HOMELAND SECURITY ADVISORY COUNCIL

FINAL REPORT OF THE EMERGING TECHNOLOGIES SUBCOMMITTEE

UNMANNED AIRCRAFT SYSTEMS

February 24, 2020

This page is intentionally left blank.

This publication is presented on behalf of the Homeland Security Advisory Council, Emerging Technologies Subcommittee, under Co-Chair Thad Allen, and Co-Chair Cathy Lanier and Vice Chair Robert Rose as the ***Final Report*** and recommendations to the Acting Secretary of the Department of Homeland Security, Chad F. Wolf, regarding Unmanned Autonomous Systems (UAS) and Counter UAS (C-UAS).

<SIGNATURE OBTAINED FOR PDF COPY>

Thad Allen (Co-Chair)

Cathy Lanier (Co-Chair)

Robert Rose (Vice-Chair)

This page is intentionally left blank.

EMERGING TECHNOLOGIES SUBCOMMITTEE

Thad Allen (Co-Chair) – Executive Vice President, Booz Allen Hamilton
Cathy Lanier (Co-Chair) – Senior Vice President and Chief Security Officer, National Football League
Robert Rose (Vice-Chair) – Founder and President, Robert N. Rose Consulting LLC
Frank Cilluffo – Director, McCrary institute for Cybersecurity and Critical Infrastructure Protection, Auburn University
Mark Dannels – Sheriff, Cochise County Arizona
Carie Lemack – Co-Founder and CEO, DreamUp
Jeffrey Miller – Vice President of Security, Kansas City Chiefs

HOMELAND SECURITY ADVISORY COUNCIL STAFF

Mike Miron, Acting Executive Director, Homeland Security Advisory Council
Evan Hughes, Associate Director, Homeland Security Advisory Council

This page is intentionally left blank.

TABLE OF CONTENTS

This page is intentionally left blank.

EXECUTIVE SUMMARY

The accelerated pace of technological change in today's global research and development ecosystem creates both risk and opportunity within the Department of Homeland Security's (DHS) mission domain. While emerging technologies may comprise powerful capabilities that can be used by operational end users, they may also pose threats for which no effective countermeasures readily exist. The challenge of addressing emerging technological threats to the Homeland while simultaneously acquiring and deploying capabilities to meet new threats is of paramount importance now and in the foreseeable future. This report provides an assessment of the current state and perceived future advancements over the next 3-10 years that could pose a threat to the homeland security of the United States, as well as recommendations for mitigation.

Evolving legal frameworks, such as the recently-passed FAA Reauthorization, provide new authorities; however, they also increase the complexity of implementing policy and deployment capabilities across the federal government and within DHS. Additional difficulties arise when implementation must be coordinated with state, local, tribal, and territorial (SLTT) authorities.

BACKGROUND

The Secretary chartered the Emerging Technologies Subcommittee of the Homeland Security Advisory Council (HSAC) in the Fall of 2018 to assist DHS with forecasting both threats and opportunities, working with partners, and improving the ability of DHS components to execute mission critical objectives. The subcommittee was charged with exploring six emerging technologies with an intent to develop recommendations for addressing and mitigating threats while also identifying capability advantages to support DHS missions. These technologies include:

- Unmanned Autonomous Systems (UAS)
- Artificial Intelligence and Machine Learning (AI/ML)
- 3/4-D Printing
- Biotechnology – Gene Editing, Splicing
- Quantum Information Science and Quantum Computing
- Advance Robotics

The subcommittee's initial work was impacted by personnel changes in DHS, the partial government shutdown, and the level of subcommittee participation. Accordingly, the subcommittee submitted an "interim" report on May 21, 2019 and recommended that its work continue until tasking provided by the Secretary was completed. The interim report addressed four of the six technologies contained in the subcommittee's tasking: UAS, AI/ML, 3/4-D Printing, and Biotechnology.

This final report addresses the ongoing technological and legal challenges posed by UAS/C-UAS in the immediate and near future. Remaining technologies will be addressed in separate reports.

This page is intentionally left blank.

.

EMERGING TECHNOLOGIES: UNMANNED AUTONOMOUS SYSTEMS (UAS)

1. DHS Authority for Countering Unmanned Aircraft Systems (UAS)

The Department of Homeland Security (DHS) and Department of Justice (DOJ) received their grant of counter-UAS (C-UAS) authority in the Preventing Emerging Threats Act of 2018, as part of the Federal Aviation Administration (FAA) Reauthorization Act. For certain authorized DHS and DOJ personnel and missions, the legislation specifically permits the departments to:

- detect, identify, monitor, and track UAS without prior consent,
- warn the operator of the UAS, including by electromagnetic means,
- disrupt control, seize control, or confiscate the UAS without prior consent, and
- use reasonable force to disable, damage, or destroy the UAS.

For DHS, the legislation authorizes the department to protect “covered assets and facilities” based upon certain missions, to include:

- Customs and Border Patrol (CBP) and U.S. Coast Guard (USCG) security and protection operations, including the security of facilities, aircraft, and vessels whether moored or underway,
- U.S. Secret Service (USSS) protection operations, and
- U.S. Federal Protective Service (FPS) protection of government facilities.

