolhyeon Kwon, "System and Cyber Security: Requirements, Modeling, and Management," *Unmanned Aircraft Systems* (New York: Wiley & Sons, 2016): 637–649.

33. Richard Whittle, "Military Exercise Black Dart to Tackle Nightmare Drone Scenario," *New York Post,* 25 July 2015, https://nypost.com/2015/07/25/military-operation-black-dart-to-tackle-nightmare-drone-scenario.

near prominent politicians. For instance, during a campaign event in Dresden, German chancellor Angela Merkel encountered a sUAS as it hovered near her face. In the same year, a drone landed on the roof of Japanese Prime Minister Shinzō Abe's residence.[34] In 2015, a small quadcopter flown by a government employee crashed on the White House lawn. Considered a recreational event gone awry, regardless, the quadcopter was able to elude the U.S. Secret Service notice.[35] These types of problems are projected to grow. In the first and second quarter of 2018, the FAA received over 200 adverse UAS reports per month—a figure that has risen steadily over the past five years.[36]

Counter sUAS Technologies

The goal of counter sUAS is to identify, target, and takedown one or more sUAS, and do so in a practical, cost efficient manner. Current counter sUAS technologies fall into three categories; traditional kinetic, directed energy, and cyber. The most appropriate countermeasure will depend upon the size of the sUAS, distance to target, as well as whether the target is civilian and on home soil, or whether the target is part of an insurgent or terrorist activity in a hostile land. We describe examples of countermeasures applicable for sUAS (class 1 and 2) only, as opposed to counter measures that are primarily applicable to larger (class 3 through 5) UAS. Of critical importance is whether the countermeasure is capable of identifying, tracking, and targeting both single, as well as swarms of sUAS.

Citing an urgent operational need, the U.S. Army began purchasing Raytheon's expendable (suicide) Coyote Block 1B UAS. The USA has the ability to fly alone or as part of a swarm, and to bring down class 1 or class 2 hostile UAS through suicide missions.[37] Drone Defender is a 20 lb. portable counter sUAS systems resembling a large, heavy rifle with the capability of disrupting the communications links—with an effective range of 400 meters, and 30-degree beam—between the sUAS and pilot-in-command.[38] This technology is limited to small areas of operations due to the limited beam width and operational range.

Current COTS GPS-capable sUAS are designed with the capability of dealing with lost communications links in several ways, including "flying home" (from their takeoff location), hovering in place, or simply landing. sUAS whose communications link has been disrupted may fly outside of the operational range of Drone Defender to fly home, resulting in the sUAS regaining its capabilities. Moreover, this technology is probably only applicable to single or a small number of

34. Palmer and Geis, "Defeating Small," 107.

35. Faine Greenwood, "Man Who Crashed Drone on White House Lawn Won't be Charged," *Slate*, 18 March 2015, https://slate.com/technology/2015/03/white-house-lawn-drone-the-man-who-crashed-it-there-won-t-be-charged.html.

36. Federal Aviation Administration, "UAS Sighting Reports," 2018, accessed 14 December 2018, https://www.faa.gov/uas/resources/uas_sightings_report.

37. Joseph Trevithick, "Army Buys Small Suicide Drones to Break up Hostile Swarms and Potentially More," *The War Zone*, 17 July 2018, http://www.thedrive.com/the-war-zone/22223/army-buys-small-suicide-drones-to-break-up-hostile-swarms-and-potentially-more.

38. Palmer and Geis, "Defeating Small," 106.

flying sUAS, and less so for swarms of highly autonomous sUAS, whose important communication links lie between the individual sUAS composing the swarm, as opposed to sUAS and pilot.

Issues in Counter-sUAS

Advances in material sciences, including adaptive printing techniques and carbon nanotubes, will result in lighter and more resilient materials, resulting in lighter and faster sUAS with the capability of loitering longer and increasing payload capacity.[39] These new materials, along with advances in computer technology, will also see reductions in size and weight of communications equipment, sensors, and kinetic payloads, will further increase the capabilities of sUAS; faster, lighter, increase flight times, etc.[40]

Identifying and targeting sUAS today has demonstrated difficulties. The structure, size, and materials used in sUAS reduce radar return, resulting in difficulties identifying and tracking them.[41] Additionally, the size of sUAS can make them indistinguishable from other airborne objects, including birds.[42] Advances in machine learning and AI will also have an impact on counter sUAS measures. These advances are predicted to support sUAS swarms that are highly autonomous imbued with the capability of reconfiguring an operation without human input. This may result in novel tactics that are unpredictable, which will make rapidly changing adaptations in an operational environment extremely difficult.

