Small Unmanned Aircraft: Characterizing the Threat

February 2019

Andrew Lacher
Jonathan Baron
Jonathan Rotner
Michael Balazs

For additional information about this white paper, please contact:

Andrew Lacher
alacher@mitre.org
703-983-7812 office
703-946-6050 mobile

Approved for Public Release

Distribution Unlimited - Case: 18-03852-2

Abstract

For several years, The MITRE Corporation has been exploring issues associated with the potential security threats that small Unmanned Aircraft Systems (sUAS)[1] present. In 2016, MITRE sponsored a competition during which eight commercial companies demonstrated in a real-world setting the effectiveness of their detect and defeat capabilities against commonly available sUAS operating in an unauthorized fashion.[2] As part of that effort, MITRE began to describe the potential threat posed by sUAS using a variety of characteristics. MITRE experts have continued to evolve this threat spectrum as we work on counter-UAS-related tasks for our sponsors and as we research the ever-evolving technology and operational capabilities of sUAS. In this paper, MITRE uses data-driven observations to characterize the sUAS threat. This paper does *not* assess the sUAS threat, nor does it discuss potential targets or vulnerabilities from national defense, homeland security, law enforcement, or commercial industry perspectives. MITRE is sharing its sUAS threat characterization to help the community understand the nature of potential sUAS threats and to provide a common vernacular for discussing the technical challenges associated with detecting and defeating the threat.

[1] A small sUAS (or sUAS) is an unmanned aircraft and associated elements that are required for the aircraft to operate safely and efficiently in the national airspace system. An unmanned aircraft is an aircraft that is operated without the possibility of direct human intervention from within or on the aircraft. A small sUAS involves an aircraft that has a gross weight of less than 55 lbs. [14 CFR Part 107; Public Law 112-95, Section 331]

[2] https://www.mitre.org/news/press-releases/mitre-names-c-uas-challenge-winners

A. Introduction

Ten years ago, most non-military unmanned aircraft, also known as drones, were remotely piloted aircraft. They were often custom built and flown by model aircraft enthusiasts for fun. Today, highly capable commercial systems are sold, for a few hundred dollars, to a wide variety of enthusiasts, many of whom are interested in more than just the act of flying. Some operators want a "flying camera" with little or no flight training.[3] Others want to race aircraft using personal point-of-view technology. Some are pursuing commercial applications by using a flying sensor to provide information previously either unavailable or only available at significant costs. However, with the good also comes the bad. There are a few operators who plan to use sUAS for illicit or illegal activities, such as spying on neighbors or manufacturing plants, disrupting flight operations, delivering contraband into prison yards, or even harming others.

Small Unmanned Aircraft Systems (sUAS) are now commonly available, with more than 1 million operators have registered their aircraft in the United States.[4] Market demands have driven sensor development, automated capabilities,[5] and new use cases. These include highly networked package delivery,[6] persistent communications for disaster relief efforts,[7] chemical dispensers for agriculture, and urban mobility systems for freight and even passengers.[8] Enterprises are employing increasingly larger fleets, and more and more individuals are registering as drone operators.[9]

Innovation in this market sector is extremely rapid, with models becoming obsolete in less than a year. This is especially true of sUAS, meaning aircraft that weigh less than 55 lbs. [10] The combination of an exponential increase in aircraft numbers operating in urban, populated areas; the ability to fly with increased autonomy and decreased human direct control; and advanced tracking capabilities poses a significant threat to public safety and security.

B. sUAS Threat Characteristics Spectrum

To illustrate development trends and their potential implications as a security threat, The MITRE Corporation developed a *sUAS Threat Characteristic Spectrum.* The sUAS threat can be

---

[3] Examples of low-cost ready to fly small sUAS involve products from a variety of vendors. Some specific examples include the following: DJI (www.dji.com), Parrot (www.parrot.com), Yuneec (http://us.yuneec.com/) and Holy Stone (http://www.holystone.com/).

