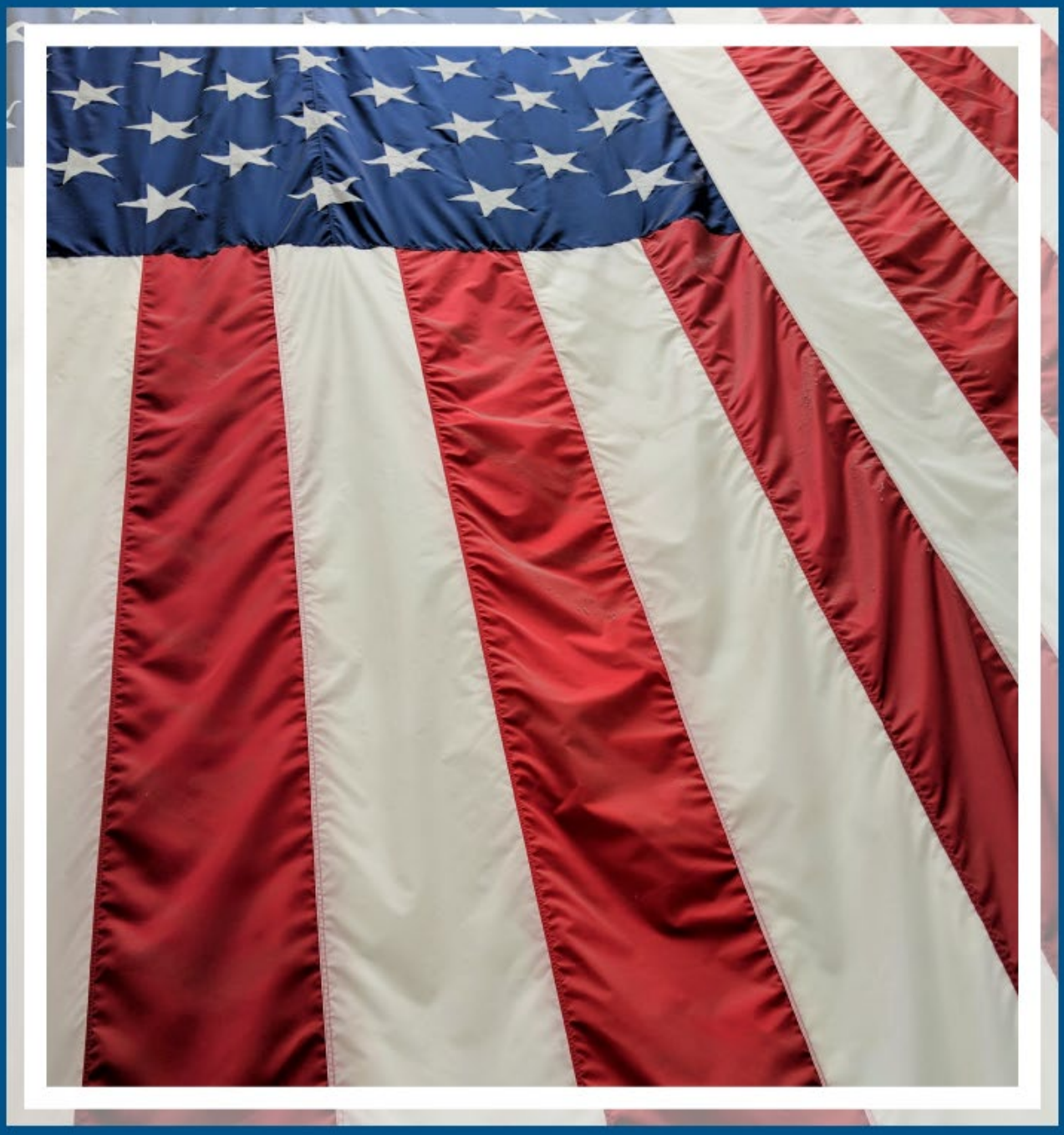

HOMELAND SECURITY ADVISORY COUNCIL

Final Report: Emerging Technologies Subcommittee Quantum Information Science

NOVEMBER 2020

Homeland Security

This page is intentionally left blank

On behalf of the Homeland Security Advisory Council, Emerging Technology Subcommittee, Robert Rose, Co-Chair, and Cathy Lanier Co-Chair, present this final report and recommendations to the Acting Secretary of the Department of Homeland Security, Chad F. Wolf.

<SIGNATURE OBTAINED FOR PDF COPY>

Robert Rose (Chair)	Cathy Lanier (Co Chair)
Founder and President	Senior Vice President and CSO
Robert N. Rose Consulting LLC	National Football League

This page is intentionally left blank.

