HOMELAND SECURITY ADVISORY COUNCIL
INTERIM REPORT OF THE EMERGING TECHNOLOGIES SUBCOMMITTEE

May 21, 2019

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 ***interim report*** and recommendations to the Acting Secretary of the Department of Homeland Security, Kevin McAleenan.

____

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
Dr. Patrick Carrick – Former Chief Scientist, S&T, DHS
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

Matt Hayden, Executive Director, Homeland Security Advisory Council
Mike Miron, Deputy Executive Director, Homeland Security Advisory Council
Catherine Fraser, Supervisory CBP Officer, Homeland Security Advisory Council
Colleen Silva, Staff, Homeland Security Advisory Council
Sarahjane Call, Staff**,** 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 the technological change in today's global research and development ecosystem is creating both risks and opportunities in the Department of Homeland Security's (DHS) mission domain. The dual challenge of addressing emerging technological threats to the Homeland while simultaneously acquiring and deploying capability to meet new threats is of paramount importance now and in the foreseeable future. Emerging technologies could pose threats for which no effective countermeasure readily exists, or they may comprise powerful new enabling capabilities that can be used by operational end-users. The problem is further exacerbated by evolving legal frameworks such as the recently passed FAA Reauthorization that provide new authorities but increase the complexity of implementation across the federal government and with DHS. In turn that complexity increases yet again when effective implementation of policy and deployment capability must be coordinated with state, local, tribal and territorial (SLTT) authorities.

To assist DHS in forecasting both threats and opportunities, work with partners, and improve the ability of DHS components to execute mission critical objectives, the Secretary chartered the Emerging Technologies Subcommittee of the Homeland Security Advisory Council (HSAC) in the Fall of 2018. The subcommittee was charged with exploring six emerging technologies and to develop recommendations to address and mitigate threats but also to take advantage of new capabilities to execute DHS missions. Those technologies include:

- Unmanned autonomous systems (UAS),
- Artificial intelligence and machine learning (AI/ML),
- 3/4D Printing
- Biotechnology – gene editing, splicing.
- Quantum information science and quantum computing.
- Advance Robotics

The subcommittee's work was impacted by personnel changes in DHS, the partial government shutdown, and the level subcommittee participation. Accordingly, the subcommittee characterizes this report as "interim" and recommends its work continue until further tasking provided by the Secretary completed. This interim report addresses 4 of the 6 technologies contained in the subcommittee's tasking: UAS, AI/ML, 3/4-D Printing and Biotechnology. The following sections define each technology, discuss the emerging features and functionality that will arise, propose some candidate use cases for the technology in the homeland security domain, and describe some of the impediments to the deployment of the technology. These sections will be refined, edited and expanded as necessary and the remaining technologies (Quantum computing and Advanced Robotics) added as the subcommittee continues its work. Finally, the subcommittee will augment with additional members and subject matter experts as needed.

This page is intentionally left blank.

RECOMMENDATIONS OF THE INTERIM REPORT

In addition to the recommendations contained in this report, the following high-level recommendations are provided.

Recommendations Regarding Further Subcommittee Work.

It is recommended that:

1. this report be considered an interim report,
2. the subcommittee continue its work for an additional 180 days,
3. the subcommittee work with the HSAC staff to identify and assign subject matter experts for the technologies under review with priority given to a technical expert on unmanned aerial systems,
4. the subcommittee chair will recommend membership adjustments to match the tasking provided

Recommendations Regarding the Unmanned Aerial 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/cUAS 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/cUAS and their relationship with SLTT authorities. While not within DHS purview or jurisdiction it is noted that US Capitol Police authorities should be addressed in any future legislation.
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 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 should move at best pace to engage SLTT authorities and identify operational, tactical, and legal issues that need to be addressed to implement UAS/cUAS locally.
5. The proposed test sites for technology evaluation 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),
6. DHS should use the implementation of UAS/cUAS 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.
7. DHS consider the current wide variation of technologies being developed and employed by the federal government and SLTT authorities a safety issue that requires close attention.

EMERGING TECHNOLOGIES: UNMANNED AUTONOMOUS SYSTEMS (UAS)

1. 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.

1.1 DHS' Authority Regarding Countering Unmanned Aerial Systems (UAS)

The Department of Homeland Security (DHS) and Department of Justice (DOJ) received their grant of counter 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:

- 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.
- 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 will have to conduct a counter-UAS (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.

The Preventing Emerging Threats Act only provides C-UAS authority to DOJ and DHS. It does not provide any authority to SLTT or private entities. As such, SLTT authorities and private entities remain subject to the same federal criminal laws that previously restricted DHS and DOJ C-UAS activities.

1.2 UAS Development

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 million registered operators of UAS.[1] 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.[2] 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.[3] 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.

1.3 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*[4]. This UAS Threat 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.

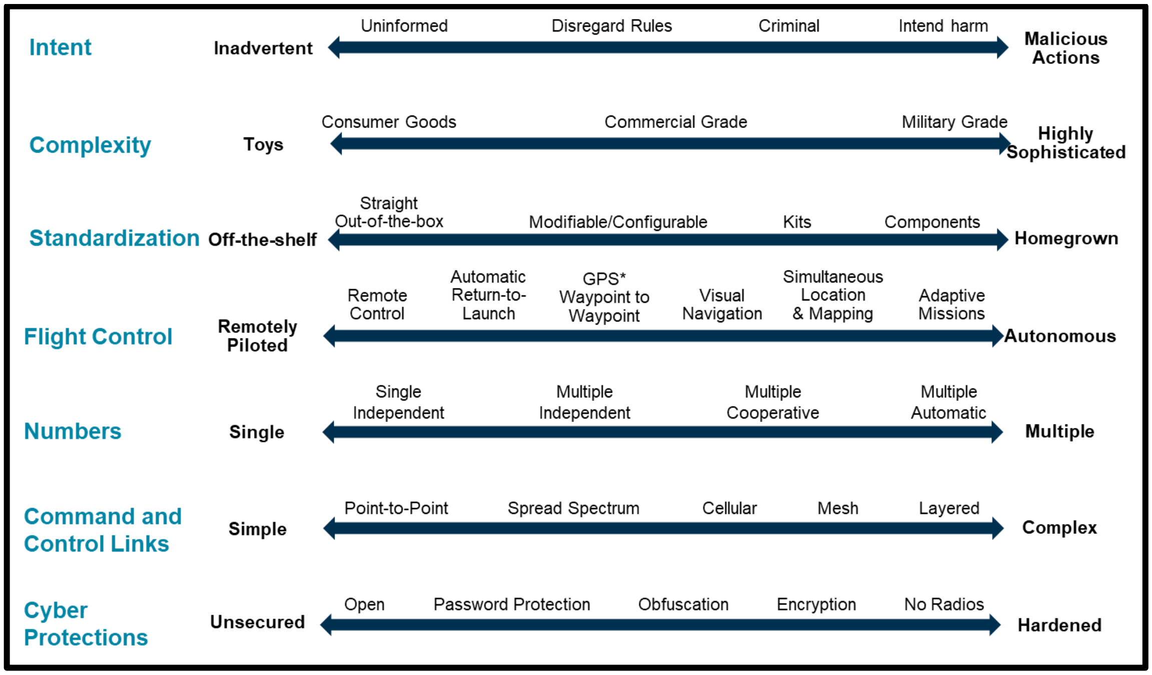
[1] U.S. Department of Transportation, "FAA Drone Registry Tops One Million," 10 January 2018, https://www.transportation.gov/briefing-room/faa-drone-registry-tops-one-million.

[2] 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/).

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

[4] 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.

Figure 1: UAS Threat Characteristics Spectrum



- **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.[5] 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.[6]
- **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

[5] 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.

[6] 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.

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.[7] 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.[8]

- **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.[9] 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 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

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

[8] 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/.

[9] 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.

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.[10]

- **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.[11]
- **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.[12] 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.[13] 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.[14]

Cyber Protections: Cyber protections, while a subset of C2 link assurance, are specifically addressed here because they are commonly exploited UAS vulnerabilities.[15] Currently, UAS employ cyber protections like those employed in information systems, such as securing networks

[10] 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.

[11] 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/.

[12] 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.

[13] 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.

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

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

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. How technologies could endanger the homeland, with a focus on those which have the highest likelihood of becoming a threat and those that pose the highest consequences to U.S. homeland security

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.

2.1 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,[16]
- interruption of sporting events due to the presence of unauthorized UAS,[17] 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.[18]

2.2 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.[19] Because of their small size, UAS can hide in plain sight. Drones do not have to be airborne to conduct ISR. 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,

[16] 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/.

[17] 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.

[18] 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.

[19] 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.

- individual privacy invasion,
- real-time target spotting/overwatch including spotting of law enforcement, such as on the southwest U.S. border,
- industrial espionage,
- coordination of ground attacks, and
- gathering of images for future operational use and propaganda purposes.

2.3 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.[20] 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.

2.4 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. Recommendations to best mitigate the perceived deleterious impacts of the assessed technological advancements, including recommended DHS near and long-term actions. Provide an assessment on the perceived opportunities for DHS components to maximize the use of these new technological advancements to guard against emerging threats.

3.1 Identification and Tracking

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.[21] 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

[20] 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.

[21] 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.

focus attention on potential bad actors operating without authorization.

3.2 Detection and Defeat Mechanisms

As technology matures, detection and defeat mechanisms that focus on RF communications links and GPS will likely become less effective. Development should focus on detect and defeat mechanisms that concentrate on immutable characteristics like the airframe mass, on-board electronics, and propulsion mechanism. [22]

3.3 Education and Training

Education and training for operators needs to continue to develop and evolve to reduce unintended operational actions that degrade safety and security and to ensure compliance with applicable laws and regulations.[23]

3.4 Technology Development

Given the rapid evolution of the technology associated with UAS, there needs to be a concentrated effort to monitor and remain apprised of the trends in available technology. Detection and defeat mechanisms need to be continually tested against and exercised with the latest available UAS systems readily available.[24]

3.5 Defense-in-Depth

There is no one sensor modality that is likely to be sufficient for detecting all small UAS in all circumstances.[25] 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, 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 mechanism used in tandem are likely to be the most effective in ensuring appropriate mitigation success.

3.6 Legislative Initiatives

The Preventing Emerging Threats Act of 2018 was the first legislative effort to successfully

[22] 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/.

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

[24] 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.

[25] 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/.

authorize testing of mitigation technology for the UAS threat that had been present for several years. Clearly this was a step in the right direction, despite the significant limitations included in the final bill. Essentially, 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. In the future, legislative efforts must move more quickly and have the flexibility to keep pace with the rapidly evolving technology.

3.7 DHS should develop Best Practice protocols for UAS Defense for venues

DHS should develop Best Practice UAS Defense protocols at FOUO level to be deployed at mass gathering venues to provide necessary guidance to mitigate 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 as needed to keep pace with emerging threats posed by hostile UAS to mass gathering venues.

3.8 DHS should develop capability to plan for future threats

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. DHS should develop the capability to monitor current and near future UAS trends to anticipate potential future threats and plan for new C-UAS strategies.

This page is intentionally left blank.

EMERGING TECHNOLOGIES: ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING (AI/ML)

1. 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.

1.1 Assessment of perceived AI/ML threats over the next 3-10 years

This section focuses on threats emerging in the field of artificial intelligence (AI). Although there is no universally accepted definition of AI, it is described loosely as "the ability of machines to perform tasks that normally require human intelligence – for example, recognizing patterns, learning from experience, drawing conclusions, making predictions, or taking action – whether digitally or as the smart software behind autonomous physical systems."[26] AI includes both logic-based and statistical approaches. A prominent area of AI is *machine learning* (ML). ML approaches use algorithms—predominantly statistical—that learn how to perform classification or problem solving without being explicitly programmed for the task domain. ML's learning ability comes from applying statistical learning algorithms, such as neural networks, support vector machines, or reinforcement learning, to expansive training data sets covering hundreds or even thousands of relevant features. For this reason, painstaking selection, extraction, and curation of feature sets for learning is often required. This limitation has been more recently addressed by deep learning, which utilizes deep neural networks with dozens of layers to not only learn classifications but also learn relevant features. This capability allows deep learning systems to be trained using relatively unprocessed data (e.g., image, video, or audio data) rather than feature-based training sets. To do this, deep learning requires massive training sets that may be an order of magnitude larger than those needed for other machine learning algorithms. When such data is available, deep learning systems typically perform significantly better than all other methods. Altogether, these advances in AI have enabled a new generation of AI applications.

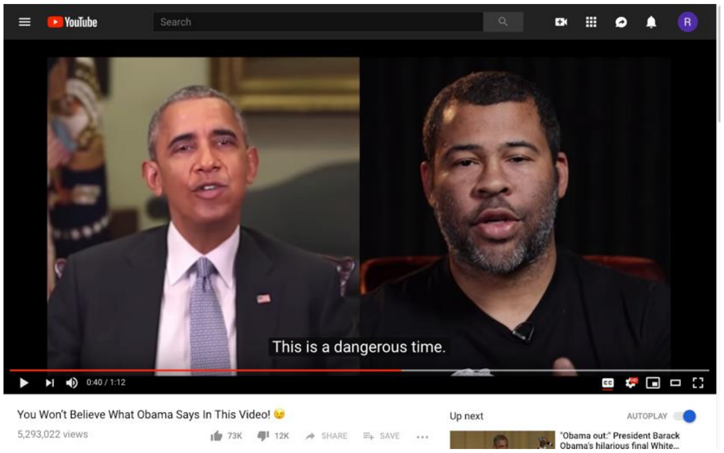
With these new AI capabilities and applications come the potential for new threats to national security.[27] We can divide the emerging technological threats into two broad areas: 1) threats that emerge due to advances in AI; and 2) threats that emerge due to the gradual integration of AI into the national infrastructure. This discussion focuses on the former, although possible instances of the latter area are included in section 1.4.

[26] Summary of The 2018 Department of Defense Artificial Intelligence Strategy, https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF

[27] M. Brundage *et al.*, "The malicious use of artificial intelligence: Forecasting, prevention, and mitigation," 2018, https://maliciousaireport.com

1.2 Emerging Technology: Deepfakes

Figure 7: Example of a Deepfake Video - "President Obama" delivers a warning message about deepfake technology


YouTube
Search
R
This is a dangerous time.
0:40 / 1:12
You Won't Believe What Obama Says In This Video! 😉
5,293,022 views
73K
12K
SHARE
SAVE
Up next
AUTOPLAY
"Obama out:" President Barack Obama's hilarious final White...

"Deepfake" algorithms utilize deep learning to almost seamlessly map target images, video, or audio content into other media content in order to create realistic depictions of situations that never occurred.[28] Most commonly this involves mapping facial portraits or video of one person onto a person in another image or video. For example, a recent deepfake video demonstration (see Figure 7) shows former President Obama giving a public service announcement on deepfakes that contains phrases Obama would never say in an address from the Oval Office, and it ends with the ironic reveal that the speech was actually by producer and Obama impersonator Jordan Peele.[29]

There are also tools in development for creating deepfakes for voice.[30] Software from Adobe that can reliably mimic a speaker based on 20 minutes of voice data has been demonstrated publicly,[31] but the prototype appears to be unreleased as of this writing.[32] Voice mimicking software that only requires one minute of voice data is publicly available but produces output with notable artifacts and a robotic tone.[33]

Current State of the Technology

While earlier deepfake technology can create a video that will pass the "first glance" test, it will contain telling artifacts on closer examination (including unnatural mouth and eyebrow movements). Newer techniques are more powerful and can capture integrated head position and rotation movements, facial expressions (including eyebrow movements and blinks), and eye movements.[34] Phone applications, such as FaceApp, permit manipulation of facial

[28] Deepfake is a portmanteau of Deep Learning and Fake.

[29] James Vincent, "Watch Jordan Peele use AI to make Barack Obama deliver a PSA about fake news," *The Verge* [Blog], 17 April 2018, https://www.theverge.com/tldr/2018/4/17/17247334/ai-fake-news-video-barack-obama-jordan-peele-buzzfeed; and, Buzzfeed, "You Won't Believe What Obama Says in this Video!," YouTube.com, 17 April 2018, https://youtu.be/cQ54GDm1eL0.

[30] A. van den Oord *et al.*, "Wavenet: A generative model for raw audio," *arXiv preprint arXiv:1609.03499,* 2016; Bahar Gholipour, "New AI Tech Can Mimic Any Voice" Scientific American, 7 May 2017, https://www.scientificamerican.com/article/new-ai-tech-can-mimic-any-voice/; "Adobe Voco 'Photoshop-for-voice' causes concern," BBC News, 7 November 2016, https://www.bbc.com/news/technology-37899902; Yaniv Leviathan and Yossi Matias, "Google Duplex: An AI System for Accomplishing Real-World Tasks Over the Phone," *Google AI Blog* [Blog]," 8 May 2018, https://ai.googleblog.com/2018/05/duplex-ai-system-for-natural-conversation.html.

[31] BBC News, 7 November 2016.

[32] See Tim Mak, "Can You Believe Your Own Ears? With New 'Fake News' Tech, Not Necessarily," *National Public Radio*, 4 April 2018, https://www.npr.org/2018/04/04/599126774/can-you-believe-your-own-ears-with-new-fake-news-tech-not-necessarily, which is the most recent confirmation in the mainstream press that Adobe Voco was unreleased as of February 2018. Google searches for Adobe Voco show no public release as of April 29, 2019.

