Quantum Computing's Cyber-Threat to National Security

By Steve Grobman

Quantum computing has the potential to bring tremendous advancements to science, including biology, chemistry, physics, and many other disciplines. The practical application will empower a stronger defense against future pandemics similar to COVID-19, not only in the acceleration of the development of vaccines and treatments, but also in optimizing currently unsolvable logistics problems such as how to deliver and route vaccines. In computer science, the "traveling salesman problem" shows it is impractical to find the optimal shortest path to visit cities once the list grows to even a few dozen. This same challenge in delivering vaccines to rural areas during a pandemic is exactly the type of problem that quantum computing will be well suited to solve.

However, like all technology, in the wrong hands, quantum computing can be a dangerous tool. In the field of cybersecurity, for example, nation-states will be able to use quantum technology to break the public cryptographic systems that secure and enable us to trust much of our digital world, including web traffic, emails, and countless uploads and downloads of everything from confidential files to software updates.

The United States has maintained a leading capability in signals intelligence and the protection of national secrets for almost a century. This position has shortened conflicts and prevented the escalation to war, saving millions of lives. Currently, publicly available information suggests there is a significant gap between the United States and our geopolitical rivals in quantum technology investment which suggests that our country could quickly find itself at a significant technological disadvantage in signals intelligence.[1] On the defensive side, we must move faster to re-tool the algorithms, protocols, and systems that encrypt our public and private sector data. Given that encrypted data can be captured today and decrypted at a later time, we cannot afford to think of quantum in terms of "eventually" or "tomorrow" because the threat it poses is a national security risk today.

What History Teaches Us

Our own history tells us that nations with superior technology in signals intelligence save lives and help determine winners and losers in war and overall geopolitics. A conservative estimate shows that, without the Allies' ability to break Axis communications encrypted by the powerful Enigma encryption machine, an additional

Steve Grobman is Senior Vice President and Chief Technology Officer of McAfee LLC.

14 million lives would have been lost during World War II. Especially impactful to the war effort was the codebreakers' ability to help the Allies dodge U-Boats and accelerate preparations for the D-Day invasion of Europe; advantages that made the difference between life and death for millions.[2]

Forty years later, on September 5, 1983, President Ronald Reagan addressed the American people and played intercepted communications from the Soviet military providing evidence that the shoot-down of Korean Air 007 was intentional. Because of this, the President was able to publicly hold the Soviets accountable for their hostile action against innocent civilians.[3]

In our modern era, the long-term national security of the United States has relied on the ability of the U.S. military to identify attacks against U.S. citizens before they occur and hold the actors accountable. It was signals intelligence that made it possible to intercept and monitor key communications that led to locating and killing Osama Bin Laden, the mastermind of the 9/11 terrorist attacks.

What these events all have in common is U.S. leadership in signals intelligence. The advantages, the lives saved, the diplomatic coups, and the maintenance of peace and stability would not have been possible had the United States and its allies fallen behind its adversaries technologically.

What does this history teach us? The story of the Enigma codebreakers does not end with World War II. It provides a cautionary glimpse of future risks organizations and nations will face once quantum computing becomes a viable security challenge. The Allies kept their codebreaking achievement secret, meaning dozens of governments inherited the Enigma machines and continued to use them for decades believing their security to be unbreakable. British and American intelligence services were able to monitor communications from other governments throughout some of the most critical years of the Cold War. Accordingly, the revelations about the compromised Enigma communications remained a secret, well into the 1970s, when a series of books exposed the work and accomplishments of the British WWII code breakers.[4]

Nations that lead in quantum computing for cryptanalysis, the science of breaking cryptography, will have a similar inherent advantage in signals intelligence in the years to come. All nations face challenges in moving to quantum resistant algorithms, including the many years it will take to transition away from the current, quantum-vulnerable implementations.

The ability to use quantum computing to decrypt data encrypted with existing implementations will enable unprecedented visibility to high valued data. Prior to quantum cryptanalysis becoming viable, data collection of encrypted, long-term, time sensitive information is still advantageous as it may be possible to decrypt it in the future when quantum cryptanalysis is practical. If the United States were to lose the quantum computing technology race with nation-state rivals such as China, our loss of signals intelligence leadership would be significant and impactful.[5]

Like the Allies following World War II, U.S. adversaries may not disclose critical breakthroughs in quantum viability. Rival nation-states could use their quantum supremacy to break encryption and access our country's most sensitive information for years without the United States and our allies becoming aware of the compromise.