[4] https://www.transportation.gov/briefing-room/faa-drone-registry-tops-one-million

[5] Examples of some commercial applications or developers of commercial platforms include: Project Wing (https://x.company/projects/wing/), CyPhy (https://www.cyphyworks.com/), Intel, and Vantage Robotics (https://vantagerobotics.com/).

[6] https://www.forbes.com/sites/startupnationcentral/2018/04/10/drone-deliveries-are-no-longer-pie-in-the-sky/#5fb439384188

[7] https://www.researchgate.net/publication/326960048_Unmanned_Aerial_Vehicles_for_Disaster_Management

[8] Urban Air Mobility Landscape Report – The MITRE Corporation, April 2018. https://www.mitre.org/publications/technical-papers/urban-air-mobility-landscape-report

[9] FAA's Drone Zone: https://faadronezone.faa.gov

[10] Examples of some commercial applications or developers of commercial platforms include: Project Wing (https://x.company/projects/wing/), CyPhy (https://www.cyphyworks.com/), Intel, and Vantage Robotics (https://vantagerobotics.com/).

characterized by seven dimensions to include operational, acquisitional, and technical aspects. By understanding the current state of each of these dimensions and analyzing where the commercial sUAS market is headed, one can identify potential future threats. Figure 1 illustrates the range of sUAS characteristics. In the following graphic, the difficulty to detect and counter sUAS threats increases from left to right.

