REPORT PREPARED BY THE CRITICAL INFRASTRUCTURE RESILIENCE INSTITUTE

Artificial Intelligence and Quantum Information Applications in Homeland Security:

SUMMARY OF THE 2017 INTERNATIONAL WORKSHOP

This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number 2015-ST-061-CIRC01-02.

CIRI | CRITICAL INFRASTRUCTURE RESILIENCE INSTITUTE

A DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

Critical Infrastructure Resilience Institute (CIRI)
A Department of Homeland Security Center of Excellence

UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN
Information Trust Institute and Coordinated Science Lab
1308 West Main Street | Urbana, IL 61801

ciri.illinois.edu

REPORT PREPARED BY THE CRITICAL INFRASTRUCTURE RESILIENCE INSTITUTE

Artificial Intelligence and Quantum Information Applications in Homeland Security:

SUMMARY OF THE 2017 INTERNATIONAL WORKSHOP

CIRI | CRITICAL INFRASTRUCTURE RESILIENCE INSTITUTE

A DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number 2015-ST-061-CIRC01-02.

Table of Contents

1. Project Overview

The International Workshop on Artificial Intelligence and Quantum Information Applications in Homeland Security was held in Arlington, Virginia on December 12–13, 2017. This document records the ideas and discussion that emerged in the Workshop, along with some additional reflections on key themes and future implications.

The Workshop was proposed by the Critical Infrastructure Resilience Institute (CIRI) to provide a forum in which international experts could discuss the application of certain technologies to enhance the security and resilience of critical infrastructures. Specifically, artificial intelligence (AI), especially machine learning and deep learning, has the potential to help humans find new solutions to complex problems much faster than humans can, and quantum information processing (QIP) has the potential to develop solutions to problems that were hitherto impossible to solve. The importance of critical infrastructures to the homeland security enterprise cannot be overestimated. It was recognized that a means of exploring how security and resiliency might be enhanced using AI and QIP would be of significant value. The Workshop was intended to serve that role, and to result in the creation of this document, with the goal of providing guidance on potential future funding of research and development focused on such applications.

Protection of critical infrastructures is a human-intensive activity. For example, humans need to gather information for risk assessment, perform analyses, develop plans for recovering from deleterious events, analyze emergencies, and make decisions leading to remediation. Critical infrastructures are becoming increasing complex, and that has at least two kinds of negative consequences. First, the tools available for planning, analysis, and response have to be used by people whose knowledge base and skill sets are significantly different from those of the experts who built the models and algorithms used by the tools. The more complex critical infrastructures become, the greater the gap between tool complexity and user skill set will be. In addition, as critical infrastructures become more complex, and as the models of those infrastructures become more complex in detail and in geographic and temporal scope, the computational challenge of analyzing those models increases as well.

The fields of artificial intelligence, machine learning, and deep learning are making rapid advances and may enable more and better analysis, planning, and response to events by relieving humans of the burden of needing to understand all this complexity in detail. Natural language processing has the potential to accelerate data collection by automating tasks now normally done by humans, and has the potential to make the space of data that can be collected much larger. Machine (and deep) learning has the promise of finding correlations in data gathered from critical infrastructures that automate the discovery of anomalies, suggest optimizations for real-time data gathering and analysis, form the basis for data-driven models of critical infrastructures and their response to events, and aid at every step when humans make decisions about planning, response, and recovery.

The field of quantum computing is newer and much less advanced than AI, but offers the promise of eventual tremendous advances in computational capability. Quantum computing could have significant ramifications in at least two areas of interest to the homeland security enterprise. The well-known ability of quantum algorithms to factor the product of two very large prime numbers threatens the foundation of most public key encryption schemes in use today. To the extent that critical infrastructures depend on computers and communication, and to the extent that protection against interference is based on cryptography, work in so-called quantum-resistant cryptography has impact on the cyber-security of future critical infrastructures. A positive potential for quantum computing is the theoretical ability of quantum computers to solve certain kinds of optimization problems that simply cannot be solved by ordinary computers. That is a very broad possibility, but also very important if, as we are able to model critical infrastructures at significant levels of detail, we encounter problems in areas such as optimal resource allocation, or optimal pre-placement of response assets. Aside from the longer-term benefits of quantum computing, there are other potentially nearer-term applications for secure communication (quantum cryptography) and quantum-enahanced metrology (for improved sensors, magnetometers, and telescopy).

The promise we see for significant positive impact in protecting critical infrastructures helped guide the discussions with AI and QC experts that led to the Workshop. The Workshop enabled discussion among government, industry, and academia on how quantum computing and artificial intelligence could affect infrastructure security and influence future policy decisions pertaining to DHS areas of responsibility. Gaps and requirements identified in this process may be used to inform strategic research initiatives for both the United States and Canada.

This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number 2015-ST-061-CIRC01. Disclosure: The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security.

2. Outcomes

The potential for and threats posed by emerging technologies are of crucial importance to homeland security and defense. Furthermore, the impacts are common to Western democracies. For that reason, the U.S. Department of Homeland Security's (DHS) Science and Technology (S&T) Directorate partnered with Defense Research and Development Canada (DRDC) to construct a collaborative Workshop on Artificial Intelligence (AI) and Quantum Information (QI) Applications in Homeland Security. The bilateral workshop was organized by the Critical Infrastructure Resilience Institute (CIRI, a DHS S&T Center of Excellence) and held in Arlington, Virginia on December 12–13, 2017. It brought together thought leaders from government (6 from Canada, 40 from the US), academia (4 from Canada, 15 from the US), and industry (2 from the US). The steering committee was composed of engaged members from both Canada and the US and assisted the program by identifying relevant topic focus areas and bringing together experts from both countries, some of whom were already collaborating. As was evidenced by the people in attendance from both countries and their interactions, both the US and Canada have a keen interest in the future of AI and QI in the realm of homeland security and defense.

The Workshop consisted of keynote presentations, sessions of technical presentations, and panel discussions, with significant blocks of time reserved for discussion among the presenters and the floor. Throughout the workshop, the organizers directed the discussion towards 2 key questions: 1) what are the gaps in AI and QI research, and 2) where should research efforts be best applied?

The key outcomes of the Workshop are summarized below. A more detailed report of the keynote talks, sessions, and discussions is provided in the following sections of this document.

2.1. Outcomes: Bilateral Support for Research

The national leaderships of both Canada and the US are keenly interested in understanding the likely trajectories of AI and QC/QI, with DHS particularly interested in the development of AI-based data analysis. All representatives anticipated that the outcomes of this workshop will help shed light on those trajectories. The national leadership was engaged throughout the Workshop, asking questions of participants and offering observations from their perspectives. The keen interest in partnership in these areas was expressed as well during networking times. An outcome of the workshop is a reinforced desire to have the US and Canada work together at the leadership level in these areas, just as we are already working together at the research level.

2.2. Outcomes: Artificial Intelligence

Presentations documented the successes that AI—and machine learning (ML), in particular—have had so far in diagnostics, image and speech recognition, and forms of automated control. However, Workshop participants were unable to identify many existing applications in homeland security and defense, the exception being some machine learning support that is available for first responders. Workshop attendees did see the potential for application in areas such as:

- Image recognition
- Identification of terrorist threats
- Automated association of documents with closely associated content
- Improved analysis of shipping at ports
- First response

Machine learning technology and ML tools that implement it are advanced, and further developments are moving forward rapidly. DHS and defense agencies can expect positive results by investing in ML development in applications where strengths have already been shown.

For example, the need to visually identify threats is widespread.

- TSA would benefit from improved visual and threat analysis of:
    - Scanned luggage
    - Human faces
    - Vehicles approaching airport entrances
- Law enforcement professionals would benefit from improved visual and threat analysis of:
    - Crowds
    - Physical objects in sensitive contexts (e.g., devices used in the Boston marathon bombing)
- The US Coast Guard would benefit from improved visual and threat analysis of:
    - Surveillance tracks of vessels in coastal waters
    - Port operations

We can expect acceleration in AI-enhanced visual analysis because of the huge push towards automated vehicles. An opportunity exists to leverage the foundational work being developed in industry and academia for key applications. The investment here would be in application of the newly emerging technology, not the new technology itself.