EMERGING TECHNOLOGIES SUBCOMMITTEE

Robert Rose (Co Chair)	Founder and President, Robert N. Rose Consulting LLC
Cathy Lanier (Co Chair)	Senior Vice President and Chief Security Officer, National Football League
Dr. Patrick Carrick	Former Chief Scientist, Science & Technology, Department of Homeland Security
Frank Cilluffo	Director, McCrary Institute for Cybersecurity & Critical Infrastructure Protection, Auburn University
Mark Dannels	Sheriff, Cochise County Arizona
Carie Lemack	Co-Founder and CEO, DreamUp
Jeffrey Miller	Vice President of Security, Kansas City Chiefs

HOMELAND SECURITY ADVISORY COUNCIL STAFF

Mike Miron	Acting Executive Director, Homeland Security Advisory Council
Evan Hughes	Associate Director, Homeland Security Advisory Council
Garret Conover	Director, Homeland Security Advisory Council
Colleen Silva	Analyst, Homeland Security Advisory Council

ADDITIONAL CONTRIBUTORS

Anne LaPerla	Independent Contributor
Anjana Rajan	Technology Policy Fellow, The Aspen Institute
Katharine Petrich	Research Fellow, Research on International Policy Implementation Lab, American University.
Amelia Mae Wolf	Truman National Security Fellow

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.

EMERGING TECHNOLOGIES: QUANTUM INFORMATION SCIENCE AND QUANTUM COMPUTING

Introduction

Quantum information science (QIS) is the field dedicated to exploiting quantum phenomena for the enhancement of information technologies. While once thought of as a niche area of physics, the last few years has seen a flurry of interest and activity from established technology companies such as Google, IBM, Microsoft, Alibaba, Honeywell, and Intel, as well as numerous startups. Broadly speaking, QIS can be divided into three areas: quantum computing, quantum communications, and quantum sensing. Quantum computers, if fully developed, could break all currently used public key encryption and solve certain other problems of importance much faster than classical computers. Quantum communications provide complete security against potential eavesdroppers. Quantum sensors can enhance a range of sensing modalities including gravimetry and electrometry. Each of these technologies has the potential to significantly impact DHS and other government agencies. In this document, we introduce these technologies and outline the threat, as well as the opportunities, they pose to homeland security.

Quantum Computers

Quantum computers exploit the quantum phenomenon of superposition, the ability for quantum systems to be in multiple states simultaneously, to compute in a massively parallel fashion. This ability leads to potential new algorithms that can efficiently solve problems that are intractable on conventional computers. Most famous of these is Shor's algorithm which allows a quantum computer to factor large numbers efficiently (polynomial time). This algorithm enables a quantum computer to break Rivest-Shamir-Adleman (RSA) encryption and other public key encryption systems which rely on a computer's inability to factor large numbers or solve related problems within a reasonable period of time.[1]

Quantum computers can also be used to more efficiently break symmetric key encryption techniques such as AES.[2] To do this, a quantum computer would utilize Grover's algorithm, a quantum algorithm that can be used to speed up searches of unsorted databases and function inversion. Unlike Shor's algorithm, which provides an exponential savings when compared with the best-known classical algorithms, Grover's algorithm provides at best a square root speed up

[1] RSA encryption is used for digital transactions conducted over the Internet, including data transmitted via email systems. It is named for its inventors, Ronald Rivest, Adi Shamir, and Leonard Adleman. It leverages the difficulty of factoring to create a secure key whose decryption is far beyond current decryption capabilities. For further details, see: Simmons, Gustavus. "RSA encryption" *Encyclopedia Britannica*. 3 August 2012. Web. 25 October 2020. https://www.britannica.com/topic/RSA-encryption

[2] AES stands for Advanced Encryption Standard, which is the Federal Information Processing Standard (FIPS) approved level of cryptographic algorithm that can be used to protect electronic data. It is a symmetric block cipher, which coverts data into ciphertext for transmission, and then decrypts back to its original plaintext form upon reception. It was adopted by the Secretary of Commerce in 2001. AES encryption provides 256 bits of security, while commonly used versions of RSA only provide up to 112 bits of security. See: National Institute of Standards and Technology. "Publication 197: Specification of the Advanced Encryption Standard (AES)." Washington, D.C.: Government Publishing Office, 2001. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

over conventional procedures. While still significant, a doubling of the key length could essentially nullify the quantum advantage.

Beyond encryption, quantum computers can implement machine learning protocols, such as clustering and image classification, and solve optimization problems more quickly than their classical counterparts. This is partly enabled by the Harrow Hassidim Lloyd (HHL) algorithm, which efficiently solves certain linear algebra problems such as determining the eigenvalues of a matrix.[3] Quantum computers could also be universal quantum simulators with the ability to simulate materials and other physical systems at their most basic level. A quantum computer would thus revolutionize computational material science and perhaps allow for greater insight into the workings of high-temperature superconductors and nitrogenases.[4]

Quantum Communications

The first commercial quantum technology was quantum key distribution (QKD), a method allowing parties separated by line of sight (or having a trusted node) to share a cryptographic key. QKD utilizes single photons (particles of light), and relies on the fact that, in quantum mechanics, measurement of a system changes the state of that system. This allows two separate systems to determine whether the key they have shared was intercepted by an eavesdropper. The key can then be used as a one-time pad, guaranteeing continual, unconditionally secure communication.[5] When implemented correctly, QKD thus provides unconditional security and a method to constantly renew a cryptographic key.