[33] Scientific American, 2 May 2017.

[34] H. Kim *et al.*, "Deep Video Portraits," in *SIGGRAPH*, Vancouver, 2018.

characteristics.[35] Video software libraries such as DeepFakeLab and FaceSwap are available as public or open-source systems.[36]

Expected Advances

Deepfake technology is anticipated to improve significantly in coming years, and the results are expected to be much harder to detect and deem fake. There are also only limited impediments to continued propagation of this technology. Many libraries are open source, and the required CPU and GPU technology is also broadly available, including through cloud systems. The required training is also available through online courses.[37]

Impediments and Countermeasures

It is often possible to spot deepfakes using techniques that detect tiny disfluencies in the generated video. For example, it is possible in some instances to detect miniscule facial artifacts due to pulsing blood flow. These artifacts track the pulse in real video but will be erratic if the video is deepfaked. Other techniques, such as watermarking images generated by deepfake tools, may also help. However, once particular artifacts of the process are identified, such differences can be trained against and eliminated using adversarial neural network techniques. The Defense Advanced Research Projects Agency (DARPA), through its MediFor program, is researching the possibility of creating an integrated media forensics platform—essentially, a deepfake detection toolkit.[38] Such a toolkit could make the production of deepfakes more computationally expensive, which may reduce their use until the cost of computation decreases significantly. The topics of deepfakes is a rapidly developing and concerning area of research and development.

Converging Technologies

Deepfake technology could be combined with other threats to improve its effectiveness. For example, the integration of deepfakes with social media attacks (see section 1.2 Emerging Technology: AI-driven Social Media Attacks) could increase the ability of such methods to disrupt social structures and political activity. Similarly, the ability to mimic voice could be used to supplement cyber-attacks by automating, for example, voicemail that suggests opening a spear-phishing email.

Projected Timeline

It appears likely that broadly available deepfake video capabilities could be available within the next 2 to 5 years. One expert noted that he believed it highly likely that a viral deepfake video will be used against a political candidate in 2020.[39] Vocal deepfake tools have somewhat lagged behind those for video but also seem likely to appear within the latter time period. The ability to simultaneously generate both voice and video has not been demonstrated but might be tractable using a combination of techniques, such as a human actor to lip-sync a generated vocal track that would then be synchronized to a generated video portrait. Use of video portraits to make dubbing of videos more realistic has already been demonstrated.[40]

[35] FaceApp, 5 December 2018, defunct as of 13 February 2018, https://faceapp.com/.

[36] K. Roose, "Here Come the Fake Videos, Too," in *The New York Times*, ed, 2018.; (2018, Dec 5, 2018); *Faceswap: [Github repository], https://github.com/deepfakes/faceswap*; and *DeepFakeLab [Github repository], https://github.com/iperov/DeepFaceLab.*

[37] "Deep Learning MOOCs and Free Online Courses," MOOC List, https://www.mooc-list.com/tags/deep-learning

[38] Matt Turek, "Media Forensics (MediFor), Defense Advanced Research Projects Agency, undated, https://www.darpa.mil/program/media-forensics

[39] J. Hsu. (2018) Experts Bet on First Deepfakes Political Scandal. *IEEE Spectrum*. Available: https://spectrum.ieee.org/tech-talk/robotics/artificial-intelligence/experts-bet-on-first-deepfakes-political-scandal

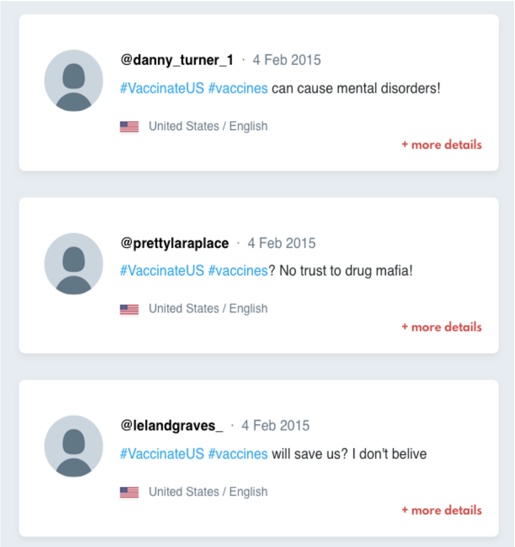
[40] H. Kim *et al.*, "Deep Video Portraits," in *SIGGRAPH*, Vancouver, 2018.

1.3 AI-driven Social Media Attacks

Social media attacks can be defined as attacks that utilize fake social media messages to influence or disrupt public discourse. The goal of social media attacks, when undertaken against the homeland, is typically the dissemination of falsehoods in order to gain temporary political advantages, delegitimize political opponents of the attacker, or damage public safety in other ways, such as misinforming the public about existing crises or fomenting rioting or acts of vandalism.[41]

Although deception operations date back many decades, AI may allow bad actors, including state actors such as Russia and international nonstate actors such as the Islamic State, to "hyperpower" deception campaigns.[42]

Figure 8: Example of Russian tweets on vaccine debate produced by Russia's Internet Research Agency.



@danny_turner_1 · 4 Feb 2015
#VaccinateUS #vaccines can cause mental disorders!
United States / English
+ more details

@prettylaraplace · 4 Feb 2015
#VaccinateUS #vaccines? No trust to drug mafia!
United States / English
+ more details

@lelandgraves_ · 4 Feb 2015
#VaccinateUS #vaccines will save us? I don't belive
United States / English
+ more details

Source: From the Russia Tweets online archive. https://russiatweets.com/hashtag/vaccines/tweets

Current State of the Art

Current types of social media attacks tend to have a relatively well-understood form, utilizing both AI-driven bots and armies of human actors. Attackers utilize social media platforms, such as Twitter or Facebook, to make it appear that certain opinions or beliefs are more common than they are among the public, often to lend public support to positions that are favorable to the attacker. Bots—software applications that run automated tasks online—can also be used to boost the visibility of actors or users on social media platforms. Indeed, it is now well known that there are companies willing to sell large numbers of faked Twitter followers for a fixed fee.[43]

These artificial social agents may or may not be easily spotted by the average user. As awareness of bots increases, it is inevitable that AI techniques will be used to make Twitter bots more human-like in their conversational style, either to give their arguments plausibility or to simply avoid being detected and culled by anti-bot measures.

Expected Advances

While many aspects of social media attacks are relatively low-tech, there are some that can be boosted by advances in AI. Technology already exists to create relatively sophisticated

[41] "Countering False Information on Social Media in Disasters and Emergencies," U.S. Department of Homeland Security Social Media Working Group for Emergency Services and Disaster Management, March 2018, https://www.dhs.gov/sites/default/files/publications/SMWG_Countering-False-Info-Social-Media-Disasters-Emergencies_Mar2018-508.pdf.

[42] Alina Polyakova, "Weapons of the weak: Russia and AI-driven asymmetric warfare," in "A Blueprint for the Future of AI," Report, Brookings Institute, 15 November 2018, https://www.brookings.edu/research/weapons-of-the-weak-russia-and-ai-driven-asymmetric-warfare/; and P. W. Singer and Emerson Brooking, "War Goes Viral" *The Atlantic Monthly*, November 2016, http://www.theatlantic.com/magazine/archive/2016/11/war-goes-viral/501125/.

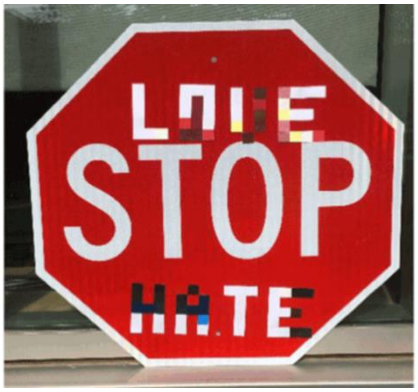
[43] Nicholas Confessore, et al., "The Follower Factory," *New York Times, 27 January 2018,* https://www.nytimes.com/interactive/2018/01/27/technology/social-media-bots.html.

narratives for well-defined domains such as sports.[44] In addition, the ability to recognize the affect (i.e., emotional valence) of a particular tweet may then also allow for sophisticated automated responses. For example, a system could automatically identify all tweets with a specific positive response to a social issue and to send out multiple responses covering different aspects of the countering narrative. It is possible to tailor responses to make them more attractive to the target community. This can be done either directly through the construction of explicit response templates, through ML-based natural language processing techniques, or by issuing multiple variants of a particular response and then reusing (and further evolving) the most successful responses. These capabilities will continue to grow in sophistication and impact as AI advances.

Impediments and Countermeasures

Many measures can be taken to fight against social media attacks. Stronger verification techniques to validate users, particularly for public figures who are likely to be impersonated, are useful. Social media platforms may also permit users to report likely bots, and this data can be combined with ML-based bot recognition and anomaly-detection algorithms to improve bot detection (as is done for email spam filtering). During localized emergencies such as floods and earthquakes, filtering by geographic location can help eliminate troll postings meant to confuse, and recognized authorities (such as the Red Cross and government agencies) can use their social media accounts to correct misinformation.[45] Other myth debunking web sites, such as Snopes and FactCheck, can serve a similar purpose.[46] Public education can teach citizens to avoid relying on social media metrics as measures of public support and instead turn to alternative measures such as validated polling. Human tests, such as CAPTCHAs, can reduce impersonation (although these can be circumvented using crowdsourcing services such as Mechanical Turk).[47]

Figure 9



Relatively simple modifications to existing signage can fool image classification algorithms. By adding "Love" and "Hate" graphics onto a "STOP" sign, researchers can trick an autonomous vehicle into seeing this stop sign as a speed limit sign.

In all these cases, there will continue to be an arms race between systems designed to fake human conversations and systems designed to detect such fakes. AI research on conversational agents, such as voice assistants and chatbots, as well as research in explanatory AI, will have the side effect of providing means for attackers to increase the believability of fake users created for social media attacks by making interactions with them seem more human.

Converging Technologies

As already noted, the ability to generate deepfakes of images, audio, or video by

[44] L. A. Birnbaum, K. J. Hammond, N. D. Allen, and J. R. Templon, "System and method for using data and derived features to automatically generate a narrative story," 2014, https://patents.google.com/patent/US8843363B2/en.

[45] U.S. Department of Homeland Security Social Media Working Group for Emergency Services and Disaster Management March 2018.

[46] See, https://www.snopes.com/ and https://www.factcheck.org/.

[47] E. Bursztein, S. Bethard, C. Fabry, J. C. Mitchell, and D. Jurafsky, "How good are humans at solving CAPTCHAs? A large scale evaluation," in *Security and Privacy (SP), 2010 IEEE Symposium on*, 2010, pp. 399-413: IEEE.

political actors will likely increase the severity of social media attacks, even when the deepfakes are not fully convincing upon close examination. Continued advances in automated cyber-attacks will likely also improve the ability of malicious actors to take over existing social media accounts in order to redirect their use to social media attacks.

Projected Timeline

Although public awareness of social media attacks rose significantly in 2016 due to Russian attacks during the 2016 election, these attacks are only a slightly more recent occurrence than the creation of the web itself. Because social media attacks are a kind of numbers-game where small improvements to individual messages can lead to large gains in the aggregate, this should be expected to be a long-term arms race with continual improvement of adversarial capabilities.

1.4 Three Potentially Emerging but not Imminent Threat Areas

In doing this research, three areas of concern were identified that, while they do not rise to the level of threats likely to occur in the 3- to 5-year timeframe, may be relevant in the 5- to 10-year time frame. These three concerns are discussed below.

Concern #1: Information Attacks on Emerging AI Infrastructure.

Over the next decade, AI is going to increasingly form a core part of U.S. infrastructure, providing capabilities that are not only useful but essential in day-to-day activities. It is reasonable to assume that actions to disrupt emerging AI capabilities—be they fleets of autonomous vehicles, voice assistants used for critical functions, or other newly-essential AI technology—will themselves constitute threats. It is possible to attack such systems by using various techniques that fool the systems into misclassifying or misinterpreting information in their environment. For example, adversarial learning and sensor spoofing can be used to confuse autonomous vehicles, making them imagine nonexistent obstacles or blinding them to real ones. (See Figure 9.[48]) Voice assistants can be subverted by using commands embedded in white noise or music that are heard and obeyed by the voice assistant but go unheard by humans.[49]

There is currently no evidence that such attacks are an imminent threat to the homeland. They rely on a fair amount of technological sophistication to be properly implemented, and there are big steps between the proof of concept demonstration of an attack in a controlled setting and the ability to deploy such attacks "in the wild". In addition, there are many alternative means of attack that are currently cheaper and more effective. However, it is worth examining methods to make AI systems less vulnerable to such attacks.

Concern #2: AI-driven Cyber-attacks

AI-driven cyber-attacks utilize AI to help direct the infiltration, capture, or disabling of targeted computer systems. Evolving AI capabilities are likely to permit a small number of human attackers to direct attacks against a much larger number of targets. It is extremely important to note that, despite the little evidence for the use of AI in cyber-attacks "in the wild" to date, there are recent research demonstrations of the utility of AI for cyber-defense—particularly the automatic detection and patching of vulnerabilities—as was demonstrated in the

[48] K. Eykholt *et al.*, "Robust Physical-World Attacks on Deep Learning Models," in *Proc of Conference on Computer Vision and Pattern Recognition*, 2018.

[49] Craig Smith, "Alexa and Siri Can Hear This Hidden Command. You Can't," *New York Times*, 10 May 2018, https://www.nytimes.com/2018/05/10/technology/alexa-siri-hidden-command-audio-attacks.html.

DARPA Cyber Grand Challenge.[50] In addition, while there have been no identified examples of AI driving cyber-attacks, there is a concerning example within the last two years of ML being deployed to sniff out user access patterns on a commercial network.[51] One concern about this attack is that the system was able to apply training updates from its observations to better mimic certain user behaviors.

Concern #3: Large-scale Social Engineering Attacks

Social engineering attacks are a kind of cyber-attack that use social vectors as part of the method for infiltrating a system. For example, an attacker may attempt to extract passwords or other key information from a company by simply calling up an employee and pretending to be someone who needs access to an account. “Spear-phishing” is a type of social engineering attack that uses knowledge about a particular individual to craft an email that is extremely likely to be clicked on by that individual based on their public persona or social media profile, with the clicked link resulting in the automatic download of a virus or other exploit. Social engineering attacks currently require careful analysis of their targets. However, advances in AI to extract information from social media and other sources of what has been called “digital exhaust” generated by individuals’ online actions (e.g., search and browser history) opens up the possibility of mass spear-phishing attacks, where an AI agent constructs targeted messages for each individual, even if the number of targets is in the hundreds or thousands.[52] A research prototype utilizing ML techniques to craft Twitter spear-phishing messages based on users’ histories was able to achieve a click rate similar to that of manually written spear-phishing messages.[53] Voice agents, such as the Google Duplex system, open up the possibility of massive phone-based social engineering attacks.[54]

1.5 How such technologies could endanger the homeland, with a focus on those which have the highest likelihood of becoming a threat and those that pose the highest consequences to U.S. homeland security. Describe Use Cases for how Technology Could Impact Homeland Security.

New Capability for Homeland Security - Use Case #1: Media Forensics Units

Special units within DHS could be provided with the latest tools to combat deepfake technology, such as DARPA’s MediFor toolkit, along with alternative means of verification, to combat arising fake videos, images, and audio.[55] Alternatively, a standards agency such as National Institute of Standards and Technology (NIST) could certify organizations that detect fake media.

[50] J. Song and J. Alves-Foss, "The DARPA Cyber Grand Challenge: A Competitor's Perspective," IEEE Security & Privacy, vol. 13, no. 6, pp. 72-76, 2015; J. Song and J. Alves-Foss, "The DARPA Cyber Grand Challenge: A Competitor's Perspective, Part 2," IEEE Security & Privacy, vol. 14, no. 1, pp. 76-81, 2016. https://www.eff.org/deeplinks/2016/08/darpa-cgc-safety-protocol

[51] S. Rosenbush, “The Morning Download: First AI-Powered Cyberattacks are Detected,” Wall Street Journal CIO Blog. Available: https://blogs.wsj.com/cio/2017/11/16/the-morning-download-first-ai-powered-cyberattacks-are-detected/

[52] *Digital Exhaust*,” Wikipedia, https://en.wikipedia.org/wiki/Data_exhaust

[53] J. Seymour and P. Tully, "Weaponizing data science for social engineering: Automated E2E spear phishing on Twitter," presented at the Black Hat USA Conference, 2016, http://www.blackhat.com/docs/us-16/materials/us-16-Seymour-Tully-Weaponizing-Data-Science-For-Social-Engineering-Automated-E2E-Spear-Phishing-On-Twitter-wp.pdf

[54] Yaniv Leviathan and Yossi Matias, 8 May 2018.

[55] DARPA, undated.

New Threats to Homeland Security - Use Case #1: Deepfake Voice Technology Used to Create Crisis

A deepfake voice tool could be used to simulate commands or instructions delivered over the phone. This could be used to generate an artificial crisis, such as an order to take a political opponent into custody, evacuate a building, or send emergency resources to a particular area, perhaps to divert them from a planned real attack.

New Threats to Homeland Security - Use Case #2: Botnets to Delegitimize Public Fora or Make Them Unusable

Instead of attacking a particular position, AI-driven botnets could be used to simply drive up the discussion level on both sides of an issue to a level that would render the social media platform unusable for discussion, or at least unusable for certain topics. This is also a matter of public trust. If all sources of information are demonstrated unreliable and compromised, the public's trust in any information, including legitimate messages, will decrease, potentially resulting in serious impacts to messaging during a time of crisis.