The statute also enables the protection of certain joint missions performed by both DHS and DOJ, to include:

- protection of National Special Security Event (NSSE) and Special Event Assessment Rating (SEAR) events,
- support to State, Local, Territorial, and Tribal (SLTT) law enforcement at the request of the governor (or equivalent) to protect mass gatherings, and
- protection of active federal law enforcement investigations, emergency responses, and security operations.

Covered assets and facilities must relate to one of the missions above and be:

- located in the United States, including territories and possession, territorial seas and navigable waters,
- identified by DHS and/or DOJ, in coordination with Department of Transportation (DOT)/FAA as high-risk and a potential target for unlawful UAS activity through a risk-based assessment, and
- designated by DHS Secretary and/or the Attorney General.

Both Departments conduct a C-UAS technology research, development, test, and evaluation (RDT&E) process, as well as operational testing in coordination with FAA at the component/user level before any technological solution can be acquired or deployed. The law requires DHS and DOT to notify Congress within 30 days of deploying any new C-UAS technology.

Since the Interim report, DOJ/DHS has conducted testing of detection, tracking, and mitigation at several venues.[1] For each test site, extensive documentation was necessary to meet the requirements of the legislation and obtain the approval of either the Attorney General or the Secretary of Homeland Security. In some cases, the process took up to eight weeks to complete. The current legal and policy framework is not agile enough to support UAS/C-UAS operations and essentially moots the authorities granted by bureaucratic processes that inhibit effective threat identification, response, and mitigation in time sensitive situations.

The Preventing Emerging Threats Act only provides C-UAS authority to DOJ and DHS. It does not provide any authority to other key Federal law enforcement agencies, SLTT, or private entities. Consequently, these Federal and SLTT agencies, which may be in the best position to deter, detect, and investigate unauthorized UAS, remain subject to the same federal criminal laws that previously restricted DHS and DOJ C-UAS activities.

2. UAS Technology Development and Threat Assessment (3 to 10 Years)

Ten years ago, most non-military UAS were remotely piloted aircraft that were custom built and flown by model aircraft enthusiasts for personal entertainment. Today, there are highly capable commercial systems available for a few hundred dollars ready to be flown by operators that require little or no training. There are now over 1.5 million registered UAS.[2] Market driven forces are encouraging rapid development of autonomous systems, subsequently yielding new use cases and technologies, such as highly networked package delivery, persistent communications, and urban mobility systems carrying freight and even passengers. Innovation in this market sector is extremely rapid.[3] Models become obsolete within less than a year. Systems are becoming more capable and sophisticated, and the barriers to entry in terms of the necessary expertise of the operator are quickly diminishing. Enterprises are employing increasingly larger fleets and more individuals are becoming drone operators.[4] This is especially true of small UAS (i.e., airframes which weigh less than 55 lbs.). This increase in aircraft volume by organizations and individuals pose a potential significant public safety and security issue, especially in urban areas.

Currently, the vast majority of industrialized countries are actively pursuing national strategies that promote widespread use and integration of UAS, with some developing small UAS weapons systems.[5] In the U.S., integration of UASs capable of sustained, routine, autonomous, beyond line of sight operations in mixed use airspace is ultimately the goal. To get there, UAS manufactures are going to have to build *systems* (both the UAS and the supporting traffic management) to support that activity. That means integrating autonomous features that allow the UAS to sense and operate in a dynamic environment. Using artificial intelligence, deep learning and big data to draw from they will be capable of navigating complex environments by understanding weather, air traffic congestion and avoidance, system health and loss of data link

[1] C-UAS Operations in 2019 include: Super Bowl LVIII (Atlanta, Ga)., United Nations General Assembly, (NY.), the New York City Marathon (NY), the Macy's Thanksgiving Day Parade (NY), and the World Series (Houston/Washington, DC)

[2] Federal Aviation Administration, "UAS by the Numbers," 10 December 2019, https://www.faa.gov/uas/resources/by_the_numbers/

[3] 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/).

[4] Federal Aviation Administration, "FAADroneZone," https://faadronezone.faa.gov.

[5] Congressional Research Service (CRS), "U.S. Ground Forces Robotics and Autonomous Systems (RAS) and Artificial Intelligence: Considerations for Congress," R45392, November 20, 2018.

protocols.[6] They will also leverage more efficient means of fuel and power management from lithium or hydrogen batteries and greater endurance in range and payload. They may leverage emerging 5G due to the size of the pipe and ability to transfer large amounts of data with reduced latency over longer distances.[7]

By 2030 we can expect to see a fully integrated airspace with UAS's operating in close proximity to airports and other sensitive sites; collecting data and doing inspections on critical infrastructure such as pipelines and power lines. Robotic features will likely be incorporated to allow simple taskings such as opening access panels, removing/tightening screws, or repairing downed lines. We should also see significantly smaller UAS's being used for internal 3-D mapping purposes in mines, collapsed structures, and other tactical applications. UAS fleet operations should be well established, with the systems capable of communicating with each other to gather data and coordinate tasks.[8]

2.1 UAS Threat Characteristics Spectrum

To illustrate development trends and their potential implications as a security threat, the MITRE Corporation developed *A UAS Threat Characteristic Spectrum.*[9] This spectrum characterizes seven different dimensions, to include operational and technical characteristics. Understanding the current state of each of these characteristics and extrapolating them into the future can help indicate potential future threats. *Figure 1* illustrates the range of UAS characteristics, with difficulty to detect and counter increasing from left to right.