Secure direct communications can also be enabled by quantum mechanics by utilizing a resource called entanglement. Entanglement is a quantum phenomenon in which two or more quantum systems (such as photons) exhibit correlations above and beyond what is possible for classical systems. Given two quantum systems that are entangled, one held by "Alice" and the other by "Bob," either party can determine the state of the other's system simply by observing the state of their own system. When abetted by classical communications, entanglement enables communication in which the information itself is not transferred directly from Alice's system to Bob's system, and thus cannot be intercepted by an eavesdropper (we note that communication in the form of instructions on how to measure the systems must be transferred between the two systems).

Quantum Networks

There are two types of quantum networks referred in the literature. Neither of them is parallel to classical networks. The first type is a QKD network which consists of a group of nodes each of

---

[3] HHL is also referred to as the quantum algorithm for linear systems of equations. It was developed in 2009 and works to speed up traditional algorithm processing speeds.

[4] Nitrogenase is an enzyme complex produced by bacteria which are extremely sensitive to oxygen and nitrogen, making it challenging to study, but which are critical to all forms of life. Our current level of understanding is limited by available computing power.

[5] A 'one-time pad' is an encryption technique that uses a single use, pre-shared random key that allows for secure encryption. The name refers to an early technique where the key was literally printed on a pad of paper, the top sheet of which could be torn off and disposed of after use.

which can implement QKD with any other node on the network. These networks must be one-to-one as QKD inherently cannot be done in such a way to guarantee that the key generated between two nodes will be the same as guaranteed between any other two nodes. It is not possible for one node to share the same key with multiple other nodes.

The second type of quantum network is a network in which the various nodes share entangled photons. As described above, the entanglement can serve as a resource enabling the nodes to communicate without fear of an eavesdropper. Sharing entanglement over long distances is not an easy task due to absorption in fiber. One may choose to employ a quantum repeater to boost the distance over which entanglement can be shared. A quantum repeater, unlike classical repeaters, cannot amplify. Instead, quantum repeaters measure entangled photons in such a way as to allow entanglement to be shared over longer distances.

Quantum Sensors

Quantum phenomena have the potential to enhance several quantum sensing modalities including magnetometry, electrometry, gravimetery, and associated techniques such as accelerometers and gyroscopes. Three platforms of interest for quantum sensors are atoms, artificial atoms, and light. A short introduction to each is included below.

Atomic sensors can operate in two different ways: as interferometers, using beams of atoms sent through atomic interferometers where, due to their extremely short wavelength they are more sensitive than typical light-based interferometers, and as sensors of magnetic and electric fields. Atomic interferometers can be built such that they are sensitive to different types of accelerations and the presence of mass. For both, one path of the interferometer will be more affected than the other, causing a path-length difference. Hence, they can be used as gravimeters, gravity gradiometers, accelerometers, and gyroscopes. All have the potential to improve upon the performance of classical sensors in both sensitivity and long-term accuracy. They are also expected to improve upon alternative quantum sensors (superconducting quantum interference device or "SQUIDs") in both Size, Weight, and Power (SWaP) and long-term accuracy.[6] Potential applications for atom-interferometer based sensors include accurate position, navigation, and timing (PNT) for navigation in GPS-denied environments, tunnel detection, detection of WMD, and detection of anomalously heavy objects (e.g., loaded trucks, shipping containers).

Atomic magnetometers detect, measure, and assess magnetic fields based on the precession rate of the atom. These systems have already demonstrated sensitivity below a femto-Tesla in the laboratory and have a very low SWAP+C compared with today's best technologies. In addition, these systems can be placed close to a potential source and thus could revolutionize magnetic resonance imaging (MRI).

Atomic electrometers are atoms with a highly excited outer electron allowing them to behave as highly sensitive electric dipoles. These systems can achieve much higher sensitivity than standard

[6] SQUIDs are highly sensitive magnetometers used to measure tiny magnetic fields, key for many scientific uses like biology and magnetic property measurement systems. They have both civilian and military uses.

antennas and they have the potential to sense carrier frequencies from DC through 10 THz (10×10^{12} Hz) without changing the physical platform. They do not follow the standard Chu limit (i.e., their bandwidth is not limited by the size of the sensors), and they inherently reject out-of-band noise. Unlike standard antennas, they do not absorb the field that they are detecting. Despite their current limitations in bandwidth and dynamic range, atomic electrometers are uniquely positioned to enable novel electric field sensing modalities including communications in the untapped THz band for terabits/sec data rates, a portable calibration standard for THz frequencies (which does not yet exist), and sub-wavelength field mapping and imaging over a broad spectral range. These "atom radios" will enable high-rate free-space communications, which could be used as secure nodes for PNT or for high-vision data delivery for telemedicine.

Defects in solid-state systems, a mis-placed atom in a crystal of other atoms, can act as artificial atoms and be used as sensors. An example is nitrogen-vacancy (NV) centers in which a nitrogen atom displaces two carbon atoms in a diamond lattice. The advantage of these sensors is their high sensitivity, which is at least partly due to their extremely low SWAP, allowing them to be placed extremely close to the sample to be tested. In addition, because these systems are in a solid-state lattice, they have the ability to be placed in biological and other environments where other sensors would not be tolerated.