1.6 Recommendations to best mitigate the perceived deleterious impacts of the assessed technological advancements, including recommended DHS near and long-term actions. Provide an assessment on the perceived opportunities for DHS components to maximize the use of these new technological advancements to guard against emerging threats.

Recommendation #1: Provide mechanisms or standards for validating user identity across platforms.

Currently, some social media platforms have mechanisms for identity validation, but widespread real-world validation of user identity—using government identification or similar means—remains rare, nor are there industry standards for identity validation for social media. While current social media validation mechanisms were primarily developed to protect famous or influential users or businesses from impersonation, identity validation is also useful in the fight against fake accounts. While social media companies may resist providing identity validation of regular users because of expense, or because of the perception that to have a validated social media account (such as the Twitter "blue check" program) implies a sort of endorsement of the user's importance, widespread identity validation for regular users, as well as open industry standards for identity validation across social media platforms, would both reduce costs and any perceptions of user endorsement.

Recommendation #2: Encourage standards for commercial providers of imagery technology to include watermarking and other anti-fraud measures to help combat deepfakes.

To help combat deepfake technology, it may be possible to embed watermarks or digital signatures to label known true images or videos or, as part of image manipulation software, to mark images or videos as modified. In addition, image creation systems could optionally register images or videos to a public ledger using blockchain technologies, as done by the camera app TruePic.[56]

[56] See, https://truepic.com

This page is intentionally left blank.

EMERGING TECHNOLOGIES: 3D PRINTING

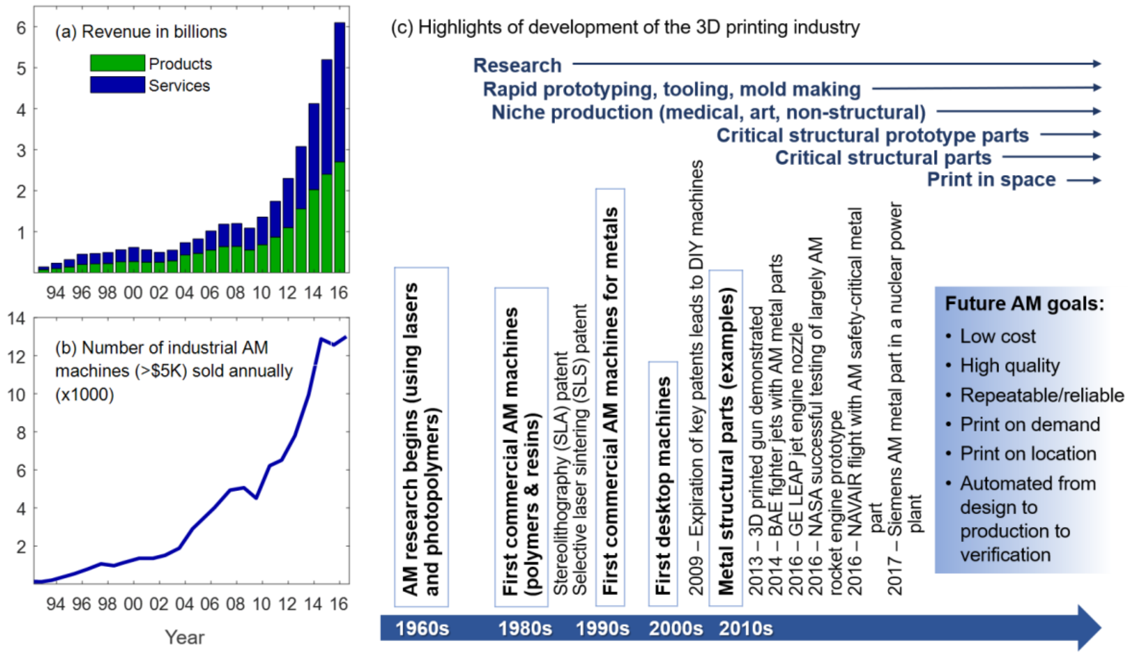
1. Assessment of the current state and perceived future advancements over the next 3-10 years that could pose a threat to the homeland security of the United States.

1.1 Current State of 3D Printing Technology

3D printing and additive manufacturing (AM) are defined in ISO/ASTM 52900.[57] AM is defined as a process that builds parts from a 3D digital model layer-by-layer rather than cutting unwanted material away (termed “subtractive manufacturing”). 3D printing is defined as “fabrication of objects through the deposition of a material using a print head, nozzle, or another printer technology.” Historically, the term 3D printing (as opposed to AM) was associated with machines that were lower in price and/or overall capability. Today, the term is commonly used interchangeably with AM.

The 3D printing industry has grown rapidly over the course of the past ten years, spurred by the expiration of key patents allowing new companies to enter the industry. At present, the revenue associated with 3D printing products and services totals more than $6 billion annually. The history and rapid growth of the industry over recent years is captured in Figure 3.

Figure 3: Development of the 3D Printing Industry



Current methods for 3D printing fall under seven process categories defined by ISO/ASTM 52900. These processes are detailed in Figure 4.

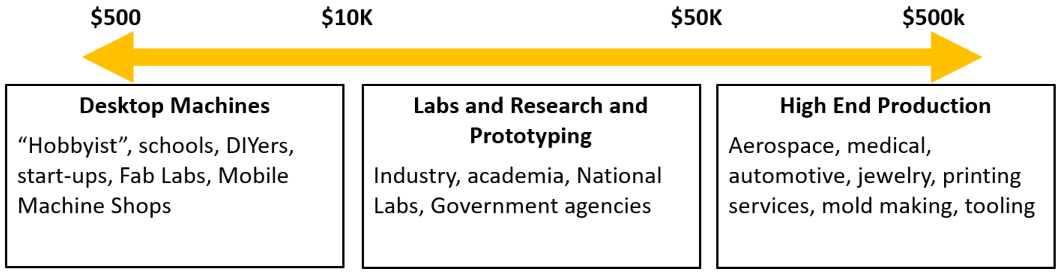
[57] ISO/ASTM 52900, “Standard Terminology for Additive Manufacturing - General Principles - Terminology,” ISO/ASTM, 2015.

Figure 4: 3D Printing Process Categories as Defined by ASTM/ISO 52900

Process	Synonyms	Description	Applicable Materials
Material Extrusion	• Fused Deposition Modeling (FDM) • Fused Filament Fabrication (FFF) • Plastic Jet Printing (PJP)	Polymer is extruded through a heated nozzle onto a support structure or the workpiece	Thermoplastics, e.g. • ABS • PLA • Nylon • Ultem
Material Jetting	• Multijet Modeling (MJM) • Droplet-on-Demand	Droplets of build material are selectively deposited onto a build bed to produce a 3-dimensional object	Polymers and waxes, e.g. • Polypropylene • HDPE • PS • PMMA • PC • ABS
Vat photopolymerization	• Stereolithography (SLA) • Resin Printing • Optical Fabrication	Liquid photopolymer in a vat is selectively cured by light-activated polymerization	Photosensitive polymers
Powder Bed Fusion (PBF)	• Selective Laser Sintering or Melting (SLS or SLM) • Direct Metal Laser Sintering (DMLS)	Thermal energy selectively fuses regions of a powder bed to build up parts	Uniform powders • Metal • Polymer
Directed Energy Deposition (DED)	• Laser Engineered Net Shaping (LENS) • Direct Metal Deposition (DMD) • Laser Consolidation (LC)	Focused thermal energy fuses materials by melting them as they are deposited	Metal powders • Uniform • Varying composition (gradient materials)
Binder Jetting	• Inkjet Powder Printing	Powder material is bonded selectively using a liquid bonding agent	• Metal powders • Plastic powders • Sand
Sheet Lamination	• Laminated Object Manufacturing (LOM) • Ultrasonic Consolidation	Sheets of material are bonded together to form a 3-dimensional object	• Paper • Metal foils • Plastic

Machine price points span the range of a few hundred dollars for low-end hobbyist systems to over $500,000 for high-end industrial systems. Figure 5 illustrates the range of 3D printing systems costs and typical applications at various price points.

Figure 5: Range of 3D Printing System Costs and Use Cases


$500
$10K
$50K
$500k
Desktop Machines
"Hobbyist", schools, DIYers, start-ups, Fab Labs, Mobile Machine Shops
Labs and Research and Prototyping
Industry, academia, National Labs, Government agencies
High End Production
Aerospace, medical, automotive, jewelry, printing services, mold making, tooling

1.2 Expected Advancements of 3D Printing Technology

As the rapid growth of the 3D printing industry continues, the technology is reaching more users and application spaces. When considering the future of the industry from the perspective of homeland security, a number of relevant expected advancements arise, which are detailed below.

Decreasing Cost of Metal Printing

Timeframe: 0-5 years

The cost of metal printing technologies has recently seen some decreases, and it is expected that with these decreases such processes will gradually become broadly available. Companies, including Markforged and Desktop Metal, have developed and brought to market systems at a significantly lower price point than that of laser- or electron beam-based sintering/melting systems. These newer, lower cost systems bind metal powder in a polymer matrix to form a part, which is subsequently sintered in a furnace. In addition to the lower cost of the system itself, the metal powders used in the polymer-binding process cost less than powders used in laser or electron beam melting processes, as the requirements on the former powder are less stringent. Systems such as the Markforged Metal X and Desktop Metal Studio have price tags on the order of $100,000. While still out of reach for many private consumers, they are certainly more accessible than laser- and electron beam-based systems that have current prices hovering above $500,000.

The cost of metal printing systems will continue to decrease. Yet, even before that happens, the accessibility of metal parts via service vendors raises similar potential security concerns. There are already many companies that own and operate metal 3D printers and market the ability to accept digital part files and turn around printed hardware. Such a business model further democratizes the access to printed metal parts. It is likely that such a service provider route could be pursued by an actor attempting to source metal parts for assembly into a weapon. Particularly if parts intended for an assembly are printed piecemeal, the intent or use of the parts may not be obvious and would not necessarily raise suspicion. The underlying presupposition is that metal parts—stronger and more durable than other types of 3D printed materials—could lead to a new class of threats in terms of 3D printed weapons.

Proliferation of Safety Critical 3D Printed Parts

Timeframe: 0-5 years

As processes mature, print quality improves, and 3D printing technologies gain acceptance within mainstream manufacturing, the use of these techniques to produce safety-critical parts is likely to rise. Research in 3D printing is driven in large part by the aerospace, automotive, and medical industries. Within these industries, high-value parts justify development cost investments for 3D printed solutions. These solutions are driven by the desire to take advantage of 3D printing for ease of producing complex geometries, which could be optimized for material and weight savings and even individualized; for example, in the case of applications for prosthetics and biomedical devices within the medical industry.

Parts produced for critical applications in the healthcare and transportation industry are likely to have significant implications for public safety. As these industries adopt 3D printing, attack vectors based on vulnerabilities of 3D printing are a significant and growing concern.

Novel Materials

Timeframe: 2-7 years

The development of new materials for 3D printing goes together with the development of 3D printing machines and deposition processes. Advancements include the development of feedstock materials (both metals and polymers) tailored to printing processes to yield higher density parts with better mechanical properties and increased reliability. Material advancements also include development of novel materials that exhibit unique mechanical, thermal, optical, electrical, and magnetic attributes. These may include anisotropic properties (e.g. preferential electrical or thermal conduction in one direction). They may also include properties that are a function of tailoring material deposition at small scale, made possible by high-resolution, automated, multi-material 3D printing processes. These “engineered materials” pave the way for unique performance attributes of printed parts, which could include parts with very high strength-to-weight ratios, explosive materials, or high-strength plastics capable of withstanding pressures such as those encountered in a firearm.

3D-printed Chemical Formulations

Timeframe: 4-9 years

Use of 3D printing techniques to realize unique chemical formulations is an active area of research. A group from the University of Illinois - Urbana Champaign demonstrated an automated method for molecular synthesis of small organic molecules using a building block approach.[58] As this application area for 3D printing matures, potential use cases include pharmaceuticals with tailored time-release profiles or those tailored to a patient’s unique physical characteristics. Furthermore, nefarious use cases could also include remote, undetectable manufacture of chemical and even biological weapons or poisons.

Multi-material Processes for Printing Embedded Electronics

Timeframe: 5-10 years

Currently available multi-material printers allow for deposition of electrically conductive traces within a polymer matrix. With a trend toward improved resolution and new materials, the ability to print electronic components is within reach in the 2- 7-year timeframe. Researchers have experimented with printing capacitors, resistors, and inductors and demonstrated use of conductive polymer for a printed high-pass filter with properties comparable to a traditional filter.[59] 3D printing will also likely yield reliable energy storage solutions within

[58] J. Li, S. Ballmer, E. Gillis, et al., “Synthesis of many different types of organic small molecules using one automated process,” Science, 347 (2015): 1221-1226.

[59] . Flowers, C. Reyes, S. Ye, et al., “3D printing electronic components and circuits with conductive thermoplastic

the 5- to 10-year timeframe.[60]

Biological/Engineered Tissue Printing

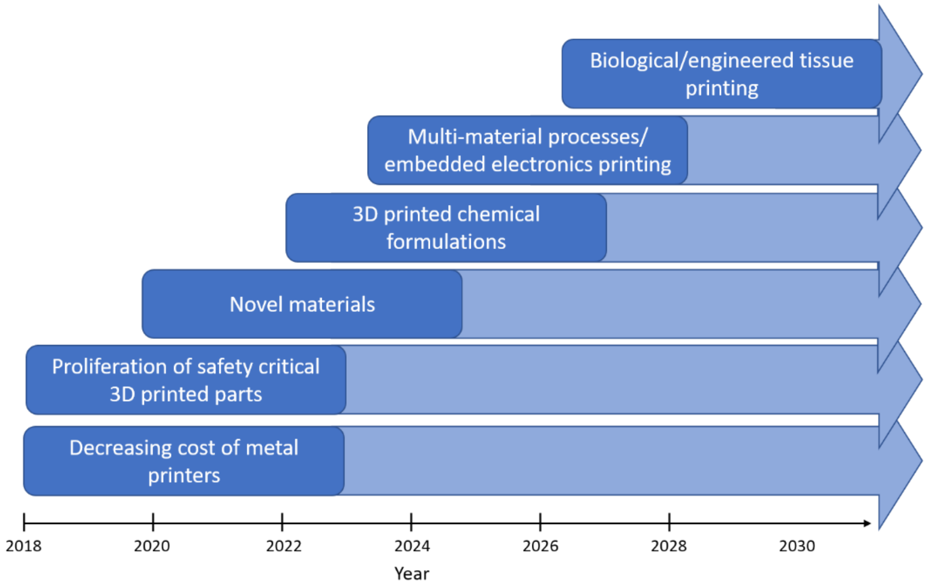
Timeframe: 10+ years

3D printing of cellular material, bio inks, and growth factors is being investigated to produce human tissue-like material and scaffolds. For engineered tissue, 3D printing offers the potential to address the needs for matching patient-specific anatomical data and producing complex features in three dimensions with high accuracy. The intersection of 3D printing with engineered tissue is one of the focus areas of the Advanced Regenerative Manufacturing Institute (ARMI), a public-private consortium opened in 2017 with the goal to "make practical the large-scale manufacturing of engineered tissues and tissue-related technologies."

1.3 Projected Timeline for Deployment of Future 3D Printing Advancements

Figure 6 illustrates a projected timeline for the advancements in 3D printing discussed above, all of which are likely to have an impact on Homeland Security.

Figure 6: Projected Timeline for 3D Printing Technology Advancements



1.4 Impediments to Deployment of 3D Printing Technology

Catastrophic Failure of a Safety Critical Part

In 2015, General Electric obtained certification from the Federal Aviation Administration (FAA) for the first 3D printed part for use in a commercial jet engine. Use of 3D printed parts for aircraft was not new—they were already used for many non-critical parts like ducting and interior cabin parts—but this was the first part performing a function critical to flight to be certified by the FAA.[61] Flight critical, 3D printed parts have also been pursued within the

filament," Additive Manufacturing, 18 (2017): 156-163.

[60] B. Yao, S. Chandrasekaran, J. Zhang, et al., "Efficient 3D Printed Pseudocapacitive Electrodes with Ultrahigh MnO2 Loading," Joule, (2018).

[61] T. Kellner, "The FAA Cleared the First 3D Printed Part to Fly in a Commercial Jet Engine from GE," GE Reports, 14 April 2015, https://www.ge.com/reports/post/116402870270/the-faa-cleared-the-first-3d-printed-part-to-fly-2/.

Department of Defense (DoD). Naval Aviation Systems Command (NAVAIR) demonstrated flight of an aircraft containing 3D printed safety critical parts in July 2016.[62]

As 3D printing is increasingly used for production of safety critical parts, the risks associated with part failure grow. A hypothetical failure of a 3D printed part resulting in loss of life or serious economic impact could heavily influence public opinion and cripple implementation of 3D printing technologies for end use applications.

Foreign Manufacturers

Most 3D printing systems are supplied by foreign entities. Only approximately 21 percent of systems sold in 2017 came from manufacturers headquartered in the United States.[63] As such, advancements in 3D printing technology are likely to be affected by international trade policy as well as political and economic factors outside of U.S. control.