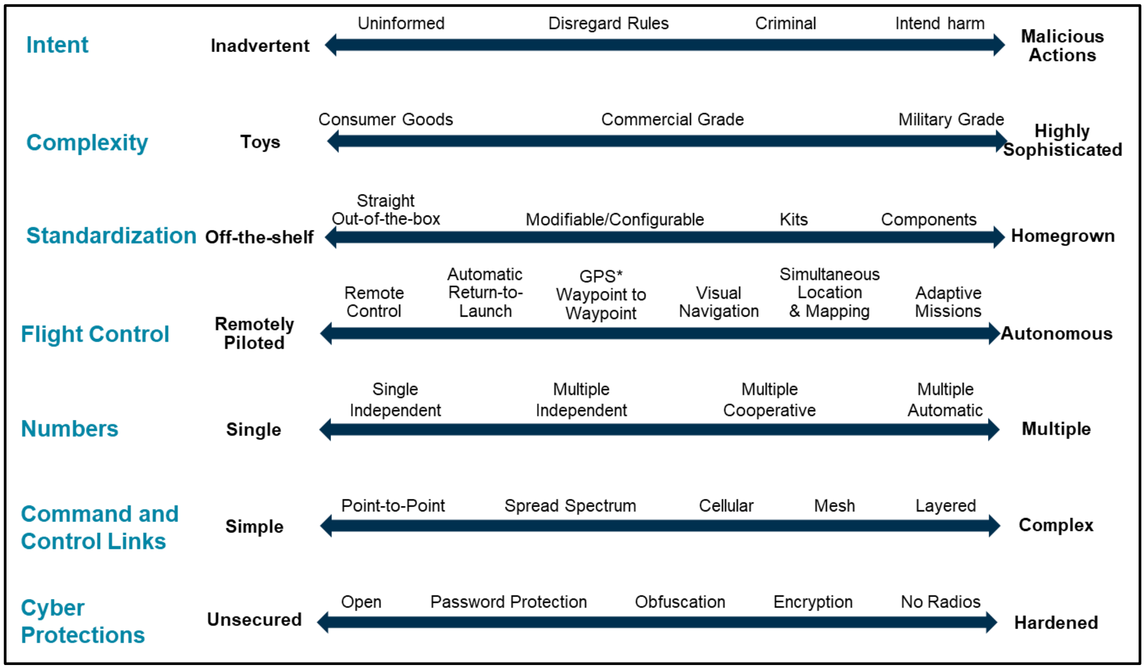


Figure 1: UAS Threat Characteristics Spectrum

[6] Hewitt, William. *"RE: UAS/CUAS SME feedback for HSAC."* Received by Cathy Lanier, 6 December 2019.

[7] ETSI Magazine, *"Unmanned Aerial Systems Over 5G",* Flynn, Kevin. November 18, 2019: https://www.3gpp.org/technologies/keywords-acronyms/2090-unmanned-aerial-systems-over-5g

[8] Ibid. Hewitt, William.

[9] See, "Small Unmanned Aircraft: Characterizing the Threat," MITRE Corporation, February 2019, https://www.mitre.org/sites/default/files/publications/pr-18-3852-small-uas-characterizing-threat.pdf.

Operator's Intent: More than any other factor, the operator's intentions determine the severity of the UAS threat. The vast majority of UAS operations are lawful and beneficial. Currently, unauthorized UAS events are typically inadvertent and benign, usually the result of operator ignorance and/or incompetence.[10] However, even innocent UAS incidents can cause disruption and harm. A motivated and competent operator, ranging from a lone-wolf to a state actor, intent on causing harm can employ highly sophisticated and lethal equipment, procedures, and tactics to that end.[11]

Technical Complexity: UAS range in sophistication from rudimentary toys barely capable of staying airborne to military grade, highly autonomous, long-range, zero- radio frequency (RF) emissions systems capable of delivering ordnance. In general, the entire spectrum of UAS is rapidly becoming more sophisticated. Even in common consumer devices, formerly high-end features such as altitude hold, GPS hold, and waypoint navigation are now commonplace. With advancements in sensors, processing capacity and propulsion systems, coupled with novel airframe configurations, drones are rapidly improving in all dimensions and performance criteria. They are becoming smaller, larger, faster, quieter, and more capable of flying further, seeing further and wider, transmitting higher resolution imagery and full-motion video, and carrying larger payloads. All these characteristics make them more disruptive, potentially lethal, and difficult to defend against. Rapid prototyping is made possible by computer-aided design, additive manufacturing (3D printing), and wide-scale collaboration enabled by the Internet. Examples of highly capable complex airframes include multi-copter/fixed wing hybrid airframes that can take off and land vertically and fly with the efficiency and range of a winged aircraft; UAS powered by smaller turbine engines and rockets that enable fast cruise speeds; and, highly efficient high-aspect ratio low-weight wings that allow extremely long endurance flights.[12] Control systems have evolved from simple direct control of flight control surfaces to multi-layered UAS control where operators provide input to onboard automatic flight control systems that manage basic flight functions. Rapid development in machine learning, which has enabled machine vision and networked sensing, in conjunction with artificial intelligence has already yielded systems with multiple aircraft that can operate with mere monitoring by an operator.[13]