When photons (particles of light) are entangled, they can be used as probes for increased sensing capability. The first example of this was quantum lithography, in which entangled light is used to make smaller lithographic lines than typical photons. Quantum illumination is a technology that can potentially use entangled photons to increase signal-to-noise ratio for radar and lidar by answering the question of whether or not there is a target at a pre-specified distance (in a given direction) from the sensor. One of the pair of photons is sent towards the target, while the other is stored until the first returns. They are then jointly measured. This technology may be useful for situations in which a warning receiver—used by an adversary to detect radio emissions of radar systems—would limit the ability to sense a target.

Quantum illumination can enhance the sensitivity of both lidar and radar systems by improving their ability to detect faint objects against noisy backgrounds. While there have been some proposals to use this technique for close-range biomedical imaging, the most commonly proposed application is quantum radar, which improves radar systems' ability to detect faint objects at long range.

In principle, quantum radar (or any other form of quantum illumination) can achieve a signal-to-noise ratio that is 6 dB higher than the best standard radar system.[7] But useful quantum radar systems have proven very difficult to engineer in practice. There are several fundamental obstacles to the useful deployment of quantum illumination and radar: for example, the transceivers must be cooled down to extremely low temperatures, and the fact that the target distance must be known in advance limits the technique's utility for detecting objects at long distances.

[7] Si-Hui Tan et al., "Quantum Illumination with Gaussian States," Physical Review Letters 101, 253610 (2008).

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.

Various governments, large multi-national corporations and innumerable startups are engaged in the research and development of quantum technologies. In what has been deemed the "Quantum Race," countries worldwide more than tripled their investment in quantum computing and software between 2012 and 2019.[8]

Today, the United States and China are the greatest investors, with other countries following close behind. As of 2018, the total U.S. federal government investment in quantum technology R&D was estimated to be $200-250 million per year.[9] U.S. investment is currently increasing significantly: in 2018 the President signed into law the National Quantum Initiative Act, which authorized $1.275 billion over five years for the Department of Energy (DOE), the National Science Foundation (NSF), and the National Institute for Standards and Technology (NIST) to invest in R&D in quantum information science.

In 2016, President Xi Jinping of China established a national strategy for the country to become technologically self-reliant. The country has stepped up its research and investment in quantum technologies significantly since then, hoping to surpass the United States as the leader in technology.[10] China's government was estimated to be investing $244 million in quantum R&D per year as of 2018.[11] As of January 2019, the US Senate's Worldwide Threat Assessment report stated that the United States' lead in technology had been significantly eroded, mainly by China.[12] The U.S.-China Economic and Security Review Commission has concluded that "China has closed the technological gap with the United States in quantum information science—a sector the United States has long dominated."[13]

The UK and the European Union, particularly Germany, France, and the Netherlands, have committed to invest heavily in quantum technology over the next ten years. The UK, for example, lined up $193 million worth of investments and commitments from industry players in 2019, bringing total funding to over $440 million.[14] The European Union has pledged $1.1 billion in

---

[8] Paul Smith Goodson, "Quantum USA Vs. Quantum China: The World's Most Important Technology Race," Forbes, October 10, 2019, https://www.forbes.com/sites/moorinsights/2019/10/10/quantum-usa-vs-quantum-china-the-worlds-most-important-technology-race/?sh=1ae9fdd472de.
[9] Congressional Research Service, "Federal Quantum Information Science: An Overview," July 2, 2018. https://fas.org/sgp/crs/misc/IF10872.pdf
[10] Goodson.
[11] Congressional Research Service, 2018.
[12] Daniel R. Coats, Director of National Intelligence, "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community," Senate Select Committee on Intelligence, January 29, 2019, https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.
[13] U.S.-China Economic and Security Review Commission, 2017 Report to Congress of the U.S.-China Economic and Security Review Commission, Washington, D.C.: U.S. Government Publishing Office, 2017, pg. 25. https://www.uscc.gov/annual-report/2017-annual-report-congress
[14] Smriti Srivastava, "Top 10 Countries Leading in Quantum Computing Technology," Analytic Insight, December 14, 2019, https://www.analyticsinsight.net/top-10-countries-leading-quantum-computing-technology/.

government investment over 10 years.[15] Japan and South Korea are making smaller but still significant investments of tens of millions of dollars per year.[16]

In recent years, a robust private sector in applied quantum information science has developed, with companies in U.S., Canada, the E.U., and Australia making hundreds of millions of dollars in private-sector investment. There appear to be many fewer private-sector companies in China and Japan investing in quantum information science R&D.[17]

Below we provide some detail of the current state of each quantum technology and possible near-term advancement.