To identify threats is one thing; to respond to them is another. ML may have application here as well. Much of the existing work on automated control is about response to inputs. In that sense, the ongoing work in ML might be leveraged in providing a framework for connecting observation with response. The closer the application is to automated control, the better the chance of success in, for example, real-time monitoring of vehicles in a transportation system. Artificial intelligence based on models of context and behavior finesse the requirement for large volumes of data, but require investment in foundational research.

Threat detection and analysis can involve correlation of different kinds of data from different sources. This seems to be another promising area for investment, in that machine learning is adept at discovering correlations that are not otherwise evident. However, the challenge here (as is often the case with machine learning) is in training the algorithms with quality data.

Workshop attendees also identified a number of technical gaps that need to be addressed before AI can reach its potential, including:

- Mapping of homeland security and defense problems into forms addressable by AI
- For ML, a number of issues related to data, including:
    - Data standards, and interoperability between standards for sharing, that are used in machine learning
    - Reduced reliance on human-based data tagging and curation, which is particularly necessary when data are sensitive and the availablity of human resources for tagging is extremely limited
- For ML, robustness concerns, as ML is susceptible to pre- and post-training attacks that can dramatically impact its predictions
- A means of validating AI-generated outcomes
- A practical online means of detecting new types of behavior (unknown unknowns) not present in the (offline) training process (i.e., unsupervised anomaly detection)
- A feasible way of interacting with human supervisors in the loop to adapt ML platforms to new observations (i.e., semi-supervised active learning)

We think a good first step to the mapping problem would be to fund a study to explore that mapping, a study that would examine leading data-intensive problem areas and point to specific examples of AI technology that might address it, and identify gaps whose closure would enable that application.

Unless a standards body like the National Institute of Standards and Technology (NIST) gets involved, the problem of data standards and curation is one that industry will have to sort out. Investment in ML research will need to go forward against the hope that the marketplace will take care of this, as it has in other cases where standards were needed but were absent.

The technology of ML is fragile. Existing work has shown how to attack the training, and how to attack the classifiers that result from the training. We still lack an understanding of how to defend against such attacks. From a legal point of view, a number of problems remain to be resolved. The most pressing issues relate to responsibility in the event that ML causes harm or damage, and ensuring that privacy laws are respected in the use of ML. Thus, robustness of ML is a very real issue, and we believe that any funding placed on development of an ML-enabled application for defense and the homeland security enterprise should be given with a requirement that the research address fragility, at least deeply enough to enable understanding of the robustness of the developed solution. Likewise, any serious investment in ML development must also demand attention to the validation of the results produced by the model. However, validation is a deep issue that may require some investment in foundational research.

The Workshop also identified a number of challenges to adoption of data-dependent decision support within organizations. They include:

- Mapping of recognized problems into forms that tools can work with
- Recognition and acceptance of the high overhead of annotating and curating data (which again is problematic when data are sensitive)
- Organizational acceptance of new approaches, which requires
    - An ability to assess the technology
    - The ability of executives to understand what the approaches tell their operators and be willing to risk their own performance assessments on use of these technologies

Practical difficulties aside, the risks of ML are significant enough when used in life-critical situations that as these risks become more widely recognized, government will be called upon to develop policy governing its use.

2.3. Outcomes: Quantum Computing and Quantum Information

Workshop presentations documented the basic principles of quantum information processing (QIP). A great driver for research into quantum computing was the discovery of Shor's algorithm by Peter Shor, an algorithm that if implemented on a quantum computer, could crack known classical public key encryption schemes. Since then, theorists have found algorithms for quantum computers for a variety of mathematical problems.

One recognized gap is in the development of effective quantum-resistant cryptography. Cryptographic algorithms whose codes cannot be broken by quantum computers are very much a gap area. Aside from the cryptographic application, the Workshop attendees did not identify a compelling quantum computing application of interest to homeland security and defense. Nevertheless, there is significant research activity on building quantum computers, and significant advances have been achieved. The gaps to be closed on that front are engineering ones, in creating qubits that are fault-tolerant enough to be assembled into so-called *logical qubits* (which are assumed by the quantum computing algorithms). The gap that must be closed to achieve the goal of using a quantum system to emulate some other real (physical) system is smaller, but again, the Workshop attendees did not identify an application of that approach that was recognizable as interesting for homeland security or defense.

Applications of quantum information, though, do have significant potential in the domain of homeland security and defense. One general application area is quantum metrology, or measurement. Useful precision sensing and measurement of many phenomena are possible, including:

- Atomic clocks
- Magnetic fields in medical applications

- Inertial navigation
- Protein concentration
- Accelerometers

Continued research in quantum metrology can be expected to improve existing accuracies and bring in new applications.

Another significant application of quantum information would be the establishment of a communication channel through which participants can generate and use an arbitrarily long, secret shared key such that if an eavesdropper observes any of the key bits in transit, both participants can detect the observation and abandon the compromised key. Also known as *quantum key distribution* (QKD), this technology is in a significantly more advanced state than quantum computing. Secure generation and sharing of a one-time pad is a bit of a Holy Grail in security, and QKD offers the best hope going for that. Progress on that front has been substantial, with several demonstrated proofs-of-concept. The gaps here are partly scientific and partly engineering. For the science piece, the security of shared secret key generation has been shown to be dependent on the security and correct implementation of the hardware implementing it. Some hardware implementations are vulnerable to so-called *side-channel* attacks in which information about the generated key can be "leaked" without detectable observation. An understanding of what constitutes a truly secure implementation is needed. For the engineering part, channels have to be constructed with sufficiently good transmission rates and sufficiently low error rates. That is seen to be an important problem to solve for defense applications. Until (and unless) a quantum-resistant algorithm for secure generation of a shared key is discovered, QKD is the best hope for finding the Holy Grail.

While quantum algorithms for cracking classical public-key cryptography have been known for some time, there is no immediate threat that quantum computers will be built to realize that threat. Nevertheless, progress on the technology front has been significant, and the community believes that effective quantum computers will eventually be built. For the time being, the pool of experts who can develop quantum algorithms is small, and the problem domain is intellectually very challenging. Still, the gains possible with important problems that cannot be effectively solved with classical computers are significant enough to warrant continued effort in making quantum computing a reality.

The Workshop specifically looked at the relationship between machine learning and QI/QC. There appears to be a rich interplay. The current trends in ML algorithm development (particularly deep learning) depend heavily on a problem solution style that currently uses optimization and linear approximations. Optimization and linear algebra are areas in which quantum computing promises to outperform conventional techniques at scale, so the support of QC for ML bears continued tracking. The benefits of quantum-based measurement for defense and homeland security seem significant as well, particularly in the GPS, imaging, and detection applications.

The Workshop also examined the two main competing approaches for building quantum computers; they vary in the physical systrems exploited to create quantum effects. Both approaches have made significant strides in recent years, and the investments by large companies in these technologies are likely to produce better insights into what is possible and what limitations still remain. Yet another approach is to build quantum-based emulators of other physical systems. Realizing the potential of quantum simulation seems nearer-term; the main challenge is that of finding a set of interesting and important problems that can be directly mapped to the Hamiltonian framework that is currently needed.

From the point of view of research investments, widespread practical application of QIP is farther off than widespread practical application of ML. However, while ML faces the very significant problem of becoming robust and verifiable, at present the main impediments to developing some sort of practical application of QIP are based on engineering challenges more than conceptual challenges. Unlike ML, the foundational theory behind QIP is solid. As the nearest-term application of QIP is more likely to be in defense than in the homeland security enterprise, our recommendation is that defense continue to invest in its development.

3. Summary of Workshop Presentations

This section of the report summarizes the presentations made, providing greater depth to the observations and recommendations made in the "Outcomes" section of this report.

3.1. Perspectives of National Leadership

The DHS Deputy Assistant Secretary for Strategy and Analysis opened the Workshop by describing the challenge of using data analysis to support decision-making at DHS with respect to resource allocation. According to the current state of the practice, development of decisions depends heavily on the subjective opinions of subject matter experts (SMEs). While SME opinions are valuable, DHS is rich in data that go unanalyzed, and it would be desirable for those data to be used systematically to improve risk mitigation in developing and supporting resource allocation decisions.