Standardization: UAS standardization ranges from ready-to-fly (RTF), standardized commercially available devices to "home grown," non-standard, highly specialized systems made from components available in the open market or made from scratch.[14] To appeal to a broader market, most commercially available consumer-grade UAS are manufactured Ready-to-Fly (RTF) "out of the box." With information about them openly available, consumer-grade RTF systems are somewhat easier to defend against. Many UAS have adjustable settings or can be easily modified. Even small changes or modifications can make UAS significantly more difficult

[10] Disruption of CAL FIRE Helicopter Operations is an example of non-malicious yet hazardous UAS operations. See, Betsy Lillian, "Drone Disrupts CAL FIRE Helicopter Operations," Unmanned Aerial Online, 27 June 2018, https://unmanned-aerial.com/drone-disrupts-cal-fire-helicopter-operations.

[11] The attack on Abu Dhabi Airport by Yemeni rebels in July 2018 is an example of planned high-end attack employing UAS. See, "Yemen's rebels 'attack' Abu Dhabi airport using a drone," AlJazeear, 27 July 2018, https://www.aljazeera.com/news/2018/07/yemen-rebels-attack-abu-dhabi-airport-drone-180726155103669.html.

[12] L3 Latitude UAS is an example of highly capable complex airframe. See, "Products," Latitude Engineering, https://www.latitudeengineering.com/products/hq/.

[13] Skydia is an example of highly automated UAS that can navigate, follow, or home without GPS employing only optical sensing, machine learning, and artificial intelligence, requiring only monitoring by an operator. See, "Technology," Skydio, https://www.skydio.com/technology/.

[14] The DJI Phantom 4 is a highly capable mass produced standardized sUAS. See, "Phantom-4," DJI, https://www.dji.com/phantom-4; For an example of an improvised, non-standard, "homemade" sUAS constructed from readily available components and "crowd-sourced" information see, "Big Wing Easystar," RCGroups.com, 7 August 2008, https://www.rcgroups.com/forums/showthread.php?810365-Big-Wing-Easystar.

to detect and harden them against attacks. The variability of custom-made UAS make their performance and composition extremely unpredictable and difficult to assess and subsequently defeat in a timely fashion. Likewise, "off the shelf" systems are also becoming more difficult to detect and mitigate. Primarily because of market demand for highly reliant and secure systems, UAS manufacturers employ technologies and techniques to increase UAS capabilities and reliability, which translate to more potential lethality and survivability when the UAS is used for nefarious purposes. These technologies include machine learning-enabled machine vision, artificial intelligence-driven autonomous control systems, and highly optimized airframes made possible by computer numerically controlled (CNC) and additive (3D printing) manufacturing.

Flight Control Autonomy: Many drones now have some measure of autonomy–the ability to operate independently without communications, determining action by itself. Currently, most UAS require significant operator input and rely on external information to properly function. Most UAS rely on real-time radio control as well as telemetry and GPS for navigation to function. Disrupting any one of these radio links can cause the drone to crash, land, stop, or return to home. With rapidly improving memory, computing power, and sensors, UAS capable of flying missions autonomously, without any user input and without relying on GPS for navigation, are fast becoming a reality. Without any emissions to detect or GPS to jam, detecting and defeating a UAS becomes extremely difficult.[15]

Numbers: Multiple air vehicles greatly improve UAS survivability and lethality while at the same time complicating C-UAS operations. Currently, most UAS have one operator per drone. Whilst still uncommon, a UAS operator can now control multiple drones. With improved autonomy, multiple drones operating in concert without direct control of an operator is possible.[16]

Command and Control (C2) Links: With very few exceptions, UAS will operate with C2 Links for at least part of, but usually throughout, operations. RF links are most common, though signals can also be passed via other means like laser or IR transceivers. Current UAS links are RF networks on standard Industrial, Scientific and Medical (ISM) Bands (such as 2.4 GHz, 5.8 GHz, 1.2 GHz, 900 MHz and 433 MHz bands), many versions of which evolved from common Wi-Fi protocols.[17] Most C-UAS technologies rely on detecting, interrupting, or introducing errors in UAS. Responding to perceived threats very similar to those posed to information systems, UAS developers and manufacturers employ ever more sophisticated systems and techniques to assure the UAS C2 integrity, such as frequency hopping and wireless mesh and layered networks.[18] Widely available links, such as cellular 4G/5G, are expected to be employed allowing UAS to "hide in plain sight" and take advantage of statutory privacy protections.[19]

Cyber Protections: Cyber protections, while a subset of C2 link assurance, are specifically addressed here because they are commonly exploited UAS vulnerabilities.[20] Currently, UAS

[15] The Pixhawk is a low-cost widely available UAS autopilot that can enable a sUAS to fly an entire mission without input from the operator. See, Pixhawk, http://pixhawk.org.

[16] Perdix demonstrated the feasibility of large numbers of swarming autonomous micro sUAS. See "Department of Defense Announces Successful Mico-Drone Demonstration," New Release No: NR-008-17, U.S. Department of Defense, 9 January 2017, https://dod.defense.gov/News/News-Releases/News-Release- View/Article/1044811/department-of-defense-announces-successful-micro-drone-demonstration/.