1.5 Convergence with Other Emerging Technologies

The convergence of 3D printing technologies with 3D scanning technologies allows for rapid generation of digital build files based on physical artifacts and subsequent reproduction of those artifacts. Potential threats exposed by the convergence of 3D scanning and printing include counterfeiting, biometrics spoofing, and intellectual property theft.

3D printing offers the ability to rapidly prototype hardware. As such, 3D printing functions as an enabler for other emerging technologies such as novel sensing and communications equipment. 3D printing as a rapid prototyping mechanism can lead to both capabilities for and threats to Homeland Security, as it will almost certainly accelerate the innovation curve for new technologies.

Convergence of 3D printing with other emerging technologies is highlighted in the section that follows.

2. How such technologies could endanger the homeland, with a focus on those which have the highest likelihood of becoming a threat and those that pose the highest consequences to U.S. homeland security.

2.1 New Capabilities for Homeland Security

Capability Use Case #1: Lightweight, Low-Cost Platforms for Intelligence, Surveillance and Reconnaissance (ISR)

3D printed assemblies can function as lightweight platforms for sensors to be used for ISR. The ability to print complex geometries, such as lattices, with relative ease enables high strength-to-weight parts that can allow for efficient airborne and ground-based platforms. Potential use scenarios for such platforms span from security to first responders. Ease of reconfiguration and customization of printed parts allows for such ISR platforms to be unique to the application and potentially easier to conceal as innocuous objects so as not to draw attention to them.

Capability Use Case #2: Supply Chain Risk Management

3D printing/additive manufacturing has the potential to mitigate supply chain risk for products critical to national security or economic stability. 3D printing technology enables the

[62] "NAVAIR marks first flight with 3-D printed, safety-critical parts," NAVAIR Press Release, 29 July 2016, http://www.navair.navy.mil/index.cfm?fuseaction=home.NAVAIR NewsStory&id=6323/.

[63] T. Wohlers, I. Campbell, O. Diegel, and J. Kowen, "Wohlers Report 2018," Wohlers Associates, Inc., March 2018.

realization of complex geometries without the need for part-specific tooling that may be required for traditional fabrication. Moreover, the digital storage of parts data means that part fabrication routines can be sent digitally between geographically separated sites. As such, employing 3D printing for critical products allows for redundant fabrication capabilities and eliminates a "single-point-of-failure" scenario whereby a single manufacturing facility responsible for production of a critical part is taken offline halting the supply chain for that part. Moreover, 3D printing facilitates fabrication of parts closer to point of need/use, thereby overcoming shipping/transport obstacles that may arise in situations where infrastructure is limited due to either attack or natural disaster.

2.2 New Threats to Homeland Security

Threat Use Case #1: Sabotage of Safety Critical Parts

3D printed parts are susceptible to sabotage via the intentional, malicious modification of digital build files. Modifications can be carried out such that the part printed via the modified file appears to meet all requirements, while it actually contains concealed flaws or flaws so minute that they are not readily identified that result in premature failure. Such an attack vector was demonstrated by Belikovetsky et al. in an experiment called "dr0wned."[64] In this experiment, a digital file for an unmanned aerial system (UAS) propeller design was intentionally modified to remove a small amount of material in a critical structural region of the propeller. The propeller was thus designed to fail catastrophically, leading to its failure during a demonstration flight and subsequent downing of the UAS.

Threat Use Case #2: Concealment

Concealment refers to embedding of illicit objects within a 3D printed part, such that the printed part appears innocuous to the casual observer. Such threats may be carried out by pausing the 3D print, embedding or placing an illicit item within the build volume, and then resuming the print. The resulting 3D printed part may appear normal and legal, but conceals illicit objects such as explosives, illegal drugs, or embedded technologies for espionage (e.g. cameras, tracking devices, RFID chips).

Threat Use Case #3: Untraceable Weapons

Untraceable weapons include "ghost guns," named as such because they have no serial number, are not traceable, and are not detectable through metal detectors if 3D printed from polymer material.[65] Metal 3D printing may be employed to produce firearms or parts of firearms that are more durable than plastic equivalents and still avoid traceability.

Untraceable weapons may also include 3D printed explosives. The ability to print in multi-materials has led to research in the area of printed explosives by the DoD as well as academic groups.[66] Such explosives may be fabricated from constituent materials, which are widely available and do not raise concern until they are combined in a formulation to produce the

[64] M. Belikovetsky, M. Yampolskiy, J. Toh and Y. Elovici, "Dr0wned cyber-physical attack with additive manufacturing," 11th USENIX Workshop on Offensive Technologies, Vancouver, BC, 2017.

[65] S. Grunewald, "What You Need to Know About 3D Printed Guns and Why You Don't Need to Fear Them," 3DPrint.com, 23 June 2016, https://3dprint.com/139537/3d-printed-guns/.

[66] H. Watkin, "Custom-Shaped Explosives for US Navy 3D Printed on HP 3D Printers," All3DP, 18 April 2018, https://all3dp.com/custom-shaped-explosives-us-navy-3d-printed-hp-3d-printers/.; S. Mraz, "3D Printing with Explosives," Machine Design, 11 January 2018, https://www. machinedesign.com/3d-printing/3d-printing-explosives/; and, J. Kerns, "A Look Inside the 'Explosive' 3D-Printing Industry," Machine Design, 26 February 2018, https://www.machinedesign.com/3d-printing/look-inside-explosive-3d-printing-industry/.

explosive material.

Threat Use Case #4: Supply Chain Exposure

While distributed manufacturing enabled by 3D printing can be an opportunity for supply chain resilience, it also poses security challenges. Specifically, vulnerabilities exist with both the distributed printers themselves as well as with the digital part data.

Distributed 3D printing capability is vulnerable to malware and malicious interference. Weak points in the security of facilities housing 3D printers create potential opportunities for a malicious actor to interfere with production capability, either by rendering the printer inoperable or causing the printer to perform sub-optimally. The 3D printer may be meddled with via direct physical contact with the system, or it may be accessed remotely if the printer is networked.

With digital storage of parts data and build instructions come inherent cyber vulnerabilities; sensitive, proprietary, or critical design information may be exposed during the digital transfer of files between designers, engineers, and manufacturing technicians. Such attacks may be aimed at stealing data or, in a more sophisticated attack, replacing files in such a way as to cause failure of the 3D printer, failure of the build, or premature failure of the part produced (see, Threat Use Case #1: Sabotage of safety critical parts).

Threat Use Case #5: Counterfeits

As the cost of 3D printing systems is reduced, fabrication capabilities become more broadly accessible. Moreover, 3D printing service providers allow sourcing of custom parts for even lower costs as such avenues preclude investment in the printing system. Illicit use of 3D printed parts encouraged by accessibility include fabrication of credit card skimmers, weapons, weaponized UASs, banned products, and explosives.

3D scanning technologies can be used in conjunction with 3D printing systems to allow for ease of reproduction. An actor with physical access to a part may readily scan the part to produce digital design files in order to replicate high value goods, thereby infringing on copyrights and trademarks. Such use of 3D printing to produce counterfeits has economic impacts in terms of loss of market, jobs, and tax revenues and may lead to distribution of lower-quality and potentially dangerous products.

Threat Use Case #6: Biometrics Spoofing

The combination of 3D scanning and printing technologies has been demonstrated as a viable approach for spoofing biometrics. Such threats include fabrication of masks to spoof facial recognition software and prosthetics and fingerprints to spoof fingerprint readers. Attributes of 3D printing which lend it to such applications include:

- ease of individualization and customization of printed parts, and
- ability to produce gradient materials with varying mechanical properties from rigid to flexible

3. Recommendations to best mitigate the perceived deleterious impacts of the assessed technological advancements, including recommended DHS near and long-term actions. Provide an assessment on the perceived opportunities for DHS components to maximize the use of these new technological advancements to guard against emerging threats

Recommendation #1: Technologies for integrated “Attribution” for AM Printers

The ability to embed information within 3D printed parts can serve as the basis for traceability of parts to the originating machines and build files. The proposed approach is analogous to methods incorporated by document printer manufacturers for embedding data within printed documents produced on laser printers.[67] Such technologies do not currently exist for 3D printers. Traceability of 3D printed parts to source machines and source files can benefit commercial entities (IP protection), end users (counterfeit detection), and law enforcement (deterrence and prosecution) in mitigating threats posed by 3D printing technology.

Blockchain—a distributed, decentralized, public ledger that encrypts, validates, and permanently records transactions—is complementary to the ability to embed information in 3D printed parts. Blockchain ledgers are well suited to tracking 3D printed parts in a distributed manufacturing environment. They allow for multiple authorized parties to update a distributed, public ledger. A unique tag embedded in a 3D printed part can be used to trace the history of that part from the time it is fabricated to the time it reaches the end-user. Such an approach to using blockchain was presented for improving the security of 3D printed parts using fluorescent nanoparticle-based tags.[68] A filament doped with fluorescent nanoparticles was used to deposit a public key (a QR code) within a 3D printed part based on asymmetric cryptography, while the emission profile from the nanoparticles served as the private key. The QR code provided a link to a blockchain ledger so that at each point in the 3D printed part's chain of custody, the QR code could be scanned and the part's digital ledger amended.

Recommendation #2: Enhanced Detection Mechanisms

Enhanced imaging and detection tools can aid in countering concealment threats. Capabilities needed include:

- rapid through-part imaging to identify objects concealed within printed parts that otherwise appear innocuous,
- high resolution through-part imaging to identify flaws intentionally embedded in critical parts that may lead to premature part failure, and
- detection of printed explosives material.

Recommendation #3: Reinforced Cybersecurity Measures

An important attribute of 3D printing is the ability to rapidly share design data, 3D models, and manufacturing (build process) files across networks with multiple users and systems. Digital data is readily shared between designers and engineers as well as manufacturing technicians and 3D printers, enabling rapid, iterative product development. To support this workflow, robust means for protecting digital data that may include sensitive, proprietary, or critical design information are needed. Such cybersecurity measures taken to protect digital data should be routinely monitored to ensure they address evolving attack vectors and cyberthreats.

[67] J. van Beusekom, F. Shafait, and T. Breuel, "Automatic authentication of color laser print-outs using machine identification codes," Pattern Analysis and Applications, 16 (2013): 663-678.

[68] Z. Kennedy, D. Stephenson, J. Christ, et. al., "Enhanced anti-counterfeiting measures for AM: coupling lanthanide nanomaterial chemical signatures with blockchain technology," Journal of Materials Chemistry C, 5 (2017): 9570-9578.

This page is intentionally left blank.

EMERGING TECHNOLOGIES: GENE EDITING TECHNOLOGY

1. 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.

1.1 Current State of Gene Editing Technology

The emergence of Clustered Regularly Interspaced Short Palindromic Repeats (CRISPR) with CRISPR-associated endonuclease 9 (Cas9) is a disruptor technology in the field of molecular biology that allows rapid and precise modification of the genome at a fidelity that did not previously exist in molecular biology. The application of this technology represents a new capability in synthetic biology that renders most other gene editing capabilities instantly obsolete. Cumbersome gene editing experiments that once took weeks, months, or years to complete can be performed with less technical skill and effort at a fraction of the previous time and cost. While a technical hurdle still exists for performing CRISPR/Cas9-mediated genome edits, this technology lowers the bar to entry significantly. Fundamentally, the technology opens research avenues for manipulating DNA and represents a paradigm shift in the manipulation of biological systems at the molecular level. The potential implications of this new technology have led to a surge in molecular biology research compared to previous years. The sudden leap of capability has pushed beyond the current level of understanding of the CRISPR technical system, the appreciation of its lasting implications for genome modification applications, and the policies that govern those applications.

Technological advances in genome manipulation such as CRISPR allow the rapid and targeted modification of genomes *in vitro* and *in vivo*, greatly increasing the speed and fidelity at which engineered genomic modifications can be made. To name a few examples, research focused on the manipulation of the genome sequence allows the development of novel gene therapies and drug target discovery, agricultural crop and livestock advancements, increases in accuracy and speed of basic scientific research to understand biological systems, and added options for control of emerging pathogen threats.

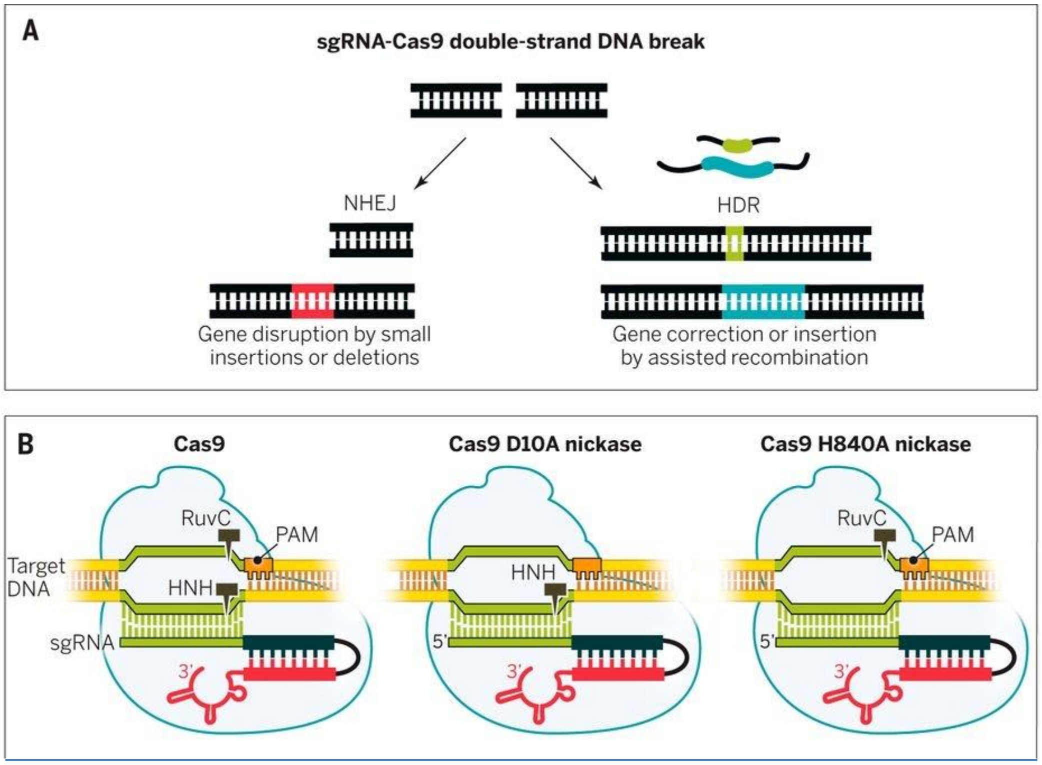
Although CRISPR technology is currently still in development, in terms of both application and basic scientific understanding, it represents a leap forward for genome engineering. The greatest advantages to the technology lie in the simplicity with which a genomic target sequence can be cut, requiring minimal molecular components to induce the DNA cut. For targeted genome modifications, donor DNA is also required to introduce the specific mutation or gene. As the scientific field actively works to understand the parameters surrounding this new molecular tool, limitations of the CRISPR technology are emerging. Unanticipated off-target cutting activity, in which CRISPR cuts unintended locations within the genome, have sparked research into the discovery of new Cas endonuclease enzymes and engineered modifications of known Cas enzymes to increase fidelity of the cutting activity, which would thereby reduce the risks of the technology to modify unintended genome regions. As with other potential gene therapies, CRISPR technology is also limited by deficiencies in effective cell delivery techniques that would move CRISPR components into all cells or targeted cell systems of a multicellular organism.

Acknowledging the imperfections of CRISPR, the technology represents a fundamental shift in genome engineering, bringing a new molecular tool to the laboratory bench that has instantly made other tools in the field less desirable or obsolete. The technology will continue to rapidly expand in the near future as the system is more completely defined and understood and new molecular applications and capabilities are developed.

1.2 CRISPR Gene Editing Technology Overview

The rapidly emerging gene editing technology of CRISPR/Cas9 has the ability to produce precise sequence-targeted cleavages of DNA *in vitro* and *in vivo*. The precision of the endonuclease sequence cleavage mechanism is attributed to the genome sequence complementarity of the guide RNA directing the ribonucleoprotein complex for cleavage at the specific genomic location. In its simplicity, the CRISPR ribonucleoprotein consists of a guide RNA (gRNA) and a non-specific CRISPR-associated endonuclease (Cas) (Figure 10). The guide RNA in the CRISPR Technology contains a region of sequence that associates with the Cas endonuclease and a region of sequence that complements the sequence of the genomic target region. The Cas enzyme recognizes a specific protospacer adjacent motif (PAM) sequence in the genomic sequence. When the Cas associates with the PAM, and if the gRNA complements that genomic region, Cas9 is stimulated to make a double-stranded break about 3-4 base pairs upstream of the PAM sequence. For example, the PAM sequence recognized by Cas9 is NGG, with N being any of the four possible nucleotides followed by two guanine residues. The requirement for the PAM limits the precise locations that can be targeted. Cas9 currently has the most evaluation in the scientific literature; however, several Cas enzymes have been and continue to be discovered and developed for incorporation into the technology as it evolves.