Quantum Versus Encryption

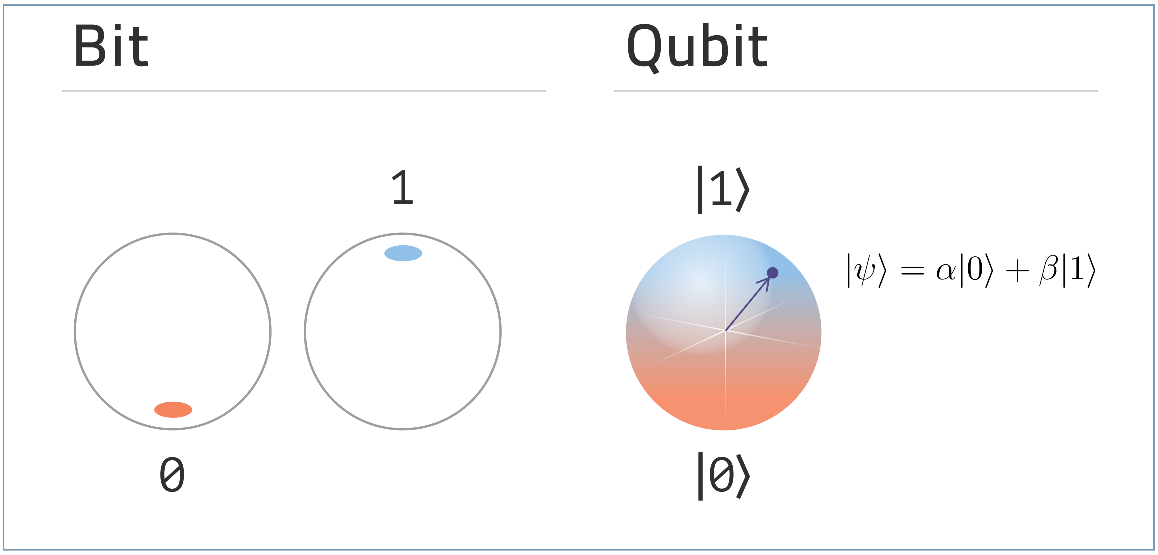
Quantum computing is a broad and complex capability that is not yet practical for real-world applications. The capability, when made practical, will be suited for special classes of problems and not a direct replacement for the general-purpose computing capabilities enabled by modern silicon compute architecture. Moore's Law, the guiding principle of expectations for the tech industry, theorized that the number of transistors and other components in dense integrated circuits would double every year: In short, doubling computing power without significantly increasing cost. The theoretical paradigm shift of quantum computing has the potential to take Moore's Law to a significantly higher level, increasing computing power by a factor of about 10,000.[6]

The quantum physics behind quantum computing exist in theory, but have not yet become practical, translatable electric processes for computing. The timeframe for building a large-scale quantum computer is complicated and uncertain with speculation varying widely. Many scientists believe the building of such a powerful computer is now limited to an engineering challenge, but controlling counter-intuitive physics of subatomic scales in a practical computer is not easy. Harnessing error-causing vibrations, electromagnetic waves, and temperature fluctuations are among the challenges facing engineers. Some scientists predict we will overcome these obstacles within the next 20 years, resulting in computers powerful enough to decrypt the predominant public key schemes currently in use. However, this speculative timeline is largely tied to the amount of research resources being focused on the challenge.

Today's encryption is built on a set of algorithms that work together and are implemented in the protocols, standards, and products that protect the world's data. Two main classes of algorithms exist; symmetric and asymmetric. Symmetric algorithms use the same key to both encrypt and decrypt data, while asymmetric algorithms use a key pair (one key is public and the other is private). The value of an asymmetric—also known as public key—algorithm is that anyone can encrypt data (using the public key) for a specific entity such that only they can decrypt it (with the private key). Generally, symmetric key algorithms in use today—AES-256 for example—are not vulnerable to known quantum (or traditional) attacks. The concern is largely on major public key algorithms in use today, namely RSA and "Elliptic Curve" which are believed to be susceptible to quantum-based attacks.

The RSA encryption algorithm is the foundational encryption standard upon which most modern secure network protocols and data security systems are built. Named for its inventors—Ron Rivest, Adi Shamir, and Leonard Adleman—it bases its security on the premise that it is computationally infeasible to factor a very large number into its corresponding primes. For example, we can easily multiply the prime numbers 13 and 97 to get 1,261; but the reverse math problem is much more difficult (starting with 1,261 and finding the two underlying primes). Today's computers can both multiply the primes and find the primes for smaller numbers, but as the numbers become exceptionally large, as they do in the generation of encryption keys, the factoring challenge becomes computationally impractical. The RSA algorithm is founded on the assumption that, even with improvements in future computing capabilities, the math required to perform the factoring would take too long to make the decryption workable in practice without possessing the decryption key.

Quantum computing, however, changes the underlying assumptions about how computing works and, therefore, how quickly computers can perform math calculations. Quantum computing relies on the principles of quantum physics to solve specialized classes of mathematical problems that are not practical to solve on traditional computers. Unlike conventional digital computers that are based on transistors and encode data into binary digits (bits), these new computers would use quantum bits (qubits). Qubits can exist in multiple states simultaneously, offering the potential to compute a large number of calculations in parallel. Similar to traditional computing where the number of bits in a compute architecture determines the size and scale of possible computations, in quantum computing the number of qubits will influence the scale of



Qubit vs. bit. States of classical bit compare to quantum bit superposition. (Shutterstock/Astibuag)

mathematical problems a quantum computer can solve. The parallel nature of the qubit creates the potential to determine the underlying RSA prime numbers used to generate encryption keys that can access RSA-encrypted data. While it is possible to factor numbers using traditional computing, the size of numbers used in encryption makes it impractical.

Mathematician Peter Shor has shown that an algorithm (Shor's Algorithm) exists to identify the underlying factors of a prime number. The unique property of this algorithm is that it executes significantly faster on a quantum computer as compared to execution on a traditional computer. This approach overall is exponentially faster than the fastest known factoring capability available today on traditional computers, the general number field sieve, which works in sub-exponential time.[7]

Quantum computers are likely to be too large and expensive for today's cyber criminals to build and maintain directly, leaving their use to large technology companies, a few well-funded research institutions, and nation-states. While cloud computing will extend the reach of quantum to cyber criminals, the scalability and opportunity cost of using quantum for cyber-crime will be outweighed by traditional criminal cyber activities. Certain nation-states on the other hand are well-funded and able to capitalize on the value of using quantum to advance their national security objectives.