[17] RMileC is an example of readily available, highly capable, "long range" UHF UAS radio control systems. See, "RMILEC NB20 20 Channel UHF LRS System," HobbyKing, https://hobbyking.com/en_us/rmilec-nb20-20-channel-uhf- lrs-system.html.

[18] The DJI Mavic uses frequency-hopping, multi-spectrum proprietary links that carry command, telemetry and sensor data which includes real time high definition video. See, "Mavic Pro," DJI, https://www.dji.com/mavic/specs.

[19] C2 systems employing existing cellular networks enable long range sUAS operations. See, Globe UAV, http://g- uav.com/en/index.html.

[20] Concerned about sUAS cybersecurity vulnerabilities, the DoD has limited its use of commercial off the shelf sUAS. See, Gidget Fuentes,

employ cyber protections like those employed in information systems, such as securing networks with passwords, data obfuscation, and encryption. In extreme C-UAS cases, the UAS is cut off from external input by deactivating or deleting communications systems through cyber channels. All these measures significantly increase UAS operational security but also complicate efforts to mitigate nefarious UAS operations. In the next 10 years, UAS toward the right side of this spectrum in *Figure 2* (more difficult to counter) will become more readily available as technology develops and their price continues to drop.

2.2 Common UAS Threat Types

The most common UAS threats can be grouped into four categories: interference; intelligence, surveillance, and reconnaissance (ISR); kinetic; and smuggling or conveyance. These are expanded on below.

Interference: The simple presence of a drone can interfere with normal operations. A drone poses a foreign object damage hazard to operating aircraft and can deny the use of airspace, a ramp, or a runway. A drone's RF emissions can interfere with wireless networks and communications systems. With some context, a drone can threaten people enough to alter their behavior. 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,[21]
- interruption of sporting events due to the presence of unauthorized UAS,[22] and
- disruption of flight operations at a major airport resulting from a UAS flying, even if absent of malicious intent, in the vicinity of the approach and departure corridors or within airport boundaries.[23]

Intelligence, Surveillance, and Reconnaissance (ISR): Due to their portability, relatively low cost, ease to operate, and capability of carrying highly sophisticated sensor packages, UAS are most commonly used to conduct ISR. Because of their small size, UAS can hide in plain sight. Drones do not have to be airborne to conduct ISR.[24] They can fly to a vantage point and "perch" to conduct ISR for extended periods of time by conserving power.

A drone could also deliver small sensors to persistently cover a wide area. Examples of ISR threats include:

- pre-mission intelligence to post-mission assessment,
- individual privacy invasion,
- real-time target spotting/overwatch including spotting of law enforcement, such as on the southwest U.S. border,

"Pentagon Grounds Marines' 'Eyes in the Sky' Drones Over Cyber Security Concerns," USNI News, 18 June 2018, https://news.usni.org/2018/06/18/pentagon-grounds-marines-eyes-sky-drones-cyber-security- concerns.

[21] sUAS have interrupted first responder operations. See, Lexy Savvides, "California's fires face a new high-tech foe: Drones," CNET, 27 August 2018, https://www.cnet.com/news/californias-fires-face-a-new-high-tech-foe-drones/.

[22] For an example of sporting events interrupted by sUAS, see Drone Tech, "Gopro Karma Drone Quadcopter Crashes Into Crowd at Baseball Game," Youtube.com, 22 May 2017, https://www.youtube.com/watch?v=MCV38rSiQnk.

[23] For an example of a small drone flying in close proximity of an airliner, see, Drone and Tech, "Drone in near miss with airliner at Las Vegas McCarran international airport," Youtube.com, 3 February 2018, https://www.youtube.com/watch?v=MCV38rSiQnk.

[24] sUAS have been used to plan coordinate, conduct attacks as well as capture propaganda video material. See, Wall Street Journal, "Islamic State Uses Weaponized Drones Against Iraqi Forces," YouTube.com, 1 March 2017, https://www.youtube.com/watch?v=Xeqz4XI4Wag.

- industrial espionage,
- coordination of ground attacks, and
- gathering of images for future operational use and propaganda purposes.

Kinetic: UAS can carry and dispense a wide variety of small payloads. These payloads can range from improvised explosive devices (IEDs) to chemical/biological agents.[25] The UAS themselves can also be used as projectiles potentially causing damage or injury. Examples of kinetic threat include UAS employed to:

- precisely deliver explosives,
- attack an aircraft in flight,
- deliver chemical/biological agents, and
- cause mass panic in a public gathering or sporting event.

