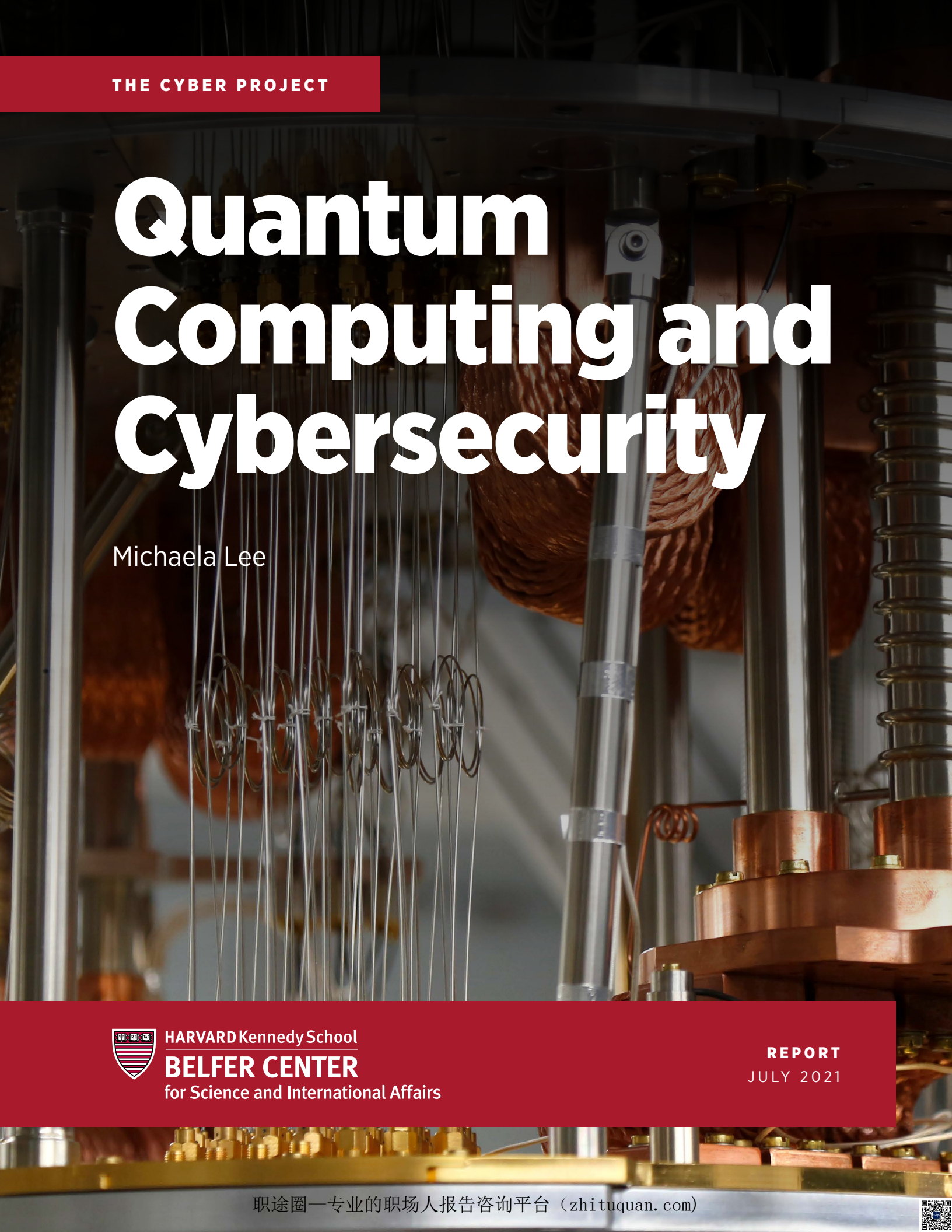


THE CYBER PROJECT

Quantum Computing and Cybersecurity

Michaela Lee

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

REPORT
JULY 2021

The Cyber Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org/Cyber

Design and layout by Andrew Facini

THE CYBER PROJECT

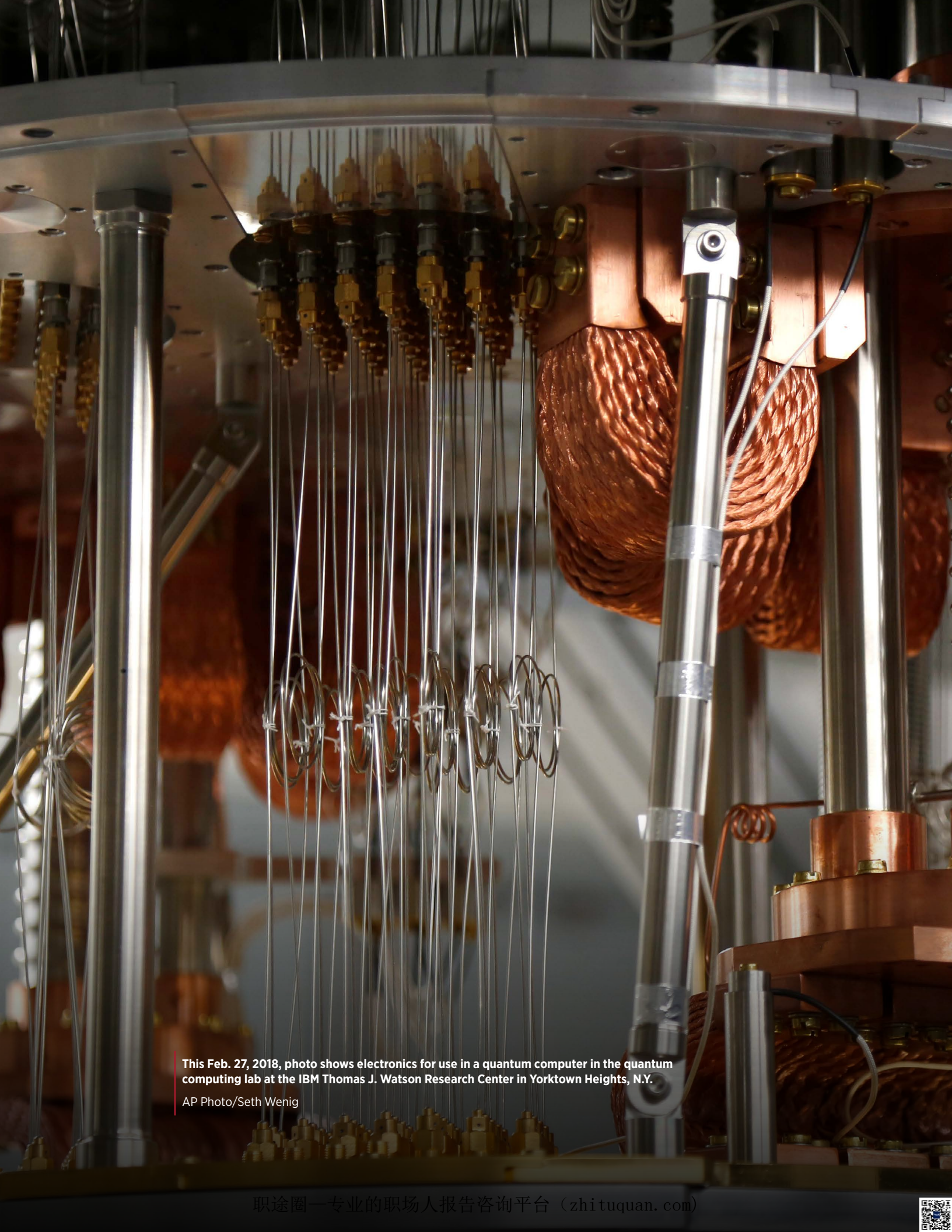
Quantum Computing and Cybersecurity

Michaela Lee

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

REPORT
JULY 2021

Table of Contents



This Feb. 27, 2018, photo shows electronics for use in a quantum computer in the quantum computing lab at the IBM Thomas J. Watson Research Center in Yorktown Heights, N.Y.

AP Photo/Seth Wenig

Executive Summary

Quantum computing poses both opportunities and risks to the cybersecurity environment in which the U.S. operates. The current state of research into quantum technologies and their applications is still nascent, leaving us with an incomplete understanding of how and when to prepare for future quantum computing breakthroughs. While quantum computers powerful enough to undermine current cryptographic defenses are a decade away or more, experience has shown that it will likely take an equivalent amount of time to transition to quantum-resistant approaches to cryptography.[1] The magnitude of the threat and the persistence of encrypted information has spurred public and private sector efforts to develop quantum-resistant algorithms and prepare for adoption.[2]

Countries are moving quickly to create applied research programs designed to accelerate progress in quantum technology development and ensure a strong, domestic quantum technology community. In order for the U.S. and its allies to retain their leading position, they must continue to invest in the creation of an enabling environment for the knowledge, talent, and infrastructure needed by the field. Simultaneously, knowing that commercial applications are decades away, the U.S. and its allies should anticipate the long game that will require continuity of effort, funding, preparation, and collaboration. Though the impacts of large-scale quantum computing will not be seen for years[3], it requires both urgent and sustained focus.

1 William Barker, William Polk, and Murugiah Souppaya, "Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms" (National Institute of Standards and Technology, April 28, 2021), https://doi.org/10.6028/NIST.CSWP.04282021.