Some tech industry luminaries question the likelihood that quantum computing will achieve the capacity to break encryption. MIT Professor Ron Rivest—the "R" in RSA—has serious doubts about whether quantum computers will become a reality at the size and scale needed to break his and other encryption algorithms. "I give fusion power a higher chance of succeeding than quantum computing," Rivest said at the 2020 RSA Conference in San Francisco. "There is a lot of scaling that has to be done before you can break cryptography, and I am not sure it can be done."[8]

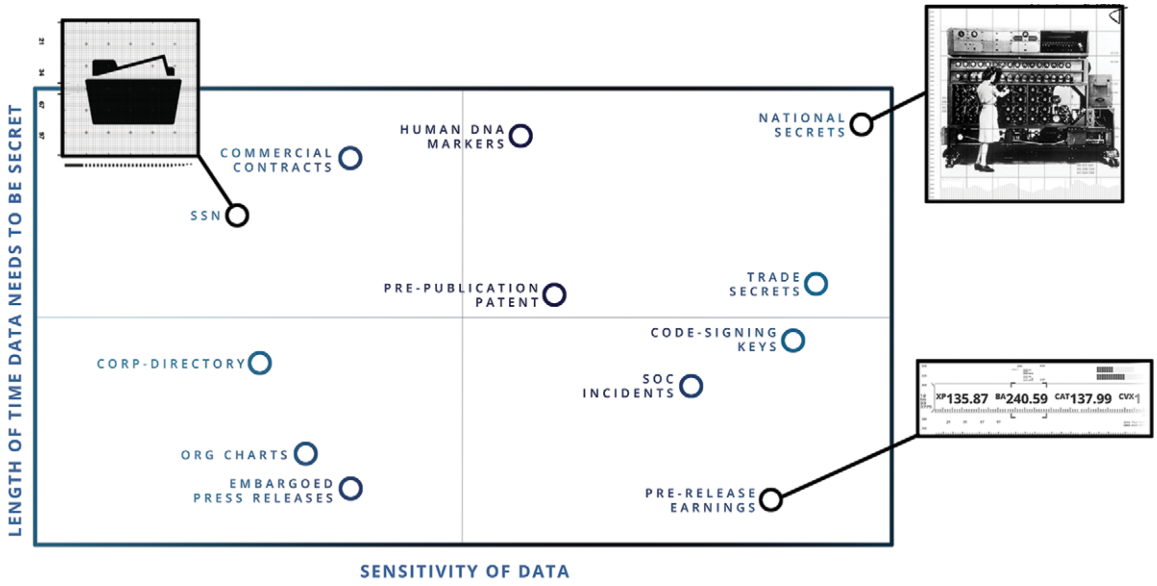
Rivest has acknowledged that small quantum computers do exist, and they have demonstrated that they can factor smaller numbers. But he characterizes these computers as merely "the foothills" of much bigger things to come in quantum. Rivest is confident in his belief that while it is possible that nation-states have more substantial capabilities, intelligence agencies are not decades ahead of the academic and other civilian quantum research and development progress.[9]

Conversely, a 2019 Global Risk Institute survey of 22 quantum computing experts agreed that the technology will definitely become a threat to encryption systems within 15 to 20 years.[10] Even Rivest acknowledges that while he hopes that the entities attempting to build quantum computers to break RSA will "fail," the work to "future-proof" encryption to repel quantum-powered attacks is without a doubt essential.[11] Most experts agree that quantum supremacy has plausible viability in the next decade, making it critical to invest and act today, as the impact of not taking action may result in the catastrophic scenario of adversarial nations holding a monopoly on universally reading the world's secrets.

A Problem for Today, Not Tomorrow

There is a common assumption that we will have stronger encryption algorithms by the time quantum cryptanalysis becomes practical and that we will know when our geopolitical rivals have that capability. But we are mistaken if we assume that the quantum risk is not a current problem simply because quantum computing is not presently viable. We should assume that nation-state adversaries are siphoning off encrypted data today that they will unlock tomorrow when quantum cryptoanalysis becomes practical. While it may seem like a stretch that an adversary would decrypt data five or ten years away, consider that today, in the year 2020, documents in the national archives related to the Kennedy Assassination nearly 60 years ago still retain redactions for current national security concerns. National secrets require long degrees of durability, especially when they contain sources and methods for the collection of intelligence. While encrypted, they still retain value over time. No matter how theoretical we may believe the capability to be, we must assume that our adversaries are already accessing our most sensitive data and communications.

More than 80 percent of all network traffic is encrypted as it travels over an untrusted network, the internet. But that protection is destined to be broken. Much of our critical data is in the cloud, accessible through collaboration platforms. In assessing the quantum risk to data in an environment, consider the sensitivity of the data not only



in terms of how important it is, but also how long it must be protected. In the graphic above, we have plotted some examples of data types in terms of importance and time of protection.

Social security numbers are plotted to the left. While we clearly never want to lose a social security number, we must be realistic given that an estimated 60 to 80 percent of social security numbers have already been compromised in data breaches. At the same time, they still serve as an identifier across a lifetime, so we place them higher on the chart.

Now contrast social security numbers with pre-release earnings data for a public company. Due to their importance prior to earnings day, they are plotted far to the right, but because of the brief time between quarter-end-close and public release, we place them near the bottom. Finally, for the reasons outlined above—the sensitivity of the content and the need to keep it confidential for an extended amount of time—national security secrets are plotted at the top right.

Systems that manage data in the top-right of the graph are the systems that need to be triaged first as new quantum-resistant technologies and products become viable. This should also help drive research priorities to understand the protocols and capabilities that are protecting secrets in the top-right of the chart.

Quantum Research and Development

Commercially viable quantum computing, comprising quantum computing chips with many thousands of qubits and requisite software, is still many years away. Progress in the field of quantum cryptography and cryptanalysis is difficult to gauge from public news reports; however, industry investment and research advancements suggest that the overall field of quantum computing is accelerating in both the private and public sectors.