DHS S&T's Chief Scientist then expanded on some of those themes, specifically in calling for data analysis to mitigate risk. The homeland security enterprise (HSE) is a vast network of interrelated pieces, and within that network, it is difficult to predict and understand an adversary's motivation or intentions, or how to influence the adversary's behavior. AI is driving markets already, and quantum computing may enable analysis of data at scale.

The Chief Scientist of Electromagnetic Sciences, DRDC, then outlined Canada's significant investments in AI and QI/QC. In 2017, the DRDC introduced a new defense policy with emphasis in data analytics, deep learning, autonomous systems, and quantum, including a $1.6 billion investment in external S&T innovation to support defense and security challenges, according to speaker Peter Mason of Defence Research and Development Canada. The agreement between Canada and the US, which enables them to work together in these areas, was highlighted. Canada is building a national research community on AI, and has a quantum strategy that has included investment of more than $1B in quantum R&D over the past decade. That investment has been aimed at protecting critical cyber systems and information, and strengthening Canada's defense and security capabilities. Canada's keen interest in the topics of the Workshop was stressed.

3.2. Keynote: Artificial Intelligence: The Next Digital Frontier?

Mr. Sree Ramaswamy of the McKinsey Global Institute offered a working definition of artificial intelligence as, "intelligence exhibited by machines, with cognitive functions that are associated [with] humans. Cognitive functions include all aspects of perceiving, reasoning, learning, and problem-solving." There has been significant industrial interest in AI; venture capitalist investment increased by nearly 300% from 2013 to 2016, and technology giants invested $35 billion in AI during that period, according to McKinsey Global Institute. AI can deliver excellent results in retail, manufacturing, electrical power, and health care. Nevertheless, there remains skepticism about AI with respect to its actual return on investment, although there is less skepticism among companies that are undergoing digital transformation in their operations. Mr. Ramaswamy noted that there is little "home-grown" development of AI in government. With respect to the potential for AI-based data analysis in defense applications, he noted that the industry is fragmented, with no standards for data, and indeed no expectation for standards. To achieve its greatest potential, AI needs to operate across organizations, and without shared standards, this is currently very difficult. In response, large organizations are pushing their own data standards, but they so far have not been interoperable.

3.3. Trust in Machine Learning

Dr. David Miller from Penn State addressed the fragility of machine learning. An adversary who can tamper with training data can befoul ML classifiers, and an adversary who has knowledge of a classifier can add carefully crafted noise to inputs to induce misclassification by the ML classifier in such a way that it is not detectable by a human observer. Such knowledge of a classifier can be obtained by "reverse engineering" attacks that employ subtle probing.

Dr. Ryan Calo from the University of Washington spoke to legal challenges related to making inferences from analysis of data. Cases that will give some insight into current legal views include ones that test whether it is legal to access an individual's cell phone records without a warrant, or whether it is legal to use a tracking device to monitor vehicle movements without a warrant; the answers to both may imply a new understanding of the Fourth Amendment. Another legal issue concerns accountability and consequences of actions taken based on application of ML. An ML tool that mispredicts some business trend has different accountability from one that misjudges an environment and physically harms property or a human as a result.

Dr. Kirsten Thomasen from the University of Windsor provided a Canadian legal perspective, particularly with respect to ML and drone technology. Their combination poses very real threats, such as automated targeting; for example, an attacker could crash a drone into the White House or attach a gun to a drone. Using drones to gather information automatically is another threat. On the other hand, drones have tremendous potential for use in monitoring borders and coastal regions. Canada has introduced a voluntary drone registration program, and has legally established limitations on using technology to gather information indiscriminately.

3.4. Artificial Intelligence for Next-Generation First Responders

Dr. Kyongsik Yun from the Jet Propulsion Laboratory (JPL) of the National Aeronautics and Space Administration (NASA) discussed the prospects for using AI in first response. He described JPL's AUDREY (Assistant for Understanding Data through Reasoning, Extraction, and sYnthesis) reasoning system, which performs data fusion and gives situational awareness to first responders. AUDREY extracts features from data and uses a Bayesian model to prioritize and advise in response. This model accommodates missing and contradictory data.

3.5. The Importance of Organizational Maturity with Respect to Artificial Intelligence and Machine Learning Automation

Mr. Stephen Dennis of DHS S&T led a panel of domain experts in discussing the application of AI in areas of DHS responsibility. He spoke to challenges in application of ML, including, first, the problem of casting a problem in a form suitable for ML; and second, the potential difficulty of gaining acceptance of ML techniques by the organization. Outsourcing of ML has been tried, but the nature of the technology is that intimate knowledge of the specific problem domain is needed; "cookie-cutter" technology or approaches don't work.

Dr. Aaron Mannes, a senior policy advisor to DHS S&T, stated that the lines between statistics, "big data," and "data analytics" are blurred, which can matter in an organization's perception. Furthermore, there are social and legal constraints on how an organization can approach development of a technological solution, and that solution needs to lead to decisions. For adoption, the effectiveness of an approach needs to be demonstrated.

Dr. Meredith Lee, the Executive Director of the West Big Data Hub, is working to find practical and effective technology for use with data. She identified questions about the data as critical for ML: Who needs the data? Who has the data? In what format? What decisions will be based on the results of the analysis?

Mr. Anil Chaudhry, the Director of the Regulatory Audit Systems and Innovation Office of Trade, U.S. Customs and Border Protection, discussed human-system integration. He works with people involved in Army logistics who will use brute force and bypass fancy solutions to get what they want, if they do not trust the fancy solutions. However, smart operators working with smart academics can lead to insightful solutions that will be used.

3.6. Keynote: Security in the Quantum Era

Dr. Michele Mosca of the University of Waterloo introduced quantum computing and quantum information and their implications for security, in particular the known threat that a quantum computer would be able to efficiently solve the mathematical problems upon which the security of most modern cryptography rests. The ability to build a scalable quantum computer depends on the ability to produce a foundational element called a *qubit*, which effectively manages quantum randomness to produce acceptable error bounds. Construction of qubits is very much an active research area, with competing approaches being pursued.

A list of research problems includes:

- Building scalable, fault-tolerant quantum computers
- Creation of a quantum software tool chain (particularly as the programming model to take advantage of quantum effects is very different from any traditional programming models)
- Development of quantum algorithms
- Development of quantum-resistant cryptographic algorithms
- Key management in quantum cryptography

Dr. Mosca commented on what an organization can do to manage the risk that quantum computing might be used to break its cryptography. First, the organization ought to assess the dependence of the execution of its mission on cryptography. Second, it ought to track the quantum computing technology development, and, as needed, manage its IT procurement in light of the threat and communicate the issue to IT vendors. Dr. Mosca does not see quantum computing as an immediate threat, but believes that the technology hurdles will eventually be overcome and that classical cryptography will be susceptible to being cracked.

Dr. Andrew Childs from the University of Maryland discussed quantum algorithms, focusing on identifying problems that could be solved efficiently on quantum computers but not classical ones. These include factoring of integers, certain problems in the structure of algebraic systems, evaluation of formulas, unstructured searching, finding of collisions, and various graph problems. Dr. Childs noted that there are limitations to quantum computing. Some problems will remain intractable even in the presence of quantum computers, and some challenges do not yet have known quantum algorithms for solution.

3.7. Applications of QI/QC

Dr. Jacob Taylor from the University of Maryland addressed two topics: the interplay of quantum technology and machine learning, and the quantum limits for measurement.

He identified ways in which ML can aid in the design of quantum lab experiments. The parameters for an experiment live in a high-dimensional space, but an interesting subset has a fairly narrow range that can be identified with human intuition. One might hope that ML would be applicable in that context, and indeed there have been demonstrations in which it found interesting parameter settings in places and ways that might have been missed by humans. Error correction in quantum systems is a fundamental problem, and ML has been demonstrated here as well.

Dr. Taylor also addressed the flip side: whether quantum computing offers computational advantages to ML model development. The answer is yes, as quantum annealing and quantum-based linear system solvers can speed up the optimization that is at the heart of ML model development. However, the sort of exponential reduction of solution complexity known to be possible for quantum solution of factoring will be enjoyed by quantum-based machine learning only if the database itself stores qubits.

Turning to the benefits of quantum limits to measurement, Dr. Taylor illustrated a number of applications of precision measurement that are made possible through quantum sensors. They include atomic clocks, magnetic fields in medical applications, inertial navigation, protein concentration, improved accelerometers, detection of astrophysical RF (radio frequency) photons, and, critically, the ranging application that detected the presence of gravity waves.