Smuggling/Conveyance: UAS 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 UAS include:

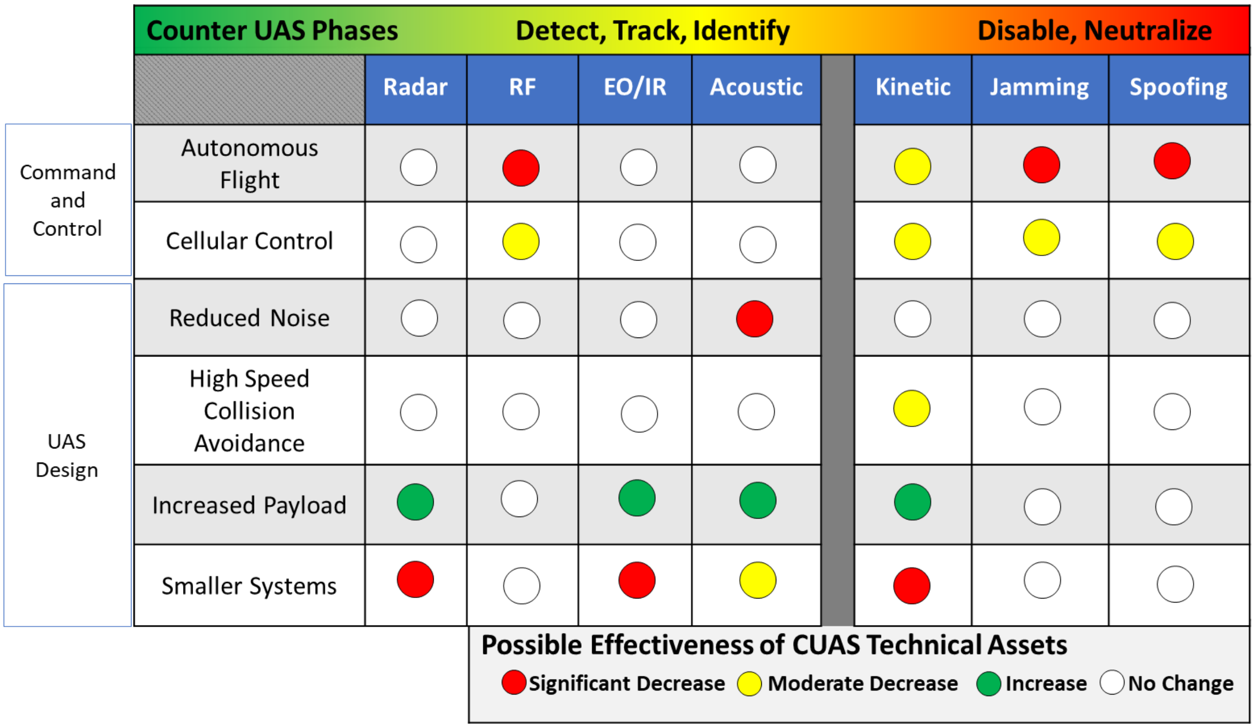
- carrying drugs, cell phones, or other contraband into federal, state and local prisons,
- transporting drugs or other contraband over international borders, and
- bypassing physical security checkpoints at federal buildings and courthouse.

3. Countering UAS (3 to 10 years)

Countering threats from nefarious or harmful UAS activity will become increasingly complex and will require the use of emerging and converging technologies in the future. The *C-UAS and Emerging Technology Matrix*[26] below illustrates the potential impact on C-UAS efforts in the future. Command and Control functions and UAS design features can also be combined resulting in different possible effects on C-UAS technical assets and alter the results. *Figure 2* illustrates the emerging and future challenges to each phase of the C-UAS options.

[25] In 2018, 2 sUAS explosives detonated in close proximity of Venezuela's president. See, Barbara Marcolini and Christoph Koettl, "How the Drone Attack on Maduro Unfolded in Venezuela," New York Times, undated, https://www.nytimes.com/video/world/americas/100000006042079/how-the-drone-attack-on-maduro-unfolded-in- venezuela.html.

[26] Unmanned Aircraft in the Homeland Security Environment. DHS Office of Intelligence and Analysis, UAS Threat Integration Cell. *"CUAS and Emerging Technology Matrix"*



	Counter UAS Phases	Detect, Track, Identify				Disable, Neutralize		
		Radar	RF	EO/IR	Acoustic	Kinetic	Jamming	Spoofing
Command and Control	Autonomous Flight	○	🔴	○	○	🟡	🔴	🔴
	Cellular Control	○	🟡	○	○	🟡	🟡	🟡
UAS Design	Reduced Noise	○	○	○	🔴	○	○	○
	High Speed Collision Avoidance	○	○	○	○	🟡	○	○
	Increased Payload	🟢	○	🟢	🟢	🟢	○	○
	Smaller Systems	🔴	○	🔴	🟡	🔴	○	○

Possible Effectiveness of CUAS Technical Assets

🔴 Significant Decrease 🟡 Moderate Decrease 🟢 Increase ○ No Change

Figure 2: C-UAS and Emerging Technology Matrix

3.1 Integrated Platforms

In the future, only advanced integrated platforms will be effective for detection and tracking, while kinetic systems will be needed for interception.[27] Some examples of emerging technologies include:

- Passive radar systems (also referred to as passive coherent location and passive covert radar) encompass a class of radar systems that detect and track objects by processing reflections from non-cooperative sources of illumination in the environment, such as commercial broadcast and communications signals. It is a specific case of bistatic radar, the latter also including the exploitation of cooperative and non-cooperative radar transmitters.
- Specialized Kinetic Payloads
    - Nanoribbons/Shape Memory Alloys
    - 40 mm Low Velocity Net Munitions
- Interceptor UAS ("Hunter Drones")
- Improvements to current radars
    - Smaller dimension, weight and cost can lead to mesh networks of radars
    - Incorporating micro-doppler radar techniques to discern UAS from biologicals and jet propulsion aircraft

[27] Patel, Bhargav. *"RE: UAS/CUAS SME feedback for HSAC."* Received by Cathy Lanier, 3 December. 2019.