1.1 Quantum Computers

To date, there are no quantum computers capable of large-scale implementations of either of the above-mentioned algorithms. However, several large corporations and startups have made significant investments in the area, resulting in small scale quantum computers on the order of 50 qubits (the quantum parallel to a classical bit). IBM, Intel, and Google have all announced the construction of quantum computers on the order of 50 superconducting qubits, while Rigetti and Alibaba are around 20 superconducting qubits. The startup IonQ has recently announced a system with 79 ion qubits. In addition, IBM, Alibaba and a startup called Rigetti allow for cloud access to their small-scale quantum computers. While this may not sound like much, it is generally agreed that a quantum computer with on the order of 100 qubits could perform certain algorithms that are not possible even for today's supercomputers.

While recent progress is encouraging, there is still a long way to go before a quantum computer would be capable of breaking RSA. Current systems with a few tens of qubits can perform, at most, a few tens of basic logic operations (known as logic "gates"). By way of comparison, for a quantum computer to break elliptic curve cryptography (with a security factor of 300) would require about 2700 qubits and $1.8X10^{11}$ gates, and that is assuming gates are implemented perfectly. A concrete metric properly characterizing the readiness of a quantum computer is still lacking.

While almost all experts agree that there will be highly capable quantum computers at some point in the future, estimates as to when a quantum computer capable of breaking public key encryption will come on line ranges from 10 to 50 years. The National Academy of Sciences issued an expert consensus that quantum computers will not threaten encryption over the next 10 years.[18] However, even in the near term of 3 – 10 years, where the number of qubits is limited and the implementations are far from optimal, there may be some problems of interest that could be tackled.

---

[15] Congressional Research Service, 2018.
[16] Jason Palmer, "Here, There, and Everywhere," The Economist, 2017. https://www.economist.com/news/essays/21717782-quantum-technology-beginning-come-its-own
[17] Elizabeth Gibney, "Quantum Gold Rush: The Private Funding Pouring into Quantum Start- Ups," Nature, Vol. 574, 2019, pp. 22–24.
[18] National Academies of Sciences, Engineering, and Medicine. 2019. Quantum Computing: Progress and Prospects. Washington, DC: The National Academies Press. https://doi.org/10.17226/25196.

Quantum Machine Learning

Quantum computers can theoretically perform various machine learning techniques more quickly, more accurately, and with less training than classical computers. These include supervised learning techniques such as neural networks and support vector machines for image classification, and unsupervised learning problems such as clustering. Quantum Machine Learning (QML) is currently one of the fastest growing research areas, and a new journal dedicated to the field has just come online (a Springer journal called Quantum Machine Intelligence). Experimental tests of QML techniques have already been performed on the Rigetti 19-qubit system and on the D-Wave system discussed below. Finding the optimal solution is not necessary for machine learning; instead the goal is to find a good (better than classical) answer in a short period of time, and many feel that errors which would derail a quantum computer performing a typical algorithm may not cause catastrophic failure to QML. Instead, errors would simply cause the answer to be less optimal. Whether this feeling is accurate is still open to question and requires additional research.

Quantum Simulations

Simulating quantum systems on classical computers is inefficient and extremely difficult. Richard Feynman was the first to note that the proper way to simulate a quantum system is to use another quantum system that we can control. Used in this way a quantum computer could revolutionize computational material science and perhaps provide needed insight into high-temperature superconducting phenomenon and nitrogenases. Like QML, there are those who feel that quantum simulations may be possible in a nearer timeframe than other quantum algorithms. This is because we do not expect systems to be simulated to be in states as complex as the qubits of a quantum computer during a typical algorithm. Again, whether this is accurate requires additional research.

Quantum Annealers

Quantum annealers are systems that exploit quantum phenomena to solve a more limited class of problems than a universal quantum computer. The quantum annealer machines produced by the company D-Wave have been demonstrated to solve optimization problems ranging from traffic patterns to materials analysis, and quantum machine learning to scheduling and navigation problems. While it has been shown that for certain problems the D-Wave system can outperform specific optimization routines, it has yet to be shown that it can outperform all classical heuristics. Nevertheless, it is possible that in the near-term these systems will prove to be both more efficient than many classical systems and more cost-effective than large-scale quantum computers.

A key distinction lies in different implementations of quantum computers. While mapping quantum logic gates poses of a number of challenges, commercially available adiabatic quantum computers using quantum annealing exist today, and are able to solve specific optimization problems. Specifically, quantum annealing can be leveraged to modestly accelerate the solution of NP-hard combinatorial optimization problems, of which the traveling salesman problem is a classic example. Adiabatic quantum computers do not rely on implementing quantum logic gates, but instead function by finding the lowest energy state. While quantum advantage has not yet been proven, these machines are actively being deployed for commercial and research use and continue to be developed.

Implications for DHS

While it may still be a decade or more before a quantum computer capable of breaking public key encryption comes online, it may also take that long to re-key secure communications. The transition to new forms of quantum-secure encryption will be complex and could introduce new cyber vulnerabilities. Moreover, adversaries could save sensitive encrypted communications produced today for later decryption once quantum computers become powerful enough.[19] Hence, the possibility of a quantum computer may already have implications for how DHS should operate. Also, in the near-term DHS may be able to look towards quantum computers and quantum annealers for machine learning and optimization capabilities that will be mission critical. We note especially the large investment made by China in quantum technologies to demonstrate that allies and adversaries alike are pursuing these capabilities.