In 2017, IBM unveiled a 50-qubit computer for laboratory research[12] and submitted a system called "Cryptographic Suite for Algebraic Lattices, or CRYSTALS" to the National Institute of Standards and Technology (NIST) for review and approval as a quantum resistant algorithmic system. That same year, Intel announced the development of a 17-qubit superconducting test chip,[13] and Microsoft announced Q Sharp, a quantum computing programming language compatible with Visual Studio.[14] D-Wave Systems announced general commercial availability of the D-Wave 2000Q quantum computer featuring 2,000 qubits.[15]

In 2018, Google announced the 72-qubit quantum chip called "Bristlecone."[16] Intel began testing a silicon-based spin-qubit processor and confirmed the development of a 49-qubit superconducting test chip called "Tangle Lake."[17] IonQ introduced the first commercial trapped-ion quantum computer, and QuTech successfully tested a silicon-based, 2-spin-qubit processor.[18]

In 2019, IBM announced the IBM Q System, the company's first commercial quantum computer featuring a 20-qubit system,[19] as well as its fourteenth experimental quantum computer featuring 53 qubits.[20] In September, it opened an IBM quantum computation center in New York and invested in Cambridge Quantum Computing, one of the first startups to become a part of IBM's Q Network.[21] In August 2019, the company announced that researchers had successfully encrypted a magnetic-tape storage drive and had plans to utilize the encryption technology across its product line.[22]

Also in 2019, D-Wave, the world's first commercial supplier of quantum computers announced a preview of its next-generation quantum computing platform incorporating hardware, software, and tools to accelerate and ease the delivery of quantum computing applications.[23] The company's systems are used by organizations such as NEC, Volkswagen, DENSO, Lockheed Martin, USRA, USC, Los Alamos National Laboratory, and Oak Ridge National Laboratory.[24]

In October 2019, Google announced that researchers working with its 53 qubit system had achieved "quantum supremacy," which CEO Sundar Pichai described as "a quantum computer capable of solving a problem that would take a classical computer an impractically long amount of time."[25] Known as Sycamore, the system was able to calculate a proof in 3 minutes and 20 seconds that showed the numbers created by a random number generator are in fact random. Theoretically, it would take Summit, one of the world's most powerful supercomputers, some 10,000 years to complete the same problem.[26]

Given the potential of quantum computing and the prevalence of cloud platforms, major cloud providers are taking the threat quantum computing may pose to their substantial businesses in the space seriously. Amazon Web Services, Google, Oracle, and others are working on both post-quantum cryptography algorithms and quantum-resistant solutions to protect their cloud offerings in the coming years.[27]

Private sector growth is expected beyond the cloud providers. Kenneth Research estimates that the market for global quantum computing was valued at $89.35 million in 2016 and is projected to reach $948.82 million by 2025, projected to grow at a compound annual growth rate of 30.02 percent from 2017 to 2025.[28] Gartner Research predicts that 20 percent of organizations will begin budgeting for quantum computing projects by 2023, and a survey by DigiCert found that one-third of organizations report having a Post-Quantum Cryptography (PQC) budget, and 56 percent are working on establishing a PQC budget. The same survey found that nearly 40 percent of respondents said it will be "somewhat" to "extremely" difficult to upgrade encryption to protect against quantum computer attacks.[29]

Nation-State Innovation Race

Beyond the corporate world, we must assume that every major nation-state power is investing in quantum technology, in part, to read protected data throughout the public and private sectors. The United States, Germany, Russia, India, Japan, and the European Union have increased investment in quantum research and development. What is notable is that the United States and U.S.-based corporations appear to be particularly focused on hardware platforms that will power the quantum computing revolution, whereas allies such as the EU and Japan and adversaries such as China appear to be focused more on the quantum applications that will run atop these platforms when they come of age.

- In 2018, the EU committed to spending $1.1 billion over 20 years on quantum research and development, including a special focus on building advanced quantum key distribution (QKD) into Europe's telecommunications networks.[30]
- In 2019, Russia unveiled a two-qubit quantum computer prototype,[31] and Germany's Fraunhofer-Gesellschaft applied research organization announced a partnership with IBM for quantum research.[32]
- Japan's Ministry of Internal Affairs and Communications submitted plans to spend $14 billion to implement post-quantum cryptography across its own IT landscape by 2025.[33]
- India's 2020 budget includes a five-year $1.12 billion allocation to the government's National Mission on Quantum Technologies and Applications.[34]
- The U.S government's Defense Advanced Research Projects Agency (*DARPA*) set up the first quantum communications network in 2003 and in subsequent years has seen increased investment.[35]
- In 2018, the White House issued a National Strategic Overview for Quantum Information Science and launched the National Quantum Coordination Office to coordinate quantum research and development across 14 U.S. government agencies.[36]

- In December 2019, the Trump Administration and Congress worked together to pass into law the National Quantum Initiative Act, which commits $1.2 billion to quantum focused efforts over five years.[37] This legislation also seeks to establish goals and priorities for a 10-year plan to establish the United States firmly in the world's leadership position in quantum computing. This includes the creation of a cross-government ecosystem, including;
    - National Quantum Information Science Research Centers within the Department of Energy.
    - Research and education centers in the National Science Foundation.
    - A "workshop of stakeholders" administered by NIST "to discuss the future measurement, standards, cybersecurity, and other appropriate needs for supporting the development of a robust quantum information science and technology industry in the United States."
    - A Subcommittee on Quantum Information Science under the National Science and Technology Council.
    - A National Quantum Initiative Advisory Committee to advise the president.[38]

The Obama Administration invested around $200 million per year on quantum research in a variety of areas during its eight years. The 2019 Trump Administration budget for Quantum Information Science raised annual spending to $430 million, a number that is expected to more than double by 2022.[39]

The Administration's fiscal year 2021 budget provides nearly half a billion dollars for quantum technology, including $25 million to construct a quantum internet that connects 17 national labs. Additionally, the budget allocated $718 million for NIST to drive "industry of the future" technologies such as quantum computing, artificial intelligence, 5G advanced communications, biotechnology, and advanced manufacturing. The budget invests over $14 billion in Department of Defense science and technology programs, but while quantum is included in this group of strategic emerging technologies, the exact allocation for quantum investment is not specified. That said, the budget is clear in that the Office of Science will receive $5.8 billion for early stage research, national laboratories, and construction projects, and $237 million of this investment is specifically committed to quantum information science research.[40]