3.8. Quantum Information Science Overview

Dr. Gerald Gilbert from the MITRE Corp. reiterated some of the introductory concepts already presented by others, but with greater emphasis on the difficulties and limitations of the technology. Some of the limitations are physical, such as the difficulty of sensing accurately through the atmosphere; others are the result of inadequate engineering, such as loss of information through cables.

Dr. Gilbert also emphasized that a logical quantum bit is a mathematical concept; it has not been built, and we need to keep that in mind. He also asked the question of *when* we find quantum effects. Every physical system has an action, but what does it even mean to “be quantum”? Dr. Gilbert warned that there are problems when we use classical mechanics to approximate effects, but for systems with large actions, quantum effects are exponentially suppressed; and for systems with actions at a scale comparable to Planck’s constant, quantum effects are strong. A quantum bit has state and action at a scale comparable to Planck’s constant.

Dr. Gilbert also reviewed the Bloch sphere, which is the basis of quantum information science. He estimated that quantum sensing needs around 10 qubits at a time, whereas there are 2,000 qubits in a D-Wave Systems machine;

but there are different qualities of qubits, so they are not comparable at all. Google claims that it is now testing a quantum computer with 72 qubits.

The area of quantum crypto is rife with threats, and the US is not the leading country in quantum information systems. Applications include adversaries' ability to have unbreakable codes and the ability to see things about satellites that are not easily seen.

3.9. State of the Art in Building Quantum Computers

Dr. Chris Monroe from the University of Maryland identified two quantum technologies that are being pursued to build quantum computers. One is based on superconducting circuits, with characteristics of fast clock speed, the ability to be created using printed circuits, and VLSI (very-large-scale integration), but qubits are not identical, and the topological connectivity between the qubits is fixed and limited. That limits the circuits that can be built for quantum computations. IBM, Intel, and Google are notable companies pursuing that approach. A second approach is based on trapped atomic ions. The qubits are identical, fully connected, and configurable. The challenges are slow clock speed and the greater amount of engineering needed to construct them. Honeywell is pursing that approach. Dr. Monroe compared the two approaches for quantum circuits built for specific search-oriented algorithms to illustrate the power of full connectivity among qubits.

Dr. Na Young Kim from the University of Waterloo discussed solid-state systems. She spoke in particular about quantum simulators, large-scale controllable quantum systems that can emulate other systems of interest. The simulated systems are themselves physical systems; exciton-polariton simulation is an example. She pointed out that mapping of problems onto Hamiltonian equations was the key to emulation (because a quantum simulator behaves in accordance with those equations), and asks how real-life problems can be so mapped.

3.10. Current Progress and Future Prospects for Advanced Quantum Communication

Dr. Paul Kwiat from the University of Illinois and Dr. Thomas Jennewein from the University of Waterloo presented this topic. The power of quantum information is that correspondents who have never coordinated before can use quantum understanding of photons to generate a shared, arbitrarily long, random key for unbreakable encoding of messages—a physical implementation of a one-time pad, called *quantum key distribution* (QKD). The quantum underpinnings mean that (in principle) if photons used in the exchange are observed by a third party, both correspondents can detect the intrusion (and therefore not use the key, as it has been compromised). Drs. Kwiat and Jennewein then considered the issues of communicating these photons, through free space or through fiber channels. However, undetected eavesdropping may be accomplished by exploiting flaws in the implementation (such as lack of protection against certain side-channel attacks). Successful deployment depends on the channel as well; attention must be paid to noise and loss that impact key distribution.

Drs. Kwiat and Jennewein discussed the logical organization of a QKD system, and the need for signal amplification through so-called *repeaters*. Security requires each repeater to be trusted. A 2,000-km quantum backbone has been built in China that is capable of generating keys (and hence communication) at 20,000 bits per second. QKD is also under study by researchers funded by the U.S. Department of Energy. Other active research areas are in using satellites as trusted QKD nodes (an effort in which China is in the lead, followed by Canada, the US, Singapore, Germany, the UK, and Japan). Drs. Kwiat and Jennewein concluded with consideration of an internet in which qubits are shared rather than simple binary digits. Such an ability might lead to as-yet-unthought-of applications and innovations.

4. Final Thoughts

Artificial intelligence, specifically machine learning, has demonstrated some remarkable successes, and a great deal of knowledge about it is being developed by the academic and private sectors. It is natural to ask if defense and the homeland security enterprise can leverage these successes to quickly apply ML to problems in their domain. The answer is a qualified yes. In the near term, problems will have to be chosen very carefully, as ones that sufficiently resemble applications for which ML has already been proven successful. The initial problems should not involve life-critical applications. While ML can be effective, it is also fragile and susceptible to malicious manipulation. There is potential, and some investment ought to be made into trying to realize that potential, but it is not clear when or if the foundational weaknesses of ML will be solved.

Quantum information processing rests on somewhat firmer theoretical ground, but practical applications are farther away. In the near term, the most promising application is in quantum key distribution for cryptography, an application that could be important to defense, but less so to the homeland security enterprise. Another near-term potential is to use quantum emulation of physical systems to better understand those systems. While the technical potential is there, anything approaching practical application in either defense or the homeland security enterprise is still missing. The great fear that quantum computing will crack decades of past cryptography is based on a scientific principle, but the realization of that threat is far enough away that we have time to invent cryptography that is provably resistant to the power of quantum computers.

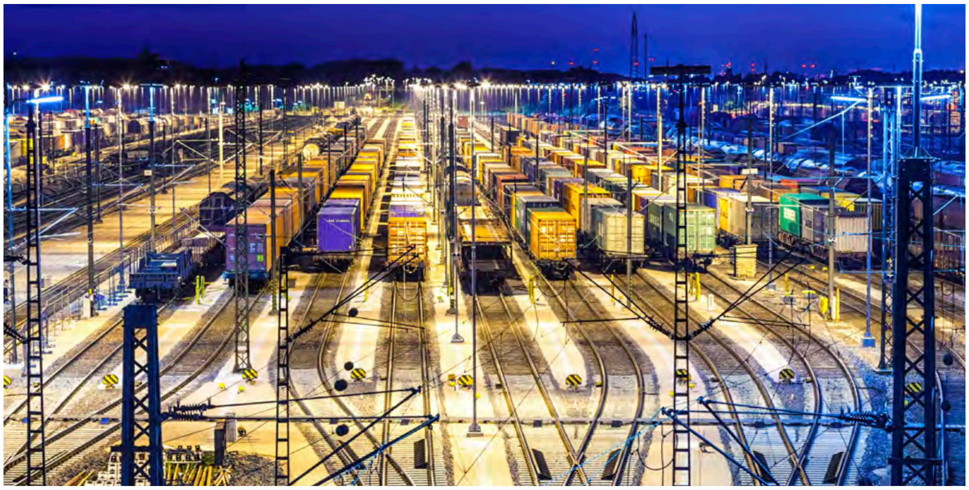
Funding metrology research has the benefit that the technology readiness levels (TRLs) vary, so government organizations can look to funding those applications that fit their horizons. For example, DHS may be more interested in applications in timing that preserve the function of critical infrastructure systems in the absence of GPS or quantum gravitometric sensors that can detect anomalies (tunnels, things inside containers). Other agencies may be more interested in low-TRL components such as quantum radars.

The conclusion is that there is potential to be realized and research investments to be made, but when the objective is to realize new capabilities in the near term, for both AI and QIP, those investments need to be carefully chosen. There is great need and ample opportunity to invest in longer-term foundational research that would correct the weaknesses of ML and expand the application of QIP.

5. Appendix: Presenter Biographies

DR. RYAN CALO is the Lane Powell and D. Wayne Gittinger Associate Professor at the University of Washington School of Law. He is a faculty co-director (with Batya Friedman and Tadayoshi Kohno) of the University of Washington Tech Policy Lab, a unique, interdisciplinary research unit that spans the School of Law, Information School, and Paul G. Allen School of Computer Science and Engineering. Professor Calo holds courtesy appointments at the University of Washington Information School and the Oregon State University School of Mechanical, Industrial, and Manufacturing Engineering.