Advances in machine learning and AI will also have an impact on counter sUAS measures.

Five-Year Technology Trends in sUAS

In 2017, the Institute for Defense Analysis published a five-year outlook for technological advancements in sUAS for the Office of Infrastructure Protection, National Protection and Programs Directorate, U.S. Department of Homeland Security.[43] They identified four general categories of trends, including platform modifications, platform operations, autonomy, and swarming. Under platform modifications, sUAS are expected to decrease in size while maintaining, or even increasing, capabilities such as flight time, payload, range, endurance, and speed. Thus, while the gross weight of sUAS are expected to decrease, those same sUAS will maintain or even increase payload capabilities. With respect to advances in platform operation, sUAS are expected to increase in speed, from approximately 40 mph for COTS sUAS on average currently to over 200 mph, as depicted in table 4.[44] sUAS will also continue to increase in range, endurance, and operating altitude due to advances

39. Anthony Tingle and David Tyree, "The Rise of the Commercial Threat Countering the Small Unmanned Aircraft System, *Joint Forces Quarterly* 85(2): 30-35.

40. Tingle and Tyree, "The Rise of the Commercial Threat," 30-35.

41. Tingle and Tyree, "The Rise of the Commercial Threat," 30-35.

42. Tingle and Tyree, "The Rise of the Commercial Threat," 30-35.

43. Herrera, Dechant, and Green, "Technology Trends."

44. As of 2018, the current fastest sUAS are reaching 176 mph.

in battery and energy technologies. Also, new electronic and mechanical capabilities will become available and be incorporated onboard sUAS, such as artificial intelligence, robotic technologies, sensor technologies, advanced enhanced audio/video, etc. While some autonomy capabilities currently exist for some sUAS, the degree of autonomy and sophistication will increase. Finally, swarming technologies will continue to increase.[45]

Year	Gross Weight	Payload	Range	Average Speed	Max Speed	Indurance	Altitude
<2019	<20 lbs.	0–7 lbs.	3–20 miles	40 mph	176 mph	1–8 hrs.	1000 ft.
>2024	<15 lbs.	.7 lbs.	>20 miles	>50 mph	>200 mph	>8 hrs.	>1000 ft.

Table 4. Five-year predicted sUAS capabilities based on author estimates.

Given these predicted advances, the sUAS five years from now will be very different than the current collection of sUAS. These advances should greatly increase the capability of the military to deploy these smaller, faster, and more advanced sUAS for infield operations. Concomitantly, this will result in the need for new counter-sUAS technologies to combat the use of these advanced sUAS. It is not out of the realm of imagination that insurgent offensive attacks once requiring at minimum a larger and expensive Class 3 UAS might in the near future be capable with a much smaller, and less expensive, COTS sUAS (class 1 and class 2).

Cyber Counter-sUAS

sUAS (and UAVs alike) are highly dependent on computer and networking technology. As such, they are potentially susceptible to various types of cyberattacks conducted on a daily basis on information computer technology. To understand potential cyber threats to sUAS (or any aircraft for that matter) requires the understanding of important cybersecurity concepts. Confidentiality, integrity, and availability are three important attributes of information. Confidentiality deals with protecting information from unauthorized access or disclosure.[46] Integrity refers to information being complete, authentic, original, and uncorrupted, and also includes the information systems themselves being free from intentional or inadvertent manipulation.[47] Availability refers to ensuring that information is available when access is required. In addition, there are three important concepts related to accessing information. Identification is the first step used in verifying a user's identity when attempting to access an information system (typically using a user name or user ID). Authentication is the second step in verifying a user's identify, involving the presentation of additional pieces of information so that the users identity can be conclusively validated, typically using a password or passphrase.[48]

45. Herrera, Dechant, and Green, "Technology Trends," 32.

46. Philip Craiger and Gary Kessler, "Cybersecurity," in Joseph R. Rudolph, Jr. and William J. Lahneman, Eds. *Combating Terrorism in the 21st Century: American Laws, Strategies, and Agencies* (Santa Barbara, California: ABC-CLIO, in press).