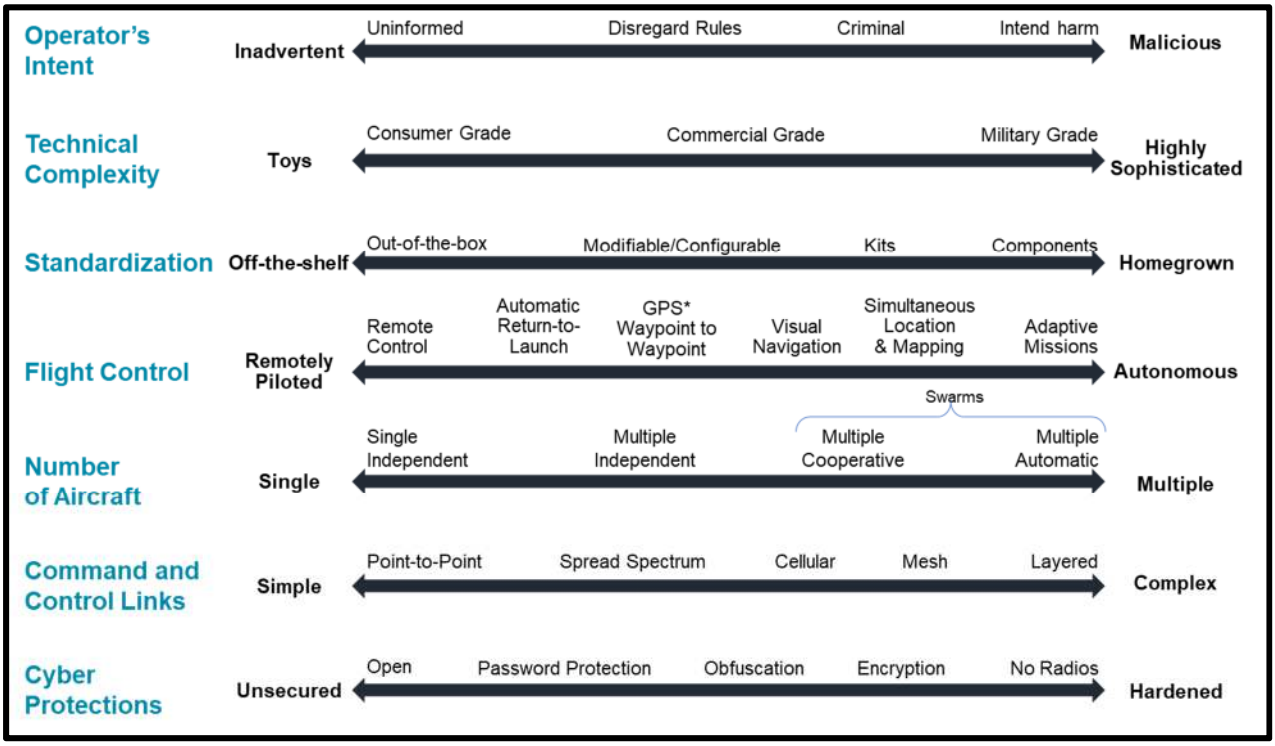

Figure 1 - UAS Threat Characteristics Spectrum

1. **Operator's Intent:** More than any other factor, the operator's intentions determine the sUAS threat. The vast majority of sUAS operations are lawful and well intentioned. Most unauthorized sUAS events are typically inadvertent, usually the result of operator ignorance, incompetence, or both.[11] That said, even innocuous sUAS incidents can cause disruption and harm—for example, when someone flies their sUAS in a restricted area, such as an approach path to an airport.[12] The biggest threats, however, come from motivated and competent operators, such as lone-wolves, asymmetric adversaries, or state actors with nefarious intentions. They could have at their disposal highly sophisticated and lethal equipment, combined with well-developed tactics, techniques and procedures.[13] It can be extremely difficult to discern intent when detecting an unauthorized sUAS and this presents significant challenges for security and law enforcement agencies.

[11] Disruption of CAL FIRE Helicopter Operations is an example of non-malicious yet hazardous sUAS operations.
[12] The FAA funded some research into the potential effects of small drones impacting an air transportation aircraft.
[13] The attack on Abu Dhabi Airport by Yemeni rebels is an example of planned high-end attack employing sUAS.

2. **Technical Complexity: sUAS** range in sophistication from rudimentary toys, barely capable of staying airborne, to military-grade, highly autonomous, long-range, zero-RF-emissions systems capable of delivering ordnance. In general, the entire spectrum of sUAS is rapidly becoming more sophisticated. Even the sUAS intended for entertainment purposes offer high-end features such as altitude hold, position hold, waypoint navigation, and even target following. With advancements in sensors, materials, processing capacity, energy storage/battery systems, and propulsion systems coupled with novel airframe configurations, drones are rapidly improving in all dimensions and performance criteria. They are becoming smaller, fly faster, and can fly further. They see further, wider, and with higher resolution—and they can carry more and operate more quietly. All these characteristics make them more disruptive, potentially lethal, and difficult to defend against. New system capabilities are made possible through rapid prototyping, computer-aided design, additive manufacturing (3D printing),[14] and wide-scale collaboration enabled by the internet. Examples of highly capable complex airframes include multi-copter/fixed wing hybrid airframes[15] that can take off and land vertically and fly with the efficiency and range of a fixed-wing aircraft; sUAS powered by small turbine engines and rockets that enable fast cruise speeds; and efficient high-aspect-ratio, low-weight wings that allow extremely long endurance flights.

3. **Standardization:** sUAS range from ready to fly[16] standardized commercially available devices to "home grown" non-standard, highly customized systems. They can be made from components available in the open market or from scratch.[17] To appeal to a broader market, most commercially available sUAS are manufactured ready-to-fly "out of the box." They are simple to fly and because information about them is openly available, they are also more straightforward to defend against. However, some commercially available drones with adjustable settings can be easily modified. Even small changes or modifications can make sUAS significantly more difficult to detect and hardened against attacks. For example, instead of automatically returning home once communications are lost, some systems allow operators to simply check a box to keep the aircraft flying on the planned path.

   The variability of custom-made sUAS make their performance and composition extremely unpredictable and difficult to assess—and defeat in a timely fashion. In addition, manufacturers are making some "off-the-shelf" systems more difficult to detect and/or defeat. Primarily because of demand for highly reliant and secure systems, sUAS manufacturers are employing technologies and techniques to increase sUAS capabilities and reliability. This translates to more lethality and hardening if the operator wants to use the sUAS for nefarious purposes. These new technologies include machine-learning-enabled machine vision, artificial-intelligence-driven autonomous control systems, and

---

[14] https://www.mitre.org/publications/project-stories/nibbler-drone-is-an-advanced-manufacturing-flagship-for-marines

[15] L3 Latitude sUAS is an example of highly capable complex airframe

[16] The DJI Phantom 4 is a highly capable mass produced standardized sUAS.