DR. PATRICK CARRICK As Chief Scientist for the Department of Homeland Security (DHS) Science and Technology Directorate (S&T), Dr. Carrick guides the strategic management of S&T's research and development (R&D) investment for DHS. He serves as the principal adviser for oversight and technical content of the R&D portfolio and evaluates the portfolio to determine its adequacy and efficiency in meeting national and DHS objectives. He joined DHS S&T, Homeland Security Advanced Research Projects Agency (HSARPA) in October 2014 as Deputy Director, becoming Director in July 2015, and was asked to serve as the acting Chief Scientist in April 2016. In his role as HSARPA Director, Dr. Carrick leads four Divisions under HSARPA, consisting of ~180 scientists, engineers, and staff with an annual budget over $300M. Prior to joining DHS, Dr. Carrick was Director of the Basic Science Program Office, and Acting Director of the Air Force Office of Scientific Research, where he guided the management of the entire basic research investment for the Air Force. Dr. Carrick led a staff of ~200 scientists, engineers, and administrators in Arlington, Virginia, and foreign offices in London, Tokyo, and Santiago, Chile. Dr. Carrick served for three years as the Chief Science, Technology and International Advisor for the Special Assistant to the Secretary of Defense, Chemical and Biological Defense (CBD) and Chemical Demilitarization Programs in the Pentagon. He interfaced with all Department of Defense (DoD) and federal government organizations (including the intelligence community) involved



in Chemical and Biological Defense programs and oversaw Congressional and International programs. He coordinated and expanded the key international CBD MOU (memorandum of understanding) agreement to include Australia and started a new CBD post-doctoral research fellowship. Dr. Carrick earned his Ph.D. in Chemistry from Rice University in 1983 and his B.S. degree in Chemistry from the University of Wisconsin–Madison in 1978. He 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 Defense Department in 1989. He served for 11 years at Edwards Air Force Base, California, becoming in 1994 the Chief of the Propellants Branch at the Air Force Research Laboratory's Propulsion Directorate, where he led a team conducting cutting-edge scientific research and engineering. As a senior research physical scientist, he envisioned the first cryogenic solid hybrid rocket engine. Dr. Carrick has published more than 25 articles in peer-reviewed professional journals.

MR. ANIL (NEIL) CHAUDHRY is Director of Systems and Innovation for Regulatory Audit in the Office of International Trade in U.S. Customs and Border Protection (CBP), U.S. Department of Homeland Security. He is responsible for systems and processes used to audit and survey stakeholders in the trade community that import $6.5 billion of products and pay over $120.5 million in duties, taxes, and other fees on a daily basis. He is also responsible for the design and implementation of the next generation of "machine augmented" intelligent enforcement systems that will ensure free, fair, and reciprocal trade with our international partners. In 2017, he served as the Associate Director for Technical Engagements in the Enterprise Analytics, Modeling, and Simulation Division, where he worked on a roadmap to implement Data Analytics as a Service (DAaaS) within CBP. Previously, he was one of three DHS employees selected to attend the National War College in 2016 as part of the DHS Senior Succession Management Program. He joined CBP in 2011 when he served as technical lead for a Senior Leadership Team organized to review the Human Capital Management Systems for law enforcement personnel management. Since then, he has held several key roles within CBP, including service as National Security Decision Directive 38 (NSDD-38) Program Manager, for which he managed over 800 international positions and executed a data-driven program that enabled the Office of International Affairs to recover $4.1 million in reimbursable funding for international operations in FY 16. He also led a User Fee working group in the Office of Finance, recovering $7 million for the User Fee Airport (UFA) program in FY 14. He was lead author of CBP's Presidential Transition Papers on International Engagements for the 2012 and 2016 presidential transitions. 2009–2011, Mr. Chaudhry was a Presidential Management Fellow at the Defense Business Transformation Agency, where he prepared the project management and life cycle sustainment plans for a $340 million enterprise software application to manage global accessions for the DoD. He served on a team that updated the electronic workflow processes for awarding contracts used to support cash-based contingency contracting for law enforcement training and related activities in Iraq and Afghanistan. His work resulted in the immediate reduction of improper cash based payments in combat theaters by 11%, saving the DoD over $87 million annually. Mr. Chaudhry entered into public service as an enlisted soldier in the U.S. Army Chemical Defense Corps. He was awarded a "Green to Gold" scholarship and earned a Commission in the U.S. Army Transportation Corps, ultimately leading a Special Police Transition Team that trained a battalion of over 3,000 Iraqi National Police guardsman on conducting counter-insurgency operations, border management, reestablishing public order, securing public infrastructure, and defending High Value Targets. Mr. Chaudhry holds a J.D. in Labor Law, an M.S. in National Security Strategy, an M.S. in Management Information Systems, and a B.S. in Architectural Engineering.

DR. ANDREW CHILDS, co-director of QuICS, is a professor in the Department of Computer Science and the Institute for Advanced Computer Studies (UMIACS) at the University of Maryland. Childs's research interests are in the theory of quantum information processing, especially quantum algorithms. He has explored the computational power of quantum walk, providing an example of exponential speedup, demonstrating computational universality, and constructing algorithms for problems including search and formula evaluation. Childs has also developed fast quantum algorithms for simulating Hamiltonian dynamics. His other areas of interest include quantum query complexity and quantum algorithms for algebraic problems. Before coming to UMD, Childs was a DuBridge Postdoctoral Scholar at Caltech from 2004 to 2007 and a faculty member in Combinatorics and Optimization and the Institute for Quantum Computing at the University of Waterloo from 2007 to 2014. He is also a Senior Fellow of the Canadian Institute for Advanced Research. Childs received his doctorate in physics from MIT in 2004.

DR. SUSAN COLLER-MONAREZ is a globally recognized leader in today's most active areas of homeland and national security. She currently serves as the Deputy Assistant Secretary for Strategy and Analysis in the Department of Homeland Security (DHS) Office of Policy. In this role, Dr. Coller-Monarez is responsible for leading the development, administration, and evolution of the Department's strategy and analytic efforts, including ensuring alignment with Presidential and Secretarial priorities. Prior to this position, Dr. Coller-Monarez served at the White House as the Assistant Director for National Health Security and International Affairs in the Office of Science and Technology Policy (OSTP) and as the Director of Medical Preparedness Policy on the National Security Council (NSC). In both White House roles, she led multiple efforts to enhance the nation's capabilities to prevent, respond, and recover from national security incidents. Dr. Coller-Monarez has led the development of several Presidential-level national strategies, action plans, and policy directives related to domestic and global security. Prior to the White House, Dr. Coller-Monarez served as Chief of the CBRN Threat Characterization and Attribution Branch within DHS and as a Biodefense Policy Advisor within the Department of

Health and Human Services (HHS). In addition to leadership roles within the Federal government, Dr. Coller-Monarez has been called upon to serve on numerous advisory panels at the National Academies of Science, the National Science Advisory Board for Biosecurity, and the Federal Experts Science Advisory Panel. Dr. Coller-Monarez has also served as the U.S. representative on several international CBRN defense cooperative initiatives, including ones with the European Union, Canada, France, The Netherlands, and the United Kingdom, in bilateral and multilateral engagements.

Dr. Coller-Monarez was an American Association for the Advancement of Science (AAAS) Science and Technology Policy fellow and a research scientist in microbiology and immunology. Her graduate work at the University of Wisconsin focused on immunology and global infectious diseases and her post-doctoral fellowship at the Stanford University School of Medicine combined traditional immunology with next-generation technologies in molecular genetics and proteomics.

MR. STEPHEN DENNIS is the Data Analytics Engine Director of the Homeland Security Advanced Research Projects Agency (HSARPA) of the Science & Technology (S&T) Directorate and the Department of Homeland Security (DHS). He provides leadership and guidance for research, development, and deployment of advanced computation and data analytics, and leads a team of subject matter experts to address a variety of homeland security challenges, including automated risk assessment, social media analytics, and data-driven investigations using big data and internet-of-things technologies. Mr. Dennis has also served HSARPA as the S&T APEX Program Manager for the Border Enforcement Analytics Program to improve utilization of DHS Big Data sources for ICE Homeland Security Investigations. That program delivered the first commercially supported open-source platforms for big data analytics to ICE to support data-driven investigations. Mr. Dennis also represents S&T to cross-departmental working groups and represents DHS analytics interests to groups within the White House Office of Science and Technology Programs. He has more than 37 years of experience managing research programs in information analysis and processing automation within the intelligence & defense communities and in collaboration with other federal agencies. He holds

MBA and MS (Electrical Engineering) degrees from the University of Maryland, College Park, and a BS in Computer Engineering from Clemson University in SC.