1.2 Quantum Communications and Networks

Quantum Key Distribution systems are currently produced by several corporations including IDQuantique (Switzerland), Quintessence Labs (Australia), Qasky, QuantumCTek (both in China), and Qubitekk (USA). In theory, these systems can provide security against any potential eavesdropper while sharing key between two parties. In practice, this is only true if the systems exactly follow the strictures of the QKD protocol and if there are no potential side channel attacks. A study of the latter has led to the sub-field of quantum hacking: determining methods of breaking QKD systems via hardware side channel attacks. Currently, there are more than a dozen of these vulnerabilities recorded in the literature and commercial systems have not closed these holes. The practical utility of QKD is thus still an open question. Because of the complexity (and potential security vulnerabilities) that would inevitably introduced during a large-scale transition to a fundamentally new hardware system for communications, the Department of Defense (DoD), the National Security Agency, and the U.K.'s National Security Cyber Centre have all publicly stated that QKD is not currently secure enough to be deployed in national security settings.[20]

In September 2016, China launched the Micius satellite to implement quantum key distribution and communication experiments from space. The reported success of their satellite as a trusted node for QKD and direct communications, demonstrates the potential of long distance QKD. The EU and others have since announced their own plans for launching satellites for the same purpose. China,

---

[19] Michael J.D. Vermeer and Evan Peet, "Securing Communications in the Quantum Computing Age: Managing the Risks to Encryption," RAND Corporation, RR-3102-RC, 2020. https://www.rand.org/pubs/research_reports/RR3102.html

[20] Department of Defense: Defense Science Board, "Applications of Quantum Technologies: Executive Summary," October 2019, https://dsb.cto.mil/reports/2010s/DSB_QuantumTechnologies_Executive%20Summary_10.23.2019_SR.pdf; National Security Agency, "NSA Cybersecurity Perspectives on Quantum Key Distribution and Quantum Cryptography," October 26, 2020, https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2394053/nsa-cybersecurity-perspectives-on-quantum-key-distribution-and-quantum-cryptogr/; National Cyber Security Centre, "Quantum security technologies," March 24, 2020, https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies.

Tokyo, and the EU have also built QKD networks to enable secure communications. We note that all these systems presumably suffer from the limitations mentioned in the previous paragraph.

Despite current weaknesses and vulnerabilities in QKD systems, lack of a hardening process, low throughput, and no standardization, it is reasonable to expect that at least some of these issues will be resolved in the 3 to 10-year time frame. Thus, QKD may provide both DHS and its adversaries the capability of both short and long-distance secure, unbreakable communications.

1.3 Quantum Sensors

Quantum sensors are thought to be the most near-term of all the quantum technologies. Atomic magnetometers are commercially available and other atomic sensors may soon follow. Defect sensors are currently being explored as "nano"-MRI systems for biological and materials characterization. China has made claims as to already possessing quantum radar—which China's biggest defense electronics company claims uses quantum physics to detect stealth aircraft, revealing their locations—and Canada is making an investment in the area.[21] The claims from China appear to be spurious but does demonstrate the interest of others in pursuing these technologies.

As discussed above, there are severe practical engineering challenges toward deploying quantum radar, such as the need to cool the transceivers down to extremely low temperatures during their operation, and so only very small and simple tabletop prototypes have been demonstrated in the public literature. Because of these practical challenges and the relatively modest benefit in signal-to-noise ratio that quantum radar would deliver, the DoD's Defense Science Board (DSB) has concluded that "Quantum radar will not provide upgraded capability to DoD."[22]

Atomic Gravimeters and Gravity Gradiometers

In the near term the sensitivity of atomic gravity detectors should surpass that of the current state-of-the-art sensors by more than an order of magnitude.[23] With continued improvements these sensors are projected to be able to passively detect a 500,000 kg object (e.g., an airplane) from more than 1 km away and a 1,000 kg object (or displaced mass, e.g., a tunnel) from more than 100 m away. Unlike radar, these sensors are passive and are impervious to shielding.

The potential applications of these devices include the detection of autonomous navigation, tunnel detection, counter-WMD, detection of anomalously heavy objects (e.g., loaded trucks, shipping containers), and mineral and geological mapping. Atomic gravimeters are already commercially available and in use for geological monitoring; however further investment is required to advance atomic interferometer technology for use in DHS applications.

