HOMELAND SECURITY ADVISORY COUNCIL

FINAL REPORT

ARTIFICIAL INTELLIGENCE / MACHINE LEARNING

EMERGING TECHNOLOGIES SUBCOMMITTEE

November 14, 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, Co-Chair Cathy Lanier and Co-Chair Robert Rose as the ***final report*** and recommendations to the Acting Secretary of the Department of Homeland Security, Chad Wolf.

<SIGNATURE OBTAINED FOR PDF COPY>

Thad Allen (Co-Chair)

Cathy Lanier (Co-Chair)

Robert Rose (Co-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 (Co-Chair) – Founder and President, Robert N. Rose Consulting LLC
Dr. Patrick Carrick – Former Chief Scientist, Science & Technology, 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

Mike Miron, Executive Director, Homeland Security Advisory Council
Evan Hughes, Deputy Executive Director, 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 - EMERGING TECHNOLOGIES SUBCOMMITTEE

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

This page is intentionally left blank.

INTRODUCTION

In recent years there has been an explosion of research and development in artificial intelligence with ever increasing application in nearly all aspects of society, economy, critical infrastructure and overall national security. The emerging and growing field of artificial intelligence (AI) promises to provide new capabilities and potentially unintended consequences that will impact the Homeland Security Enterprise. AI, including machine learning (ML), is broad and plays a major role in areas such as autonomous cars/drones, cyber and the "Internet of Things" (IoT), and critical infrastructure, for example.

The importance of AI and its impact is demonstrated in the Executive Order (EO) 13859, Maintaining American Leadership in Artificial Intelligence[1]signed by the President on February 11, 2019. The national AI Research and Development (R&D) Strategic Plan, which supports the EO, defines priority areas for federal investments in AI R&D.[2] The increase in federally sponsored AI R&D, combined with investments from private industry and other R&D organizations, will foster the development of a large set of technologies that undoubtedly will have lasting impacts on national security and the entire homeland security enterprise.

The emerging technological threats can be divided 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 paper focuses on the former, although possible instances of the latter area are also included. The paper uses two threat areas to highlight the potential impacts of AI/ML and then describes three emerging but not imminent threat areas for consideration. Finally, it provides some high-level policy recommendations for DHS to consider as it strives to establish a posture of preparedness, readiness, and resilience against these emerging threats.

1. ASSESSMENT OF PERCEIVED AI 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 l—for example, recognizing patterns, learning from experience, drawing conclusions, making predictions, or taking action l—whether digitally or as the smart software behind autonomous physical systems."[3] 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

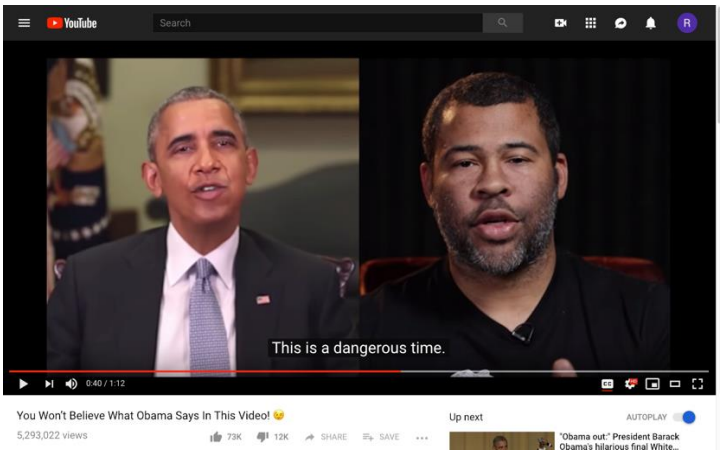
networks with dozens of layers to not only learn classifications but also learn relevant features. This capability allows deep learning systems to be trained using relatively unprocessed data (e.g., image, video, or audio data) rather than feature-based training sets. To do this, deep learning requires 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.[4] 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. Sections 1-3 focus on the former, although possible instances of the latter area are included in section 4.

2. EMERGING TECHNOLOGY: DEEPFAKES

"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.[i] Most commonly this involves mapping facial portraits or video of one person onto a person in another image or video. For example, a well-known deepfake video demonstration (see Figure 1) 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.[5]

Figure 1: Example of a Deepfake Video – "President Obama" delivers a warning message about deepfake technology



There are also tools in development for creating deepfakes for voice.[6] Software from Adobe that can reliably mimic a speaker based on 20 minutes of voice data has been demonstrated publicly,[7] but the prototype appears to be unreleased as of this writing.[8] Voice mimicking software that only requires one minute of voice data is publicly available but produces output with notable artifacts and a robotic tone.[9]

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

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.[10] Phone applications, such as FaceApp, permit manipulation of facial characteristics.[11] Video software libraries such as DeepFakeLab and FaceSwap are available as public or open-source systems.[12]

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.[13]

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.[14] 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 3: 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