DR. GERALD GILBERT As chief scientist and director for quantum systems at The MITRE Corporation, Dr. Gerald Gilbert leads all MITRE research in this area. He is the founder of the Quantum Information Science Program at MITRE and founder of the MITRE Quantum Information Science Group, and has been principal investigator of the MITRE Quantum Information Science Research Project since its inception. He is the founder of the MITRE site located on the campus of Princeton University and served as the first site leader. Dr. Gilbert is on the Defense Science Board and has served as a consultant to the Air Force Scientific Advisory Board as an expert on quantum information science. Dr. Gilbert received his Ph.D. in Theoretical Physics under the supervision of Nobel Laureate Professor Steven Weinberg at the University of Texas at Austin. He subsequently held positions as Weingart Prize Research Fellow in Theoretical Physics at the California Institute of Technology under Professor John Schwarz, as University Research Fellow at Cambridge University under Professor Stephen Hawking, and at the University of Maryland at College Park. Dr. Gilbert founded the MITRE Quantum Information Science Program, and has led its growth over the past 19 years. At MITRE he has received a number of awards, including the Program Innovation Award, the MITRE Best Paper Award, and three Director's Awards for Technical Excellence. Dr. Gilbert is co-inventor on five U.S. patents in the area of quantum information science.

DR. THOMAS JENNEWEIN is a faculty member in the department of Physics and Astronomy, and the Institute for Quantum Computing, at the University of Waterloo. His research is focused on experimental implementations of quantum photonics and quantum optics, foundational questions and experiments of quantum entanglement and quantum science, and, in particular, performing quantum communications between ground and space. He is the inventor and Principal Scientist for the Canadian QEYSSAT space mission proposal. In 2002, Dr. Jennewein completed his Ph.D. at the University of Vienna on quantum communication and teleportation experiments with entangled photon pairs. He spent one year in the automotive

industry, followed by several years as a Senior Scientist at the Vienna Institute for Quantum Optics and Quantum Information (IQOQI).

DR. NA YOUNG KIM is an Associate Professor in the Institute for Quantum Computing and the Department of Electrical and Computer Engineering at the University of Waterloo. She leads the Quantum Innovation (QuIN) laboratory, aiming to build large-scale quantum processors based on novel materials and advanced technologies. Two kickoff projects are underway: (1) the semiconductor quantum processors project is establishing controllable optical and electrical domains, where we are gaining insights into exotic materials and the fundamental nature of symmetries; and (2) a project on multifunctional classical and quantum device arrays is establishing a planar architecture comprising nanoscale devices with electrical, optical, thermal, and mechanical functionality. Prior to joining the University of Waterloo in 2016, Dr. Kim worked on the development of small display products at Apple Inc., where she got to experience delivering beloved products to worldwide consumers. She received a B.S. in Physics from Seoul National University and pursued her graduate studies exploring mesoscopic transport properties in low-dimensional nanostructures in the Department of Applied Physics at Stanford University. During her post-graduate research, she expanded her scope to the fields of quantum optics and nanophotonics, working on several experimental and theoretical projects in collaboration with graduate students, postdoctoral scholars, and other collaborators.

DR. PAUL G. KWIAT is the Bardeen Chair in Physics at the University of Illinois at Urbana-Champaign. A Fellow of the American Physical Society and the Optical Society of America, and the recipient of the OSA's 2009 R. W. Wood Prize, he has given invited talks at numerous national and international conferences and has authored over 150 articles on various topics in quantum optics and quantum information, including several review articles. His research includes optical realizations of various quantum information protocols, particularly using entangled photons to implement advanced quantum communication.

DR. MEREDITH LEE is the Executive Director of the West Big Data Innovation Hub, a consortium launched by the National Science Foundation to address societal challenges with Big Data innovation. The West Hub is led by UC Berkeley, UC San Diego, and the University of Washington, and includes Alaska, Arizona, California, Colorado, Hawaii, Idaho, Montana, Nevada, New Mexico, Oregon, Utah, Washington, and Wyoming. Dr. Lee previously served as a Science & Technology Policy Fellow at the U.S. Department of Homeland Security (DHS) Homeland Security Advanced Research Projects Agency (HSARPA), guiding strategic research in graph analytics, risk assessment, machine learning, data visualization, and distributed computing. She co-led the White House Innovation for Disaster Response and Recovery Initiative as well as the Ideation Community of Practice, a network of Federal innovators from more than 25 agencies. Meredith completed her Ph.D. in Electrical Engineering at Stanford University and was a postdoctoral researcher at the Canary Center for Cancer Early Detection. She was previously at MIT Lincoln Laboratory, Intel, IBM T.J. Watson Research Center, and Agilent Laboratories. Dr. Lee is a co-founder of NationOfMakers.org and past president of the Stanford Optical Society of America/SPIE, and served on the first Steering Committee for the National Photonics Initiative. Her work has been featured by whitehouse.gov, Make:, Ars Technica, The Washington Post, Forbes, and Fast Company.

DR. AARON MANNES (DHS S&T HSARPA DA-E) is the Senior Policy Advisor at the Apex Data Analytics Engine of the DHS Science and Technology Directorate, where he has written extensively on technology governance issues and collaborated with a range of DHS partners on various data analytics issues. Dr. Mannes initially joined DHS as an AAAS Fellow. Prior to joining DHS, Dr. Mannes worked for more than a decade at the University of Maryland Institute for Advanced Computer Studies, serving as the subject matter specialist in terrorism and international affairs on interdisciplinary teams modeling terrorist group behavior. Dr. Mannes earned his Ph.D. in Public Policy at the University of Maryland College Park, where his dissertation examined the national security role of the vice president. Dr. Mannes is the author or co-author of four books and numerous scholarly and popular articles, which have appeared in various publications including *The Wall Street Journal*, *Foreign Policy*, and *The Guardian*.

DR. PETER C. MASON earned an undergraduate degree in mathematics and a Ph.D. in physics at McMaster University. He spent a year as a physics professor at Mount Allison University before taking a post-doctoral fellowship with the National Research Council of Canada, which included time working at Chalk River National Lab, Oak Ridge National Lab, and Cornell's High Energy Synchrotron Source. He followed that with two years in industry working in photonics R&D. He joined Defence Research & Development Canada in 2002 as a defence scientist working in wireless network security, later becoming the head of the Cyber Operations and Signals Warfare section. In 2017, he was named Chief Scientist of Electromagnetic Sciences for DRDC. Most of his free time is spent cycling and coaching hockey.

DR. DAVID J. MILLER received the B.S.E. degree from Princeton University, Princeton, NJ, in 1987, the M.S.E. degree from the University of Pennsylvania, Philadelphia, in 1990, and the Ph.D. degree from the University of California, Santa Barbara in 1995, all in electrical engineering. From January 1988 through January 1990, he was employed by General Atronics Corporation, Wyndmoor, PA. In August 1995, he joined Penn State, University Park as an Assistant Professor of electrical engineering; he has been full professor there since 2007. His research interests include machine learning (in which he has worked for more than 25 years), source coding, bioinformatics, and biomedical signal processing. Dr. Miller received the National Science Foundation Career Award in 1996. He chaired the 2001 IEEE Workshop on Neural Networks for Signal Processing. He was Associate Editor for *IEEE Transactions on Signal Processing* from 2004 to

2006. He was chair of the Machine Learning for Signal Processing technical committee, within the IEEE Signal Processing Society, from 2007 to 2009. He has received multiple Best Paper awards from conferences. Dr. Miller is co-founder (with G. Kesidis) of the startup company Anomalee, Inc.