2 Martin Giles, "Explainer: What Is Post-Quantum Cryptography?," *MIT Technology Review*, July 12, 2019, https://www.technologyreview.com/2019/07/12/134211/explainer-what-is-post-quantum-cryptography/.

3 Predictions about the timescale for quantum technology development vary.

Recommended actions by government and private sector include:

Government

1. Continue to advance quantum computing research
2. Continue to strengthen international cooperation
3. Assess quantum vulnerabilities
4. Pass legislation and implement policies designed to better recruit, develop, and retain cyber talent
5. Incentivize wide-scale adoption of new encryption standards
6. Convene experts across security, quantum computing, government, and private sector to establish how quantum computing's impact on cybersecurity will affect the digital ecosystem

Business

7. Participate in cross-sectoral collaborations to address the impact of quantum computing on cybersecurity
8. Assess quantum vulnerabilities
9. Prepare for transition to quantum-resistant encryption
10. Enhance security of cloud computing
11. Support infrastructure investments

This brief focuses on how the cybersecurity landscape will be changed by quantum computing advances and is aimed at preparing the public and private sector for accompanying cybersecurity risks and opportunities.

What is Quantum Computing

Quantum computing is a subfield of quantum information science—including quantum networking, quantum sensing, and quantum simulation—which harnesses the ability to generate and use quantum bits, or qubits.

Quantum computers have the potential to solve certain problems much more quickly than conventional, or other classical, computers. They leverage the principles of quantum mechanics to perform multiple operations simultaneously in a way that is fundamentally different from classical computers. While quantum computers are not likely to replace classical computers, there are two key properties of qubits that fundamentally change the way quantum computers store and manipulate data compared to classical computers:

1. Superposition: the ability of a particle to be in several different states at the same time.
2. Entanglement: the ability of two particles to share information even at a distance.

To conceptualize these properties, envision a coin that has two states—heads or tails. That coin represents traditional bits. If you spun the coin, it would be both heads and tails at the same time (superposition). If you spun a pair of two entangled coins, the state of one would instantly change the state of the other (entanglement). Superposition and entanglement enable a connected group of qubits to have significantly more processing power than the same number of binary bits.

However, qubits are also subject to decoherence, a process in which the interaction between qubits and their environment changes the state of the quantum computer, causing information from the system to leak out or be lost. You can imagine the table under the spinning coin shaking, and the coin being knocked over. In order for a quantum computer to actually perform computations, it requires coherence to be preserved. Noise in the system, caused by vibration, changes in temperature, and even cosmic

rays, leads to errors in a quantum computer's calculations. It is possible to address this by running a quantum error correction (QEC) algorithm on a quantum computer to create redundancy, but the process is very resource intensive. The interplay between error correction and decoherence is the strongest determining factor as to when a large scale, cyber-relevant quantum computer will be built.

The aim of quantum computing research today is to build a stable and coherent quantum computer system while developing new applications for these devices. While quantum computers are unlikely to be useful as a direct replacement for classical computers, they will be able to solve certain problems that are practically impossible for today's classical computers. In a similar manner to how graphics processing units (GPUs) accelerate specific tasks for today's computers, quantum processing units (QPUs) will do the same. Already the quantum computing community has identified a range of problems across material science, biophysics and chemistry, machine learning and artificial intelligence that will have transformative solutions driven by quantum computers.

Given quantum computing's potential for impact, the United States, the European Union, China, Japan, and others are making significant investments in quantum computing, as well as related fields of quantum communication and quantum sensing. Research universities and technology companies have made notable progress in the hardware, software, and algorithms underlying quantum computers, as well as in the fields where quantum computing could be applied.

Quantum Computing Applications

The theoretical potential of quantum computers is significant and wide-ranging. Many fields could benefit from the computational advantages of solving problems in a completely different way compared to classical computers. The key properties of qubits illustrated above make quantum computers very good at general optimization problems and problems tied to understanding complex molecules. Below is an illustrative list of the ways in which quantum computers could address existing questions and challenges:

- Use molecular simulation to improve electric vehicle batteries[4]
- Analyze and compare compounds that could lead to the development of new drugs[5]
- Optimize traffic flows in a city[6]
- Enhance generative models that build datasets for training better machine learning algorithms[7]
- Decrypt data secured with public-key encryption[8]

While these diverse applications will no doubt be critical to economic growth and long-term global competitiveness, the disruptive ability of a quantum computer to break current public-key cryptography remains one of the most challenging. Furthermore, there are likely to be a variety of additional changes, risks, and opportunities in applied cybersecurity as both adversaries and defenders develop quantum computing capabilities and revise their infrastructure and practices to account for the changes. We now examine these impacts and consider potential pathways for improved outcomes.

4 Jeannette Garcia, "IBM and Daimler Use Quantum Computer to Develop Next-Gen Batteries," *IBM Research Blog* (blog), January 8, 2020, https://www.ibm.com/blogs/research/2020/01/next-gen-lithium-sulfur-batteries/.

5 Rick Mullin, "Let's Talk about Quantum Computing in Drug Discovery," *Chemical & Engineering News*, September 13, 2020, https://cen.acs.org/business/informatics/Lets-talk-quantum-computing-drug/98/i35.

6 Florian Neukart et al., "Traffic Flow Optimization Using a Quantum Annealer," August 4, 2017, https://arxiv.org/abs/1708.01625v2.

7 Tom Taulli, "Quantum Computing: What Does It Mean For AI (Artificial Intelligence)?," Forbes, August 14, 2020, https://www.forbes.com/sites/tomtaulli/2020/08/14/quantum-computing-what-does-it-mean-for-ai-artificial-intelligence/.

8 Dorothy Denning, "Is Quantum Computing a Cybersecurity Threat?," *American Scientist*, January 30, 2019, https://www.americanscientist.org/article/is-quantum-computing-a-cybersecurity-threat.

Impacts of Quantum Computing on Cybersecurity

Current Encryption

There are two primary types of digital encryption used today:

- Symmetric encryption: The sender and receiver have identical digital keys to encrypt and decrypt data. Current symmetric cryptographic algorithms are considered to be relatively secure against quantum computer-enabled attacks.
- Asymmetric (public-key) encryption: A publicly available key encrypts messages for recipient that has a private key for unscrambling. Public-key cryptography methods such as RSA and elliptical curve cryptography use algorithmic trapdoor functions to create keys that are relatively easy to compute in one direction, but very hard for a classical computer to reverse-engineer.

Shor's Algorithm

Quantum computing will accelerate the ability to decrypt information protected by current public-key encryption techniques. Current public-key encryption relies on the fact that a classical computer can easily multiply large prime numbers but is unable to reverse such a calculation without thousands of years of processing. In 1994, Peter Shor theorized that a large, fault-tolerant quantum computer could find the prime factors of integers in a fraction of the time. This would render many of today's common encryption standards obsolete.

However, this capability is, as of yet, out of reach. Cryptographically relevant quantum computers are likely at the scale of 1,000-10,000 error-corrected quantum bits (which in turn require around 1,000 physical qubits per error-corrected qubit), and, as of writing, the largest functional quantum computers range from 50-60 qubits without error correction. It is estimated

that the development of a quantum computer that can compromise RSA 2048 or comparable public-key encryption is more than a decade away.[9]

Quantum-resistant cryptography

Though the risk to current encryption standards is likely over a decade away, the implications for national security, civilian communications, and stored data are significant. Many systems and processes, such as digital signatures, communications, e-commerce, and digital identity, all rely on mechanisms that would be vulnerable if asymmetric encryption is breakable. Every industry and sector will be affected. This poses a massive problem for governments trying to protect state secrets as well as for companies responsible for protecting customer and user data.