Figure 10: CRISPR as a Genome Editing Technology


A
sgRNA-Cas9 double-strand DNA break
NHEJ
HDR
Gene disruption by small insertions or deletions
Gene correction or insertion by assisted recombination
B
Cas9
Cas9 D10A nickase
Cas9 H840A nickase
RuvC
PAM
Target DNA
HNH
sgRNA
3'
5'

Upon insertion of a double-stranded break into the targeted region of the genome, the non-homologous end-joining (NHEJ) or homology-directed recombination (HDR) technique is used to insert the mutation into the genome (A). Cas9 complexes with the scaffolded sgRNA to form the ribonucleoprotein complex (RNP). The Cas9 of the RNP recognizes its specific protospacer adjacent motif (PAM) sequence within the genome. If the PAM is adjacent to a sequence that complements the gRNA sequence of the sgRNA, the complementary bases pair in a zipper-like manner that stimulates the RuvC and HNH catalytic sites to cleave both strands of the genomic DNA, 3-4 bases upstream of the PAM (B). The Cas9 enzyme can be engineered to have nickase activity, cleaving only one strand of the target genomic region. Cas9 D10A contains a mutation in the RuvC active site, while Cas9 H840A contains a mutation in the HNH active site (B). The image is modified from Doudna and Charpentier.[69]

The targeted genome breaks induced by CRISPR activate cellular repair mechanisms. During the process of repair of these nicks and double-stranded breaks within the genome, exogenous DNA molecules can be inserted randomly or in a directed manner. Random insertions using the non-homologous end-joining (NHEJ) technique are less predictable and result in uncontrolled insertion and deletion (indel) events. NHEJ is most useful when trying to knock-out gene function. Directed insertions using the homology-directed recombination (HDR) technique rely on the provided donor DNA to contain homologous arms with sequence homology to the genome, flanking each side of the desired sequence modification or insert. In this manner, the repair mechanism recognizes the donor DNA as more closely resembling the natural repair of the diploid genome and results in precise DNA insertions. The generation of highly efficient and precise double-stranded breaks is an essential prerequisite to attempt gene knock-out or knock-in assays using CRISPR.[70] According to Baud, *et al*., the simplicity and high efficiency of the CRISPR/Cas9 system makes it a very attractive alternative to traditional knockout procedures.[71]

1.3 Applications of Note

The introduction of CRISPR technology in 2012 was a game-changer for genomic manipulations, making them less challenging and more precise.[72] Since then, the technology has been utilized to induce DNA edits *in vitro* and *in vivo* across numerous biological organisms. The simplicity and efficiency of the application of CRISPR technology in seemingly any animal model are major advantages and may hold the future of animal model-based investigations of complex traits.[73] The speed with which a disease model can be constructed for a given organism may allow construction of very specific disease states to discover new, customized treatments. In addition, the methodology allows modification of multiple genomic loci in a single experiment, facilitating complex observations and affecting gene discovery through multiple mutation interactions. While the list of applications expands well beyond Figure 11, CRISPR applications in several common model systems are

[69] Doudna JA, Charpentier E. 2014. Genome editing. The new frontier of genome engineering with CRISPR-Cas9. Science 346:1258096.

[70] Albadri S, Del Bene F, Revenu C. 2017. Genome editing using CRISPR/Cas9-based knock-in approaches in zebrafish. Methods doi:10.1016/j.ymeth.2017.03.005.

[71] Baud A, Flint J. 2017. Identifying genes for neurobehavioural traits in rodents: progress and pitfalls. Dis Model Mech 10:373-383.

[72] Jinek M, Chylinski K, Fonfara I, Hauer M, Doudna JA, Charpentier E. 2012. A programmable dual-RNA-guided DNA endonuclease in adaptive bacterial immunity. Science 337:816-821.

[73] Baud A, Flint J. 2017.

highlighted.

Figure 11: A Selection of Model Organisms with CRISPR Applications

Organism	Common Name	References
Homo sapiens	Human	(14, 18)
Drosophila melanogaster	Fruit Fly	(26, 27)
Ovis aries	Sheep	(28)
Glycine max	Soybean	(29, 30)
Triticum aestivum	Wheat	(5)
Arabidopsis thaliana	Arabidopsis	(31)
Danio rerio	Zebra Fish	(32, 33)
Caenorhadbitis elegans	Nematode	(34)
Ambystoma mexicanum	Salamander	(35)
Xenopus tropicalis	Frog	(36, 37)
Mus musculus	Mouse	(38-40)
Rattus rattus	Rat	(41, 42)
Sus scrofa	Pig	(43, 44)
Rhesus macaque	Monkey	(45)

1.4 Delivery Systems for CRISPR

CRISPR technology components must be delivered to the nucleus of the cell to induce genomic modifications. As with predecessor gene therapies, delivery systems that can move the CRISPR components efficiently and completely to targeted cells are lacking, which represents a technical hurdle. Once a path over this hurdle is discovered, many more avenues and applications for CRISPR will open. Current delivery strategies include physical delivery by microinjection or electroporation, viral delivery methods like adeno-associated virus (AAV), and non-viral delivery methods like liposomes, polyplexes, or gold particles.[74]

While the delivery systems employed today hold technical limitations for gene therapy applications and experimentation, they can still pose a threat. In one application published in 2014, an animal model for human lung cancer was develop in mice using CRISPR components packaged into adenovirus particles for delivery into the lung epithelial cells of the mice.[75] The CRISPR system was used to introduce breaks in two genes of the

[74] Lino CA, Harper JC, Carney JP, Timlin JA. 2018. Delivering CRISPR: a review of the challenges and approaches. Drug Delivery 25:1234-1257.

[75] Maddalo D, Manchado E, Concepcion CP, Bonetti C, Vidigal JA, Han YC, Ogrodowski P, Crippa A, Rekhtman N, de

mouse chromosome 17 by co-expression of Cas9 endonuclease and two guide RNAs targeting the two sites. The Cas9 restriction in these two chromosome locations of the lung epithelial cells induced a flipped rearrangement of the internal sequence, mimicking similar cancerous Eml4-Alk inversion mutations observed in the human homologs of human chromosome 2.

Beyond the efficiencies observed in the induction of the cancerous Eml4-Alk inversion mutation within the mice, the use of adenovirus to deliver the CRISPR components to the lung epithelial cells is concerning. The application of the CRISPR components into the mouse lungs was facilitated by inhalation of the adenovirus, packaged with the CRISPR components. While the adenovirus used in this study was specific to the mouse model organism, human-specific adenoviruses exist and could be used for delivery of similar CRISPR components into human lung epithelial cells. With this study, the researchers not only demonstrated an efficient methodology for constructing a disease model within the mouse lung but also highlighted a delivery system that with minimal modification could be implemented with humans.

1.5 Modifying the Food Source – Livestock

Using CRISPR, a boost in the speed with which genomic modification can be introduced for genetic engineering of livestock genomes for use as food sources for the U.S. population. Traditionally, these types of transgenic animals undergo many years of scientific evaluation to ensure that they are safe for human consumption and have only recently gained traction for approval by the Food and Drug Administration (FDA). In 2015, the AquAdvantage Salmon, a transgenic animal with increased growth rate, became the first genetically engineered organism approved by the FDA for human consumption in the United States in a process that took six years after the FDA established guidelines for evaluation in 2009. The approval by the FDA of the AquAdvantage salmon as safe for human consumption opens a potential path for other genetically engineered food sources. The introduction of CRISPR technology provides a means to greatly increase the rate and the scope of transgenic animal production.

Breeding livestock to marketable and nutritional needs is a practice that is thousands of years old. Desirable traits are identified in offspring and encouraged through selective breeding practices. A massive and lucrative sector of business surrounds this practice and industry. The application of an effective genome editing technology like CRISPR would greatly shorten the time to achieve desired mutations or added traits within livestock. In one example, CRISPR has been used to manipulate the desired traits in the commercially valuable Shanbei cashmere goat. In a study by Wang, *et al.*, the gene for fibroblast growth factor 5 (*FGF5*) was targeted for knock-out mutagenesis to increase the number of secondary hair follicles and the length of hair fibers in the goats. *FGF5* is the gene that controls fur length in the short- and long-haired Dachshund dog breed. The wild type state is to have the *FGF5* gene intact and functioning within the genome, producing a short-hair phenotype. When the gene is knocked out of the genome, the long-hair phenotype with increased follicle production is observed. Using CRISPR to create this knock out of the *FGF5* homolog within the goat

Stanchina E, Lowe SW, Ventura A. 2014. In vivo engineering of oncogenic chromosomal rearrangements with the CRISPR/Cas9 system. Nature 516:423-427.

genome, Wang, *et al*. produced cashmere goats with increased secondary hair follicles and longer hair fibers.[76] The resulting goats produced more marketable cashmere per individual goat.

A second application of CRISPR mutated the gene for myostatin (*MSTN*) in goats and sheep.[77] *MSTN* is associated with muscle development and inhibits muscle differentiation and growth. Selective breeding of cattle for a knock-out of functional myostatin produced the double-muscled Belgian Blue and Piedmontese cattle lines.[78] Knocking-out this gene is known to cause hypertrophy of muscle mass in several mammal models, including mice, dogs, cattle, and humans.[79]

1.6 Modifying the Food Source – Agricultural Crops

Commodity crops have increased demands on their yields as the global human population increases. According to Doudna and Charpentier, the application of CRISPR technology to these crop plants promises to change the pace and course of agricultural research.[80] For example, the efficiency of CRISPR increases the yield of impactful genome manipulation (nearly 50 percent transformant yields) in rice, and these modifications are passed to progeny in a stable manner with few off-target editing events.[81] Doudna, *et al*. speculate that these findings point to CRISPR providing a method to genetically program protection from disease and resistance to pests in a manner that is superior to predecessor technologies. Development of technologies like CRISPR that facilitate rapid and precise genome editing in agricultural crops provide an opportunity for future food security.[82]

[76] Wang X, Cai B, Zhou J, Zhu H, Niu Y, Ma B, Yu H, Lei A, Yan H, Shen Q, Shi L, Zhao X, Hua J, Huang X, Qu L, Chen Y. 2016. Disruption of FGF5 in Cashmere Goats Using CRISPR/Cas9 Results in More Secondary Hair Follicles and Longer Fibers. PLoS One 11:e0164640; and, Wang X, Yu H, Lei A, Zhou J, Zeng W, Zhu H, Dong Z, Niu Y, Shi B, Cai B, Liu J, Huang S, Yan H, Zhao X, Zhou G, He X, Chen X, Yang Y, Jiang Y, Shi L, Tian X, Wang Y, Ma B, Huang X, Qu L, Chen Y. 2015. Generation of gene-modified goats targeting MSTN and FGF5 via zygote injection of CRISPR/Cas9 system. Sci Rep 5:13878.

[77] Wang X, et al., 2015; and, Crispo M, Mulet AP, Tesson L, Barrera N, Cuadro F, dos Santos-Neto PC, Nguyen TH, Creneguy A, Brusselle L, Anegon I, Menchaca A. 2015. Efficient Generation of Myostatin Knock-Out Sheep Using CRISPR/Cas9 Technology and Microinjection into Zygotes. PLoS One 10:e0136690.

[78] Kambadur R, Sharma M, Smith TP, Bass JJ. 1997. Mutations in myostatin (GDF8) in double-muscled Belgian Blue and Piedmontese cattle. Genome Res 7:910-916.

[79] robet L, Martin LJ, Poncelet D, Pirottin D, Brouwers B, Riquet J, Schoeberlein A, Dunner S, Menissier F, Massabanda J, Fries R, Hanset R, Georges M. 1997. A deletion in the bovine myostatin gene causes the double-muscled phenotype in cattle. Nat Genet 17:71-74; Kim JS, Petrella JK, Cross JM, Bamman MM. 2007. Load-mediated downregulation of myostatin mRNA is not sufficient to promote myofiber hypertrophy in humans: a cluster analysis. J Appl Physiol (1985) 103:1488-1495; McPherron AC, Lee SJ. 2002. Suppression of body fat accumulation in myostatin-deficient mice. J Clin Invest 109:595-601; and, Mosher DS, Quignon P, Bustamante CD, Sutter NB, Mellersh CS, Parker HG, Ostrander EA. 2007. A mutation in the myostatin gene increases muscle mass and enhances racing performance in heterozygote dogs. PLoS Genet 3:e79.

[80] Doudna JA, Charpentier E. 2014.

[81] Zhang H, Zhang J, Wei P, Zhang B, Gou F, Feng Z, Mao Y, Yang L, Zhang H, Xu N, Zhu JK. 2014. The CRISPR/Cas9 system produces specific and homozygous targeted gene editing in rice in one generation. Plant Biotechnol J 12:797-807.

[82] Georges F, Ray H. 2017. Genome editing of crops: A renewed opportunity for food security. GM Crops Food 8:1-12.

The technological advance of CRISPR Technology also side-steps a previously limiting factor for development of transgenic animals as food sources, as was observed in the modification of the white button mushroom. In April 2016, the United States Department of Agriculture (USDA) declined to regulate the cultivation and sale of the CRISPR-edited white button mushroom in the United States.[83] This decision made the mushroom the first CRISPR-modified organism to receive approval by the U.S. Government, but it also highlighted the reduction of a previous technical limitation for producing these type deletion edits. The CRISPR genome modification of the mushroom knocked-out six polyphenol oxidase (PPO) genes, which cause the caps of the mushrooms to brown, making them more desirable for sale for a longer period. The CRISPR-edited mushroom evaded the USDA regulatory process because it was not modified using foreign DNA from viruses or bacteria. When the U.S. Government developed the framework for regulating genetically modified organisms (GMOs) in the 1980s and 1990s, these organisms were necessary to implement these type genome modifications.[84] The advent of rapid and precise genome editing by CRISPR is forcing the U.S. Government to rethink its regulations on GMOs with regard to these advances in genome editing technologies, as the surge in their application is bringing a new generation of plant varietals to the market.[85] In March 2018, the USDA elaborated on its position in a published statement on plant breeding innovation.[86] The statement describes the application of gene editing technologies like CRISPR as plant breeding innovations that can introduce new plant traits more rapidly than traditional breeding techniques, potentially saving years or even decades from the introduction of new, robust plant varieties to farmers. In the statement, the USDA declines to provide oversight for the use of genetically altered plants, if the alterations could have been developed through traditional breeding methods likes cross-breeding and desirable trait selection. Transgenic plants that contain inserted genes from other species will continue to be regulated by the USDA.

1.7 Gene Drives

Gene drive is the introduction of a genetic trait or allele into a system with the added pressure that the introduced allele is favored over the wild-type allele. In natural breeding, a mutant allele along with a wild-type allele would be passed to progeny. In gene drive, the CRISPR components of Cas9 and the single guide RNA sequence, targeting the wild-type allele, are packaged into the mutant allele. Once the copy of the mutant allele is inherited, it actively cuts the wild-type sequence that is present, allowing the wild-type allele to be replaced by the mutated allele through recombinant repair mechanisms. In this manner, gene drive works best in organisms that reproduce sexually and have short generations.

Gene drives have been proposed as a method to control insect vectors that carry diseases like malaria, dengue, and Lyme. Dissemination of gene drives into the insect population might make the insects sterile and unable to replicate or disrupt the ability of the

[83] Waltz E. 2016. Gene-edited CRISPR mushroom escapes US regulation. Nature 532:293.

[84] Ibid.

[85] Ledford H. 2016. Gene-editing surges as US rethinks regulations. Nature 532:158-159.

[86] USDA. 2018. Secretary Perdue Issues USDA Statement on Plant Breeding Innovation, Release No. 00070.18 ed. United States Department of Agriculture.

insect to transmit the disease. Applications of gene drive in herbicide resistant weeds that harm agricultural crops could be used to reverse their resistance mechanisms, making them once again susceptible to the herbicide.[87] Limitations of gene drives include their vulnerability to inactivation due to natural selection, especially if the gene drive produces a deleterious effect on the organism. A gene drive of this type would require continual monitoring and modification as resistance to the drive is developed within the population.[88] Further, gene drive has been described as a potential bioweapon that could be directed toward a population or its food supply. For example, a gene drive introduced into a commodity crop like corn or wheat could limit production of the crops. Gene drive could be used to target key insect pollinator species in order to decrease the numbers available to conduct pollination, thereby indirectly affecting the production of a wide number of crops that rely on insect pollination. In February 2016, James Clapper, the then-U.S. Director of National Intelligence, included gene editing in his annual Worldwide Threat Assessment report to the U.S. Congress as a global threat.[89]

1.8 Human Applications

Although CRISPR applications in the human genome have raised the greatest debate in recent years, many examples exist for the application of CRISPR in mammalian systems, leading to its application in humans. These types of applications within the human genome can be categorized as either somatic or germline edits. Genome edits within somatic cells typically affect localized regions or tissue types. The CRISPR components are delivered to the cells using a delivery system such as cationic lipid vesicles, gold particles, or adeno-associated virus.[90] Currently, clinical trials are underway to evaluate the utility of these types of edits for gene therapies in humans. Germline edits are performed very early in embryonic development or even during or before fertilization. The goal of this type edit is to modify the genome location in every cell of the organism. In this application, the CRISPR components are typically introduced using a microinjection technique directly into the nucleus of the zygote.[91]

[87] Simon S, Otto M, Engelhard M. 2018. Synthetic gene drive: between continuity and novelty: Crucial differences between gene drive and genetically modified organisms require an adapted risk assessment for their use. EMBO reports 19:e45760.

[88] Ouagrham-Gormley SB, Vogel KM. 2016. Gene drives: The good, the bad, and the hype, *on* Bulletin of the Atomic Scientists. https://thebulletin.org/2016/10/gene-drives-the-good-the-bad-and-the-hype/. Accessed December 7, 2018.