[17] This is an example of an improvised, non-standard, "homemade" sUAS constructed from readily available components and "crowd-sourced" information.

highly optimized airframes made possible by computer numerically controlled processes and additive manufacturing (i.e., 3D printing).

4. **Flight Control:** Control systems have evolved from being very simple (the operator directly issues commands that manipulate flight control surfaces) to multi-layered sUAS control systems (operators provide input to onboard automatic flight control systems that manage basic flight functions and issue commands to manipulate flight control surfaces). Currently, most sUAS require some operator input to function properly during flight. For sUAS that rely on real-time radio control and telemetry, disrupting the communications link can cause the drone to crash, land, stop, or return to launch location. However, technology continues to evolve toward increasingly autonomous systems that can operate independently of the human operator and thus without constant direct communications. This technology is enabled by rapidly improving memory, computing power, and sensors.[18] In addition, advances in automated algorithms, including visual navigation, and simultaneous location and mapping[19], have reduced drones' dependency on GPS for navigation. Without any RF emissions to detect and/or interfere with (or without GPS to jam) detecting and defeating a sUAS becomes extremely difficult.[20]

5. **Numbers of Aircraft:** Currently, most sUAS have one operator per drone. In the future, a single sUAS operator will routinely be able control multiple drones. With improved autonomy, multiple drones operating in concert without direct control of an operator is possible.[21] Researchers are working on technology that would enable swarms of drones to operate cooperatively and self-organize to fulfill missions. The downside of this technology is that multiple air vehicles used in an attack greatly improve their chance of survivability and lethality, complicating counter-UAS operations.

6. **Command and Control (C2) Links:** Today, C2 for most sUAS is conducted through radio frequency (RF) communication links for at least part of the flight. While RF links are most common, signals can also be transmitted via other means, such as laser or infrared transceivers. Most sUAS C2 links use direct RF radio communications on standard Industrial, Scientific and Medical (ISM) Bands, such as 433 MHz, 900 MHz, 1.2 GHz, 2.4 GHz, and 5.8 GHz.[22] Many of these sUAS C2 links evolved from common WiFi protocols. Much of today's counter-UAS technology relies on detecting, interrupting, or introducing errors in C2 RF links. To increase the reliability and integrity of operations, sUAS developers and manufacturers employ ever-more sophisticated systems and techniques, such as frequency

---

[18] Skydia is an example of highly automated sUAS that can navigate, follow or home without GPS employing only optical sensing, machine learning and artificial intelligence, requiring only monitoring by an operator.
[19] http://everobotics.org/pdf/SLAMTutorial.pdf
[20] The Pixhawk is a low-cost widely available sUAS autopilot that can enable a sUAS to fly an entire mission without input from the operator.
[21] Perdix demonstrated the feasibility of large numbers of swarming autonomous micro sUAS.
[22] RMileC is an example of readily available, highly capable, "long range" UHF sUAS radio control systems.

hopping and wireless mesh networks[23]. This has the unintended consequence of making it difficult for the appropriate authorities to detect and defeat unauthorized operations. Soon, widely available links such as cellular 4G/5G are expected[24] to be employed, which would allow sUAS to effectively "hide in plain sight," by appearing like any other mobile device on the network. As swarms become more popular, we will see increases in the use of mesh-based links capable of robust reconfigurations to ensure solid communications between drones. Commercial drone manufacturers will use more layered approaches, similar to military communication systems, giving drones several communications options ranging from ISM to cellular to satellite communications.

7. **Cyber Protections:** Cyber protections are a subset and entwined with both C2 link and autopilot capabilities and vulnerabilities.[25] Most of today's sUAS employ the same cyber protections as those used in information systems, including securing access with passwords, data obfuscation[26], and encryption. In sophisticated applications, a sUAS can be cut off from external input by deactivating or removing communications systems. These measures significantly increase sUAS security, but also complicate efforts to mitigate nefarious sUAS operations.