The China Challenge

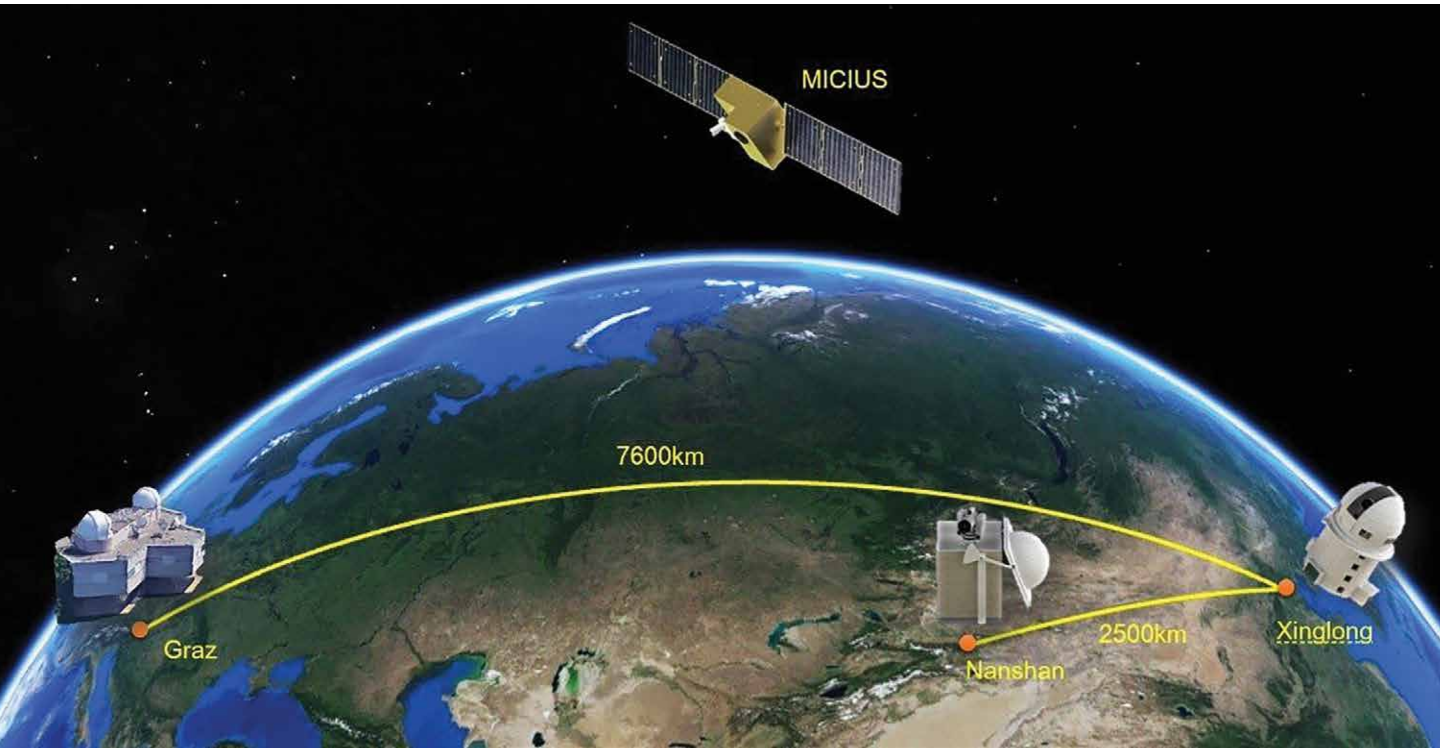
Geopolitical and technology thought leaders agree that the People's Republic of China (PRC) poses the greatest technological challenge to U.S. leadership in quantum computing. The Chinese government is quite public about its long-term national goal to become the global leader in critical emerging technologies, particularly those with military and commercial applications.

From a strategic perspective, China seeks to never again be subject to western or other foreign powers due to economic and technological inferiority. China's "century of humiliation," the period of European and Japanese imperialism between 1839 and 1949, is just yesterday for a 4,000-year old culture with a long memory. Historians note that China was victimized by industrialized foreign powers with technologically superior militaries from the 1842 Treaty of Nanjing at the end of the First Opium War with Great Britain to the end of the Second Sino-Japanese War in 1945. The Chinese government's very public initiatives like Made in China 2025 are part of a grander national strategy to create a reality in which the country will never again be at the mercy of foreign powers. [41]

To this end, China has included quantum informatics as a featured component within the PRC's

13th Five-Year Plan and the Made in China 2025 plan.[42] In November 2015, at the 5th Plenum of the 18th Party Congress, Chinese Premier Xi Jinping specifically called out quantum communications as a critical strategic technology project that must be prioritized and achieve major breakthroughs by 2030. Xi has continued, in subsequent years, to emphasize the importance of advancing indigenous innovation in quantum communications and other critical cyber and information technologies.[43]

Hartmut Neven, engineering director for Google's AI Quantum team, notes that China, as a society today, is capable of steering tremendous resources to gain the world's leadership position in quantum as well as other emerging technology fields,[44] and recent history suggests China is willing and able to invest in emerging technologies in a big way. The total quantum budget for China, including covert intelligence agency and military research and development budgets is not public. However, various public Chinese government investments and policy initiatives at multiple government levels and across sectors have shown a steady increase in quantum research. This leads observers to estimate that China's total spend may be in excess of $2.5 billion per year since 2017, a sum observers point out that makes investments from the United States and other countries pale by comparison.[45] From 1998 to 2018, China's central and provincial governments invested an estimated $987 million into research on quantum communication, quantum computation, and quantum metrology.[46] From 1998 to 2006, the National Natural Science Foundation of China (NSFC), the Chinese Academy of Science (CAS) Institute of Physics, the University of Science and Technology



Mozi, or Micius, named after the famous 5th century BCE Chinese scientist, is the first quantum communications satellite launched by China on August 16th, 2016; Illustration of the three cooperating ground stations (Graz, Nanshan, and Xinglong). (University of Science and Technology of China) of China (USTC), the Shanxi University, and other universities received around $10 million to pursue a variety of early stage projects.