[89] Clapper JR. 2016. Worldwide Threat Assessment of the U.S. Intelligence Community, *on* Office of the Director of National Intelligence. https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf. Accessed December 7, 2018.

[90] Zuris JA, Thompson DB, Shu Y, Guilinger JP, Bessen JL, Hu JH, Maeder ML, Joung JK, Chen Z-Y, Liu DR. 2015. Cationic lipid-mediated delivery of proteins enables efficient protein-based genome editing in vitro and in vivo. Nature biotechnology 33:73-80; Lee B, Lee K, Panda S, Gonzales-Rojas R, Chong A, Bugay V, Park HM, Brenner R, Murthy N, Lee HY. 2018. Nanoparticle delivery of CRISPR into the brain rescues a mouse model of fragile X syndrome from exaggerated repetitive behaviours. Nature Biomedical Engineering 2:497-507; and, Ehrke-Schulz E, Schiwon M, Leitner T, Dávid S, Bergmann T, Liu J, Ehrhardt A. 2017. CRISPR/Cas9 delivery with one single adenoviral vector devoid of all viral genes. Scientific Reports 7:17113.

[91] Liang P, Xu Y, Zhang X, Ding C, Huang R, Zhang Z, Lv J, Xie X, Chen Y, Li Y, Sun Y, Bai Y, Songyang Z, Ma W, Zhou C, Huang J. 2015. CRISPR/Cas9-mediated gene editing in human tripronuclear zygotes. Protein Cell 6:363-372; and,

In humans, publications have described the application of germline edits in zygotes that are not allowed to develop into humans. Recently, a scientist from China claimed to have performed germline edits to knock-out the CCR5 gene of twin human girls; however, the controversial germline modifications within the genomes of the twins have not been independently verified. Regarding prospects as therapies, somatic edits and germline edits have their respective situational uses.

Cancer Biology

During the summer of 2017, the FDA completed a multi-year evaluation of the chimeric antigen receptor (CAR) T cell cancer therapy for application to blood cancers like acute lymphoblastic leukemia, reviewed by Jackson, *et al*.[92] In this method of cancer treatment, T cells harvested from the patient are genetically modified to recognize markers on the specific cancer cells that have developed within the patient. This highly customized method relies on genomic modifications of the T cells from the patient. Researchers from Memorial Sloan Kettering Cancer Center have applied CRISPR in the mouse model to more rapidly and precisely introduce these genome modifications, providing an efficient means to introduce very specific mutations in a manner that increases the speed of the modification and does not exhaust the T cells.[93] The result is a CAR T cell lineage that contains the necessary targeting modifications but retains viability to be more effective against the cancer target.

Human Germline Editing

The application of CRISPR to humans immediately raises ethical concerns. CRISPR has no boundaries in the scope of its application and can be used to modify any genomic sequence. These genome edits are performed with unprecedented speed and accuracy and, if applied early in development as to modify all cells within the organism, are inheritable modifications that affect the germline of that organism. Human germline engineering represents permanent changes that are disseminated into the human population, influencing and shaping future generations. Members of the scientific community acknowledge that these modifications should be deliberate and that their potential impact should be fully considered. Further, most of the scientific community acknowledges that CRISPR is not understood well enough for use in human germline editing. With unpredictable phenomena like off-target cutting associated with the use of CRISPR, germline editing could introduce unintended mutations into the genome.

A moment of concern occurred following the 2015 publication of a Chinese study that applied CRISPR to the genomes of trinucleated zygotes.[94] This first publication regarding the application of CRISPR in human embryos was published in the journal *Protein and Cell* after being rejected by the journals *Nature* and *Science* due to its controversial application and

Ma H, Marti-Gutierrez N, Park S-W, Wu J, Lee Y, Suzuki K, Koski A, Ji D, Hayama T, Ahmed R, Darby H, Van Dyken C, Li Y, Kang E, Park AR, Kim D, Kim S-T, Gong J, Gu Y, Xu X, Battaglia D, Krieg SA, Lee DM, Wu DH, Wolf DP, Heitner SB, Belmonte JCI, Amato P, Kim J-S, Kaul S, Mitalipov S. 2017. Correction of a pathogenic gene mutation in human embryos. Nature advance online publication.

[92] Jackson HJ, Rafiq S, Brentjens RJ. 2016. Driving CAR T-cells forward. Nat Rev Clin Oncol 13:370-383.

[93] Eyquem J, Mansilla-Soto J, Giavridis T, van der Stegen SJ, Hamieh M, Cunanan KM, Odak A, Gonen M, Sadelain M. 2017. Targeting a CAR to the TRAC locus with CRISPR/Cas9 enhances tumour rejection. Nature 543:113-117.

[94] Liang P, et al., 2015.

the implications of human embryo editing.[95] In the study, Liang, *et al*., modified the endogenous β-globin gene (*HBB*) within zygotes. The result was a zygote with a mixture of both modified and unmodified cells. These results were deemed mixed and deficient by the greater scientific community. Although the efforts of Liang, *et al*., were considered a rush to apply CRISPR within humans, it was a first step in that direction. In late 2017, a study was published by Ma, *et al*., that built upon the findings of Liang, *et al*.[96] In the study, microinjection was used to act at an earlier stage of development than the Chinese study of 2015, decreasing the occurrence of mixed genotypes in the developing embryos.

In late November 2018, two days before the International Summit on Human Genome Editing in Hong Kong, China and in a disclosure that outraged many scientists based on its disregard for ethical concerns, a Chinese scientist named He Jiankui disclosed that he had CRISPR-modified the genomes of twin human babies. In his work, he used CRISPR technology to knock-out the C-C chemokine receptor type 5 (CCR5) gene in early embryos. The CCR5 receptor gene has been linked to the susceptibility of human immunodeficiency virus (HIV) to enter the cell.[97] If validated, the twins are the first CRISPR-edited humans. Because He performed these experiments largely in secret, the announcement was followed by an international outcry denouncing the work as careless. The particular genome modification is seen as largely unnecessary with modern HIV treatments that control the virus, and there is concern that off-target modifications could have been introduced into the genomes unintentionally. While the summit was meant to bring together the international scientific community to debate and discuss human genome editing and the ethical considerations of it, the careless and self-driven actions of He were largely greeted with rebuke from the scientific community. His claims and the results of his studies have not been confirmed or vetted to determine if the edits were actually conducted and if they were safe; however, his secretive approach to conducting human genomic modifications cannot be denied. Further, it highlights the threat that scientists can use CRISPR to quietly modify the human germline with no oversight from the greater scientific community.

1.9 The Evolution of CRISPR Technology

To overcome the limitations of Cas9 endonuclease, scientists have begun to develop variants of Cas for gene therapies. Researchers have modified Cas9 into single base editors, eliminating the need to supply donor DNA to introduce a point mutation, and they have developed Cpf1 endonuclease, also known as Cas12a, that has increased sequence specificity over Cas9 and tolerates only a few mismatches to the genome complementary sequence within the single guide RNA sequence.[98] Cpf1 provides an option for decreasing the occurrence of off-target cutting events that could erroneously knock-out an unintended gene target.

The scientific community is only just beginning to develop the CRISPR technology.

[95] Cressey D, Cyranoski D. 2015. Gene editing poses challenges for journals. Nature 520:594.

[96] Ma H, et al., 2017.

[97] Lopalco L. 2010. CCR5: From Natural Resistance to a New Anti-HIV Strategy. Viruses 2:574-600.

[98] Eid A, Alshareef S, Mahfouz MM. 2018. CRISPR base editors: genome editing without double-stranded breaks. The Biochemical journal 475:1955-1964; and, Strohkendl I, Saifuddin FA, Rybarski JR, Finkelstein IJ, Russell R. 2018. Kinetic Basis for DNA Target Specificity of CRISPR-Cas12a. Mol Cell 71:816-824.e813.

New enzymes and capabilities like single base editors and Cpf1 endonuclease will continue to emerge as discoveries and innovations in the usage of CRISPR are defined and developed. The drive to overcome the limitations of Cas9 endonuclease for the use of CRISPR technology in gene therapies will continue to fuel innovation in this area. For example, in the spring of 2018, Hu, *et al*., reported the development of xCas9 through phage-assisted continuous evolution, expanding the protospacer adjacent motif (PAM) sites that the enzyme recognizes. The resulting xCas9 enzyme can recognize a broad range of PAM sequences.[99] The modification of Cas9 in this way opens much more of the genome for editing, increasing the specificity of CRISPR by increasing the number of sites that are available to be cut.

1.10 Expected Advancements of Technology

New Cas Enzymes and Engineered Capabilities

CRISPR technology is in its infancy, and researchers have only begun to characterize the scope of what CRISPR can do or become. Over the next several years, as the basic science of CRISPR Technology is characterized, new Cas enzymes with varying capabilities will emerge. These capabilities will include more accurate cutting with fewer off-target cuts, resulting in increased fidelity and precision of genomic modifications. Acquiring this fidelity in genome cutting is being driven by the prospect of using CRISPR as a gene therapy to treat rare diseases and reverse cancerous mutations.

As was seen in the development of Cas nickase enzyme, the protein fusions of the single base editors, and the expansion of PAM recognition sites in xCas9 enzyme, scientists will not only leverage the naturally occurring Cas enzymes, but will engineer new modalities within the available suite of enzymes.[100] These advances in the molecular engineering of CRISPR will allow scientists to develop capabilities beyond those seen in natural systems.

Developing New Applications for CRISPR Technology

A few alarming applications have driven an ongoing conversation around CRISPR technology as it applies to safety and, more importantly, preservation of the human germline. CRISPR provides a means to drive evolution with efficiencies that have not been previously available. Combining this newly acquired power with the desires of individual or rogue scientists to “be the first” in their applications, the scientific community is struggling to restrain and self-govern itself. As was seen with the claimed CRISPR modification of two human babies in China in late November 2018, it is anticipated that more unsanctioned applications of CRISPR will occur in the future. That the scientist in that case conducted his work secretively without oversight of fellow scientists speaks to the profound power of CRISPR and the potential threat of those that will wield it for their own gain. The highly debated concept of designer humans is obtainable and not far from reality. The greater majority of the scientific community will move with caution and strive to apply CRISPR toward improving the human condition. The emergent threat, as was highlighted with the

[99] Hu JH, Miller SM, Geurts MH, Tang W, Chen L, Sun N, Zeina CM, Gao X, Rees HA, Lin Z, Liu DR. 2018. Evolved Cas9 variants with broad PAM compatibility and high DNA specificity. Nature 556:57.

[100] Ran FA, Hsu PD, Lin CY, Gootenberg JS, Konermann S, Trevino AE, Scott DA, Inoue A, Matoba S, Zhang Y, Zhang F. 2013. Double nicking by RNA-guided CRISPR Cas9 for enhanced genome editing specificity. Cell 154:1380-1389; Eid A, et al., 2018; and, Hu JH, 2018.

announcement of the CRISPR-edited human babies, is from those scientists who would conduct their experiments in secret with no oversight, while single-handedly modifying the heritable germline of the human species. Though it has not yet been seen, rogue countries could modify humans and other organisms to serve their own interests, which may run counter to U.S. interests.

CRISPR represents a groundbreaking technology for developing clinical treatments for the prevention of diseases and curing heritable and non-heritable genetic diseases. Limited by delivery systems for targeting specific cells or tissues, scientists will, in the near future, continue to develop cleaver means to apply CRISPR as potential methods for gene therapies. Breakthroughs in delivery systems will be quickly adopted by this scientific group to facilitate and expand their respective applications.

Synthetic gene drive systems using CRISPR have the potential to knock down the number of pests like malaria-carrying mosquitos and to contain other vector-borne diseases such as dengue, Lyme, and Zika.[101] Gene drives are also being applied to contain the emergence of drug resistance in *Candida albicans*, a human pathogen that is the leading cause of fungal infections.[102] Further, gene drives have been proposed as strategies to control unwanted and invasive weed species that deplete nutrients from commodity agricultural crops, making them more sensitive to herbicides.[103] In a report published in July 2018, strategies for gene drive technologies are now moving into experiments in rapidly reproducing mammalian systems.[104] Because gene drives have the ability to address vectors of human and animal disease and increase production in profitable agriculture crops while limiting the development of increasingly toxic herbicides, research and application into synthetic gene drive systems will continue in the near future. With the threat of the use of gene drives as bioweapons that could cripple the food resources of a nation or alter whole ecosystems, monitoring the advancements in gene drives will be necessary.

Development of Detection and Inhibition Capabilities

CRISPR technology has the ability to reach deep into the biological thread of society—to the core of the information that makes us the human species. It can enhance human health and food supplies while providing a means to sustain humanity and reduce human suffering. The tremendous advantages to be gained from CRISPR will continue its feverish drive toward innovation and discovery; however, the risks and threats associated with these rapid developments cannot be denied. Methods for inhibiting or controlling the activity of Cas enzymes will be critical. In January 2017, Maji, *et al.*, reported a multidimensional chemical control of Cas9 that was modified with a fusion to a small molecule-dependent

[101] Gantz VM, Jasinskiene N, Tatarenkova O, Fazekas A, Macias VM, Bier E, James AA. 2015. Highly efficient Cas9-mediated gene drive for population modification of the malaria vector mosquito &lt;em&gt;Anopheles stephensi&lt;/em&gt;. Proceedings of the National Academy of Sciences 112:E6736.

[102] Shapiro RS, Chavez A, Porter CBM, Hamblin M, Kaas CS, DiCarlo JE, Zeng G, Xu X, Revtovich AV, Kirienko NV, Wang Y, Church GM, Collins JJ. 2018. A CRISPR–Cas9-based gene drive platform for genetic interaction analysis in Candida albicans. Nature Microbiology 3:73-82.

[103] Simon S, et al., 2018.

[104] Grunwald HA, Gantz VM, Poplawski G, Xu X-rS, Bier E, Cooper KL. 2018. Super-Mendelian inheritance mediated by CRISPR/Cas9 in the female mouse germline. bioRxiv doi:10.1101/362558:362558.

destabilized domain.[105] The protein fusion makes the Cas enzyme active only in the concentration-dependent presence of small molecules that can bind the destabilized domains. While this is a means to control Cas activity and may have applications in timing or spatially sensitive edits, this approach requires that the Cas is fused to the destabilized domain and would not have applications to unmodified Cas. Research groups at Harvard University and Sandia National Laboratories are actively searching for small molecules that would inhibit Cas9 activity.

With the expansion of applications for CRISPR and the recent birth of allegedly RISPR-modified human babies, it will be critical for determining the cues that CRISPR has been employed to direct a mutation event. Making this determination will help investigators understand if a biological attack has been deployed or if a naturally occurring mutation has emerged. For example, in the case of CRISPR components delivered to the epithelial cells of mouse lungs to induce oncogenic mutations and resulting in cancerous tumors within the lungs, how would one determine that CRISPR was employed to cause an oncogenic mutation if these mutations were induced in human lungs using a similar inhalation-based viral delivery system? Looking further into the future and considering recent claims of the birth of the first CRISPR-modified humans, it may become necessary to determine if a human has been biologically enhanced using CRISPR.

Advancements in CRISPR Delivery Systems

The substrate of Cas nuclease activity is DNA, which is located within the nucleus of the cell. To reach its substrate, the enzyme or the genetic template for the enzyme along with the single guide RNA and donor DNA require a delivery system to reach the nucleus. While there are a few options for delivery systems, they are not precise or efficient. Delivery systems have historically been a limitation for gene therapies; however, with the advent of the simple yet precise CRISPR technology, there is increased demand for delivery systems. Rapidly making the precise edit is no longer the limiting factor; moving the CRISPR components into the correct vicinity is. The drive to use CRISPR in potential gene therapies will stimulate research in delivery system development. In turn, advancements in delivery systems will widen the scope of CRISPR applications.

Impediments that Could Delay or Stall Deployment of Technology

CRISPR technology has arrived and is aggressively under investigation by scientists around the world. The technology has proven itself to be a useful tool for expediting gene modification steps, subsequently opening unprecedented options for genome modification. New aspects of CRISPR or new scientific steps taken using the technology are described almost monthly in journal publications. Advancements using the technology frequently appear in mainstream news reports, making it clear that CRISPR will be a part of molecular biology and affect the lives of individuals for the foreseeable future. The promise of the applications and advances in science that could be facilitated by the technology are opening sources of funding to fuel the research. In January 2018, the National Institutes of Health (NIH) announced the Somatic Cell Genome Editing Program, which will provide funding to

[105] Maji B, Moore CL, Zetsche B, Volz SE, Zhang F, Shoulders MD, Choudhary A. 2017. Multidimensional chemical control of CRISPR-Cas9. Nature chemical biology 13:9-11.

researchers at approximately $190 million over the next six years.[106] Further, numerous companies have emerged around the technology including Editas Medicine, Inc., Intellia Therapeutics, and Caribou Biosciences, Inc., all grappling over intellectual property rights. Researchers across academia are leveraging CRISPR in their laboratories or engaging fee-for-service companies like Sigma-Aldrich or Genscript to design their CRISPR research strategies for use in their laboratories. The aggressive and rapid pace that CRISPR is being unpacked and the amount of resources directed at the research are not limiting factors for the development of the technology. Business Wire forecasts that CRISPR technology investments will grow rapidly from $550M (2017) to greater than $3B in 2023.