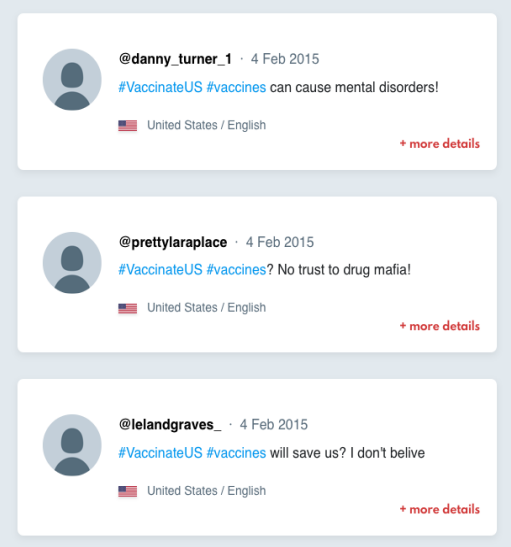
It appears likely that broadly available deepfake video capabilities could be available within the next 2 to 5 years. One expert noted that he believed it highly likely that a viral deepfake video will be used against a political candidate in 2020.[15] Vocal deepfake tools have somewhat lagged behind 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.[16]

3. EMERGING TECHNOLOGY: 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.[17]

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.[18]

Figure 2: Example of Russian tweets on vaccine debate produced by Russia's Internet Research Agency.



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.[19]

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 narratives for well-defined domains such as sports.[20] 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.[21] Other myth debunking web sites, such as Snopes and FactCheck, can serve a similar purpose.[ii] 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

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.

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

reduce impersonation (although these can be circumvented using crowdsourcing services such as Mechanical Turk).[22]

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 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.

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 3.[23]) 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.[24]

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 DARPA Cyber Grand Challenge.[25] 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.[26] 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.[27] 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.[28] Voice agents, such as the Google Duplex system, open up the possibility of massive phone-based social engineering attacks.[29]

5. HOW SUCH TECHNOLOGIES COULD ENDANGER THE HOMELAND

New Capabilities 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.30 Alternatively, a standards agency such as National Institute of Standards and Technology (NIST) could certify organizations that detect fake media.

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.

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.

6. RECOMMENDATIONS TO MITIGATE THE PERCEIVED DELETERIOUS IMPACTS OF THE ASSESSED TECHNOLOGICAL ADVANCEMENTS

It is anticipated that the AI technologies will be used in the DHS operational environments to support DHS in executing various missions and priorities. Therefore, it is important for DHS to invest in workforce development for an AI-ready work place. Additionally, capabilities such as AI Testbeds and AI Forensic teams can be established through a combination of Public-Private Partnerships, as well as federally funded multi-agency/multi-use infrastructure, to ensure DHS is prepared to deter potential threats that may arise from malicious AI systems.

With regards to the specific three concerns described in this paper the following recommendations are also proposed.

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.[iii]

[1] White House, "Executive Order on Maintaining American Leadership in Artificial Intelligence," 11 February 2019, https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/

[2] Select Committee on Artificial Intelligence of the National Science and Technology Council, "The National Artificial Intelligence Research and Development Strategic Plan: 2019 Update," White House, June 2019, https://www.whitehouse.gov/wp-content/uploads/2019/06/National-AI-Research-and-Development-Strategic-Plan-2019-Update-June-2019.pdf.

[3] 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

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

[5] 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.

[6] 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.

[7] BBC News, 7 November 2016.

[8] 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.

[9] Scientific American, 2 May 2017.

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

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

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

[12] 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.*
[13] "Deep Learning MOOCs and Free Online Courses," MOOC List, https://www.mooc-list.com/tags/deep-learning
[14] Matt Turek, "Media Forensics (MediFor), Defense Advanced Research Projects Agency, undated, https://www.darpa.mil/program/media-forensics
[15] 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
[16] H. Kim *et al.*, "Deep Video Portraits," in *SIGGRAPH*, Vancouver, 2018.
[17] "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.
[18] 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/.
[19] 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.
[20] 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.
[21] U.S. Department of Homeland Security Social Media Working Group for Emergency Services and Disaster Management March 2018.
[22] 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.
[23] K. Eykholt *et al.*, "Robust Physical-World Attacks on Deep Learning Models," in *Proc of Conference on Computer Vision and Pattern Recognition*, 2018.
[24] 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.
[25] 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
[26] 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/
[27] *Digital Exhaust*," Wikipedia, https://en.wikipedia.org/wiki/Data_exhaust
[28] 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
[29] Yaniv Leviathan and Yossi Matias, 8 May 2018.
[30] DARPA, undated.

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 (Co-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 serves in various advisory positions in the areas of national security, cybersecurity, and homeland security. He currently serves as Senior Advisor to the Chairman and as an Advisory Board member for 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 The Chertoff Group, MITRE's Homeland Security Experts Group, Cyber Florida, Opora, Plurilock, and the Council of Executives for Auburn University's 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 of America Distinguished Citizen Award.

Dr. Patrick Carrick

Dr. Patrick Carrick, previously served as a member of the Senior Executive Service, as Director, Homeland Security Advanced Research Projects Agency (HSARPA), Science and Technology Directorate, Department of Homeland Security. As the HSARPA Director, he guided the management of the national technology research and development investment for DHS. Carrick led 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 was the primary authority for the technical content of S&T's portfolio. He evaluated the directorates' entire technical research program to determine its adequacy and efficiency in meeting national and DHS objectives in core technical competency areas, and identified research gaps and analyzes advancements in a broad variety of scientific fields to provide advice on their impact on laboratory programs and objectives. He recommended new initiatives and adjustments to current programs required to meet current and future Homeland Security needs. Carrick earned his Doctor 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.

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, DHS

Yaakov Weinstein, PhD, MITRE, Emerging Technologies