DR. CHRISTOPHER MONROE is a quantum physicist who specializes in the isolation of individual atoms for applications in quantum information science. After graduating from MIT, Monroe earned his Ph.D. in Physics in 1992 from the University of Colorado (under Carl Wieman and Eric Cornell), where he paved the way toward the achievement of Bose-Einstein condensation. From 1992 to 2000 he was a postdoc, then staff physicist, at NIST, in the group of David Wineland. With Wineland, Monroe led the team that demonstrated the first quantum logic gate in 1995, and exploited the use of trapped atoms for the first controllable qubit demonstrations. In 2000, Monroe became Professor of Physics and Electrical Engineering at the University of Michigan, where he pioneered the use of single photons to couple quantum information between atoms and also demonstrated the first electromagnetic atom trap integrated on a semiconductor chip. From 2006 to 2007 he was the Director of the National Science Foundation Ultrafast Optics Center at the University of Michigan. In 2007, he became the Bice Zorn Professor of Physics at the University of Maryland and a Fellow of the Joint Quantum Institute. In 2008, Monroe's group succeeded in producing quantum entanglement between two widely separated atoms and, for the first time, teleported quantum information between matter separated by a large distance. Since 2009 his group has investigated the use of ultrafast laser pulses for speedy quantum entanglement operations, pioneered the use of trapped ions for quantum simulations of many-body models related to quantum magnetism, and proposed and made the first steps toward a scalable, reconfigurable, and modular quantum computer.

DR. MICHELE MOSCA is co-founder of the Institute for Quantum Computing, University Research Chair, Professor in the Department of Combinatorics & Optimization at the University of Waterloo, and a founding member of the Perimeter Institute for Theoretical Physics. He is globally recognized for his drive to help academia, industry, and government prepare our cyber systems to be safe in an era with quantum computers. He co-founded evolutionQ Inc. to provide services and products that enable organizations to evolve their quantum-vulnerable systems and practices to quantum-safe ones. His research interests include quantum computation and cryptographic tools designed to be safe against quantum technologies.

DR. DAVID M. NICOL is the Franklin W. Woeltge Professor of Electrical and Computer Engineering at the University of Illinois at Urbana-Champaign, and Director of the Information Trust Institute. He is PI for two recently awarded national centers for infrastructure resilience: the DHS-funded Critical Infrastructure Reliance Institute, and the DoE-funded Cyber Resilient Energy Delivery Consortium. He is also principal investigator for the Boeing Trusted Software Center and the NSA-funded Science of Security lablet. Prior to joining UIUC in 2003, he served on the faculties of the computer science departments at Dartmouth College (1996–2003) and the College of William and Mary (1987–1996). He has won recognition for excellence in teaching at all three universities. His research interests include trust analysis of networks and software, analytic modeling, and parallelized discrete-event simulation, research which has led to the founding of startup company Network Perception, and election as Fellow of the IEEE and Fellow of the ACM. He is the inaugural recipient of the ACM SIGSIM Outstanding Contributions award, and co-author of the widely used undergraduate textbook *Discrete-Event Systems Simulation*. He received M.S. (1983) and Ph.D. (1985) degrees in computer science from the University of Virginia, and a B.A. degree in mathematics (1979) from Carleton College.

MR. SREE RAMASWAMY is a Partner at the McKinsey Global Institute (MGI), McKinsey's business and economics research arm. He leads research on the economics of digitization and the economics of multinational corporations. He is responsible for shaping MGI's research initiatives, leading research on trends in competition, technology, and global forces influencing multinationals. He is also a co-leader of MGI's research on North America, and has authored reports and articles on the ongoing digital transformation of the US economy, on new investment opportunities, on opportunities and challenges for the NAFTA region, and on the role of US multinational firms in the global economy. Ramaswamy is a frequent speaker at conferences; policymaker, business, and media roundtables;

and media briefings on topics related to his core research and to MGI's broader themes around global forces, technology, trade and investment, and the global and US economic outlook. His research is frequently cited in *The Economist*, *The Financial Times*, *Harvard Business Review*, and *The Wall Street Journal*, among other publications. Prior to joining McKinsey, Ramaswamy spent a decade in the US telecom and aerospace sector. He worked in regulatory affairs and engineering research for broadband satellite networks and holds three patents. He has an MBA and Master's and Bachelor's degrees in engineering and telecommunications. He is based in Washington, DC.

DR. JACOB TAYLOR is co-Director of the Joint Center for Quantum Information and Computer Science (quics.umd.edu), a Fellow at the Joint Quantum Institute, and a physicist at NIST. A student of Misha Lukin's at Harvard, he was a Pappalardo Fellow at MIT before starting his group at NIST in 2009. His research explores the fundamental quantum limits to measurement and computation. He can be found on Twitter @quantum_jake.

DR. KRISTEN THOMASEN is an Assistant Professor of Law, Robotics and Society at the University of Windsor, Faculty of Law. She is also currently completing her Ph.D. in Law on the topic of drones and privacy in public at the University of Ottawa, where she is under the supervision of Dr. Ian Kerr, Canada Research Chair in Ethics, Law and Technology. Her doctoral work received an SSHRC Joseph-Armand Bombardier Canada

Graduate Scholarship. Kristen researches and writes about the legal, social, and ethical implications of robotic and autonomous machines, and she teaches Robotics Law & Policy at the University of Windsor. Prior to starting her Ph.D., Kristen clerked for the Honourable Madam Justice Rosalie Abella at the Supreme Court of Canada. She also clerked for the Alberta Court of Queen's Bench and articled with Alberta Justice in Calgary (2013). Kristen is a member of the Law Society of Alberta. You can follow her on Twitter @KristenThomasen.

DR. KYONGSIK YUN is a technologist at NASA's Jet Propulsion Laboratory. His research focuses on building brain-inspired technologies and systems, including deep learning computer vision, natural language processing, brain-computer interfaces, and noninvasive remote neuromodulation. He received the Marie Curie Fellowship for Neuroscience, the International Federation for Medical and Biological Engineering (IFMBE) Young Investigator Award, and the Society for Neuroscience (SfN) Hot Topic Award. In addition to his research, Kyongsik co-founded two biotechnology companies, Ybrain and BBB Technologies, that have raised nearly $10 million in investment funding. Kyongsik received his B.S. in Bioengineering and Ph.D. in Computational and Cognitive Neuroscience from the Korea Advanced Institute of Science and Technology (KAIST). He then worked as a postdoctoral scholar at the California Institute of Technology.

6. Appendix: Questions and Discussion

During Workshop discussions, questions and responses came variously from the moderator, other speakers or panelists, and members of the audience. While this record is fragmentary, it is included here for completeness, and also because the exchanges provide noteworthy factual information and an interesting range of perspectives.

6.1. Highlights of the AI Discussions

QUESTION: What are the gaps in AI technology?

A representative from the Homeland Security Advanced Research Projects Agency (HSARPA) stated that when large amounts of information are obtained, something must be done with that information. Having a system that is aware of a change in the threat environment and can draw conclusions would be a use case for AI.

QUESTION: How can we use unmanned systems, and how can we protect against them?

After the gyrocopter incident at the Capitol, some have wanted to establish an intergovernmental team for the use of unmanned systems. Perhaps we can use such teams to protect against unmanned drones, and use policies to test these systems. An additional approach would be to classify drones that are produced as aircraft. However, there is pushback from industry, and there are laws against taking control of an aircraft remotely.

QUESTION: Are there any components of government that produce or use AI?

The DHS S&T Integrated Product Team (IPT) wants to understand how these different components integrate, and they form teams from different areas. There is a data analytics engine that does R&D on promoting better decision-making. The analytics look across components to determine how to do a job better.

One attendee, who used to work on HSARPA/SCT for federal employees and contractors, said that these agencies do not have the resources to do much R&D themselves; so they need to reach out and inspire others to do more. There is an ongoing effort in Silicon Valley to understand fundamental security problems.

QUESTION: How can AI be used to understand terrorist threats?

There is a complex question on law enforcement versus homeland security, and whether AI will be used to find criminal activity versus terrorist activity. One person stated that AI gives value daily and that there is a "winner takes all" aspect of AI, making reference to a comment made by Sree Ramaswamy. AI and ML in general are becoming more important in linking data. However, detecting connections ahead of time, to identify potential problems before they emerge, is difficult.

QUESTION: What risks are there in the use of AI?

Human decision-making is slow and costly, and humans use tools to optimize decision-making. But on the other hand, if we trust the AI, how do we perform sanity checks to be sure that we are getting the right information? AI is, after all, owned by a few, and is intelligent in that it knows much about the organization.