47. Craiger and Kessler, "Cybersecurity."

48. Craiger and Kessler, "Cybersecurity."

Finally, authorization is a process where the information system determines whether a validated user has been granted access to a particular resource (e.g., a particular, file, application, network share, etc.).[49]

In 2012, cyber technology researchers developed a cyber-based threat model for UAVs from the perspective of cybersecurity.[50] Like any aircraft, sUAS require clean, uncorrupted, and uninterrupted communications, both internal and external to the sUAS, in order to conduct its mission. Figure 2 demonstrates a myriad of possible cyber-attacks potentially causing issues with the confidentiality, integrity, and availability of information from the perspective of an operational sUAS.

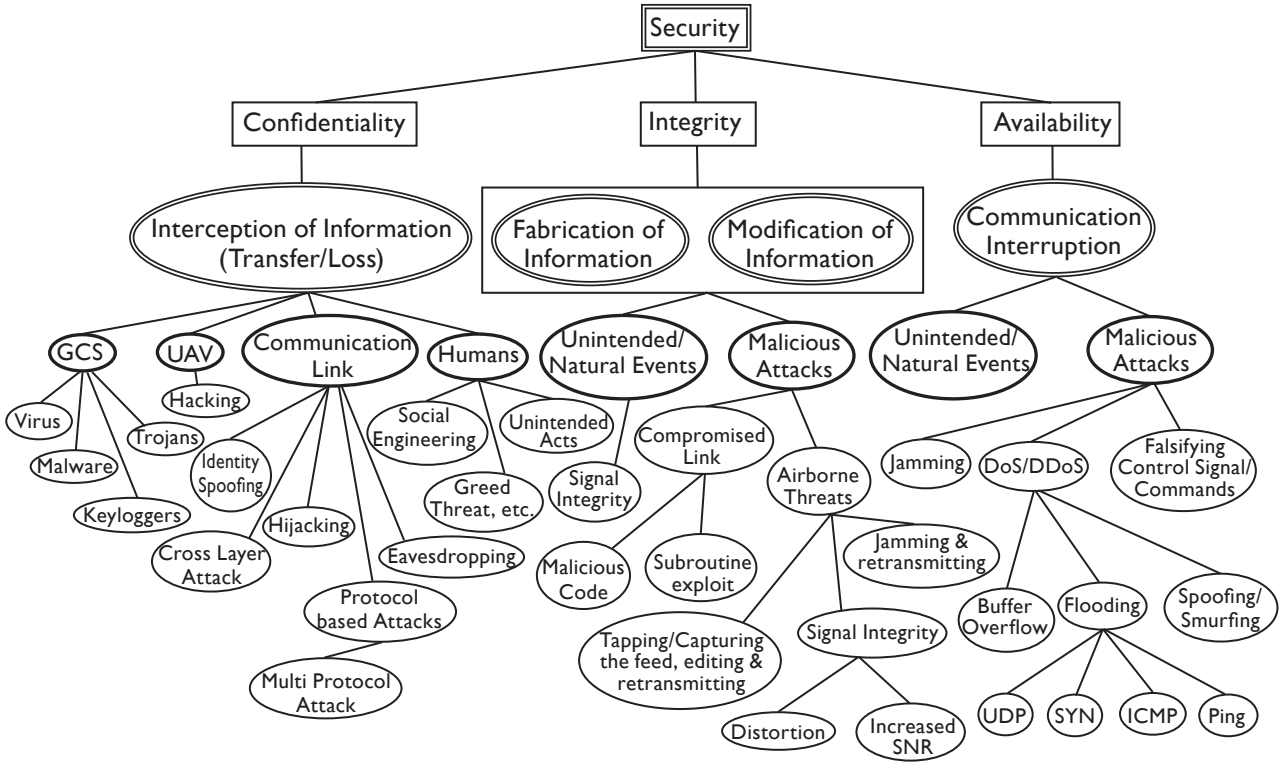

Figure 2. UAV Cyber Threat Model. SOURCE: AHMED JAVAID, ET AL., "CYBER SECURITY THREAT ANALYSIS AND MODELING OF AN UNMANNED AERIAL VEHICLE SYSTEM," IEEE CONFERENCE/ USED WITH PERMISSION FROM AHMAD JAVAID