Limitations on the technology could come in the form of policy constrictions. When considering the application of CRISPR genome editing technologies, ethical considerations are an immediate concern. How should society approach a technology that can, with unprecedented speed and accuracy, modify the germline of species in a permanent manner that can be passed to future generations and disseminated into the population of that species? The power of CRISPR escalated rapidly to the first application in human embryos, leaping in front of regulations and highlighting the need for oversight. Following the April 2015 publication of the results from CRISPR editing in human embryo genomes reported from China, a moratorium on the application of gene editing technologies in the clinical setting on the human germline was called at the *International Summit on Human Gene Editing* at the National Academy of Sciences in December 2015.[107] This type of moratorium is an attempt by scientists to self-regulate; however, as was seen with the recent use of CIRSPR by Jiankui, a moratorium will not be followed by all scientists when the perception of scientific glory is attainable. In November 2018, the United Nations (U.N.) signed a treaty that agreed to limit the use of gene drives but rejected a moratorium on the development of the technology.[108] The U.N. acknowledged the restraint that needs to be implemented but also recognized the enormous value that gene drive represents. The vague nature of the treaty has been seen as more of a non-declaration of a stance on gene drives. Further, the USDA has clarified its regulatory stance by allowing CRISPR genome edits of agricultural crops that could also be achieved by natural breeding processes. The topic of CRISPR technology and its application is under debate and review; however, no significant regulations restrict its use. Without the development of any formal restrictions, technological development is likely to outpace the policy constrictions.

Currently, the pace of discovery in CRISPR is held by the research itself. In many aspects, CRISPR is uncharted territory. Technical hurdles with the technology exist, which researchers must discover or engineer methods to overcome. One example is the frequency of off-target cutting observed with Cas9. The ability of researchers to conscientiously define new aspects and applications of CRISPR becomes a pace-limiting factor. As the rogue and secretive application of CRISPR to modify the genome of human babies continues to undergo

[106] Britt R. January 23, 2018. NIH to launch genome editing research program, *on* National Institutes of Health. https://www.nih.gov/news-events/news-releases/nih-launch-genome-editing-research-program. Accessed December 12, 2018.

[107] Liang P, et al., 2015.

[108] Callaway E. November 30, 2018. UN treaty agrees to limit gene drives but rejects a moratorium, on Nature. https://www.nature.com/articles/d41586-018-07600-w. Accessed December 12, 2018.

review, scientists are monitoring how policy makers, funding agencies, and the world will react to the researchers involved with this secretive application of CRISPR that affects all humans. The reaction to and subsequent consequences of performing the experiments will define the level of impedance that is placed on other researchers that might do the same thing.

How Convergence of Other Emerging Technologies Could Increase Threat/Opportunity

As with other predecessor genome editing technologies, delivery systems that would move the CRISPR components into the nucleus of appropriate cells for directing genome edits are a limiting factor but also represent a close kinship to the technology. As new delivery systems emerge, they will provide the vehicle for opening applications of CRISPR technology. Similarly, advances in replicative gene drives to better utilize CRISPR technology for selfish allele advancement into the population will bolster the impact of gene drives. For example, a gene drive that evades adaptive mutation resistance within populations would extend the effectiveness of the gene drive for longer periods of time and deeper into the target population.

In emerging fields not typically associated with molecular biology, mechanisms for mechanical delivery systems can be imagined. For example, an unmanned aircraft system (UAS) could be used to disperse adenovirus particles packaged with mutation-causing CRISPR components across a crowd of people.

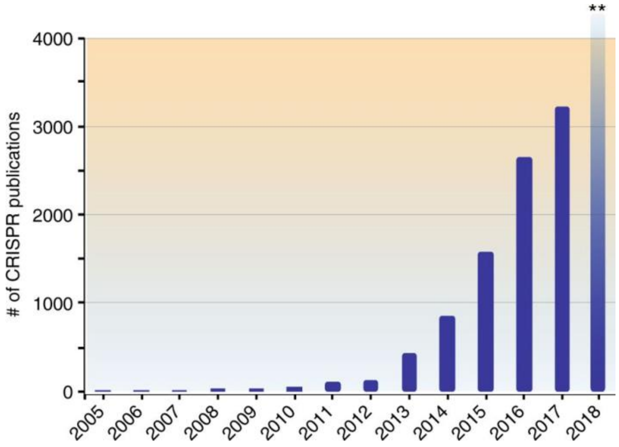
Dissemination of new achievements and milestones in CRISPR research occur at lightning speed. Advanced communications are the most sophisticated in the history of humanity. The development of occurring events are known rapidly around the globe. CRISPR is frequently described as a paradigm shift in molecular biology that is similar to that of polymerase chain reaction (PCR) in the early 1980s. That shift occurred without the presence of the Internet and modern communications. New scientific discoveries at that time were published in printed journal articles that could take weeks or months to review prior to publication. Developments were revealed at a slower, digestible rate. The CRISPR paradigm shift is unfolding in the modern communication age where research is released ahead of formal journal publication, which is for the most part all electronic now. In some cases, the announcement of scientific information is self-published by the scientist in alternative formats like *ReseachGate*, bypassing peer review processes. Internet forums centered on a given topic of research cater to a range of scientists from amateurs to experts; however, the information is available to all. Whole podcasts, like *CRISPR Cuts*, are centered on CRISPR technology. These podcasts are meant to be easily digestible and disseminate knowledge of CRISPR. The term and concept of a podcast did not even exist in the 1980s. Similarly, Twitter feeds like *CRISPR News* are solely devoted to rapidly reporting the newest developments in CRISPR. The vehicles for rapid dissemination of scientific information are drastically different from the emergence of PCR in the 1980s. The presence of this multifaceted platform for monitoring what seems like real-time news in the field of CRISPR unifies the research community but makes predicting next steps and determining who has what information available to them more difficult.

Projected Timeline for Deployment of Technology

CRISPR technology is emerging now. Innovation in this field is advancing in multiple areas of molecular biology with numerous applications. Figure 12 illustrates the surge of research publications surrounding CRISPR over the past 12 years. The breakthrough capability that this technology allows will affect many aspects of life within the homeland including food products, healthcare, and national defense. Figure 13 illustrates the timeline of development for CRISPR with a rapid expansion after its application in eukaryotic cells in

2013.

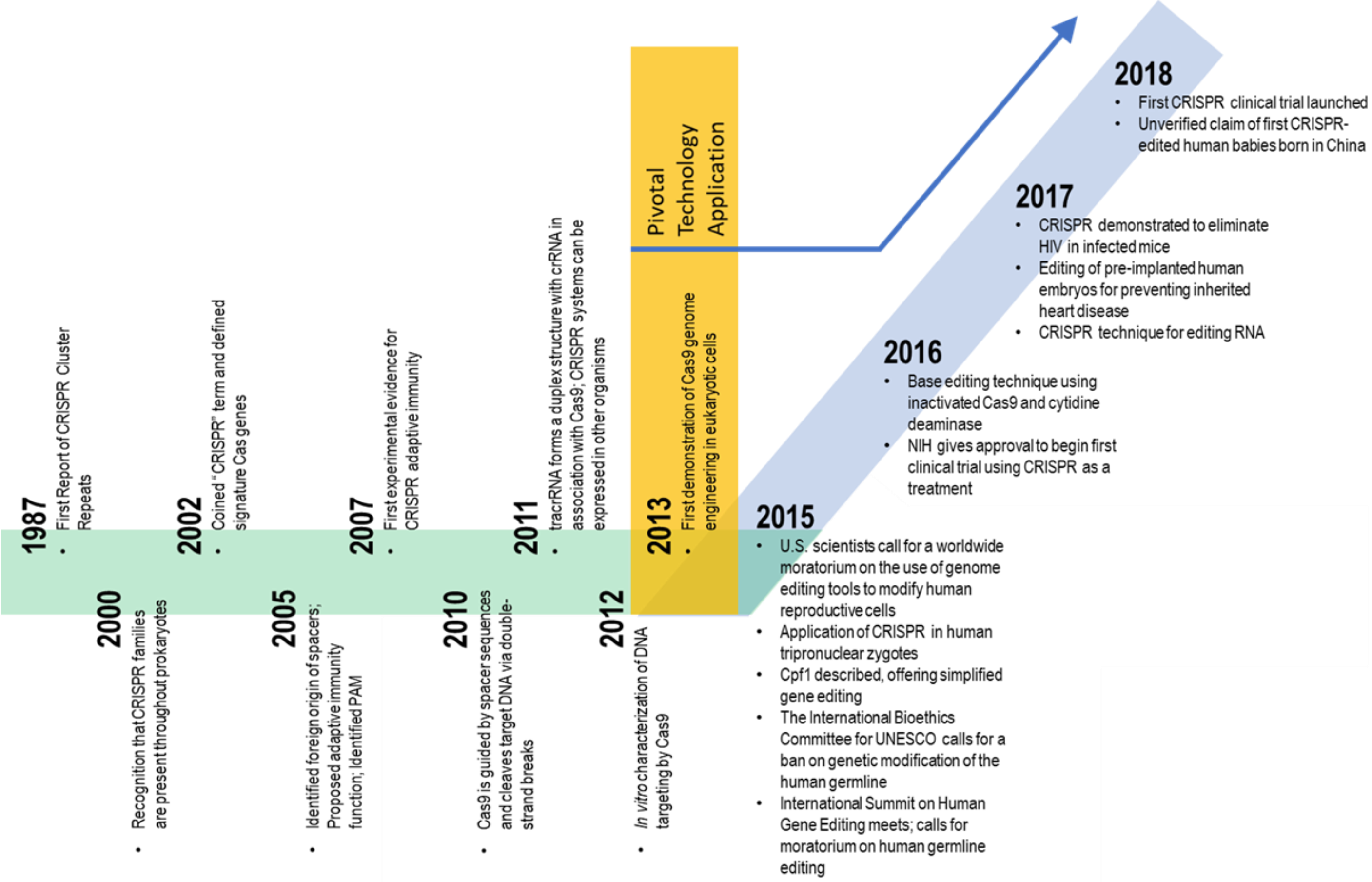
Figure 12: CRISPR Journal Publications



The number of publications within PubMed over the last 12 years that have the word "CRISPR" or "Cas9" in the abstract or title has exponentially grown since its application as a technology in 2012. **Projections for the number of publications in 2018 are estimated to be more than 5000. Image from *Nature Communications*.[109]

[109] Adli M. 2018. The CRISPR tool kit for genome editing and beyond. Nature Communications 9:1911.

Figure 13: CRISPR Timeline


1987
• First Report of CRISPR Cluster Repeats
2000
• Recognition that CRISPR families are present throughout prokaryotes
2002
• Coined "CRISPR" term and defined signature Cas genes
2005
• Identified foreign origin of spacers; Proposed adaptive immunity function; Identified PAM
2007
• First experimental evidence for CRISPR adaptive immunity
2010
• Cas9 is guided by spacer sequences and cleaves target DNA via double-strand breaks
2011
• tracrRNA forms a duplex structure with crRNA in association with Cas9; CRISPR systems can be expressed in other organisms
2012
• In vitro characterization of DNA targeting by Cas9
2013
• First demonstration of Cas9 genome engineering in eukaryotic cells
Pivotal Technology Application
2015
• U.S. scientists call for a worldwide moratorium on the use of genome editing tools to modify human reproductive cells
• Application of CRISPR in human tripronuclear zygotes
• Cpf1 described, offering simplified gene editing
• The International Bioethics Committee for UNESCO calls for a ban on genetic modification of the human germline
• International Summit on Human Gene Editing meets; calls for moratorium on human germline editing
2016
• Base editing technique using inactivated Cas9 and cytidine deaminase
• NIH gives approval to begin first clinical trial using CRISPR as a treatment
2017
• CRISPR demonstrated to eliminate HIV in infected mice
• Editing of pre-implanted human embryos for preventing inherited heart disease
• CRISPR technique for editing RNA
2018
• First CRISPR clinical trial launched
• Unverified claim of first CRISPR-edited human babies born in China

As CRISPR Technology has developed, key points within its path have defined its use for editing the genome. Initially, basic scientific discoveries and characterizations of CRISPR components were distributed across the 2000s. After the demonstration of CRISPR Technology in eukaryotic cells in 2013, the applications of CRISPR have rapidly expanded. The illustration is modified from that of Norman, *et al*. and CRISPR-Cas9: Timeline of Key Events.

2. How such technologies could endanger the homeland, with a focus on those which have the highest likelihood of becoming a threat and those that pose the highest consequences to U.S. homeland security

2.1 New Capability for Homeland Security

Use Case #1

CRISPR technology could be used to control pathogens and pests in livestock and crops. For example, modification of the livestock genome to subvert the mechanisms of pathogenesis utilized by microbial pathogens could increase yields of livestock production. Gene drive utilizing CRISPR technology is currently under debate for use in targeting herbicide resistance factors that have developed over time in weed plants that deplete nutrients from agricultural crops. By knocking down herbicide resistance in the weeds, the development of increasingly toxic herbicides is avoided, and resources are not diverted away from crops.

Use Case #2

CRISPR technology is gaining traction for use as a gene therapy for genetic and pathogenic diseases. For example, a version of CRISPR might one day be used to correct cancer mutations in tumor cells or eliminate retroviruses like HIV from infected human genomes. Currently, the basic science aspects of CRISPR are not fully understood or predictable as seen in the case of the occurrence of off-target cutting.

Use Case #3

Coupling CRISPR to that of gene drive provides a potential capability to control insect vectors that spread disease. For example, using gene drive to knock down numbers of mosquitos in malaria-prone regions of the world can result in the control of malarial outbreaks. This type of vector control can be applied to insects that distribute Lyme, Zika, and other diseases to humans and livestock.

2.2 New Threat to Homeland Security

Use Case #1

CRISPR technology could be used to induce a mutation into a population or crowd of people. For example, CRISPR has been used to induce a cancerous mutation within the epithelial cells of the lungs of mice by packaging the CRISPR components for the mutation into mouse adenovirus particles. Upon inhalation, the adenovirus bound to receptors on the lung epithelial cells and delivered the CRISPR components to the nucleus of the cell.[110] A similar delivery method could be developed to affect humans using the human adenovirus to package and deliver the CRISPR components. Because the virus is inhalable, the release of the particle could affect many individuals in a given release area. Similarly, the particles could be released into air handling systems to affect whole buildings.

Use Case #2

Gene drive with CRISPR technology could be used to propagate a mutation into livestock or agricultural crops to weaken the food supply of the homeland. In a process similar to how gene drive could be used to make weed plants sensitive to herbicides or prevent insect pests from reproducing, a mutation could be introduced with gene drive that weakens or eradicates a species. Beyond the most extreme example of directly targeting a plant or animal, the viability of

[110] Maddalo D, et al., 2014.

plants could be influenced indirectly by introducing a gene drive that eradicates critical pollinator species like honeybees.

Use Case #3

CRISPR technology could be used to rapidly mutagenize or manipulate the genomes of pathogens to quickly escalate pathogenicity. For example, seasonal influenza results from antigenic drift within the virus as it replicates and is passed from host to host. Periodically in history, the influenza virus has experienced an antigenic shift when it crosses species. An example would be in agrarian societies where humans work closely with livestock that can also contract influenza. The antigenic shift is a dramatic variation from what the immune system has seen in previous seasonal strains and can cause harmful pathogenicity and mortality as a result. CRISPR could be used to develop a shifted strain of influenza virus that a nation state could vaccinate their own population against prior to releasing the shifted strain. Similarly, genome editing could be used to change or enhance virulence factors of known pathogens or even bacteria or viruses that are not typically considered pathogens. For example, a non-pathogenic strain of anthrax, commonly found in nature, could be converted into a highly virulent form by altering its genome.[111] Others have raised the concern of whether CRISPR could be used to introduce antibiotic resistance into a bioweapons agent or to develop chimeric bioweapons that cause symptoms of one disease but attack the body with a different, undetectable disease.[112]

Use Case #4

With the declaration of the application of CRISPR technology in humans to modify the germline, it should be anticipated that other scientists and potentially rogue states would secretively perform similar experiments to modify genetic material in an effort to leap ahead of the understanding of the technology. While the directed evolution of the human species in this manner has the ability to help the human condition and eradicate certain types of diseases, the idea of developing designer humans with abnormal strength or advanced intelligence has been suggested by others and should be considered a threat.

3. Recommendations to best mitigate the perceived deleterious impacts of the assessed technological advancements, including recommended DHS near and long-term actions. Provide an assessment on the perceived opportunities for DHS components to maximize the use of these new technological advancements to guard against emerging threats

Recommendation #1

Actively get ahead of advances in CRISPR and gene therapy delivery systems. DHS should have a task force focused on developments in the field of CRISPR and its applications. CRISPR is an unprecedented technological advancement in molecular biology. It poses many benefits but also many threats. In the coming years, threats to the Homeland will develop from CRISPR genome manipulations. The committee tasked with monitoring the technology as it expands would predict witting and unwitting threats of CRISPR that might harm the health, food resources, and/or national interests of the United States. The committee could serve as a resource

[111] Gerstein DM. 2016. How genetic editing became a national security threat, *on* Bulletin of the Atomic Scientists. https://thebulletin.org/2016/10/gene-drives-the-good-the-bad-and-the-hype/. Accessed December 7, 2018.

[112] Vogel KM, Ouagrham-Gormley SB. 2018. Anticipating emerging biotechnology threats: A case study of CRISPR. Politics and the Life Sciences 37:203-219.

to propose government or international policies for engaging the technology responsibly. Such a committee would network with the leading CRISPR researchers and entities in government, academia, and industry to keep a close track on avenues of leading research, giving the committee the ability to anticipate threats that could be on the horizon.