From 2006 to 2010, China's 11th Five-Year Plan allocated an estimated $150 million to quantum research. The Ministry of Science and Technology (MOST) and CAS launched the "Long Distance Quantum Communication" and "Key Technology Research and Verification of Quantum Experiments at Space Scale" projects to support large-scale quantum communication research. From 2011 to 2015, the nation's 12th Five-Year Plan boosted quantum research and development funding to $490 million in areas such as quantum control (MOST), scientific research instruments and equipment development (NSFC), quantum experiments at space scale (CAS), coherent control of quantum systems and metrology physics in atomic systems (CAS), and continued work on building quantum secure communications (NDRC and CAS).

Notably the National Development and Reform Commission (NDRC), Anhui Province, Shandong Province, and CAS launched the Beijing-Shanghai Quantum Secure Communication Backbone project to accelerate industrial applications of quantum key distribution (QKD), a critical area for ensuring secure government and private sector communications.

Between 2016 and 2019, China's quantum research funding reached around $337 million under the nation's 13th Five-Year Plan. Notable projects launched in this period include the Quantum Control and Quantum Information National Key Research and Development Project.[47]

As a result of these efforts, Chinese researchers have achieved some notable milestones, such as the first quantum science satellite,[48] a quantum resistant encrypted network connecting Beijing and Shanghai, and related developments in QKD.

Observers note that while China seeks to dominate all areas of quantum computing, its most notable accomplishments in the field to date are focused on quantum communications rather than overall quantum computing research and development that would touch a variety of technology fields.[49] Patent consulting firm Patinformatics assesses which organizations are accumulating patents in critical emerging technology fields. According to the firm's 2018 report on quantum patents, Chinese organizations dominate patents on quantum applications, with nearly twice as many publications as the United States in 2017, with the applications very focused on cryptology. Since 2012, approximately 72 percent of the academic patent families published in quantum information technology are from Chinese universities, with the United States coming in a distant second place with a mere 12 percent.

The University of Science and Technology of China, the Chinese Academy of Sciences, and Beijing University have established significant portfolios associated with the hardware aspects of quantum applications that could enable China to dominate quantum cryptology and communication. Patinformatics asserts that the leading quantum computer manufacturers tend to be based in North America while the greatest accomplishments by Chinese and other Asian entities are focusing on quantum cryptology and communication.[50] "North American organizations may control the (quantum) computer," the report observed. "But Asian organizations may end up controlling how those machines are used." [51]

The annual Five-Year Plan investments might not capture the full picture of China's "all of nation" commitment to quantum research and development. The central government and regional governments are teaming to build the National Laboratory of Quantum Information Sciences in the capital of eastern Anhui province. The governments boast that the research facility will be the largest of its kind in the world, and even assert that its research will produce quantum technologies "of immediate use" to the country's military.[52] The new institution has received an initial $1.06 billion in funding and the governments involved plan to invest an additional $14.76 billion over the next five years.[53]

Other regionally funded research is taking place through the Anhui Quantum Science Industry Development Fund, Shandong Province Quantum Technology Innovation and Development Program, and an emerging quantum ecosystem in Jinan Hi-tech Zone's "Quantum Valley".

China's private sector is also playing a role with internet giant Alibaba, planning to invest $15 billion in technologies such as artificial intelligence and quantum technologies, complementary to the government's own work.[54]

In addition to funding research, the PRC has also worked, through its Thousand Talents Plan, to recruit talented quantum technologists by providing incentives. As of 2018, the program had incentivized the return of around 7,000 quantum computing specialists studying or working abroad, including Pan Jianwei, known as the nation's "father of quantum."[55] Pan pursued his doctorate at the University of Vienna and conducted research at the University of Heidelberg before rallying several Chinese colleagues back to China to drive quantum research and development for his home government.[56]

China's drive to lead the world in dominating the most pivotal 21st century technologies is currently unmatched by the United States. Washington is simply not investing in these technologies at the level the country invested during the Cold War to dominate the most pivotal technologies of the last century. During the Cold War, the United States invested in advanced technologies because it realized that it could not afford to lose the technology race to a hostile power like the Soviet Union. Losing that race in the most critical technologies that defined the last century and remain critical to this day represented nothing less than an existential threat to the nation. Today, China's "all of nation" investments in technologies such as quantum show that their leadership recognizes that the nation-state that dominates these technologies will have significant power in the 21st century in much the same way the United States dominated the last 70 years of geopolitics.

Developing Quantum-Resistant Algorithms

The U.S. Department of Commerce's National Institute of Standards and Technology (NIST) is leading a selection and standardization effort for proposed quantum-resistant algorithms from academic and governing bodies around the world.[57] The goal of post-quantum cryptography research is the development of cryptographic systems that are secure against both quantum and classical computers and can interoperate with existing communications protocols and networks. Of the 69 initial quantum-resistant algorithms proposed to NIST, 12 were broken or attacked within three weeks and, after three years of evaluation, NIST has managed to narrow the field of candidates to 26.

While NIST's work in this area is promising, it must move faster and should receive greater investment by government and industry. Cooperation from across both groups is essential to developing and understanding quantum-resistant algorithms. Lack of funding for development of quantum-resistant algorithms is also part of the problem. NIST's quantum research budget is $30 million, just 0.0006 percent of the U.S. federal budget; too little to solve a problem that is such a serious threat to national security.