The researchers identified several cyber threats to the confidentiality of UAV information, the primary of which is malware. Malware is an umbrella term for malicious software that is harmful to a system.[51] Malware can be planted on sUAS in various ways, the easiest of which is through defects in supply chain security. For instance, before a sUAS is purchased, it is intercepted en route during shipping, or at the factory where assembled, where malware can be surreptitiously uploaded to

49. Craiger and Kessler, "Cybersecurity."

50. Ahmed Javaid, et al., "Cyber Security Threat Analysis and Modeling of an Unmanned Aerial Vehicle System," *IEEE Conference on Technologies for Homeland Security* (13–15 November 2012): 585–590.

51. Javaid, et al., "Cyber Security," 589.

the onboard computer of the sUAS. The malware can later be triggered through various means, such as when the sUAS hits a pre-determined flight parameter (GPS location, altitude, etc.), or by a maligned actor gaining unauthorized access to the sUAS and manually running the malware.

Malware can be planted on sUAS in various ways, the easiest of which is through defects in supply chain security.

Also, COTS sUAS are particularly vulnerable to various forms of hacking as security for these devices is usually an afterthought by manufacturers. Hacking is defined as the act of acquiring unauthorized access to a computer or network.[52] There are demonstrated instances of researchers hacking into COTS sUAS, identifying system vulnerabilities, and running damaging commands, resulting in the termination of the flight, and potential destruction of its operating system capabilities.[53] These researchers first performed a vulnerability assessment of the sUAS using commonly available cybersecurity software, which resulted in the identification of multiple security vulnerabilities that were easily exploitable. Security vulnerabilities included various unencrypted communication services, open services not requiring identification and authentication in order to gain access to the sUAS onboard computer, and after access was gained, all commands could be run as superuser—accounts primarily used for administrators with virtually unlimited privileges—allowing the researchers to take complete control of the sUAS. Additionally, Craiger, Kessler, and Rose were able to intercept the first-person video FPV feed of a COTS sUAS.[54] Intercepting the FPV would allow a bad actor to see what the operator is seeing, providing them with possible actionable intelligence on the operator's missions.

sUAS are also susceptible to integrity attacks through modification of existing onboard information, or through the creation of new, fabricated information.[55] For example, many sUAS support the uploading of pre-determined flight patterns to the onboard computer; if a bad actor can gain access, these pre-determined flight patterns can be changed either pre- or in-flight to force the sUAS to follow a secondary flight path. As described previously, signals, including C2, GPS, or FPV feeds, are susceptible to jamming, allowing a bad actor to disrupt a sUAS flight. As described previously, many sUAS have the capability of dealing with these disruptions through either hovering in place, gracefully landing, or if GPS is available, returning to the location from whence they took off.

52. Craiger and Kessler, "Cybersecurity."

53. P. Craiger, Gary Kessler, and William Rose, "sUAS Cybersecurity Threats, Vulnerabilities, and Exploits: A Case Study" (presentation, National Training Aircraft Symposium. Embry-Riddle Aeronautical University, Daytona Beach, FL, 2018); Johann-Sebastian Pleban, Ricardo Band, and Reiner Creutzburg, "Hacking and securing the AR Drone 2.0 Quadcopter: Investigations for Improving the Security of a Toy," *Proceedings of SPIE—The International Society for Optical Engineering* (February 2014); Manuel Kramer and Martin Schmeisser, "Drones InSecurity," University of Tartu Institute of Computer Science, December 2014, accessed 14 December 2018, https://infoscience.epfl.ch/record/204987/files/DronesInSecurity.pdf.

54. Craiger, Kessler, and Rose, "sUAS Cybersecurity Threats;" Pleban, Band, and Creutzburg, "Hacking and securing;" Kramer and Schmeisser, "Drones InSecurity."

55. Javaid, et al., "Cyber Security," 589.

Finally, availability attacks are composed of jamming, spoofing, or DOS attacks.[56] Jamming is most notably the easiest form of attack for sUAS and jamming technologies can be purchased over the internet (although any such jamming devices are illegal in the U.S., they can be obtained from foreign countries). Spoofing is more complicated and difficult; successfully spoofing a C2 or GPS signal requires *a priori* intelligence and planning, which would most likely limit this type of attack to technically sophisticated adversaries. DOS attacks are easy to accomplish, as there are many free and open source software packages that support the execution of a DOS attack. The result of a DOS attack would be similar to a jamming attack, as the sUAS would be unable to receive the signal (C2, GPS, etc.) in either case.