RECOMMENDATIONS OF THE FINAL REPORT

The issues involving UAS/C-UAS are complex and extend across the federal government and vertically to state, local, tribal, and territorial governments. Accordingly, this report includes recommendations that are specific to DHS, as well as high-level recommendations regarding future HSAC efforts and challenges that extend beyond DHS.

Recommendations for Further Subcommittee Work

It is recommended that:

1. The subcommittee transition into a standing committee to continue its work until all of the taskings are completed and needed updates are submitted for UAS/C-UA.
2. The subcommittee work with the HSAC staff to identify and assign subject matter experts for the technologies under review, including access to technical writing staff at DHS Federal Funded Research and Development Centers (FFRDCs).
3. The subcommittee chair recommends membership adjustments to match the tasking provided.

Recommendations Regarding the Unmanned Aircraft System subset of the Unmanned Autonomous Systems

It is recommended that:

1. DHS continue to place a high priority on the implementation of the new authorities granted in the 2018 FAA Reauthorization, including adequate resourcing (staffing and operating funds) for DHS staff and components. To that end, the DHS implementation of the legislation and ongoing UAS/C-UAS efforts should be made a permanent program of record in appropriations.
2. DHS review the FAA legislation and consider proposing changes that would identify TSA’s role and authorities related to UAS/C-UAS and their relationship with SLTT authorities. While not within DHS purview or jurisdiction, it is noted that in addition to SLTT, there are other Federal partners whose authorities should be addressed in any future legislation; specifically, the United States Capitol Police and the United States Park Police. Additional consideration should be given to proposing changes in the limitation on information sharing during mitigation deployments.
3. DHS develop a capabilities matrix that arrays individual component activity across the following categories: internal policy guidance; doctrine development and maturity; research, development, test and evaluation of C-UAS; current and planned procurements; and, component specific missions and or authorities that preexist the FAA Reauthorization. As this technology advances the need to rapidly share test and evaluation information and evolving CONOPS will be critical.
4. DHS and components move at best pace to engage SLTT authorities and identify operational, tactical, and legal issues that need to be addressed to implement UAS/C-UAS locally.
5. DHS and DOJ take the lead on development of a national C-UAS policy (similar to the

U.S. Government Deadly Force Policy).[28] This joint-use authority will ensure the use of C-UAS technology is not only justified but is also proportionate to the threat.

6. DHS select test sites for technology evaluation and develop operating procedures that allow larger DHS doctrine development focused on unity of effort. Doctrine and CONOPS should address four use cases: fixed locations (covered assets), regional locations (SW Border), temporary locations (special events), and mobile locations (dignitary, mobile asset protection). This Doctrine and CONOPS should be developed jointly with the FAA and other stakeholders and should include streamlined tools for airspace management that will allow critical infrastructure operators, regional officials, temporary locations (special events) and mobile locations to follow clearly defined (and rapidly implemented) procedures for requesting DROTAMS, TFR's or other special-use airspace[29].
7. DHS use the implementation of UAS/C-UAS authorities and capability as a use case to operationalize the "unity of effort" concept across the Department. This will require an assessment of the current capability at the Departmental level to coordinate operations nationally when needed. The challenge of unifying DHS effort across components, creating a truly centralized and effective National Operations Center, development of a Common Operating Pictures, and the development of doctrine is a challenge that remains 17 years after the creation of the Department. The ability to address any emerging technology will be hampered by the lack of enterprise maturity in these areas.
8. DHS consider the current wide variation of technologies being developed and employed by the federal government and SLTT authorities as a safety issue that requires close attention. Additionally, DHS should consider in coordination with other cognizant Departments a list of approved UAS/C-UAS technologies for SLTT authorities.
9. DHS encourage Congress to authorize and appropriate the necessary funds for the FAA to support C-UAS operations to include; adequate testing, acquisition, deployment, staffing, and maintenance of DTI technology in the airport environment.[30]
10. DHS support a requirement for the FAA to establish and publish UAS detection and mitigation system standards and provide straightforward guidance to those seeking to deploy DTI technologies.[31]
11. DHS support the urgent need for the FAA and DOJ to issue clear direction to other Federal and SLTT law enforcement regarding the current legal, statutory and regulatory limitations regarding technological enablers that are used to detect, track, identify and disable potential threat UAS.
12. DHS encourage Congress to extend C-UAS authority to other Federal and SLTT law enforcement partners. Such authority could be limited initially to trained and deputized

[28] Deadly Force: Constitutional Standards, Federal Guidelines and Officer Standards https://www.ncjrs.gov/App /Publications /abstract.aspx?ID=235824

[29] Jones, G.B. *"RE: UAS/CUAS SME feedback for HSAC."* Received by Cathy Lanier, 8 December. 2019.

[30] Blue Ribbon Task Force on UAS Mitigation at Airports. https://uasmitigationatairports.org/wp-content/uploads/2019/10/BRTF-Report2019.pdf

[31] BRTF, p. 11

officers, consistent with existing task forces, overseen by DOJ.[32]

13. DHS identify whether a private entity (stadium or airport) can procure, store, and maintain DTI equipment which DHS or DOJ can operate under certain conditions.

Recommendations for Mitigating Future Threats from Emerging UAS Technologies

It is recommended to:

1. Establish a mechanism to identify and track authorized drone operations in real-time, especially for drones operated beyond the visual line of sight of the operator.[33] 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, and aviation regulators to ensure that authorized drone operations do not pose safety and security threats and to distinguish and focus attention on potential bad actors operating without authorization.
2. Focus development on detection and defeat mechanisms that concentrate on immutable characteristics like the airframe mass, on-board electronics, and propulsion mechanism.[34] As technology matures, detection and defeat mechanisms that center on RF communications links and GPS will likely become less effective.
3. Continue to develop and evolve education and training for operators to reduce unintended operational actions that degrade safety and security and to ensure compliance with applicable laws and regulations.[35]
4. Given the rapid evolution of the technology associated with UAS, dedicate a concentrated effort to monitor and remain apprised of the trends in available technology. Detection and defeat mechanisms must be continually tested against and exercised with the latest available UAS systems readily available.[36]
5. Utilize multiple sensor modalities and defeat mechanisms. It is unlikely that one sensor modality is sufficient for detecting all small UAS under every circumstance.[37] The most effective system is one that leverages multiple sensor modalities (e.g., radar, RF, and audio) to detect aircraft. Acquired tracks from multiple sensor modalities, which will likely require at least a moderate artificial intelligence (AI) system, must be correlated to ensure an accurate operational understanding of potential threats. Similarly, no single defeat mechanism is likely to possess sufficient system-level performance in terms of probability

[32] BRTF, p. 14

[33] The FAA has commenced the process of developing sUAS identification and tracking rules. See, "RTF ARC Recommendations Final Report November 20, 2015 UAS Identification and Tracking (UAS ID) Aviation Rulemaking Committee (ARC) ARC Recommendations Final Report," Federal Aviation Administration, 30 September 2017, https://www.faa.gov/regulations_policies/rulemaking/committees/documents/media/UAS%20ID%20ARC%20Final%20Report%20with%20Appendices.pdf.

[34] Radar and Interceptor drones are examples of detection and defeat systems that exploit immutable characteristics instead of RF signatures. See, Tammy Waitt, "Coyote UAS & KRFS Radar to Acquire, Track & Engage US Enemy Drones," American Security Today, 23 July 2018, https://americansecuritytoday.com/coyote-uas-krfs-radar-acquire- track-engage-us-enemy-drones/.

[35] "Know Before You Fly" educational program is a collaboration between industry and the FAA. See Know Before You Fly, http://knowbeforeyoufly.org.

[36] DHS Conducted Technical Assessment of C-UAS Technologies in Cities (TACTIC) to evaluate the state current C-UAS systems. See, "Snapshot: Countering Unmanned Aerial Systems in Urban Environments," U.S. Department of Homeland Security, 11 May 2018, https://www.dhs.gov/science-and-technology/news/2018/05/11/snapshot-c-uas- urban-environments.

[37] AUDS is an example of multi-mode C-UAS system. See, "Blighter to supply counter-UAS radar technology for US DoD," Air Force Technology, 26 October 2018, https://www.airforce-technology.com/news/blighter-counter-uav- radar-us-dod/.

of success, range, and minimization of collateral risks to mitigate all threats. Thus, multiple defeat mechanisms used in tandem are likely to be most effective in ensuring appropriate mitigation success.

6. Ensure that future legislative efforts are fast-paced and flexible, to keep pace with rapidly evolving technology. The Preventing Emerging Threats Act of 2018 was the first legislative effort to successfully authorize testing of mitigation technology for the UAS threat that had been present for several years. This was a step in the right direction, despite the significant limitations included in the final bill. The conditions that must be met to gain approval, even for testing C-UAS technologies, are extremely time consuming and difficult to achieve. Additionally, the legislation's exclusion of the use of approved mitigation technology by state and local law enforcement and the Transportation Safety Administration (TSA) essentially eliminates C-UAS capabilities at the vast majority of mass gatherings and commercial airports nationwide. Lastly, the legislation as written prohibits the sharing of even basic information with critical partners, hampering coordinated mitigation efforts.

7. Develop Best Practice UAS Defense protocols at the FOUO level and deploy at mass gathering venues to provide necessary guidance for mitigating UAS threats. This will most likely involve a layered approach consisting of passive RF detection, short range radar for active detection, EO/IR cameras for ID and tracking, RF mitigation (C2 or GPS signal jamming if permitted by statute), and kinetic mitigation. Ideally, these Best Practices for UAS Defense would be reviewed and updated annually and as needed to keep pace with emerging threats posed by hostile UAS to mass gathering venues.

8. Develop a capability to monitor current and near-future UAS trends to anticipate potential threats and plan for new C-UAS strategies. The advancement of commercial UAS airframes and command and control (C2) will result in more capable and survivable UAS able to fly faster, for greater distances, with expanded payload capabilities, whilst being more difficult to detect and mitigate. These advancements, for example, enable an adversary to launch multiple autonomous UAS from a remote point targeting one venue and overwhelming the mitigation systems deployed to safeguard the venue, all the while being relatively undetected.

This page is intentionally left blank.