Beyond the Math

Organizations, both public and private, must commit to starting the technical work on elements beyond just the new mathematical algorithms that will power post-quantum cryptography. We must begin to inventory, understand, and retool the protocols and systems that will be vulnerable to quantum attacks.

Planning the Rollout

Retooling our network and data protection solutions will take time; not only to develop the technology, but to roll it out throughout the world's compute and network deployments. Once replacement algorithms are complete, the implementation of related network protocols, key management, and other supporting technologies will take time, as will the integration of the algorithms into commercial products. To hasten this, organizations should commit to building post-quantum action plans that measure time and impact sensitivity so that they are ready to rapidly retool the systems protecting their data as the post-quantum ecosystem is ratified. Organizations can start prioritizing data that needs protection today, including what data is accessed or stored by vulnerable paradigms.

TLS 1.3.

Additionally, organizations and technology industry partners can move their network traffic to Transport Layer Security (TLS) version 1.3, the latest generation of technology that secures computer-to-computer communications. TLS 1.3 removes RSA encryption key negotiation options and requires Diffie-Helman encryption. The main driver for this is to prevent the loss of a private RSA key which would result in the ability to decrypt all sessions based on it. The side benefit is that every session has unique Diffie-Helman key exchanges. While Diffie-Helman is not quantum safe, the move would require an adversary to break a specific session using quantum cryptanalysis on that session as compared to breaking the RSA key on the publicly available certificate. This requires adversaries to possess significantly higher compute scalability as well as the encrypted stream prior to beginning cryptanalysis. While this mitigation does not remove the need to aggressively move to a post-quantum ecosystem, it does provide a tangible action organizations can take today.

More Post-Quantum Standards

Technologists should also work to develop additional standards, protocols, and products for a post-quantum ecosystem, such as working with the Internet Engineering Task Force to support a post-quantum TLS or code-signing standards. Furthermore, once these standards come to fruition, platforms need to be plug-and-play to facilitate rapid adoption.

A Race We Can't Afford to Lose

The United States and its allies are in a technology race with China and other geopolitical rivals, and quantum computing is an important front of that competition—a competition we cannot afford to lose. While quantum computing still has many challenges ahead, including the time to achieve true viability, the actions we take today will have profound impact on whether we are protected when that day comes.

There is a reasonable chance that nation-states will have this computing power in the foreseeable future. It is naïve to assume that the rest of the world will immediately become aware of the viability of pragmatic implementations of quantum cryptanalysis and take action to narrow the technology gap between nation-states.

We should be realistic and understand that the largest investors in this area are committed to achieving their objectives and supplanting U.S. technology and strategic leadership. In doing so, they can tighten their grip to better determine their own geopolitical destiny in the same way the United States has since the end of the Second World War.

Quantum is both a national security threat and a potential strategic advantage. To ensure our place in the future, we must focus on both elements today. PRISM

Endnotes

[1] "Quantum Information Research In China", Qiang Zhang et al 2019 Quantum Sci. Technol. 4 040503 and Trump Administration Fiscal Year 2021 budget outline: https://www.whitehouse.gov/wp-content/uploads/2020/02/budget_fy21.pdf.

[2] James Gannon *(2002), "Stealing Secrets, Telling Lies: How Spies and Codebreakers Helped Shape the Twentieth Century", Washington, D.C.: Brassey's, ISBN 978-1-57488-367-1.*

[3] "Speech to the National Military Intelligence Association", *Aerospace Daily*, September 25, 1983.

[4] F. W. Winterbotham, "*The Ultra Secret*", Dell, August 15, 1975; Gordon Welchman, "*The Hut Six Story: Breaking the Enigma Codes*", McGraw-Hill, March 1, 1982.

[5] Morgan Wright, "America's Enigma Problem with China: The Threat of Quantum Computing", *The Hill*, March 8, 2018.

[6] Brian Wang, "Quantum Annealer 10,000 times faster than classical computers by 2023", *Next Big Future*, June 23, 2017.

[7] P.W. Shor, (1994). "Algorithms for quantum computation: discrete logarithms and factoring". *Proceedings 35th Annual Symposium on Foundations of Computer Science*. IEEE Comput. Soc. Press: 124–134.

[8] Shaun Nichols, "'I give fusion power a higher chance of succeeding than quantum computing' says the R in the RSA crypto-algorithm", *The Register*, February 26, 2020.

[9] Numberphile, Quantum Computing and Other Extras with Ron Rivest, https://www.youtube.com/watch?v=tX7e7CgWrvM.

[10] Quantum Threat Timeline, Dr. Michele Mosca, Dr. Marco Piani, Global Risk Institute, October 19, 2019.

[11] Sara Peters, "Cryptographers Panel Tackles Espionage, Elections, and Blockchain", *Dark Reading*, February 26, 2020.

[12] Will Knight, "IBM Raises the Bar with a 50-Qubit Quantum Computer", *MIT Technology Review*, November 10, 2017.

[13] Will Knight, "Quantum Inside: Intel Manufactures an Exotic New Chip" *MIT Technology Review*, October 10, 2017.

[14] Peter Bright, "Microsoft makes play for next wave of computing with quantum computing toolkit", *Ars Technica*, September 25, 2017.

[15] D-Wave Systems Press Release, "D-Wave Announces D-Wave 2000Q Quantum Computer and First System Order", January 24, 2017.

[16] Emily Conover,"Google moves toward quantum supremacy with 72-qubit computer", *Science News*, March 5, 2018.

[17] Jeremy Hsu, "CES 2018: Intel's 49-Qubit Chip Shoots for Quantum Supremacy", Institute of Electrical and Electronics Engineers, January 9, 2018.