Eventually, algorithms have to be proven correct to be trusted by humans, but how do we even start to validate the decisions made by AI? This is part of the motivation for a Defense Advanced Research Projects Agency (DARPA) call for Explainable AI. Deep neural networks work well, but it may be difficult to explain how they work; furthermore, if the data are even slightly altered, problems arise. For example, in music classification, if one changes the tempo slightly, it changes the categorization produced by the AI, although it should not. It is not always clear (1) what is being learned, and (2) how fragile the algorithm actually is.

One participant claimed that deep neural networks create the cult of the amateur. There is a talent gap, and personnel often train themselves. The technology itself is old; what has changed is the availability of lots of data and computational power.

QUESTION: What's the story on the FAA's grounding of the first commercial drone?

The US Federal Aviation Administration (FAA) grounded the first commercial drone, which was being tested for use in delivering beer to people ice fishing on the Great Lakes. Hundreds of billions of dollars were lost as a result of FAA's policy. In general, we must wait and see as the courts fight out the debate over automated shipping in America. As a result, Amazon has begun testing automated drones in Canada. Norway is starting to look into automated ships. Some participants argued that the lesson here is that if the US ignores this developing trend, other countries will leave the US behind.

QUESTION: What are the challenges with respect to AI and privacy?

As a matter of policy, when using AI in surveillance, it would seem that privacy cannot be ensured.

An attendee from the Intelligence Advanced Research Projects Activity (IARPA) stated that homomorphic encryption techniques may allow one to construct a database consisting of encrypted data that can be accessed only via a limited set of questions that are "legal" to ask. Great strides have been made on that front, but there is a long way to go. If one wants general-purpose computation, then the operations available via homomorphic encryption are constrained. Moreover, there is a large overhead that impacts efficiencies.

QUESTION: What are the best use cases of AI for DHS?

Image recognition may prove valuable for both DHS and the Transportation Security Administration (TSA).

Much is lost at ports. Bad actors make some items look duty-free when in fact they are not. Others use identity theft to divert shipments. There is a huge amount of criminal activity in this space.

DHS generates a tremendous amount of reports. How can one find needed information within that huge body of output? How can we find the things that we really want to read, whether they're incident reports, regulations, or whatever? Also, work is being done in infrastructure and in policy, and we

need to be able to pull all such information together. Currently, everyone works on their own topic. AI might help link associated documents together.

Natural language processing of communications might help identify terrorists. There should be larger investment in that area.

Some attendees said “If I could, I would” invest in the internal analytic maturity of DHS, since there are many products, but no clear way to evaluate them. Further, while tools exist, there is a mismatch between those tools and the problems faced by DHS.

An additional problem is that we don’t know what we don’t know, and analysts may not have time to think about how else to use data.

QUESTION: For collection, preparation, and curation of data, what affects best practices?

There needs to be a cohesion of stakeholder goals. Feedback mechanisms built into the design of an interface can help, as well as the ability to balance between agility and stability.

From an operational perspective, technologies are changing rapidly. Operators do not understand the data preparation problem, and tools are often limited by the operators’ technical capacity to absorb information efficiently.

Annotation of datasets is labor-intensive. For example, a large information technology corporation may use 10,000 humans every day to annotate data.

There is also need for an ontology of the data so that one can use datasets across different apps. Moreover, there is a challenge involved in being able to explain one's business in terms of events and do a data audit, have descriptive statistics, and so forth. Is the information such that it can be leveraged to build business?

QUESTION: What would be an accurate breakdown of how to understand analysis? How does one evaluate an organization's analytic maturity? Can you define your problem in such a way that it can be solved? What is your capacity to absorb the solution?

One should take into account technical possibility as well as organizational infrastructure (e.g., the path from development to operations).

Consider data analytics as a service. How can one engage with the resources one already has? There is certainly a gap between deploying a model in a lab and deploying a model in operations. One major financial corporation has 35 people who work on models; quality control is an issue.

There is a need for a framework for failure analysis and stress testing. How does one understand what the behavior of a product will be 100 years after one releases it?

Analytic maturity needs to consider biases in the methods and robustness. DHS is a very data-rich organization, but needs to see what more it can do with such data in operational contexts.

We need to think through the business case and get to the stage where we can think strategically. That can be difficult, because DHS consists of "cops and firefighters," and it can be difficult to think in the longer term with this mentality.

An attendee recommended Daniel Kahneman's book *Thinking, Fast and Slow*, which, among other things, discusses cognitive biases and the limitations of human cognition.

QUESTION: Are there capabilities for measuring accuracy in decision-making? One needs mature data and analytics. How can one quantitatively measure executive success? Is there a qualitative measure, at least? If an executive can fail "within reason," then he or she can do really good things. Otherwise, it is difficult.

We have the analytic capability to understand the ideal operator. One could then use that characterization of ideal operators to train others.

There is a need for tools to help communicate analysts' findings to decision-makers.

QUESTION: What are your recommendations on getting AI and analytics to work together?

Focus on completing the mission. There needs to be a community of practice; to support that, we should have events, and learn who is curious to learn.

6.2. Highlights of the Discussions on QC/QI

QUESTION: How can we achieve breakthroughs in quantum-resistant algorithms?

Quantum-resistant algorithms could be achieved by improving the incentives that we give people to work on them. Only a handful of people have the knowledge, skill, and intelligence to be successful. It might be possible to consider a teaching reduction for the top 10 academic researchers in the field; the process of trying and failing involved in working on big problems requires significant free time. Otherwise, researchers are going to pursue incremental improvements.

QUESTION: How significant is the threat?

The first people to use quantum computing will be limited in number, as this work is highly specialized. However, on matters of national importance, the adversaries will have those specialists.

QUESTION: Are there problems in DHS that are optimization problems?

There are problems within the government that are of interest. For example, IARPA is interested in quantum annealing. Other people are looking into quantum computing to make scientific efforts better, especially in the context of their high-performance computing efforts (e.g., the U.S. Department of Energy). The idea is to bring the domain scientists together with quantum computing people and foster conversation.

QUESTION: How do quantum-generated data samples get labels?

We focused on reinforcement learning scenarios in which label generation is secondary. In an unsupervised context, we use algorithms to do the labeling.

QUESTION: What are the future benefits of nearly accurate sensor measurement?

The benefits include:

- Improved GPS navigation
- Improved imaging and detection technology
- Quantum key distribution

QUESTION: The ion trap and superconducting approaches seem not to worry about connectivity. Are you looking at any nearest-neighbor error-correcting codes?

There is funding to make (only) a single logical qubit. What kind of error-correcting code would one invest in? If there is a large number of errors, then one needs tremendously more physical qubits for each logical qubit.

QUESTION: Superconducting approaches to qubits are not all the same. As one increases the number of qubits, how does that change the manufacturing constraints?

As long as one knows what the fluctuations are, one can address them. Google actually tunes each of their qubits. With the superconductor approach (e.g., D-Wave's), one has dozens of qubits.

QUESTION: Do any of these approaches result in the accumulation of error over time? Is that an issue?

That is an important question. It is very hard to calibrate how errors accumulate. This is a hard problem and a significant research area.

QUESTION: Analog quantum simulators: can we have one soon?

It is not yet clear how useful they will be, perhaps for optimization. Quantum computing may not be able to solve a certain kind of optimization problem outright, but might be able to find approximations faster than a classical heuristic could. The field needs a recognizable killer app. For some problems, one does not need the absolute optimum, just a good answer. For such problems, imperfect quantum simulators might be good enough.

QUESTION: There is a lot of capacity in a channel; don't you think passing a single photon is wasteful of that channel in terms of bandwidth, timing, etc.?

Classical technology allows people to play with terabits in optical fiber along with multiple frequency band and polarization. The problem in quantum is that each of the channels needs a detector. Therefore, the lack of fast and cheap detectors is a challenge so far. With high-bandwidth data, processing might be another problem.

QUESTION: Do you have any thoughts about secure storage using quantum encryption?

One challenge of secure data storage is that you have to store one-time pad keys; that is the current major source of overhead. A multi-priority protocol for key transfer might be useful in this case.

QUESTION: How can one increase the rate of quantum communication?

The current bottleneck is detectors; speeding them up should be the priority.

CIRI | CRITICAL INFRASTRUCTURE RESILIENCE INSTITUTE

A DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

MAY 2018