Fortunately, in the late 2000s researchers discovered cryptographic protocols for public-key cryptography that appear to be resistant to decryption by a quantum computer. However, it takes decades to develop quantum-resistant encryption and transition to a new security protocol. As the time frames for both the development of quantum computers and the mitigation of quantum threats are equally long and uncertain, it is critical that the U.S. prioritizes the development, standardization, and deployment of quantum-resistant cryptography. The government and business community must be proactive, rather than reactive, so that we are prepared for the moment when the theoretical potential of quantum computers becomes a reality.

In 2016, the National Institute of Standards and Technology (NIST) initiated a process to solicit, evaluate, and standardize quantum-resistant cryptographic algorithms. By July 2020, they narrowed the pool to nine public-key encryption candidates and six digital signature algorithm candidates. Their goal is to identify one or more encryption algorithms that can be used by classical computers and are "capable of protecting sensitive government information well into the foreseeable future, including after the

9 National Academies of Sciences, Engineering, and Medicine, "Quantum Computing: Progress and Prospects," 2019, https://doi.org/10.17226/25196.

advent of quantum computers."[10] The standardization process is expected to complete in 2022, at which point vendors can begin the decade-long process of deployment.

One challenge with the development of quantum-resistant encryption is that a sufficiently large, fault-tolerant quantum computer does not exist to test an algorithm's resiliency to a quantum attack. This is a cryptographic problem that is not exclusive to quantum cryptography—the security of an algorithm cannot be proven and must continue to be evaluated over time. Testing methods will continue to improve, but it will take years to ratify the security of a quantum-resistant algorithm.

Another challenge is one of efficiency. Quantum-resistant cryptosystems are more computationally intensive (due to public-key size, signature size, speed of encryption and decryption algorithms, speed of key generation algorithm, etc.[11]) than current cryptosystems. Users are often comfortable using less secure but higher speed services, posing a barrier to the uptake of quantum-resistant encryption. Furthermore, there are substantial equity and energy concerns if quantum-resistant cryptography requirements dramatically increase the cost of internet and related business transactions.

Quantum Cryptography

Quantum cryptography is distinct from quantum-resistant cryptography. While quantum-resistant cryptography refers to a new set of classical cryptographic algorithms, quantum cryptography uses the properties of quantum mechanics as the basis of security. Quantum key distribution (QKD) could be used to secure quantum communications via satellites and long-path optical fibers.

Theoretically, QKD creates a level of secrecy that prevents eavesdroppers since any attempted interference or eavesdropping can be readily detected. This could greatly enhance the security of networks and communications

10 NIST, "Post-Quantum Cryptography Standardization," CSRC | NIST, January 3, 2017, https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization.

11 Petros Wallden and Elham Kashefi, "Cyber Security in the Quantum Era," *Communications of the ACM*, April 2019, https://cacm.acm.org/magazines/2019/4/235578-cyber-security-in-the-quantum-era/fulltext.

since it is one of the few methods that can be "provably secure."[12] However, the NSA currently does not recommend the use of QKD due to the following technical limitations:[13]

- QKD does not authenticate the transmission source
- QKD requires special hardware
- QKD increases infrastructure costs and insider threat risks
- QKD security and validation is a challenge
- QKD increases risk of denial of service

These systems are likely to be fragile, slow, and more expensive. In addition, there are many potential vulnerabilities throughout the security chain that quantum cryptography cannot address. Often, hackers prefer to identify vulnerabilities on the periphery of a system, rather than attack it head on. Even if a key is secured through QKD, the network of routers, repeaters, and hubs all offer potential points of vulnerability.[14]

China has invested significantly in QKD using both ground-based fiber networks and satellite-to-ground links (see box on page 17).[15] The U.S., Japan, Canada, European Union, and others also research QKD, but have tended to focus more investments in quantum computing.[16]

While theoretical and experimental research on quantum cryptography continues to advance, we will need quantum-resistant cryptography to secure the majority of devices.

12 Elsa B. Kania and John K Costello, "Quantum Hegemony? China's Ambitions and the Challenge to U.S. Innovation Leadership" (CNAS, September 12, 2018), https://www.cnas.org/publications/reports/quantum-hegemony.

13 "Quantum Key Distribution (QKD) and Quantum Cryptography (QC)," NSA, accessed April 12, 2021, https://www.nsa.gov/what-we-do/cybersecurity/quantum-key-distribution-qkd-and-quantum-cryptography-qc/.

14 Maria Korolov and Doug Drinkwater, "What Is Quantum Cryptography? It's No Silver Bullet, but Could Improve Security," *CSO*, March 12, 2019, https://www.csoonline.com/article/3235970/what-is-quantum-cryptography-it-s-no-silver-bullet-but-could-improve-security.html.

15 University of Science and Tehnology of China, "The World's First Integrated Quantum Communication Network," January 6, 2021, https://phys.org/news/2021-01-world-quantum-network.html.

16 Tom Stefanick, "The State of U.S.-China Quantum Data Security Competition," *Brookings*, September 18, 2020, https://www.brookings.edu/techstream/the-state-of-u-s-china-quantum-data-security-competition/.

Risks and Mitigations

Given the significant risk that a large, fault-tolerant quantum computer poses to cybersecurity, it is crucial that we consider the full range of implications now in order to mitigate potential harms. There are four key ways in which quantum computers can be exploited to undermine cybersecurity:

1. Information intercepted in the past, if recorded and stored properly, can be decrypted in the future by quantum computers. This is an inevitable risk that exists today—state actors or criminals may collect encrypted data with the hope that future advancements will enable them to decrypt it later. There are limited ways to protect against the pre-capture of data. Migrating applications to quantum-resistant encryption as quickly as possible will help mitigate this risk.

2. Organizations that do not assess their risks and migrate in time to quantum-resistant encryption will be susceptible to systemic data insecurity. This risk is systemic due to the hyperconnected nature of the digital ecosystem. As connectivity becomes more ubiquitous, a greater amount of critical data, communications, and services are reliant on the security of our systems. In addition, greater interdependency exacerbates the risk that incidents occurring in one part of the ecosystem can impact organizations on the other side. We must ensure that the security of our systems runs across end-to-end processes, supply chains, and shared infrastructure in order to develop resilience to the advancing threat of quantum computers.

3. Organizations that procrastinate and then rush to migrate to quantum-resistant encryption will likely be vulnerable to design and implementation flaws across IT platforms, creating errors that can be exploited by hackers without quantum computers. Organizations should proactively assess quantum vulnerabilities and develop a plan for transitioning to quantum-resistant encryption.

4. Without clear communication about our preparations for the cybersecurity risks of quantum computing, trust and confidence in

the digital ecosystem will continue to erode. Quantum readiness plans from public and private sector entities and clear federal guidance on the transition to quantum-resistant encryption would help mitigate this risk.

Quantum Computing Development

Predictions around the timing of quantum computing advances vary considerably. There are a number of engineering challenges that have yet to be overcome, making it hard to anticipate when we will be able to realize the theoretical potential of quantum computers. Generally, experts estimated that large fault-tolerant quantum computers are more than a decade away, while other applications of small quantum computers may become practical within the decade.[17] [18]

Notably, there are multiple ways to build quantum computers, each with its own challenges and opportunities for scaling. The trapped ion and superconducting approaches have been most successful in achieving small demonstration quantum computers, even as other technologies to create physical qubits continue to being explored. Given the early stage of research on these approaches, it is not yet known whether one approach is best, or whether multiple will prove to be plausible for different applications.

Short-term

We can expect that the cost of quantum error correction will make it difficult to build anything beyond **noisy intermediate scale quantum computers** (NISQ) in the near future. NISQ computers, which became

17 National Academies of Sciences, Engineering, and Medicine, "Quantum Computing."

18 World Economic Forum and University of Oxford, "Future Series: Cybersecurity, Emerging Technology and Systemic Risk" (World Economic Forum, November 16, 2020), https://www.weforum.org/reports/future-series-cybersecurity-emerging-technology-and-systemic-risk/.

available in 2017, are considered noisy because of their error rates but are stable enough to carry out a computation before losing coherence. It is unclear what the practical applications NISQ computers are, given that classical computers can often undertake the same calculations with fewer resources.[19]

Medium-term

Researchers and companies are quickly increasing the number of qubits their quantum computers can handle. In the next decade, we will likely see the emergence of **small quantum computers** containing tens of error-corrected, also known as logical, qubits, or several hundred non-error-corrected qubits. The most promising applications of these devices are in the fields of quantum chemistry, quantum machine learning, and quantum optimization.

Long-term

Large fault-tolerant quantum computers represent the promise of quantum technology. These quantum computers will have a low enough error rate and a sufficient number of logical qubits to do things far beyond the reach of classical computers, including simulating physics or chemistry, materials science, machine learning, and breaking public-key encryption.

Quantum-enabled opportunities for cybersecurity

In addition to the threats posed by quantum computing to public-key cryptographic systems, there are additional opportunities they may provide to help reduce cyber-related threats. For example, advances in machine learning can dramatically reduce the threat profile and improve the latency in vulnerability reduction. Also, improvements in operations research-related algorithms can lead to faster upgrade, patching, and verification methods which in turn can reduce windows for attack. Finally, experts

19 National Academies of Sciences, Engineering, and Medicine, "Quantum Computing."

generally assess that future quantum algorithms with substantial impact in these domains are likely to be discovered. Thus, is it essential for organizations to be 'quantum-aware' to ensure timely application of such results to mission-relevant tasks.

Overview of Current State of Research and Development

National Quantum Initiative Act of 2018: Established a coordinated federal program to accelerate quantum research and development with $1.275 billion in funding over five years. It assigned specific roles to the National Institute for Standards and Technology (NIST), Department of Energy, and the National Science Foundation. It also established responsibilities for the National Science and Technology Council Subcommittee on Quantum Information Science, the National Quantum Coordination Office, and the National Quantum Initiative Advisory Committee. Notably, spending in 2019 and 2020 has exceeded the congressionally-mandated budget, reflecting the U.S.' priority to grow quantum research and development.[20]

National Defense Authorization Act (NDAA): Additional authorization for quantum-related research has been provided in the NDAA since FY2019. The 2021 NDAA requires a comprehensive assessment and recommendations on the current and potential threats and risks posed by quantum computing technologies to critical national security systems. It also directed the Office of Science and Technology Policy to put forward a plan to double baseline investments in quantum information science by 2022.

A number of other countries have recently announced significant investments in quantum research and development:

- The EU has moved quickly in establishing their EU Quantum Flagship, a project launched in 2018 to support quantum technology development with €1 billion ($1.2 billion) over ten years.[21]

20 Subcommittee on Quantum Information Science, "National Quantum Initiative Supplement to the President's FY 2021 Budget," January 2021, https://www.quantum.gov/wp-content/uploads/2021/01/NQI-Annual-Report-FY2021.pdf.

21 "Introduction to the Quantum Flagship," Quantum Flagship, accessed April 12, 2021, https://qt.eu/about-quantum-flagship/introduction-to-the-quantum-flagship/.

- In 2020, Germany pledged €2 billion ($2.4 billion) from the country's pandemic recovery fund to be spent on quantum research.[22]
- In 2020, India established a National Mission on Quantum Technologies and Applications with INR 80000 crore ($1.12 billion) over five years.[23]
- In 2021, France pledged to triple their investments in quantum and spend €1.8 billion ($2.15 billion) over the next five years.[24]
- China is reportedly spending $10 billion on the country's National Laboratory for Quantum Information Sciences.[25]

The private sector is leading the way in establishing research centers, building hardware and software, and making engineering breakthroughs. More information on public-private collaborative developments can be found here.

- Big tech companies, such as Amazon, Google, IBM, Microsoft, and Honeywell have invested heavily in quantum computing. They have also sought partnerships with academic collaborators and potential customers in other industries in the pursuit of real-world applications of quantum computers.
- Smaller companies, such as D-Wave Systems, IonQ, Cambridge Quantum Computing, QC Ware, and 1QB Information Technologies, and Rigetti represent the first wave of companies building out the hardware, software, tools, and services necessary for commercial quantum computing.
- The quantum computing market, which was $472 million in 2021, is projected to reach $1.765 billion by 2026.[26]

22 Fintan Burke, "Qubit to Get Ahead: Germany Is Racing to Catch up with the Quantum Revolution," *Science|Business*, August 4, 2020, https://sciencebusiness.net/news/qubit-get-ahead-germany-racing-catch-quantum-revolution.

23 T. V. Padma, "India Bets Big on Quantum Technology," *Nature*, February 3, 2020, https://doi.org/10.1038/d41586-020-00288-x.

24 Anne-Françoise Pelé, "French President Details €1.8b Quantum Plan," *EE Times Europe*, January 22, 2021, https://www.eetimes.eu/french-president-details-e1-8b-quantum-plan/.

25 Fred Guterl, "As China Leads Quantum Computing Race, U.S. Spies Plan for a World with Fewer Secrets," *Newsweek*, December 14, 2020, https://www.newsweek.com/2020/12/25/china-leads-quantum-computing-race-us-spies-plan-world-fewer-secrets-1554439.html.

26 "Global Quantum Computing Market" (Research and Markets, February 2021), https://www.researchandmarkets.com/reports/5241699/global-quantum-computing-market-with-covid-19.

Road Map: An Action Agenda to Advance Cybersecurity in the Quantum Era

Government

1. Continue to advance quantum computing research

In 2018, the National Quantum Initiative Act authorized $1.275 billion in funding over the next five years. Consistent, significant funding to both public and private sector research efforts will be necessary to build the hardware, software, and algorithms underlying quantum computers. If near-term quantum computing research is not commercially successful, the government's role in funding advancements in the field will become more essential. Close collaboration between the public and private sectors will remain important for the knowledge and technology transfer that is necessary for pre-competitive quantum research and development.

2. Continue to strengthen international cooperation

In addition to funding, a key component of advancing quantum computing is continued collaboration with other countries who are investing in quantum. The National Strategic Overview for Quantum Information Science highlights the importance of bilateral agreements to support joint projects, as well as the international flow of capital, knowledge, and talent.[27] Notably, in 2019 the U.S. and Japan signed the Tokyo Statement on Quantum Cooperation, the first bilateral diplomatic agreement regarding quantum information science cooperation.[28] The U.S.' investments in research and technological development will benefit from continued

27 Subcommittee on Quantum Information Science, "National Strategic Overview for Quantum Information Science" (National Science and Technology Council, September 2018), https://www.quantum.gov/wp-content/uploads/2020/10/2018_NSTC_National_Strategic_Overview_QIS.pdf.

28 "Tokyo Statement on Quantum Cooperation" (U.S. Department of State, December 19, 2019), https://www.state.gov/tokyo-statement-on-quantum-cooperation/.

engagement and openness with other nations in cooperative efforts to advance quantum computing. There has been limited discussion around international norms and standards, but voices from the private sector and academia have begun to push for a more comprehensive approach to building and deploying quantum technology with ethical considerations and standardized guidance.[29]

Furthermore, there is a need for international collaboration in addressing and mitigating quantum threats. The transition to quantum-resistant encryption will pose challenges for many countries, particularly those who have fewer cybersecurity capabilities and resources. International initiatives that promote information sharing, education, and training will help improve the overall resilience of the cyber ecosystem. Without a global readiness effort, the interconnected nature of critical infrastructure and supply chains will further increase the U.S.' vulnerability to disruption and exploitation by malicious cyberactivity.

3. Assess quantum vulnerabilities

In the FY21 NDAA, Congress directs the Department of Defense to comprehensively "assess the risks and threats posed by quantum technologies to national security systems as well as strategies, plans, and investments needed to mitigate risks toward these systems."[30] This shall include the following components:

A. an identification and prioritization of critical national security systems at risk;

B. an assessment of NIST standards for quantum-resistant cryptography and their application to cryptographic requirements of the Department of Defense;

29 Sara Castellanos, "Quantum Computing Scientists Call for Ethical Guidelines," *Wall Street Journal*, February 1, 2021, https://www.wsj.com/articles/quantum-computing-scientists-call-for-ethical-guidelines-11612155660.

30 Adam Smith, "National Defense Authorization Act for Fiscal Year 2021," Pub. L. No. H.R.6395 (2021), https://www.congress.gov/bill/116th-congress/house-bill/6395/text.

C. an assessment of the feasibility of alternate quantum-resistant algorithms and features;

D. a description of any funding shortfalls in public and private developmental efforts relating to quantum-resistant cryptography, standards, and models; and

E. develop recommendations for research, development, and acquisition activities, including resourcing schedules, for securing the critical national security systems against quantum computing code-breaking capabilities.

This risk assessment process is important for the Department of Defense, but should also be applied to other government departments and agencies. In March 2021, the Government Accountability Office (GAO) released a report on the urgent need for the federal government to address major cybersecurity challenges, including the risk of quantum computing. GAO calls on the Department of Homeland Security and Office of Management and Budget to build out initiatives to improve agencies' capabilities for managing cyber risks.[31] The federal government should invest time and resources into identifying and prioritizing the activities required to improve understanding of vulnerabilities and migrate to quantum-resistant encryption. This may include both legislative and executive actions to provide federal Chief Technology Officers (CTOs) with the authorization and resources needed to assess these risks.

Space Industry

Space exploration and industry is looking to benefit greatly from various quantum technologies, including quantum metrology and sensing. There is also significant interest in using quantum key distribution (QKD) to secure quantum communications.

In particular, China has invested a significant amount of research and development into space-based QKD as a primary area of research. In 2016, China

31 U. S. Government Accountability Office, "High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges," March 2021, https://www.gao.gov/products/gao-21-288.

launched the Micius satellite, which has successfully transmitted entangled photons between the satellite and multiple ground stations.[32] [33]

While QKD will likely not be a method that can be deployed widely, it provides some advantages for very long-range secure information. Due to the properties of superposition and entanglement, observation from an outsider will disrupt the quantum state, giving QKD a built-in ability to detect intrusion. It is important to note that QKD will not ensure comprehensive security to space communications as there are a range of other intrusion vectors which can create vulnerabilities (see box on page 8). Regardless, future research experiments with space-based QKD will advance understanding of how to build provably secure quantum networks.

4. Pass legislation and implement policies designed to better recruit, develop, and retain cyber talent.

Without strategic investment in the education and cultivation of a future workforce, the U.S. will soon face a major skill shortage in the quantum information science field. In addition to technical researchers, there is a need for quantum-informed workers to develop the supply chain and operational infrastructure needed to support the industry. Once a large, fault-tolerant quantum computer is developed, there will be a race to build and deploy quantum computers and develop commercial applications. Because of the range of applications of a quantum computer, we will need skilled employees across many disciplines, including physics, engineering, applied mathematics, materials science, and computer science. This quantum upskilling should cover multiple levels of education and training—from middle and high school programs, to curriculum at the undergraduate and graduate level, to training for current employees. Various programs, including the National Q-12 Education Partnership,

32 Yu-Ao Chen et al., "An Integrated Space-to-Ground Quantum Communication Network over 4,600 Kilometres," *Nature* 589, no. 7841 (January 2021): 214–19, https://doi.org/10.1038/s41586-020-03093-8.600 Kilometres,\\uc0\\u8221{} {\\i{}Nature} 589, no. 7841 (January 2021

33 Kania and Costello, "Quantum Hegemony? China's Ambitions and the Challenge to U.S. Innovation Leadership."

have been established to address this skills gap, but they will require sustained funding in order to develop a stable workforce pipeline.[34]

5. Incentivize wide-scale adoption of new encryption standards.

NIST's Post-Quantum Cryptography Project is working toward the standardization of quantum-resistant public-key encryption. It will be crucial to provide funding and support for NIST to continue focusing on the development and rollout of new standards. These standards represent security best practice controls to help organizations manage and reduce risks, and they're typically followed by both public and private sector entities. An example of a widely adopted NIST standard is the NIST Cybersecurity Framework, which lays out how organizations can prevent, detect, and respond to cyberattacks.[35]

Once the current standardization process is complete, there will be an urgent need to quickly deploy the new standard across public and private sector information security systems. Replacing the old standards will be very challenging, given the extent to which it is embedded in every platform and device. It took almost two decades to deploy our modern public-key infrastructure, indicating that it will take significant effort to ensure this transition is efficient and comprehensive.

Government agencies should begin to prepare to transition encrypted communications and data to new quantum-resistant cryptography standards and require critical commercial partners to do the same. A communications campaign about the upcoming transition—perhaps spearheaded by a coalition of NIST, CISA, and others—may also help raise business awareness of the preliminary steps they can take in anticipation of the transition. In addition, federal and state governments and regulators should consider the level to which requirements should be put in place to ensure that risks to critical infrastructure and the public good are sufficiently addressed.

34 "NSF Expands Quantum Education to Students Nationwide in Collaboration with Industry, Academic Leaders," August 5, 2020, https://www.nsf.gov/news/special_reports/announcements/080520.jsp.

35 NIST, "Cybersecurity Framework," text, NIST, November 12, 2013, https://www.nist.gov/cyberframework.

6. Convene experts across security, quantum computing, government, and private sector to establish how quantum computing's impact on cybersecurity will affect the digital ecosystem.

Other recommendations highlight the importance of government agencies and companies assessing their individual risks and transitioning to quantum-resistant encryption. These actions are necessary, but not sufficient. With the increasing scale, complexity and interdependencies of the digital ecosystem, the threats are systemic and must be addressed in a systemic way. Isolated mitigation leaves gaps and vulnerabilities—the system must be strengthened across end-to-end processes, supply chains, and shared infrastructure. The government should convene major players in this space to examine the distributed and systemic risks of quantum computing. These discussions should lay the groundwork for the development of new governance frameworks and incentive models that will improve the resilience of the ecosystem

Business

7. Participate in cross-sectoral collaborations to address the impact of quantum computing on cybersecurity.

As stated in previous recommendations, collaboration is crucial to addressing the systemic risks that quantum computing poses. Information sharing within the private sector and between the private and public sectors will help strengthen the collective capacity of the ecosystem to build mitigations into the design and deployment of quantum-related technologies. In addition, this collaboration can inform the development of defensive capabilities that may be needed if an adversary uses quantum computing technology against U.S. interests.