As technology develops and prices continue to drop, sUAS with characteristics on the right side of the sUAS Threat Characteristics Spectrum will become increasingly available to more people. And with that increased availability, the volume and possibly the degree of sUAS threats will grow.

C. Category of Threat

The most common sUAS threats can be grouped into the following four categories:

Interference: The simple presence of a drone in the wrong place can interfere with the operations of a government agency or industry. For example, a drone can pose a foreign-object-damage hazard that will shut down an airspace, airport ramp, or runway. A drone's RF emissions can interfere with wireless networks and communications systems. In some situations, a drone in the air can threaten people enough to alter their behavior on the ground.[27] Examples of interference that have already been observed include:

- Interruption of first responder and emergency flight operations during disaster events, such as wildfires and hurricanes.[28]
- Interruption of sporting events due to the presence of unauthorized sUAS.[29]

---

[23] The DJI Mavic uses frequency-hopping, multi-spectrum proprietary links that carry command, telemetry and sensor data which includes real time high definition video.

[24] C2 systems employing existing cellular networks enable long range sUAS operations.

[25] Concerned about sUAS cybersecurity vulnerabilities, the DoD has limited its use of commercial off the shelf sUAS.

[26] Data obfuscation (DO) is a form of data masking where data is purposely scrambled to prevent unauthorized access to sensitive materials.

[27] https://mwi.usma.edu/drones-tactics-unmanned-platforms-will-change-way-infantry-fights/

[28] sUAS have interrupted first responder operations.

[29] Example of sporting events interrupted by sUAS. Drone Crashes into Stands During Tennis Match

- Rerouting of flight operations at a major airport resulting from a sUAS simply flying in the vicinity of the approach and departure corridors[30] or within the airport boundaries.

Intelligence, Surveillance, and Reconnaissance (ISR): sUAS that are portable, relatively low-cost, easy to operate, and capable of carrying highly sophisticated sensor packages are most commonly used to conduct ISR[31]. Because of their small size, sUAS can hide in plain sight. Drones do not have to be airborne to conduct ISR. They can fly to a vantage point and "perch," allowing them to extend time for conducting ISR by conserving power. A drone can also deliver small sensors to persistently cover a wide area. Examples of ISR threats include:

- Pre-mission intelligence
- Post-mission assessment
- Individual privacy invasion
- Real-time target spotting/overwatch, including spotting of law enforcement on the Southwest border[32] [33]
- Industrial espionage[34]
- Coordination of ground attacks
- Gathering of images for future operational use and propaganda purposes

Smuggling/Conveyance: sUAS have proven to be an effective means of bypassing traditional checkpoints and other physical security by allowing contraband to infiltrate otherwise secure perimeters. Examples of smuggling with sUAS include:

- Delivering drugs, cell phones, or other contraband into prisons[35] [36]
- Transporting drugs and other illegal material across international borders[37]

Weaponization: sUAS can carry and dispense a wide variety of small payloads. These payloads can range from improvised chemical, biological, radiological, nuclear, and explosives devices to RF jammers.[38] The sUAS themselves can also be used as projectiles, potentially causing damage or injury. Examples of kinetic threat include sUAS employed to:

- Precisely deliver explosives[39]
- Attack aircraft in flight

---

[30] An example of a small drone flying in close proximity of an airliner; Gatwick Airport Disruptions

[31] sUAS have been used to plan coordinate, conduct attacks as well as capture propaganda video material

[32] https://www.upi.com/Australian-drug-gang-suspected-of-using-drone-to-monitor-police/2911498801791/

[33] https://www.washingtonpost.com/world/national-security/illicit-drone-flights-surge-along-us-mexico-border-as-smugglers-hunt-for-soft-spots/2018/06/24/ea353d2a-70aa-11e8-bd50-b80389a4e569_story.html?utm_term=.faf0548967d1

[34] https://www.dedrone.com/press/corporate-espionage-being-enabled-by-drones

[35] https://www.bbc.com/news/av/uk-36302136/footage-shows-drone-delivering-drugs-to-prisoners

[36] https://abcnews.go.com/beta-story-container/US/mother-daughter-arrested-drone-deliver-contraband-prison-roof/story?id=59894154

[37] https://www.washingtontimes.com/news/2017/aug/20/mexican-drug-cartels-using-drones-to-smuggle-heroi/

[38] In 2018, 2 sUAS explosives detonated in close proximity of Venezuela's president.

[39] On January 10, 2019 a drone reportedly targeted a Yemeni government base during a military parade, allegedly killing six people and wounding many others, including several senior officers. BellingCat Article

- Deliver chemical/biological agents[40] [41]
- Cause mass panic in a public gathering such as a stadium

D. Concluding Thoughts

MITRE's experience working with various detection and defeat technologies coupled with our focus on our sponsors' missions and our deep understanding of sUAS capabilities have led to the following observations/recommendations:

- **Make sUAS Readily Identifiable:** Establish a mechanism to identify and track in real-time authorized drone operations, especially for drones operated beyond the visual line of sight of the operator.[42] This would likely include requiring all drones to broadcast a unique identification and their position at regular intervals. This will assist security agencies, law enforcement officials, and aviation regulators in ensuring authorized drone operations do not pose safety and security threats. It would also help to quickly rule out compliant from non-compliant drones and allow law enforcement and security personnel to focus attention on potential bad actors operating without authorization (e.g., those operating without identification). A mechanism to detect unauthorized operations (e.g., radar, acoustic sensors, lidar) will complement tracking of authorized operations.

- **Focus Detection and Defeat Mechanisms on Immutable Features:** As technology matures, detection and defeat mechanisms relying on RF communications links and GPS will become less and less effective. Research and development should focus on detect and defeat mechanisms that concentrate on immutable features[43], such as the 1) airframe mass, 2) on-board electronics, and the 3) means of propulsion. As legal authorities for using counter-UAS technology continue to mature, ensuring law enforcement and security personnel are well positioned to detect and defeat new and emerging UAS threats is critical.

- **Increase Operator Education and Training:** Continue to develop and evolve education and training for operators[44] to ensure compliance with applicable laws and regulations and reduce unintended operational actions that degrade safety and security.

- **Maintain sUAS Technology Awareness:** Given the rapid evolution of the technology associated with sUAS, there needs to be a concentrated effort to monitor trends in the

---

[40] https://www.reuters.com/article/us-venezuela-politics-drones/apparent-attack-in-venezuela-highlights-risk-of-drone-strikes-idUSKBN1KQ0MG

[41] https://www.washingtonpost.com/news/monkey-cage/wp/2018/08/10/are-drones-the-new-terrorist-weapon-someone-just-tried-to-kill-venezuelas-president-with-a-drone/?noredirect=on&utm_term=.0485b83aac2c

[42] The FAA has commenced the process of developing sUAS identification and tracking rules.

[43] Radar and Interceptor drones are examples of detection and defeat systems that exploit immutable characteristics instead of RF signatures.

[44] "Know Before You Fly" educational program is a collaboration between industry and the FAA

advancement of technology. In addition, detection and defeat mechanisms need to be continually tested against and exercised with the latest sUAS systems.[45]

- **Enhance Defense Through Resiliency and Layers:** There is no one sensor modality that is likely to be sufficient for detecting all sUAS in all circumstances.[46] The most effective system is one that leverages multiple sensor modalities (e.g., radar, RF, and acoustic) to detect aircraft. Acquired tracks from multiple sensor modalities will need to be correlated to ensure an accurate operational understanding of potential threats. Similarly, no single defeat mechanism is likely to have sufficient system-level performance in terms of probability of success, range, and minimization of collateral risks to mitigate all threats. Thus, multiple defeat mechanisms used in tandem are likely to be the most effective in ensuring appropriate mitigation success.

MITRE is sharing our sUAS threat characterization to help the community understand the nature of potential threats and to provide a common vernacular for discussing the technical challenges associated with detecting and defeating them. MITRE continues to work with the community to address the challenges posed by the sUAS threat.

[45] DHS Conducted Technical Assessment of C-UAS Technologies in Cities (TACTIC) to evaluate the state current C-UAS systems.
[46] AUDS is an example of multi-mode C-UAS system.