---

[21] Martin Giles, "The US and China are in a quantum arms race that will transform warfare," *Technology Review*, January 3, 2019, https://www.technologyreview.com/2019/01/03/137969/us-china-quantum-arms-race/.
[22] Department of Defense: Defense Science Board, 2019.
[23] Vincent Ménoret et al., "Gravity measurements below 10^{-9} *g* with a transportable absolute quantum gravimeter." Scientific Reports 8, 12300 (2018), https://doi.org/10.1038/s41598-018-30608-1

Atomic Accelerometers and Gyroscopes

Atomic gyroscopes are not expected to surpass the performance of classical hollow-core fiber-optic gyroscopes but should best current linear accelerometers technologies. Linear accelerometers are vital for a full inertial measurement unit (IMU) but current technologies are insufficient for long-term autonomous navigation. Atomic interferometer-based accelerometers are expected to achieve unmatched performance for long-term accuracy in GPS-denied environments, with projections of approximately 100-meter position error after one week of autonomous navigation. These systems are based on cold-atom interferometers.[24]

A technology which may come online in an even shorter-term is an atomic interferometer for IMUs that use thermal atoms. While not as sensitive as cold-atom interferometers, these systems have high data acquisition rates and are inherently robust against vibrations. In addition, they are expected to be both more cost-effective and achieve smaller position errors than current classical IMUs.

Rydberg Atom Electrometers

An additional technology that may come on line in the near terms is based on Rydberg atomic electrometers,[25] which measure electric charge or electrical potential difference by means of electrostatic force. While currently still a laboratory device only, they have demonstrated three order-of-magnitude improvements in sensitivity in the GHz range and have achieved seven times below the classical Chu-limit of conventional antennas. Overall, this discovery means that scientists are able to more accurately measure the precision of an electric field, subsequently extending the realm of potential electrometric techniques. One key application of these Rydberg atom sensors would be for sensitive radio receivers that can receive over a very wide range of frequencies, which could be useful for covert communications, jamming avoidance, and the detection of very weak signals. Moreover, these receivers could be much more compact that standard radio antennas.[26]

Artificial Atom Sensors

While the sensitivity of the defect centers cannot beat that of atomic sensors, they can be emplaced close to the systems. The field of nano-MRI continues to be explored academically and continued maturation of this technology will likely continue.

---

[24] Pierrick Cheiney et al., "Navigation-Compatible Hybrid Quantum Accelerometer Using a Kalman Filter," Physical Review Applied 10, 034030 (2018); Remi Geiger et al., "High-accuracy inertial measurements with cold-atom sensors," AVS Quantum Science 2, 024702 (2020), https://doi.org/10.1116/5.0009093.

[25] A Rydberg atom is an atom whose outermost electron is only loosely bound to the atomic nucleus, so that the electron's behavior is significantly affected by (and therefore very sensitive to) external electric or magnetic fields.

[26] This is because unlike with standard radio antennas, a Rydberg atom sensor could be much smaller than the wavelength of the radio signals that it is capable of receiving.
U.S. Army Research Laboratory, "Army scientists create innovative quantum sensor," March 19, 2020. https://www.army.mil/article/233809/army_scientists_create_innovative_quantum_sensor

Quantum Illumination

As mentioned above, quantum illumination acts on the same principle as quantum radar but also incorporates lidar signals at visible frequencies. Several experiments have already been performed in the laboratory and claims of achievement have been made by China. Canada has announced a few million-dollar effort into this technology. However, there are significant questions regarding the CONOPS of this technology and whether the inefficiency in creating entanglement can be overcome. A possible useful application may be in a noisy environment on a target when the target has a warning receiver.

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

2.1 Quantum Computers

Though it is unlikely that fully functional quantum computers will come online within the next three years, the technology may ultimately pose a high threat to the security of the US homeland. A quantum computer could allow an enemy to decrypt any classified communications that were encrypted with public key encryption it may have intercepted in the past, plus put at risk all future such communications. In addition, the party could effectively shut down e-commerce due to the vulnerability of RSA and other encryption encodings used for online transactions. Beyond decryption, a quantum computer could provide an enemy with increased computing power for optimization, logistics and machine learning. While not a direct threat, this would put US forces at a disadvantage. A fully capable quantum computer, combined with large classical supercomputing, could enable forms of Artificial Intelligence that are difficult to predict and that may provide an adversary with capabilities that are difficult to counter or duplicate. Finally, quantum computers could enable the design and creation of higher-functioning materials. This could increase capabilities in everything from weapons to batteries while enabling new technologies of which we are not currently aware.

Quantum communications are not the only defense against the threat that quantum computers pose to encryption. NIST is currently standardizing a new set of encryption algorithms (fundamentally different from RSA and currently used encryption) which are believed to be resistant against attacks by quantum computers. These standards are expected to be finalized around 2022.[27] An advantage that these new encryption algorithms have over QKD is that they could be used over existing communications hardware, so their deployment would probably be less expensive and disruptive than switching to QKD communications technology. Because of these lower transition costs, the NSA and the U.K. government's National Security Cyber Centre have both encouraged the adoption of these

[27] National Institute of Standards and Technology, "NIST's Post-Quantum Cryptography Program Enters 'Selection Round,'" July 22, 2020. https://www.nist.gov/news-events/news/2020/07/nists-post-quantum-cryptography-program-enters-selection-round

new post-quantum cryptography algorithms instead of QKD.[28]

2.2 Quantum Communications

Secure quantum key distribution and communication systems would effectively block US ability to eavesdrop on enemy communications. This would remove one method of learning about enemy plans.