Conclusion

With the increase in COTS sUAS capabilities becoming faster, smaller, more resilient, cheaper, and more easily available, their use will increase among nefarious actors, insurgents, VEOs, and terrorists—and the problem will continue to worsen.[57] Concurrently, the growth in technology will result in more lethality and effectiveness on the battlefield.[58] Thus, the implications for SOF are profound. SOF strategists likely recognize that not only will insurgents, terrorists, and VEOs become more competitive in this space, but so will near-peer adversaries such as China and Russia, and malicious regimes like Iran and North Korea. It will be essential to recognize the importance of empowering SOF operators and making provisions for them to stay flexible and adaptable, especially as the Chinese military incorporates the concepts of innovation and originality into their defense planning and acquisition cycle.

Army General (Ret.) Raymond A. Thomas III, then U.S. Special Operations Command Commander, visits SOFWERX's ThunderDrone Rapid Prototyping Event II in Tampa, Florida, on 31 January 2018. The event enabled collaboration to combat threats from enemy UAS such as quadcopters and drones. PHOTO BY U.S. AIR FORCE MASTER SGT. BARRY LOO

SOF leaders have long recognized the importance of increasing technical capability and keeping par with the latest advances. Organizations such as SOFWERX are closing the collaboration and innovation gap. SOFWERX—created under a partnership intermediary agreement between the

56. Javaid, et al., "Cyber Security," 589.

57. Palmer and Geis, "Defeating Small," 112.

58. Tingle and Tyree, "The Rise," 31.

Doolittle Institute and USSOCOM—combines public-private innovators of technology with "academia, civilian companies, and other nontraditional DOD partners who work on United States Special Operations Command's most challenging problems."[59] It will also be imperative for SOF commanders to recognize the importance of defending and countering adversarial sUAS payload technology, which should include active hacking, counterintelligence, and subsequent psychological operations. Another area of growing importance will be in the systems architecture of multiple, disparate military sUAS, and their ability to coordinate on a single line of effort. Given the inherently joint nature of special operations, the command could lead in integration, security, and synchronization of multiple sUAS systems. Of particular importance to special operators will be the concepts derived from Urban Air Mobility, or safe and effective air operations in an urban environment.[60] In addition, as the quantity of sUAS and their use on the battlefield increases, and sensors become more readily available, another area of concern will be in transforming the vast quantity of data gathered by sUAS sensors into discrete and actionable intelligence.[61] Likewise, as sUAS technology rapidly advances, international norms and standards behavior has struggled to keep pace, which has created new areas for nefarious actors to exploit. This will be of particular concern in gray zone conflicts where malicious actors regularly disregard international norms of behavior.

Given the inherently joint nature of special operations, the command could lead in integration, security, and synchronization of multiple sUAS systems.

As has occurred with many technologies in the last century, their second- and third-order effects and uses have not been easily predictable, as has been the case with sUAS. Continuously forecasting advances in sUAS technologies and capabilities will be crucial for SOF into the next decade. Thus, providing avenues for the real-time development of threat models and concomitant countermeasures to combat malicious actors' use of sUAS on the battlefield will be critical in maintaining superiority in this domain.

59. "SOFWERX: A Smart Factory of Innovation Helping the Warfighter," USSOCOM Office of Communication, Michael Bottoms, 2 February 2018, https://www.socom.mil/sofwerx-a-smart-factory-of-innovation-helping-the-warfighter.

60. David Thippahavong, et al., "Urban Air Mobility Airspace Integration Concepts and Considerations," National Aeronautics and Space Administration, presentation at the 2018 Aviation, Technology, Integration, and Operations Conference, June 2018.

61. Sonya McMullen, et al., "From Sensors to Knowledge: The Challenge of Training the Next Generation of Data Analysts," *Proceedings 10653, Next Generation Analyst VI* (2018).

Joint Special Operations University
Department of Strategic Studies
7701 Tampa Point Blvd.
MacDill AFB, FL 33621

JOINT SPECIAL OPERATIONS
JSOU
UNIVERSITY
PRESS