8. Assess quantum vulnerabilities

Given the extent to which society relies on modern public-key cryptographic systems for communications, data, and digital transactions, businesses need to evaluate their existing processes and infrastructure to prioritize threats and vulnerabilities. Similar to the government-level process discussed above, businesses should invest time and resources into a quantum risk assessment. Elements of this assessment may overlap with the cyber security planning companies already do, including understanding the nature of their sensitive information, access control and data sharing agreements, backup and recovery processes, and end-of-life procedures. Businesses should also consider their dependence on vendors' and suppliers' cybersecurity measures as part of their risk assessment.

9. Prepare for transition to quantum-resistant encryption

Once NIST has validated standards for quantum-resistant encryption, businesses will need to move quickly to migrate business processes and communications to the new cryptographic standards. This requires prework for organizations to articulate their quantum readiness plans. This preparation should occur within the next 12-24 months in preparation for the draft standards, which are expected between 2022 to 2024. Once a quantum readiness plan is established, businesses can update the plan

yearly to show how they're achieving key milestones. This will inevitably involve engagement with their vendors and vendors' vendors all through the supply chain. Planning and budgeting for this transition will be complicated but necessary to ensure business resilience and security.

10. Enhance security of cloud computing

Given the nature of quantum computers (need for well-controlled environments, high cost of development and maintenance), it is likely that the majority of quantum computing processing will be delivered via the cloud. A secondary implication is that customers of cloud technology will also be more likely to be early users of quantum computing. Cloud providers may need to develop new security approaches to build trust with potential enterprise customers. There are theorized ways, e.g., quantum homomorphic encryption[36], to ensure the cloud provider knows neither the program nor the data.[37]

Quantum and Cloud

Quantum computers today are large, expensive, and difficult to build and maintain. This will make on-premise quantum computers unlikely in the near future. Instead, commercial uses of quantum computers will be enabled through the cloud, with a third-party controlling access to quantum computing power and algorithms.

The increasing value in shared infrastructure and resources widens the attack surface for cyber threats. These threats will arise long before the creation of a large fault-tolerant quantum computers. Attackers won't need a quantum computer to break your encryption, but could instead steal the credentials that protect your access to cloud quantum services. Distributed denial-of-service (DDoS) attacks could also put your organization or data at risk. Securing cloud-based quantum computing is not substantially different from securing other cloud services. Since sending data to the cloud currently relies on public-key encryption, cloud providers will need to be some of the first to deploy quantum-resistant encryption.

36 Homomorphic encryption is a technique that allows for computations to be done on encrypted data, without requiring access to a secret key.

37 Jonas Zeuner et al., "Experimental Quantum Homomorphic Encryption," *Npj Quantum Information* 7, no. 1 (February 5, 2021): 1–6, https://doi.org/10.1038/s41534-020-00340-8.

11. Support infrastructure investments

Quantum computers require high performance components, specialized equipment, rare materials, and fabrication capabilities. The lack of sufficient components and infrastructure will pose a barrier to the advancement of near-term research, as well as the capacity to scale-up the development and adoption of quantum computers. The private sector, particularly large tech companies, venture capital firms, and the start-up community, will need to identify and invest in quantum infrastructure gaps. Participation in initiatives such as the Quantum Economic Development Consortium (QED-C) is also an important component of the cross-sector collaboration needed to grow the quantum economy.[38]

Financial Services Industry

The financial services industry is expected to be an early adopter of quantum computing and benefit from quantum computers' ability to solve optimization problems as applied to areas such as risk management and financial modeling. A number of companies are exploring the potential applications of quantum computing. Goldman Sachs, Wells Fargo, JPMorgan and others have partnered with IBM to experiment with its Q Network and explore use cases like option pricing.[39] Toshiba recently announced an initiate to test quantum cryptography in the financial sector.[40]

At the same time, financial services firms are a frequent target of cyberattacks and, by nature of their activities, will be vulnerable to quantum computers' ability to break public-key cryptography. Processes that ensure confidentiality and authenticity of financial transactions will be at risk of failure. Given the complexity of the financial services industry, companies should prepare now for the transition to quantum-resistant encryption.

38 "QED-C," QED-C, accessed April 12, 2021, https://quantumconsortium.org/.

39 Sophia Chen, "Goldman, Wells Fargo, JPMorgan Embrace Quantum Computing," *Protocol*, May 4, 2020, https://www.protocol.com/manuals/quantum-computing/finance-banks-investing-investment-edge.

40 "Beginning Joint Verification Tests on Quantum Cryptography Technology to Enhance Cybersecurity in the Financial Sector," Toshiba, December 21, 2020, https://www.global.toshiba/ww/technology/corporate/rdc/rd/topics/20/2012-04.html.

Preparing for the Future

Quantum computing provides exciting possibilities for the future of science, healthcare, machine learning, and communications, but the importance of maintaining security of our cyber environment is paramount. As quantum technology progresses, the networks we use will become more complex with the integration of both classical and quantum devices and links. It is crucial that we foresee the threats and opportunities that quantum will bring to our computing and communicating landscape.

In particular, government and business have a challenging task ahead to prepare and prioritize for the threats to cybersecurity that large scale, fault-tolerant quantum computers will bring. We must not waste time in the development and adoption of quantum-resistant encryption.

The Cyber Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org/Cyber

Printed in the United States of America