2.3 Quantum Sensors

The various quantum sensors would provide an enemy with increased sensitivity and enable a host of capabilities. For example, enhanced IMUs would allow an enemy to disable or destroy GPS with little loss to themselves. In addition, quantum sensors would enable better LPI-LPD communications, more compact antenna systems, and, perhaps in certain circumstances, be able to better identify targets of interest.

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.

First, DHS should establish a department-wide specialized team that closely monitors US and adversary advances in quantum computing (QC) to rapidly assess and warn of any impending ability of an adversary to overcome state-of-the art encryption.

Second, DHS should begin preparing to transition all of the encrypted communications used by U.S. critical infrastructure to new post-quantum cryptography systems once NIST finishes standardizing these systems around 2022. DHS should encourage critical commercial sectors to make this transition as well. In parallel, DHS should study the feasibility and security of adopting and using new quantum communication systems to potentially provide more secure communications. Both of these systems could help to protect U.S. critical infrastructure from eavesdropping attacks by adversaries with quantum computers once that technology becomes mature.

Finally, DHS should invest in quantum sensing research and development to provide the ability for highly sensitive tunnel detection, detection of WMD, etc. In addition to directly providing DHS with new operational capabilities, these investments would ensure that DHS maintains expert personnel on its workforce who can provide DHS leadership with rapid advice on appropriate responses to new developments in quantum technology, which could either provide new opportunities for DHS or pose new threats to the homeland.

[28] National Security Agency, 2020; National Cyber Security Centre, 2020.

This page is intentionally left blank

APPENDIX A: SUBCOMMITTEE MEMBER BIOGRAPHIES

Robert Rose (Co-Chair)
Founder and President
Robert N. Rose Consulting LLC

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.

Cathy Lanier (Co-Chair)
Senior Vice President and Chief Security Officer
National Football League

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).

Dr. Patrick Carrick
Former Chief Scientist, Science & Technology, Department of Homeland Security

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.

Frank Cilluffo (Chair)
Director of Auburn University's
McCrary Institute for
Cyber and Critical Infrastructure Security

Frank J. Cilluffo directs the McCrary Institute for Cyber and Critical Infrastructure Security at Auburn University. Prior to joining Auburn, Cilluffo founded and directed the Center for Cyber & Homeland Security at George Washington University where he led several national security and cybersecurity policy and research initiatives. Cilluffo previously served as Special Assistant to the President for Homeland Security. Immediately following the September 11, 2001 terrorist attacks, Cilluffo was appointed by President George W. Bush to the newly created Office of Homeland Security. Before his White House appointment, Mr. Cilluffo spent eight years in senior policy positions with the Center for Strategic & International Studies (CSIS), a Washington-based think tank.

Mark Dannels
Sheriff, Cochise County Arizona

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
Co-Founder and CEO, DreamUp

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
Vice President of Security, Kansas City Chiefs

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: SUBCOMMITTEE TASKING

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

1. **JB Baron**, MITRE, CUAS, Lead Systems Engineer, Next Generation UAS
2. **Brien Beattie,** Director, Foreign Investment Risk Management, DHS Office of Policy
3. **Carlo Canetta**, PhD, MITRE, Mechanical & Reliability Systems
4. **Patrick Carrick**, PhD, Chief Scientist, S&T
5. **Susan Coller Monarez**, PhD, DAS, PLCY
6. **Heath Farris,** PhD, MITRE, Gene Editing, Chief Scientist, Advanced Technology
7. **John Felker,** Director, National Cybersecurity and Communications Integration Center (NCCIC), DHS
8. **Dr. Ron Ferguson**, MITRE, Cognitive Science & AI
9. **Stacy Fitzmaurice,** Transportation Security Administration
10. **Emily Frye**, MITRE, Cybersecurity, Director, Cyber Integration
11. **Gerry Gilbert**, PhD, MITRE, Chief Scientist & Director, Quantum Systems
12. **Brendan Groves,** Department of Justice
13. **David Harvey**, PhD, MITRE, Homeland Security Research
14. **Chuck Howell**, MITRE, AI/ML, Chief Scientist, Dependable AI
15. **James Murray**, Director, United States Secret Service (USSS)
16. **General Robert Newman,** Operations Chief, Counter UAS, DHS S&T
17. **Edward Parker**, PhD, RAND Corporation, Physical Scientist
18. **Robert Perez**, Deputy Commissioner, U.S. Customs and Border Protection (CBP)
19. **John Pistol**, former Administrator, Transportation Safety Administration (TSA)
20. **Daniel Price**, Principle Director, DHS Office of Policy
21. **Gary Seffel,** National Security Council, The White House
22. **Angela Stubblefield,** Federal Aviation Administration
23. **Nitin Sydney**, PhD, MITRE, Advanced Robotics, Group Leader
24. **Gary Tomasulo,** National Security Council, The White House
25. **John Vehmeyer**, Portfolio Manager, S&T, DHS
26. **Yaakov Weinstein,** PhD, MITRE, Emerging Technologies
27. **Emma Westerman,** RAND Corporation, Director Acquisition and Development Program, Homeland Security Operational Analysis Center