Recommendation #2

At some point, it will become essential to determine whether CRISPR has been used, regardless of whether it was an accidental or intentional deployment of the technology. As the basic science of CRISPR is rapidly becoming a tool for genome modification, DHS should be concerned with also developing means to detect its use.

Recommendation #3

DHS should be monitoring and/or developing means to prevent the action of CRISPR technology or their delivery systems to prevent unwanted CRISPR modifications. For example, in the case of an accidental or intentional release of a gene drive that might harm U.S. citizens, U.S. food supply, vegetation, or wildlife, it may become necessary to understand mechanisms to inhibit the action of CRISPR technology.

This page is intentionally left blank.

This page is intentionally left blank.

APPENDIX A – PANEL MEMBER BIOGRAPHIES

Thad W. Allen (Co-Chair)

Thad Allen is a retired Admiral of the U.S. Coast Guard. He is currently the Executive Vice President at Booz Allen Hamilton and is a national thought leader and strategist in homeland security, maritime security, disaster response and recovery, and energy. He is known for his expertise in public-private sector collaborative efforts to improve national resiliency and create whole of community solutions to complex man-made and natural disasters. Allen completed his distinguished thirty-nine-year career in the U.S. Coast Guard as its 23rd Commandant in May 2010, when President Barack Obama selected him to serve as the National Incident Commander for the unified response to the Deepwater Horizon oil spill in the Gulf of Mexico. Prior to his assignment as Commandant, he served as Coast Guard Chief of Staff. During his tenure in that position, he was designated Principal Federal Official for the U.S. government's response and recovery operations in the aftermath of Hurricanes Katrina and Rita. For his service in those responses, Admiral Allen was the first recipient of the Homeland Security Distinguished Service Medal. Allen also currently serves as a director on the Coast Guard Foundation and Partnership for Public Service, a Fellow in the National Academy of Public Administration, and a Member on the Council on Foreign Relations.

Cathy Lanier (Co-Chair)

Cathy Lanier is currently the Senior Vice President and Chief Security Officer for the National Football League. She previously served as the Chief of Police with the Washington, DC Metropolitan Police Department (MPD) from 2007 to 2016. Ms. Lanier also served as the Commanding Officer of the Department's Major Narcotics Branch and Vehicular Homicide Units. In 2006, the MPD's Office of Homeland Security and Counter-Terrorism (OHSCT) was created, and Chief Lanier was tapped to be its first Commanding Officer. Ms. Lanier is a highly respected professional in the areas of homeland security and community policing. She took the lead role in developing and implementing coordinated counter-terrorism strategies for all units within the MPD and launched the department's Operation TIPP (Terrorist Incident Prevention Program).

Robert Rose (Vice-Chair)

Robert Rose is a recognized expert providing the U.S. government and companies strategic counseling and governance on a full array of cyber-related issues at the nexus of technology, national security, law enforcement and privacy. Bob is Founder and President of Robert N. Rose Consulting LLC and currently serves in various advisory positions in the areas of national security, cyber and homeland security. He currently serves as Senior Advisor to the Chairman and as an Advisory Board member of both 1Kosmos and Securonix. Bob is a member of the U.S. Department of Homeland Security's Homeland Security Advisory Council. Additional corporate and non-profit advisory board service include CrowdStrike Services, Plurilock, SquirrelWerkz, The Chertoff Group, the Aspen Institute Homeland Security Group, Cyber Florida, the Open Commons Consortium at the University of Chicago and the George Washington University Center for Cyber and Homeland Security. Bob previously served as a senior advisor to the Chairman of Bridgewater Associates, and received appointments to the National Security Agency's Cyber Awareness and Response Panel, the Department of State's International Security Advisory Board, the National Counterterrorism Center's (NCTC) Advisory Board, and the Director of National Intelligence's Financial Sector Advisory Board. Bob has received numerous honors and awards, including: a presidential appointment to the J.

William Fulbright Board of Foreign Scholarship, a fellowship with the Wexner Heritage Foundation, the recipient of the U.S. Secret Service's "Outstanding Dedication and Contributions" award and the Connecticut Yankee Council of the Boys Scouts' Distinguished Citizen Award.

Dr. Patrick Carrick

Dr. Patrick Carrick, a member of the Senior Executive Service, is Director, Homeland Security Advanced Research Projects Agency (HSARPA), Science and Technology Directorate, Department of Homeland Security. As the HSARPA Director, he guides the management of the national technology research and development investment for DHS. Carrick leads five divisions, consisting of a staff of more than 200 scientists, engineers, and administrators in Washington, D.C. Each year, HSARPA selects, sponsors, and manages revolutionary research that impacts the future of the Homeland Security Enterprise. As HSARPA's principal scientific and technical adviser, he is the primary authority for the technical content of S&T's portfolio. He evaluates the directorates' entire technical research program to determine its adequacy and efficiency in meeting national and DHS objectives in core technical competency areas, and identifies research gaps and analyzes advancements in a broad variety of scientific fields to provide advice on their impact on laboratory programs and objectives. He recommends new initiatives and adjustments to current programs required to meet current and future Homeland Security needs.

Carrick earned his doctorate of philosophy degree in chemistry from Rice University in 1983 and was an assistant professor of physics at Mississippi State University, and Director of the Shared Laser Facility at the University of Oregon prior to joining the Department of Defense in 1989. He served for 10 years at Edwards Air Force, California becoming Chief of the Propellants Branch at the Air Force Research Laboratory Propulsion Directorate in 1994. He successfully led a team conducting cutting-edge scientific research and engineering. He also directed the High Energy Density Matter Program, which develops advanced rocket propellants and energetic materials. As a senior research physical scientist, he developed the first cryogenic solid hybrid rocket engine.

Carrick served for two years as the Air Force Program Element Monitor for Propulsion and Power Technologies and Deputy for Science and Technology Policy in the Office of the Deputy Assistant Secretary for Science, Technology and Engineering. He monitored and provided guidance for the $300 million science and technology investment in propulsion and power. He served on national steering committees for both rocket propulsion and turbine programs and was the lead editor and coordinator of the national report on hypersonic technology. Carrick also served as the Air Force representative to the Department of Defense Functional Integrated Process Team on Scientist and Engineer Career Field Management.

Prior to becoming part of HSARPA, Carrick was the Director of the Basic Science Program Office and the Acting Director of the Air Force Office of Scientific Research, in Arlington, Virginia where he guided the management of the entire basic research investment for the Air Force. He led a staff of 200 scientists, engineers and administrators in Arlington, VA., and foreign technology offices in London, Tokyo and Santiago, Chile. Dr. Carrick has published more than 25 articles in peer-reviewed professional journals.

Mark Dannels

Mark J. Dannels is the Sheriff of Cochise County, Arizona and is a 34-year law enforcement veteran. Sheriff Dannels holds a Master's Degree in Criminal Justice Management from Aspen University and is a Certified Public Manager accredited from Arizona State University. He is the current Chair of the Immigration and Border Committee with the National

Sheriff's Association, a member of the Board of Directors for the Southwest Border Sheriff's Coalition, and President of the Arizona Sheriff's Association. Sheriff Dannels has been recognized and awarded the Medal of Valor, Western States Sheriff of the Year, Sheriff's Medal, Deputy of the Year, Distinguished Service Award, Unit Citation Award, National Police Hall of Fame, Lifesaving Award, and dozens of community-service awards from service groups and governmental organizations.

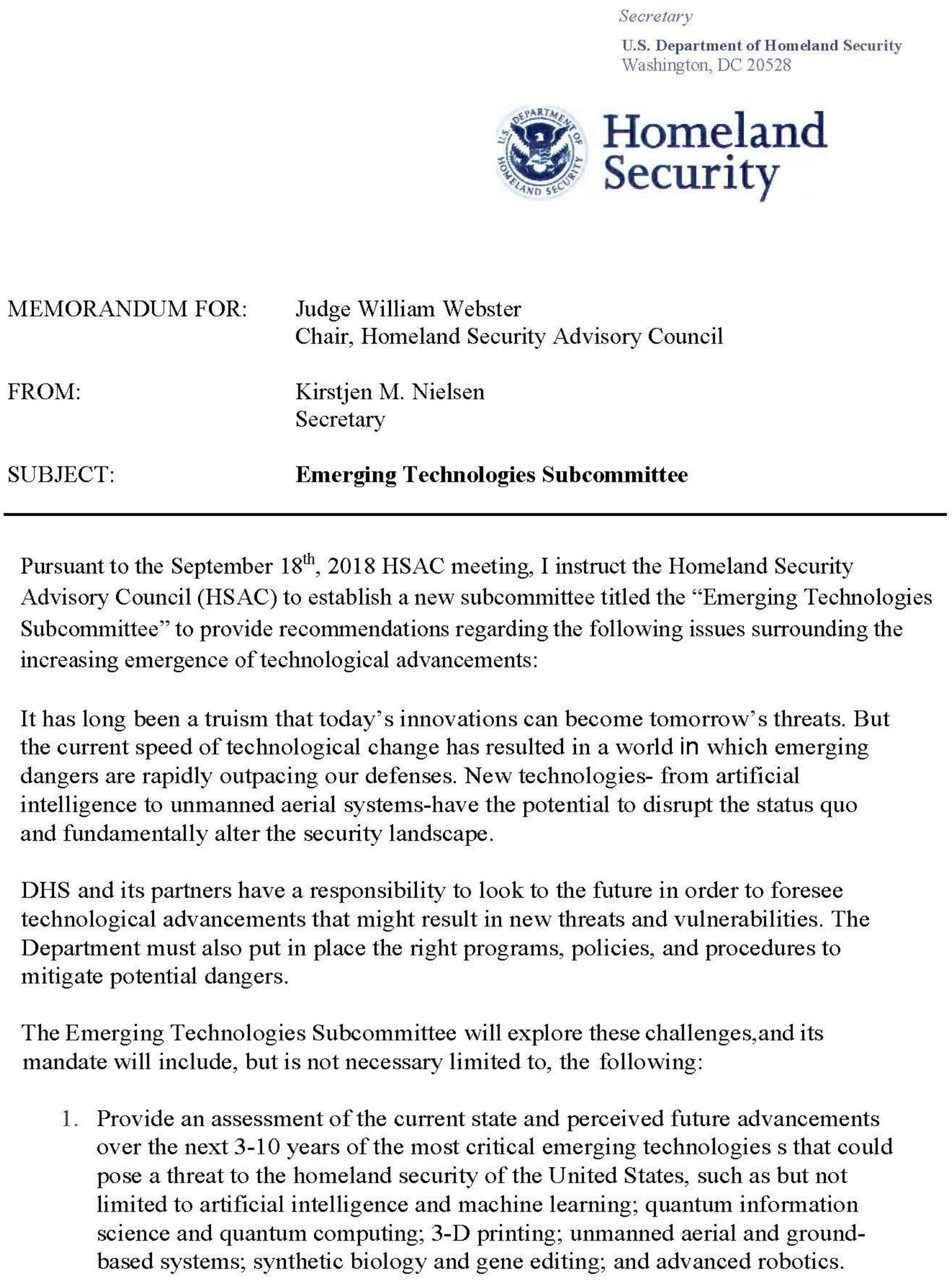
Carie Lemack

Carie Lemack is the co-founder and CEO of DreamUp, a provider of space-based education and media services. She is also the co-founder of Global Survivors Network, a global organization for victims of terror to speak out against terrorism and radicalization. Ms. Lemack has coordinated and inspired events in Jordan, Pakistan, and Indonesia, produced the award-winning documentary film *Killing in the Name,* spearheaded the website www.globalsurvivors.org, and generated interest and coverage in media outlets worldwide. Ms. Lemack co-founded and led the non-profit, non-partisan organization Families of September 11th. She was previously an International Affairs Fellow at the Council on Foreign Relations and is currently a Senior Fellow at the Center for Cyber and Homeland Security at George Washington University

Jeffrey Miller

Jeffrey Miller is the Vice President of Security for the Kansas City Chiefs. Mr. Miller is responsible for developing and managing all safety and security plans and programs for all facets of club operations, including facility security for the training complex, Arrowhead Stadium, event day safety, vendor-operated security and traffic procedures, as well as team security. He also serves as the primary liaison between the club and the National Football League office with regards to all security matters. As Senior Vice President with MSA Security, he was involved in business development in all aspects of the company including Entertainment and Sports Venue Security, Crisis Communications, Explosive Detection K9, SmartTech, Investigations, Social Media Intelligence, Cyber Security and Executive Protection. As the CSO for the National Football League, he oversaw all facets of security for the league including all investigative programs and services, event security (including Super Bowl and International Series), Game Integrity Program, executive protection, the Stadium Security Program, the Fan Conduct Initiative and the Fair Competition Initiative. Additionally, he completed a 24-year career with the Pennsylvania State Police, retiring in 2008 as Commissioner, serving for nearly six years as the 18th Commissioner. As a cabinet secretary, he was responsible for implementing crime and crash reduction strategies, anti-terrorism efforts, and general policing practices including emergency response in all 67 counties in Pennsylvania. He holds an Associate Degree from the University of South Florida, a Bachelor's Degree in Criminal Justice from Elizabethtown College, and a Master's Degree in Public Administration from the Pennsylvania State University. He is also a graduate of the 194th Session of the FBI National Academy in Quantico, Virginia, as well as the 27th Session of the FBI National Executive Institute. He is a Distinguished Alumnus of the Pennsylvania State University as well as an Alumni Fellow of the school

APPENDIX B – TASK STATEMENT



Secretary
U.S. Department of Homeland Security
Washington, DC 20528

Homeland
Security

MEMORANDUM FOR: Judge William Webster
Chair, Homeland Security Advisory Council

FROM: Kirstjen M. Nielsen
Secretary

SUBJECT: **Emerging Technologies Subcommittee**

Pursuant to the September 18th, 2018 HSAC meeting, I instruct the Homeland Security Advisory Council (HSAC) to establish a new subcommittee titled the "Emerging Technologies Subcommittee" to provide recommendations regarding the following issues surrounding the increasing emergence of technological advancements:

It has long been a truism that today's innovations can become tomorrow's threats. But the current speed of technological change has resulted in a world in which emerging dangers are rapidly outpacing our defenses. New technologies- from artificial intelligence to unmanned aerial systems-have the potential to disrupt the status quo and fundamentally alter the security landscape.

DHS and its partners have a responsibility to look to the future in order to foresee technological advancements that might result in new threats and vulnerabilities. The Department must also put in place the right programs, policies, and procedures to mitigate potential dangers.

The Emerging Technologies Subcommittee will explore these challenges,and its mandate will include, but is not necessary limited to, the following:

1. Provide an assessment of the current state and perceived future advancements over the next 3-10 years of the most critical emerging technologies s that could pose a threat to the homeland security of the United States, such as but not limited to artificial intelligence and machine learning; quantum information science and quantum computing; 3-D printing; unmanned aerial and ground-based systems; synthetic biology and gene editing; and advanced robotics.

2. Analyze and provide insight into the ways in which such technologies could endanger the homeland, with a focus on those which have the highest likelihood of becoming a threat and those that pose the highest consequences to U.S. homeland security.

3. Provide recommendations to best mitigate the perceived deleterious impacts of the assessed technological advancements, including recommended DHS near and long-term actions. Provide an assessment on the perceived opportunities for DHS components to maximize the use of these new technological advancements to guard against emerging threats.

These recommendations are due to the full Council no later than 180 days from the date of the subcommittee's formation.

Thank you, in advance, for your work on these recommendations.

APPENDIX C – SUBJECT MATTER EXPERTS

JB Baron, MITRE, CUAS, Lead Systems Engineer, Next Generation UAS

Brien Beattie, Director, Foreign Investment Risk Management, DHS Office of Policy

Carlo Canetta, PhD, MITRE, Mechanical & Reliability Systems

Patrick Carrick, PhD, Chief Scientist, S&T

Susan Coller Monarez, PhD, DAS, PLCY

Heath Farris, PhD, MITRE, Gene Editing, Chief Scientist, Advanced Technology

John Felker, Director, National Cybersecurity and Communications Integration Center (NCCIC), DHS

Dr. Ron Ferguson, MITRE, Cognitive Science & AI

Stacy Fitzmaurice, Transportation Security Administration

Emily Frye, MITRE, Cybersecurity, Director, Cyber Integration

Gerry Gilbert, PhD, MITRE, Chief Scientist & Director, Quantum Systems

Brendan Groves, Department of Justice

David Harvey, PhD, MITRE, Homeland Security Research

Chuck Howell, MITRE, AI/ML, Chief Scientist, Dependable AI

James Murray, Director, United States Secret Service (USSS)

General Robert Newman, Operations Chief, Counter UAS, DHS S&T

Robert Perez, Deputy Commissioner, U.S. Customs and Border Protection (CBP)

John Pistol, former Administrator, Transportation Safety Administration (TSA)

Daniel Price, Principle Director, DHS Office of Policy

Gary Seffel, National Security Council, The White House

Angela Stubblefield, Federal Aviation Administration

Nitin Sydney, PhD, MITRE, Advanced Robotics, Group Leader

Gary Tomasulo, National Security Council, The White House

John Vehmeyer, Portfolio Manager, S&T

Yaakov Weinstein, PhD, MITRE, Emerging Technologies