[18] Martin Giles,"Old-fashioned silicon might be the key to building ubiquitous quantum computers", *MIT Technology Review*, February 15, 2018.

[19] Frederic Lardinois, "IBM Unveils Its First Commercial Quantum Computing", *Tech Crunch*, January 8, 2019.

[20] Stephen Shankland, "IBM's New 53 Qubit Quantum Computer Is Its Biggest Yet", *CNET*, September 18, 2019.

[21] "Quantum Computing: How to Invest in it and Which Companies are Leading the Way", NASDAQ.com, February 11, 2020.

[22] Adam Janofsky,"Companies Explore Encryption that Withstands Quantum Computing", *Wall Street Journal*, September 9, 2019.

[23] D-Wave Press Release, "D-Wave Previews Next Generation Quantum Computing Platform", February 27, 2019.

[24] "Quantum Computing: How to Invest in it and Which Companies are Leading the Way", NASDAQ.com, February 11, 2020.

[25] "What Our Quantum Computing Milestone Means," Sundar Pichai, Google Blog, October 23, 2019.

[26] Chris Holt, "The U.S. Again Has the World's Biggest Supercomputer", *Engadget*, June 8, 2018.

[27] Alex Weibel, "Round 2 Hybrid Post-Quantum TLS Benchmarks", *AWS Security Blog*, April 13, 2020; Barbara Darrow, "How Much Should CIOs Care About Quantum Today", *CIO Magazine*, July 13, 2018; Jeremy Kirk, "Google Tests Post-Quantum Crypto," *Bank Info Security*, July 11, 2016.

[28] "Quantum Computing Market Size Growth Opportunity and Forecast to 2025", *Market Watch*, November 5, 2019.

[29] Dan Timpson, "Staying Secure in a Post-Quantum World", *Forbes*, March 12, 2020.

[30] Elizabeth Gibney,"Europe plans giant billion-euro quantum technologies project", *Nature*, April 21, 2016.

[31] "First Prototype of a Quantum Computer on Superconductive Materials Successfully Launched in Russia", https://en.misis.ru/university/news/misc/2019-10/6277/.

[32] Fraunhofer Press Release, "IBM and Fraunhofer team up to promote quantum computing in Europe", September 10, 2019.

[33] "Japan Aims to Put Quantum Cryptography to Practical Use", *Japan Times*, August 24, 2019.

[34] "India Finally Commits to Quantum Computing, Promises $1.12B Investment," *The Next Web*, February 3, 2020.

[35] Quantum Key Distribution Network, Defense Advanced Research Projects Agency https://www.darpa.mil/about-us/timeline/quantum-key-distribution-network.

[36] "White House Launches National Quantum Coordination Office", Government Innovators Network, March 2019.

[37] Tajha Chappellet-Lanier, "White House Launches National Quantum Coordination Office", *Fedscoop*, March 4, 2019.

[38] Tajha Chappelet-Lanier, "President Trump launches National Quantum Initiative Advisory Committee", *Fedscoop*, September 3, 2019.

[39] "Why Should I Care About Quantum Computing", *The Cipher Brief*, March 19, 2020.

[40] Trump Administration Fiscal Year 2021 budget outline: https://www.whitehouse.gov/wp-content/uploads/2020/02/budget_fy21.pdf.

[41] Martin Jacques, *When China Rules the World: The End of the Western World and the Birth of a New Global Order* (Penguin Press, New York, NY), 2009.

[42] "Thirteenth Five-Year Science and Technology Military-Civil Fusion Development Special Plan" (Full Text), September 26, 2017, http://www.aisixiang.com/data/106161.html.

[43] Elsa B. Kania and John K. Costello, "Quantum Hegemony: China's Ambitions and the Challenge to U.S. Innovation Leadership, Center for the New American Century", September 12, 2018.

[44] Center for Strategic and International Studies (CSIS) speaking engagement, "American Innovation in the Quantum Future", featuring Hartmut Neven, Engineering Director, Google AI and Quantum Team, January 20, 2020.

[45] Arthur Herman,"The Quantum Computing Threat to American Security", *The Wall Street Journal*, November 10, 2019.

[46] "Quantum Information Research In China", Qiang Zhang et al 2019 Quantum Sci. Technol. 4 040503.

[47] "Quantum Information Research In China", Qiang Zhang et al 2019 Quantum Sci. Technol. 4 040503.

[48] "China launches world's first quantum science satellite," *Physics World*, August 16, 2016.

[49] Elsa B. Kania and John K. Costello, "Quantum Hegemony: China's Ambitions and the Challenge to U.S. Innovation Leadership, Center for the New American Century", September 12, 2018.

[50] Patinformatics, Quantum Information Technology (QIT): A Patent Landscape Report, 2018.

[51] Patinformatics, Quantum Information Technology (QIT): A Patent Landscape Report, 2018.

[52] "Hefei's Construction a National Science Center from 'Design' to 'Construction Map,'" *China News Network*, September 12, 2017.

[53] Stephen Chen, "China building world's biggest quantum research facility," *South China Morning Post*, September 11, 2017,; and "Hefei's Construction a National Science Center from 'Design' to 'Construction Map'", *China News Network*, September 13, 2017.

[54] "Alibaba to spend more than US$15bn on technology research with launch of collaborative academy," *South China Morning Post*, October 11, 2017.

[55] "China's plan to recruit talented researchers," *Nature*, January 17, 2018; and "China's programme for recruiting foreign scientists comes under scrutiny," *South China Morning Post*, November 3, 2017.

[56] Jeanne Whalen,"The quantum revolution is coming and Chinese scientists are at the forefront," *The Washington Post,* August 8, 2019.

[57] U.S. Department of Commerce, National Institute of Standards and Technology (NIST) https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization.