The Heritage Foundation

SPECIAL REPORT

No. 268 | APRIL 5, 2023

Beating China in the Race for Quantum Supremacy

Dustin Carmack

Beating China in the Race for Quantum Supremacy

Dustin Carmack

SPECIAL REPORT

No. 268 | APRIL 5, 2023

CENTER FOR TECHNOLOGY POLICY

About the Author

Dustin Carmack is a former Research Fellow for Cybersecurity, Intelligence, and Emerging Technologies in the Border Security and Immigration Center at The Heritage Foundation. The author is grateful to Alexandra Yoeckel, former Research Assistant in the Border Security and Immigration Center, for her assistance.

This paper, in its entirety, can be found at **http://report.heritage.org/sr268**

The Heritage Foundation | 214 Massachusetts Avenue, NE | Washington, DC 20002 | (202) 546-4400 | heritage.org

Beating China in the Race for Quantum Supremacy

Dustin Carmack

How the United States positions itself for success in the era of quantum computing, sensing, and encryption will have ramifications for the future of manufacturing, the development of medical cures, the national security needs of the military, the ability to protect information, and more. In addition, which country reaches quantum supremacy first will determine global power dynamics. The United States cannot allow power to be centralized in the hands of one actor, especially the Chinese Communist Party. For the U.S. to lead in quantum technology, it must employ a whole-of-government and whole-of-industry approach alongside foreign allies and partners. While many challenges remain in bringing quantum technology to scale, the scientific race and outcome amongst nations, militaries, academia, and technology companies will define the 21st century.

China's potential to eclipse the United States in a quantum-technology arms race is an issue of acute concern to U.S. national security. Within the past decade, China has identified quantum capabilities as a mission-critical technology for its economic and national security measures. China's developments in the quantum arena have drawn a heavy-handed response from the United States, with the Department of Commerce placing multiple Chinese quantum computing (QC) firms on an export blacklist and the Department of Defense (DOD) issuing a memorandum calling on the public and private sector to develop and adopt post-quantum encryption standards.[1]

However, developments in quantum technology are not limited to the Chinese mainland. Quantum technologies are being developed at a breakneck pace in research labs around the globe. Quantum computers exponentially use quantum physics to make computational speeds faster than those of legacy computer systems. The potential ability of nations like China and Russia to conduct quantum computational functions puts nearly every encrypted file in the United States—for both the public and private sectors—at risk of decryption and exploitation. At the same time, various quantum science fields present challenges and opportunities by introducing new defense and intelligence capabilities and systems. U.S. policies must focus on expediting post-quantum encryption throughout the government, prioritizing national security systems while expanding international collaboration with allies and partners, and fiercely protecting quantum intellectual property (IP).

The Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party has an opportunity to oversee the Biden Administration's quantum policy developments, provide further legislative recommendations on quantum policy to authorizing committees, and press government-wide movement toward understanding quantum applications for defense and non-defense purposes.

Computing Overview

Quantum computing is not the progression of traditional computing—it transcends the boundaries of physics. Using the principles of quantum mechanics, quantum computations use subatomic particles, such as photons or electrons in the form of quantum bits, to allow the particles to exist in more than one state at the same time.

Traditional Computing. Traditional computing uses binary units, known as "bits," to store information using complex strings of ones and zeroes. Traditional computers can read, write, and delete data at will by assembling microscopic electrical circuitry to transmit and store bits. By reading these bits and their stored values, the computer can generate user interfaces, run complex mathematical functions, and execute elaborate lines of code. While infinitesimally small, computational parts that run on the latest processing chips still must abide by the laws of physics.

Quantum Computing. By transcending the boundaries of classical physics and using quantum physics, QC can produce results that outclass its conventional counterparts by orders of magnitude. While traditional computing uses bits to transport and store information, QC uses "qubits," short for "quantum bits," to assemble programs and execute code. Qubits use two physical mechanics unique to the quantum plane: superposition and entanglement. While a bit can hold only a value of 0 or 1, quantum superposition dictates that a qubit can have a spectrum of values between 0 and 1 co-occurring at any given time. When a qubit is "observed," it will

FIGURE 1

Fundamental Computing Concepts

Classical computing
Light switch is either On or Off

Quantum computing
Light on a dimmer switch, with a continuum of possible states between On and Off

SOURCE: Karti Mahendran et al., "Quantum Computing: Hype or Reality?" Deloitte, July 2021, p. 3, https://www2.deloitte.com/content/dam/Deloitte/au/Documents/deloitte-au-quantum-computing-hype-reality-290721.pdf (accessedmarch 28, 2023).

SR268 heritage.org

collapse into either a positively or negatively charged state. An array of qubits could simultaneously exhibit the characteristics of every possible combination of positive and negative charges, leading to exponential performance increases.

Quantum entanglement is the idea that by observing one qubit, one can necessarily infer the polarization of another "entangled" qubit, no matter the physical distance separating the two. Both superposition and entanglement allow computational efficiency of which traditional computers will never be capable. Thus, quantum computers are not a more powerful version of a traditional computer. They use an entirely different technology based on deeper scientific understanding, which will affect virtually all aspects of society dramatically.

Recent Quantum Developments. It is not surprising that researchers worldwide are driving the rapid growth of QC capabilities, considering the unrivaled potential of quantum technology. With nearly $30 billion[2] being spent across the globe to facilitate quantum development, it is clear that "quantum computing is at the forefront of national initiatives."[3]

The push for advancements in quantum technology comes as the scientific and military communities develop new applications for QC. Applications include quantum-powered artificial intelligence (AI),[4] quantum cryptanalysis,[5] and quantum-sensing technology.[6]

The future of quantum technologies will be heavily based on the modalities of quantum computation. Which variable subatomic particle is being manipulated will play a significant factor in the future of commercial ecosystems. Researchers are continuously learning new ways to control modalities for quantum computation through superconducting qubits, silicon quantum dots, trapped ions, neutral atoms, photonic qubits, and topological qubits.

- **Superconducting qubits.** Quantum computation using superconducting qubits will manipulate an electromagnetic pulse to control the magnetic fluctuation, an electric charge, or the "phase difference across a Josephson junction," a device with "nonlinear inductance and no energy dissipation."[7] Advantages include the ability to design electrical circuits to achieve the subtleties needed to test and scale the number of qubits. Disadvantages include these circuits' susceptibility to quantum noise and their inability to hold quantum states for longer periods of time, their larger sizing, and their being more error-prone at scale due to differences in circuit structures and "decoherence" in the qubits. Google, IBM, and Intel are significant researchers in this modality field and have shown promising abilities to scale the number of qubits.[8]

- **Silicon-quantum-dot qubits.** These qubits are metal-free, biologically compatible quantum dots—semiconductor nanocrystals, which are particles only nanometers in size that can contain optical and electronic properties. Possible advantages include a smaller size than other qubit technology silicon spin qubits, which are made from single electrons, abundant material to reproduce, and coinciding scalability with existing silicon-based semiconductor fabrication manufacturing.[9] Different modalities have shown maturing development in the number of qubits, and silicon quantum dots have shown recent promise and potential.

- **Trapped-ion qubits.** Trapped-ion computing uses charged atomic particles within electromagnetic fields in a shared trap where lasers induce a qubit(s) coupling. The modality has exhibited some of the most promising QC capabilities. Honeywell, IonQ, Universal Quantum, and Alpine Quantum Technology have announced rapid developments in this modality in recent years and benefit from fewer errors than other modalities and longer-lasting quantum states with individual ions. Disadvantages include slower interactions than superconducting qubits and limitations in how many ions can fit in a trap to allow interaction. Ongoing work is occurring in this field to link chains of qubits using photons or interconnecting ions around a giant chip.[10]

- **Neutral-atom qubits.** This modality is similar to trapped ion qubits, except with uncharged atoms. Using lasers, alkaline earth metal atoms are trapped to hold in position. Advantages include being able to operate at room temperature and lengthy coherence times with the possibility to scale into a large single qubit.[11] Alkali-metal atoms have disadvantages as the "electronic spin states used to store quantum information can be corrupted by the light field used for trapping the atoms."[12] Quantinuum, Rigetti, Atom Computing, and IonQ are companies currently active in this modality sector.[13]

- **Photonic qubits.** Photonic computation happens when a photon and atom interact in a quantum state using photons as qubit representation. Advantages include "simple components, the ability to run a variety of quantum operations, and most importantly, photonic quantum computers can perform at room temperature, which reduces the size of the extreme cooling systems."[14] Photonic quantum capabilities could also integrate into existing fiber-optic-based telecommunications infrastructure, thus opening possibilities in quantum communication networking and quantum Internet.[15] Some disadvantages include multiple qubit gates being challenging to construct, photon loss during operations, and difficulty detecting. Recent breakthroughs have shown promise in overcoming some difficulties by developing a photonic quantum chip that is "programmable, can execute multiple algorithms, and is potentially highly scalable."[16] Companies in the field include Xanadu Quantum Technologies, Orca Computing, Psiquantum, and Tundrasystems Global.

- **Topological qubits.** Using pairs of Majorana Zero Modes (MZMs), a specific type of quasiparticle that acts as only half of an electron, topological qubits would theoretically layer on superconducting materials and be nearly impervious to noise that plagues other modalities. The theory of this possibility bore out in a 2018 *Nature* study that was later retracted for "insufficient scientific rigour."[17] Since then, though, Microsoft has heavily invested in research to prove the reliability of the physics needed to build scalable topological qubits, believing that they show the most promise for constructing reliable, mountable QC capabilities. Researchers were recently able to produce a topological phase and measure the topological gap to, in turn, measure the stability of the phase.[18] There remain many questions about whether a topological qubit can be constructed. Still, if it can be done, there could be exponential possibilities in stability, size, and speed compared to other qubit modalities.

The U.S. Quantum Computing Program

Quantum computers will drive innovation across government and the American economy. As such, private-sector actors are driving many of the developments in quantum technology within the U.S. Through companies like Google,[19] Honeywell,[20] IBM,[21] Amazon,[22] Intel,[23] Lockheed Martin,[24] Microsoft,[25] Northrop Grumman,[26] D-Wave,[27] Rigetti Computing,[28] and other quantum start-ups, it is clear that America's technological leadership is headed toward groundbreaking changes if the U.S. maintains a strategic edge over adversarial competitors. Several private-sector companies have hit milestones in QC technology. In 2019, Google unveiled a 54-qubit superconductor-based quantum processor that could solve a complex problem in three minutes and 20 seconds, which would take a traditional computer 10,000 years to solve.[29] Then, in November 2021, IBM launched the Eagle, a 127-qubit computer, which surpasses China's 113-Qubit Jianzhong Chinese machine and is designed to operate in the cloud.[30] This computer follows IBM's initial successes with the 27-qubit Falcon process unveiled in 2019 and the 65-qubit Hummingbird processor released in 2020.[31] IBM announced a 433-qubit Osprey processor in November of 2022 with the goal of an 1121-qubit Condor processor in 2023.[32]

As private corporations have dominated the production and innovation of quantum technology, the U.S. government has pledged at least $1.2 billion in sizeable public funding projects. In addition, numerous ongoing projects fall outside the $1.2 billion pledge under the National Quantum Initiative.[33] The Biden Administration released the National Security Memorandum on promoting QC in May 2022. This memorandum outlines the policy to drive the American quantum sector, mitigate the risk of threats to the nation's cyber, economic, and national security domains, and dangers to encryption.[34] In addition, executive action agencies, such as the Defense Advanced Research Projects Agency (DARPA), continue to work on pivotal investments in breakthrough national security technology. In January 2022, DARPA moved to a phase-two program to develop quantum computers capable of solving complex optimization problems on Rigetti Computing's 80-qubit system Aspen-M.[35] And, DARPA continues to research the physical composition of quantum technology.

In 2022, President Joe Biden signed the Creating Helpful Incentives to Produce Semiconductors (CHIPS) and Science Act of 2022, which, in addition to funding subsidies for semiconductor fabrication production in the United States, authorized additional investments in quantum research programs.[36] The CHIPS and Science Act includes the Quantum User Expansion for Science and Technology (QUEST) Act, which allows $30 million per year over five years to increase researcher access to "leading edge quantum computing resources." Other authorizations included a program for quantum network infrastructure to research networking devices and methods; a supply chain for networking technologies using quantum, material science, and experimental tools; and testbeds for quantum networking. Finally, the CHIPS and Science Act authorized a pilot program to advance the "next generation" of quantum-capable students and teachers in quantum mechanics.[37]

The Intelligence Advanced Research Project Activity (IARPA) is developing quantum technologies for application to the U.S. Intelligence Community and government. Under recent and current programs, such as quantum-enhanced optimization (QEO), which, with coordination from the University of Southern California, led a consortium of universities and private companies, began developing quantum computers that are 10,000 times faster than classical computers with the use of quantum annealers.[38]

The annealers allow "high coherence" time for qubits to maintain sustained periods such as superposition when in two or more states.[39] Other programs, such as Logical Qubits (LogiQ), are working to create an error-corrected logical qubit that will encode quantum information and enhance the performance of the block.[40] Entangled Logical Qubits (ELQ) is a program that advances "universal fault-tolerant quantum computing (UFTQC) by demonstrating high-fidelity entanglement between error-corrected logical qubits using a modular architecture."[41] These programs aim to improve the value of collected data from all sources by developing quantum-enabled sensors, improved collection techniques, and, more precisely, target information for intelligence, surveillance, and reconnaissance (ISR) roles.[42]

Some challenges and risks with QC include the possibility of a "zero-day" scenario in which traditional encryption regimes are compromised worldwide.[43] In July 2022, the National Institute of Standards and Technology (NIST) announced the first series of quantum-resistant computer algorithms, a significant development to secure digital information in a post-quantum world. The NIST identified four encryption tools designed to withstand future hacking by a quantum machine. Referred to as

Crystals-Kyber, Crystals-Dilithium, Falcon, and SPHINCS+, the four algorithms will be finalized in roughly two years. These algorithms, in practice, will be able to withstand an assault of a future quantum computer that could crack the security "used to protect privacy in the digital systems we rely on every day—such as online banking and email software."[44]

The news of the NIST algorithms also signals the beginning of the final phase of the NIST's research, one step closer to developing a public-key cryptology standard.[45] The NIST development is a massive step toward protecting entities for the U.S. government and personal and private information for the American public. While identifying the algorithms is a significant step toward forming the basis of new standards and greater resilience of encryption mechanisms, extensive work remains to be done. The NIST selected 12 companies to guide the nation's cryptographic standards. The companies collaborating with NIST include Amazon Web Services (AWS), Cisco Systems, Cryptosense, Crypto4A Technologies, InfoSec Global, ISARA Corporation, Microsoft, Samsung, SandboxAQ, Thales, Thales Trusted Cyber Technologies, and VMware.[46] In conjunction with the NIST, the National Security Agency (NSA) recently released new encryption standards algorithms to transition to quantum-resistant networks for national security system owners and vendors, with accompanying standards coming later.[47] Recent advances in AI have demonstrated the difficult tasks ahead of post-quantum encryption. One of the new NIST-recommended encryption algorithms is vulnerable to being broken, for example, after Swedish researchers used recursive-trained AI combined with side-channel attacks, showing the need to account for rapid advances happening in AI.[48]

The risks associated with QC will begin during the implementation stages as technology successfully transitions to operational applications in industry and the "majority of risk likes in the vendors." So it is critical to involve essential companies that provide the foundation for IT security and management through implementing critical infrastructure, updating technologies, and moving unsupported technology out of the ecosystem.[49] Collaboration between these companies as well as with the government and policymakers will help to mitigate the risk, enable the growth of quantum technologies by ensuring safeguards for usage, and bring the U.S. one step closer to reaching these technological breakthroughs and novel applications.

European Quantum Computing Programs

The European Union is also making strides to develop quantum technology production and research. Quantum Flagship, a 10-year research initiative led by the European Union, was launched in 2018 with an expected budget of €1 billion (around $1.06 billion) to pursue quantum computing, simulation, and communication.[50] Other areas included in the flagship project are basic research in quantum physics, quantum metrology, and sensing. Quantum Flagship consists of a project building a future communication network based on quantum key distribution (QKD), a technology that uses the principles of quantum mechanics for cryptography.

In 2019, seven member states (Belgium, Germany, Italy, Luxembourg, Malta, the Netherlands, and Spain) signed a declaration agreeing to work together to make a quantum communication infrastructure (QCI) network available in Europe. The QCI would boost European quantum technology, cybersecurity, and industrial competitiveness capabilities. Additional states (Austria, Bulgaria, Croatia, Czech Republic, Cyprus, Denmark, Estonia, Finland, France, Greece, Hungary, Ireland, Latvia, Lithuania, Poland, Portugal, Romania, Slovakia, Slovenia, and Sweden) joined subsequently. The infrastructure network would integrate quantum technologies into conventional communication infrastructures between earth and space-based transmissions to connect long distances across the European continent and globally.

Recently, the European Space Agency, supported by the French and Austrian space agencies, has been working with satellite company Thales Alenia Space on the TeQuantS project to develop future quantum information networks and cybersecurity applications to "demonstrate the performance of long-distance quantum satellite links."[51]

An abundance of innovation is coming from U.S. allies in the EU. In October 2021, the European Commission announced the creation of a prototype for the most miniature quantum computer based on industry standards.[52] The EU is also building a 50-qubit variant of the compact quantum computer based in Innsbruck, Austria.[53]

The Delft University of Technology in the Netherlands recently published research indicating the ability to use quantum teleportation to send data across three physical locations.[54] Albert Einstein theorized this to be impossible, and "spooky action at a distance" allows data transfer between locations without moving the physical matter that holds it.[55]

In 2021, Germany also announced an investment of €2 billion (around $2.12 billion) in quantum sciences. Ten leading German corporations jointly founded the Quantum Technology and Application Consortium. The newly established consortium aims to further develop the existing fundamentals of QC into usable industrial applications.[56]

Lastly, the United Kingdom has allocated £1 billion toward a collaborative quantum project using industry, academia, and government resources.[57]

Russian Quantum Computing Programs

While less robust than the U.S., China, or European counterparts, Russia also competes in the quantum arms race. By 2020, the Russian government established the National Quantum Laboratory (NQL) under the state nuclear corporation Rosatom. Russia's NQL aims to produce a 100-qubit quantum computer by the end of 2024;[58] however, the rate of development may be halted. With the war in Ukraine continuing unabated, industries are affected by war and economic sanctions. Leaders of quantum companies and research institutions in Russia must anticipate the ramifications of their invasion on other industry sectors.

Additionally, as Russia continues its focus on defeating Ukraine, its pariah-like status could affect its ability to develop and acquire new technologies, especially quantum technology. Like other industries, the most apparent effects will be on supply chains that provide everything from raw materials to highly engineered equipment that make up quantum computers and sensors. Current and additional technology export restrictions will likely delay Russia's R&D in quantum sciences.

Before it invaded Ukraine, the Russian government incorporated quantum technologies into its technological road map. In 2019, the Russian government signed multiple agreements with several state-owned corporations to begin development of quantum technology. Russian Railways is managing the development of quantum communications, and Rosatom is driving the growth of QC and material sciences. Rostec is developing quantum sensors, and both Rostelecom and Rostec are heading the development of Russia's 5G infrastructure.[59]

Near the end of 2021, Russia saw some tangible outcomes. First, a Russian scientist at Rosatom developed a four-qubit ion quantum-computer prototype.[60] Second, the National University of Science and Technology completed a prototype two-qubit computer capable of solving Grover's Quantum Algorithm, a fundamental quantum computational performance benchmark.[61] These two developments have made minimal public announcements about Russia's quantum industry. Still, Moscow is continuing to back state-owned projects seeking to reduce economic and intellectual dependence on the West.

As the war in Ukraine continues, export controls that the United States and other nations have placed on Russia have already affected domestic production, semiconductor, aerospace, and automotive industries.[62] With supply-chain issues moving everything in the quantum industry from raw materials to equipment that makes quantum computers and sensors, innovation and production from Russia are jeopardized.

But while Russia feels the impacts of sanctions on its industry, the rest of the world will also experience reverberating effects on the quantum industry. For example, the helium supply is being disrupted, which is essential to the operation of superconducting quantum computers. Helium reserves are being depleted as Russian state-owned company Gazprom brought 20 million m^3 of new helium capacity online when it opened three helium production lines at a gas-processing plant in southeastern Russia. This logistics center is intended to also package liquid helium into cryogenic containers to ship worldwide, which is necessary for cooling quantum systems. This facility in operation is likely to increase the global supply of helium by about 11 percent.[63] The helium supply, other raw materials sourced in Ukraine and Russia, and the worldwide supply chain's general state are experiencing turbulence.

With impacts on the economy and production, and an inhibited talent pool, Russia is looking to China to alleviate pressures from the restrictions and sanctions. Russia expects to rely on China for collaboration on programs, critical capabilities, infrastructure needs, material demands, and financial assistance as sanctions and other costs of war impede Russian industries. Although the two countries cooperated on technology R&D before the Ukraine invasion, it is hard to predict the longevity and stability of the Russian–Chinese alignment in this space.[64]

Chinese Quantum Computing Program Is a National Security Threat

China aims to be a global leader in technology innovation and, as a nation, it is the closest to the United States in competition for the best software. Xi Jinping aspires to surpass the United States in developing quantum sciences and all technological innovations, including AI, cyberspace, and warfare. In 2016, China launched a megaproject for quantum communications and computing, which aims to achieve significant breakthroughs by 2030. This includes expanding China's national quantum communications infrastructure, computing systems, and practical quantum simulators. Since then, the Chinese Communist Party (CCP) has pledged in its 14th five-year plan from 2021 to 2025 to fund an estimated $15.3 billion in quantum R&D.[65] This amount accounts for public disclosures and does not include classified programs.

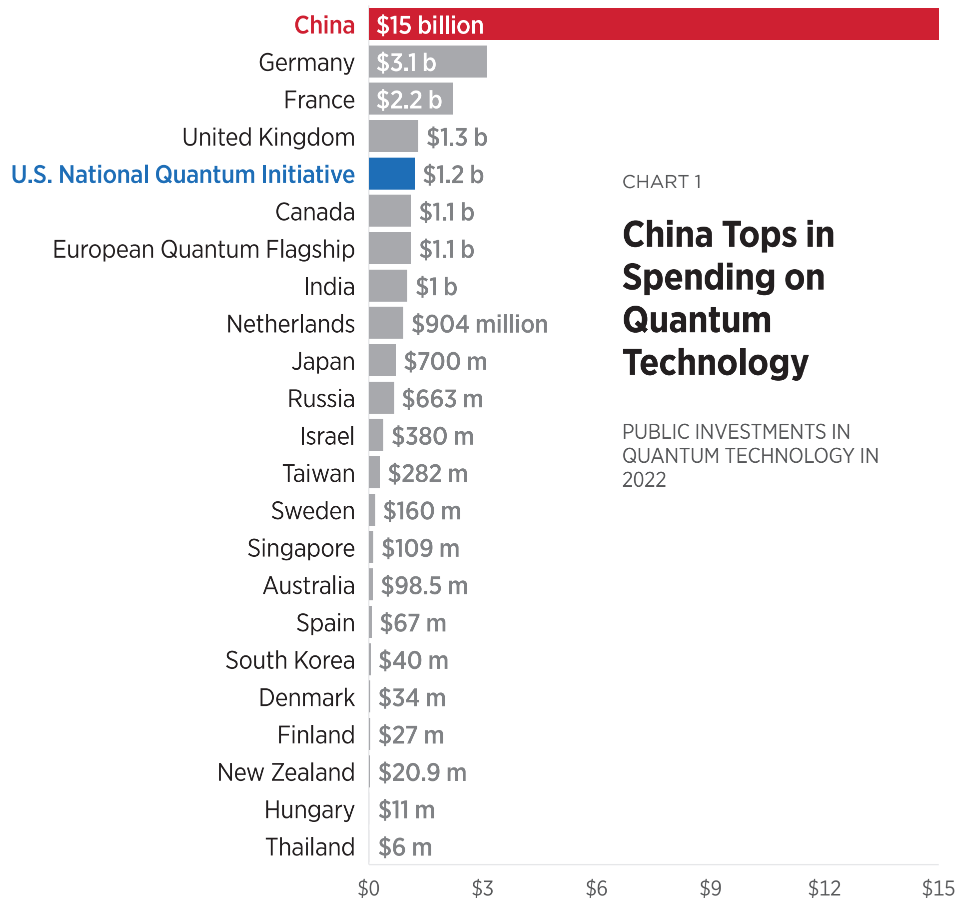


CHART 1

China Tops in Spending on Quantum Technology

PUBLIC INVESTMENTS IN QUANTUM TECHNOLOGY IN 2022

SOURCE: World Economic Forum, "State of Quantum Computing: Building a Quantum Economy," September 2022, Figure 2, p. 9, https://www3.weforum.org/docs/WEF_State_of_Quantum_Computing_2022.pdf (accessed March 28, 2023).

SR268 heritage.org

Most recently, physicists in China claim to have constructed two quantum computers with performance speeds faster than Google's 54-qubit Sycamore processor: the Jiuzhang 2.0 and the Zuchongzhi 2.0.[66] The Jiuzhang 2.0 is a 113-qubit machine that can calculate in one millisecond a task that would otherwise take the world's fastest conventional computer 30 trillion years to process. Zuchongzhi 2.0, a 66-qubit computer, can run a calculation task one million times more complex than Google's Sycamore quantum machine. While these developments do not surpass IBM's 433-qubit Condor processor, China is working to outpace its competitors.

In late 2023, a group of Chinese researchers associated with leading Chinese laboratories and institutions claimed to have found a mechanism to combine classical and quantum computing to break modern public-key Rivest–Shamir–Adleman (RSA) encryption using a 372-qubit computer.[67] Their paper,[68] which has not been peer-reviewed, has caused a cascade of concern from those who believed that a much larger qubit capability would be needed to break modern-day encryption, and unleashed skepticism among many other experts of its underlying merits. Still, the likelihood of a quantum computation and technology breakthrough, either via increased capabilities in qubits, modality stability, or along with traditional advanced computation, is on the horizon. Additionally, a quantum actor like China, which seeks to achieve and understand how to harness these capabilities, will likely not advertise it for as long as possible to seek to decrypt as much data as feasible.

China's work in quantum sciences is a geopolitical threat and a major national security threat. China plans on fielding AI systems backed by quantum technology that could "improve the already-extensive analytics and surveillance capabilities deployed in the name of national security."[69] China is reportedly developing quantum military applications, including stealth aircraft and communications systems.[70] Although China has claimed advancements in this area, experts believe that it is "not likely to be an imminent threat to stealth technology."[71]

China's Quantum Key Distribution: The Space, Sea, and Ground Race?

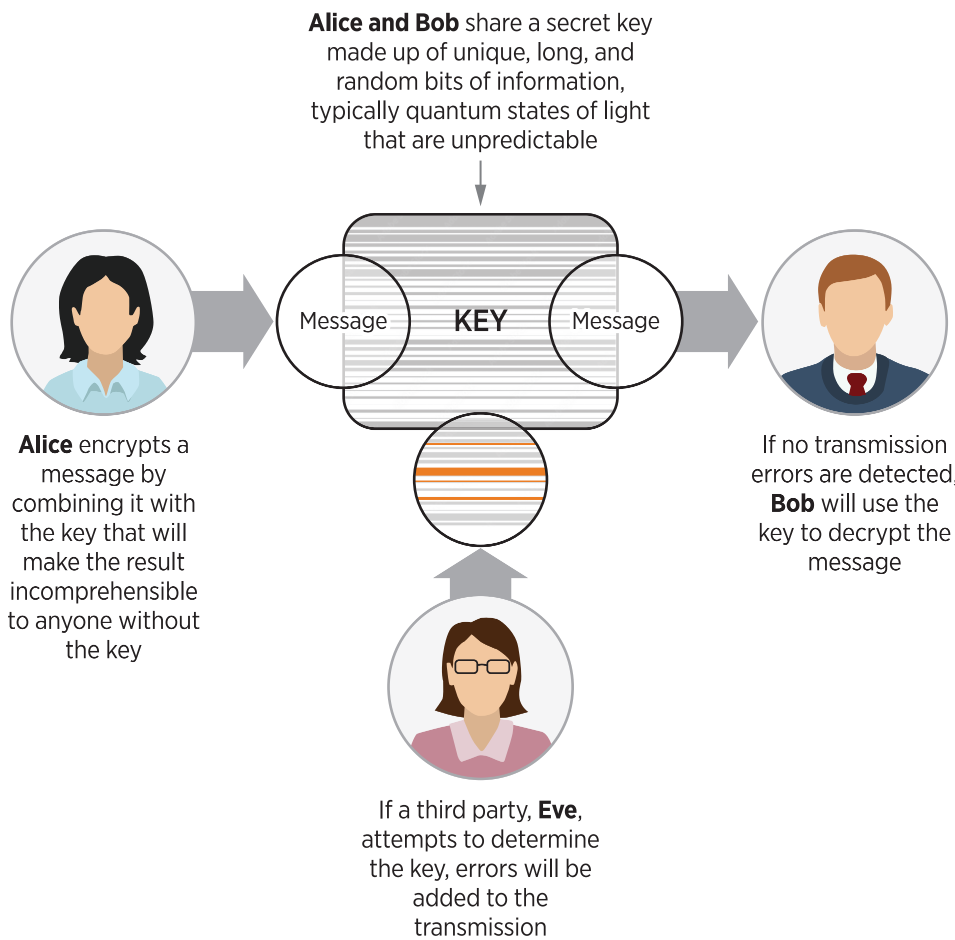
China has used quantum to deploy QKD, which enables China to encrypt communications with quantum-entangled cryptographic keys. QKD will be an essential part of data security as it provides a fundamental layer of production that "shields confidential data from exposure to attacks."[72] Using quantum properties to exchange information, such as a cryptographic key that can encrypt messages, QKD addresses the challenges of class key distribution approaches by "providing a secure cryptographic block for remote parties to share cryptographic keys."[73]

QKD works due to the fragility of quantum mechanics. For example, when the system experiences a disruption, such as when someone is trying to intercept a communications exchange, it will leave detectable traces in the quantum system. With the traces being discovered, legitimate exchanging parties can discard the corrupted information or reduce the information available to the eavesdropper by distilling a shorter key. QKD typically uses fiber-optic cables or free-space quantum channels to send quantum states of light between the transmitter (Alice) and receiver (Bob). See Figure 2**.** QKD secures a line through a public and

FIGURE 2

How Quantum Technologies Can Encrypt Messages

Quantum key distribution (QKD) is a technique used to send encrypted messages. In the example below, Alice will use QKD to transmit a message to Bob.



SOURCE: Heritage Foundation research.

SR268 heritage.org

authenticated communication link between two parties to perform the post-processing step, but with a correct and secret key. The key exchanges ensure that Alice and Bob are securely on the line. If the QKD calculates an eavesdropper or error, the system is notified, and the information is intercepted. Both mistakes and information leakage are removed during error correction and privacy amplification, leaving Alice and Bob with a shared key known only to them.

The Chinese government has developed a network for QKD linking four quantum metropolitan area networks (QMANs) in cities in eastern China with a location in the far west of the country. The QMAN comprises a 1,240-mile fiber-optic link among the cities of Beijing, Hefei, Jinan, and Shanghai and a satellite link spanning 1,616 miles between two observatories—one east of Beijing and the other just a few hundred miles from China's border with Kazakhstan.[74] According to the University of Science and Technology of China, there is the potential to expand plans for expanding the network by working with partners in Austria, Canada, Italy, and Russia.[75]

Other potential breakthroughs for China's quantum networks include experimentation with underwater communications, which the Center for a New American Security described as

> within a blue-green optical window in seawater of 400–500 nautical miles, in which "photons experience less loss and can therefore penetrate deeper." Hypothetically, Chinese quantum networks might extend underwater to include submarines, though water quality and potential interference could sometimes be a constraint.[76]

In 2016, China launched its Micius satellite, which established a QKD network that transmits information in quantum form between the satellite and multiple ground stations. This launch was a component of Quantum Experiments at Space Scale (QUESS), a project initiated in 2011 that involved collaboration between a team led by Pan Jianwei from the Chinese Academy of Sciences and the Austrian Academy of Sciences.[77] Although the Austrian and Chinese teams initially competed, this collaboration arose after the European Union was unwilling to fund a similar project. Through the program, Chinese scientists explored space-to-ground QKD, in which quantum keys were sent from Micius to ground stations at distances ranging from 645 kilometers (km) to 1,200 km, 20 orders of magnitude greater than optical fiber. In September 2017, Micius was used for a video call secured through QKD between the Austrian and Chinese Academies of Sciences presidents, the first intercontinental QKD, at a distance of 7,600 km.

It is a high priority for China's foremost quantum scientists to develop "unhackable systems" via post-quantum encryption and, in general, quantum supremacy over the globe. There remains a debate about the extent to which programs like QKD have been implemented, the costs, and whether their breakthroughs have just "resulted in excessive hype or alarm."[78] For example, the Center for a New American Security observes that "it remains to be seen whether the major state-directed investments in quantum cryptography and large-scale construction of quantum communications infrastructure will deliver the desired dividends in the long term."[79] Additionally, propaganda may also be a driving factor either exaggerating the narrative of Xi's "nation of innovation," signaling prowess, or provoking undue concerns from potential adversaries, such as the United States and Western allies.[80]

Cooperation of Friends and Foes

The U.S. is integrating quantum cooperation agreements into existing alliances, such as the North Atlantic Treaty Organization (NATO), as well as into more recent strategic arrangements, such as the Australia–U.K.–U.S. (AUKUS) security pact and the Quadrilateral Security Dialogue (the Quad) among Australia, India, Japan, and the U.S.[81] In April 2022, Sweden and Finland entered into agreements with the United States on their quantum initiatives.[82] Aside from U.S. work with EU allies and the U.K., the Quad countries continue to make some promising developments in quantum possibilities. Along with working closely on critical and emerging technologies, such as AI, QC, 5G, and semiconductors, the Quad also seeks to develop and set new global cybersecurity standards across various technology sectors.

In India, a joint team of scientists from the Defence Research and Development Organisation and the Indian Institute of Technology in February 2022 successfully demonstrated a QKD link between two northern cities over 100 km from each other. They made this link using commercial-grade optical fiber already in the field and demonstrated "indigenous technology of secure key transfer for bootstrapping military grade communication security key hierarchy."[83] India's Ministry of Defence released a "commercial request" to procure an "advanced communications solution" using quantum key distribution, likely in response to China's growing interest in the field and growing security concerns for India.[84] The Indian government is continuing to expand its quantum ecosystem. In 2020, the country allocated $1.12 billion over five years as part of the national mission on quantum technology. With the funds, India has already established between 10 and 15 government agencies, 20 to 30 service providers, 15 to 20 start-ups, and 40 to 50 academic institutions to support these efforts.[85] The development of quantum tech across industries will add an estimated $280 billion to $310 billion to the value of the Indian economy.[86] While the U.S. has not officially signed an agreement with India for a partnership on quantum, President Biden and Indian Prime Minister Narendra Modi have discussed expanding partnerships in the areas of space, cyberspace, health security, semiconductors, AI, 5G, 6G, future-generation communications technology, and blockchain, all of which could expand to quantum-related projects.[87]

Australia is ramping up its investments in the quantum space by allocating $111 million toward a blueprint action plan of critical technology priorities set by former prime minister Scott Morrison, as well as more than $70 million over the next 10 years for a quantum commercialization hub.[88] The government also highlighted QC as a critical emerging technology in the Digital Economy Strategy because the quantum industry can add $4 billion and 16,000 new jobs to the Australian economy by 2040. In the November 2021 agreement signed between the U.S. and Australia on quantum science and technology cooperation, the two nations look to collaboration, continued information-sharing practices, and building a trusted global quantum marketplace.[89] The AUKUS Quantum Arrangement has been an underappreciated value added to the overall agreement with initial joint efforts on quantum capabilities for "positioning, navigation, and timing" and later opportunities to "integrate emerging quantum technologies in trials and experimentation over the next three years."[90]

Swiss researchers, in conjunction with U.S. bilateral collaboration and funding, have made strides toward using traditional and quantum technology to potentially increase the cybersecurity of modern digital networks using QC as an add-on structure.[91] By encrypting transmitted data using photons, quantum superposition observation would allow the transmitter to understand if the data flows were being attacked or intercepted. Much more R&D will need to be done to account for the types of fiber-optic cables and satellite systems needed to advance such structures.

The Japanese government this year decided to revamp its quantum technology strategy to catch up to the U.S. and China's capabilities in the global computing race. A part of the Japanese strategy is to invest upwards of $590 million to build quantum technology for the country, doubling its investment this fiscal year.[92] Japan estimates that its first quantum computer will be developed by March 2023. The government expects 10 million users across Japan to use quantum technology by the decade's end.[93] The government-backed Riken research institute will add two new research sites to explore industrial applications, bringing 10 research sites to Japan. While the government sector is developing the means for growth, the private sector is working through the Quantum Strategic Industry Alliance for Revolution (Q-STAR), which is a coalition of 24 companies, including Toyota, Hitachi, and NTT, to collaborate with industry, academia, and government in promoting technology platforms.[94]

While the Quad countries are looking for greater collaboration and development of critical and emerging technology by fostering healthy competition and international cooperation to "advance the frontier of science and technology," threats from competitors, such as China and Russia, will likely strengthen the Quad alliance against their technological pursuits.

Technological collaboration has been essential to the Chinese–Russian bilateral relationship. The former Soviet Union long prided itself on scientific and technological advancements. During the initial years of the Cold War, the USSR promoted a "comprehensive program of technology transfer to China."[95] Not only did China model its ideological policy after that of the USSR, it also modeled its economic policy planning on that of the Soviets. China benefited greatly from the USSR with assistance in the military and technical domain during the early years of the relationship. The USSR provided missiles, airplanes, weapons, and equipment, and sent thousands of engineers and technical experts to China. The two states' cooperation was temporarily stalled from the 1960s until the late 1980s as the two nations split relations. Still, in the post–Cold War period, relations were normalized and science and technology exchanges began again.

While growth between China and Russia's scientific and technological developments have traditionally been tailored to military, nuclear, and space programs, since the 2010s, the relationship has gathered pace as a key pillar in the bilateral relationship.[96] In 2019, China and Russia elevated their ties to a "Comprehensive strategic partnership of coordination for a new era."[97] Examples of their increased collaboration include China's Ministry of Science and Technology (MOST) and Russia's Ministry of Science and Higher Education collaborating to identify priorities and facilitate linkages broadly; MOST and Russia's Ministry of Economic Development (MED) signed a Memorandum of Understanding on Launching Cooperation in the Domain of Innovation; MOST and MED hold regular meetings, convened by the Russia–China Working Group for High Technologies and Innovations; and the two ministries held the first annual Sino–Russian Innovation Dialogue in 2017.[98] A high-level Chinese–Russian political initiative designated 2020 and 2021 as years of "innovation and technology cooperation" between the two nations.[99] An estimated 800 events were expected to be held, including high-level conferences, scientific and technical exhibitions, youth innovation competitions, and exchanges of highly qualified specialists.[100]

Moreover, joint investments and funding schemes have proliferated, creating more outstanding capital for further technology cooperation. For example, in 2019, the Russian Direct Investment Fund (RDIF) and the

China Investment Corporation (CIC) created a $1 billion research and technology investment fund specifically for supporting small-and-medium enterprises (SMEs) and Chinese and Russian technology enterprises.[101] This allowed the two countries to work closely on areas deemed suitable for closer cooperation, including AI and robotics, information and communications technology, biotechnology, space, emerging technologies, and the digital economy.[102]

While the two have not publicly agreed to cooperate on quantum technology, China and Russia have advanced their work in the military, communications, and other strategic fields, which may include quantum projects. In 2017, China and Russia signed a road map to strengthen military cooperation.[103] Although the details remain elusive, the road map's implied ambitions are to promote collaboration in areas such as hypersonic technology, the construction of nuclear submarines, and strategic missile defense, which, if both nations incorporate quantum and AI capabilities into their systems, could give them a strategic edge.

Engagement between the two countries seemed productive until 2021. Still, engagement is stalled with the current war in Ukraine and the reverberating impact across Russia's quantum industry, economy, and applications to the military programs. And while Russia sees China as a near-peer competitor and ally, pushed together by a common enemy (the United States), the Chinese view the relationship in a limited way.[104] China no longer views Russia as a great power. With a stagnated and shrinking economy, capital flight, deteriorated external relations in the international financial system and trade, war crimes committed in Ukraine, and a deteriorated military,[105] in Chinese discourse, Russia is beginning to become a "gas station disguised as a nuclear power."[106]

Opportunities, Risks, and Challenges

Quantum computing systems offer the potential to process billions of functions in seconds, but their computational power currently has limited relevant applications. However, there is great potential for its adoption in government and civilian applications once the technology is further developed.

Aside from the work of DARPA, IARPA, and the Defense Science Board (DSB), which have explored QC, quantum communications, and quantum sensing, Congress has maintained a vested interest in developing quantum technologies. Recent National Defense Authorization Acts (NDAAs) have included a variety of proposals, mandated reports, and funding for quantum-computing-related projects.[107] Requested budgets for quantum programs rose 37 percent from fiscal year (FY) 2020 to FY 2022 across different DOD organizations.[108] Per the Congressional Research Service and data analytics firm Govini, the DOD requested approximately $688 million for quantum technologies and research in FY 2021.[109] This amount is in addition to the substantive monies included in the recently passed CHIPS and Science Act of 2022 devoted to various federal quantum initiatives.

Additionally, the Biden Administration has taken action diplomatically and through executive directives on quantum technology.[110] This includes the May 2022 signing of National Security Memorandum 10, which seeks to drive U.S. leadership in quantum information science (QIS) and plans to address threats that QC could pose to encrypted data systems.[111] The NIST and the NSA is set to develop technical standards for quantum-resistant cryptography by 2024 and, more broadly, pursue a "goal of mitigating as much of the quantum risk as is feasible by 2035."[112] The United States has signed bilateral cooperation agreements on quantum R&D with Japan, the United Kingdom, Australia, Denmark, Finland, Sweden, and, most recently, Switzerland.[113]

In the private sector, speculation about innovative quantum technology applications is endless. In the health care industry, quantum technology could optimize the administrative backend for health care providers while also assisting medical researchers in genome mapping.[114] Quantum sensing could also replace traditional magnetic-resonance-imaging (MRI) sensors and detect diseases like multiple sclerosis. Banks and cybersecurity companies could benefit from data encryption by QC in the financial sector.[115]

By using quantum uncertainty to produce un-hackable private keys to encrypt or decrypt transactions or messages from one location to another, hackers would have to break the laws of quantum physics to access sensitive data and information. Emerging developments in cryptocurrency and blockchain technology will also have to adjust in a post-quantum supremacy era in which traditional cryptography used in traditional blockchain will likely need to change its algorithms.[116] Applied to other areas, these quantum capabilities could enable secure voting, increase data transmission, and much more.

Technology companies may need help to hire people with deep technical expertise. This knowledge delta results from a need to accelerate the importance of expanding the American high-tech workforce through educational programs. While quantum development is heavily driven by national security and business structures, creating a workforce that can apply QC in practice is essential.

However, many U.S. companies' international presence (research labs and offices) presents more significant security challenges to IP theft. Securing U.S. data is a priority.[117] China's worldwide espionage and past cyberpilfering of government, corporate, and personal data could be a significant threat if "encrypted data with intelligence longevity," such as "biometric markers, covert source identities, Social Security numbers, and weapons' design" could be decrypted and used against U.S. interests.[118]

The United States generally leads the world in QC hardware and software patents, but China is quickly catching up and leading in other areas. In quantum communication and cryptography hardware and software, China leads the field. Overall, China holds more than 3,000 patents related to quantum technology, nearly twice the U.S. number.[119]

Preventing further acts of espionage is essential for the growth and protection of quantum systems in the U.S. The Department of Commerce placed eight Chinese companies on an export blacklist for quantum technologies in November 2021.[120] Secretary of Commerce Gina Raimondo added 66 Chinese companies to an export blacklist.[121] In addition to the threat from China, the Biden Administration announced export controls in 2022 on semiconductors, lasers, and other technology to Russia's defense industries in February and June in response to its invasion of Ukraine and to undermine its technology industries, manufacturing, and QC aspirations.[122] The Biden Administration in October 2022 advanced an array of new export controls targeting China on semiconductors and equipment used to produce cutting-edge circuitry, with advanced QC being a priority in addition to high-end memory-chip manufacturing capabilities.[123]

Challenges: Keeping It Cool and Reducing the Noise

Aside from the international threat from adversarial actors, technological and infrastructure challenges exist. Most quantum computers being developed worldwide will only work at fractions of a degree above absolute zero.[124] This temperature keeps atoms and molecules in a quantum state. Any disruption (for example, a temperature increase), can cause a qubit's voltage to spike and flip from one state to another,[125] requiring multi-million-dollar refrigeration, which is incompatible with conventional electronic circuits as they will instantly overheat. Maintaining quantum computers at temperatures colder than deep space is expensive and daunting, but researchers worldwide are working on innovations. In Finland, researchers from the University of Helsinki have been developing cryostats for quantum computers since 1979.[126] When IBM announced its system with 127 qubits, Bluefors, a Finnish start-up, stated that "we can handle that many in one enclosure using the most powerful system we have today."[127]

While the compositional structure of quantum machines has traditionally used cryogenic cooling for large-scale quantum computers, DARPA has looked at alternative compositions of quantum machines. Quantum systems traditionally use magnetic traps to isolate ions, and then organize the ions into a chain of qubits. But with DARPA's recent development, scientists have discovered a configuration optimized for a more efficient process using rare-earth materials.[128] In a process called the Penning trap, scientists used a "combination of a magnetic field and an electric field to configure two-dimensional ion crystals that perform quantum operations."[129] Rare-earth metals (such as neodymium or samarium cobalt) form powerful and permanent magnets, which the trap uses instead of cryo-cooled superconducting magnets. The research team built an ion chain using this method for the length of 10 qubits, which has promising results for adding more quantum systems to the chain and more accurate computations.[130]

Rare-earth metals mining, development, and processing are essential components of thousands of consumer products to military weapons. China currently leads global trade and the acquisition of exclusive mining licenses worldwide. China has about 35 percent of the world's reserves of rare-earth metals and refines about 70 percent of rare-earth elements for the rest.[131] China has built factories close to the mines so that the raw material can quickly go into production. This increases efficiency and lowers production costs, making China an advantaged supply-chain provider and making it difficult for other countries to compete with it. For example, the country produced 120,000 metric tons (70 percent) of total rare earths in 2018, according to the United States Geological Survey. The U.S. pales in comparison, mining 15,000 metric tons of rare earths in 2018.[132]

Additionally, through the Belt and Road Initiative, in which China has strategically positioned itself around the globe, the CCP has moved to obtain exclusive mining rights in African countries such as the Democratic Republic of Congo and Kenya, where "big ticket" infrastructure project deals have been secured for data centers and highways.[133] China targets other locations with military-critical rare-earth minerals, including Angola, Cameroon, Tanzania, and Zambia.[134] China's breadth across the rare-earths industry could prove the CCP's strategic position in developing quantum technology and other military, communications, and general industrial products.

The U.S. needs to diversify outside the Chinese supply chain to create a competitive market and meet the growing demands of the technology industry. Currently, the United States has a 1.4-million-ton reserve of rare-earth elements, one of the world's largest, yet the U.S. only mines a fraction of available bedrock.[135] Relying on China for this industry limits U.S. potential, and American stakeholders need to direct the rare-earth needs of the U.S. industry. The 2020 NDAA directs most Pentagon systems to only use non-Chinese rare-earth metals by 2025, and dictates that the federal government give preference to U.S. suppliers of these materials in government acquisitions.[136] As part of the U.S. government's strategy to ensure safe and reliable supplies of critical minerals, the DOD has recently announced contracts and agreements with several rare-earth-element producers. These contracts and agreements include using the Defense Production Act to invest nearly $200 million in three companies to boost capacity to produce neodymium, a vital magnet material, and other critical processed elements.[137]

Another potential approach to cryo-cooling alternative was discovered by U.S. Army researchers, suggesting that using photonic circuits and optical crystals may no longer require quantum circuits to operate at frigid temperatures.[138] MIT professor Dirk Englund stated on the Army research project: "Photonic circuits are a bit like electrical circuits, except they manipulate light instead of electrical signals."[139] And unlike quantum systems that use ions or atoms to store information, photons can bypass the cold temperature limitation. While photons must interact with other photons for this theory to work, researchers suggest that they temporarily engineer crystal cavities to trap them inside. This would allow the quantum system to establish the different possible states a qubit can hold.[140] Removing the high costs and infrastructure demands of cryo-cooled conducting units could significantly expand the playing field of quantum technology. While the proposal for the room-temperature systems looks promising, the U.S. Army speculates that it will take "about ten years for the necessary improvements to be realized."[141]

A group of MIT researchers recently developed a way to let wireless communication allow a quantum computer to "send and receive data to and from electronics outside the refrigerator using high-speed terahertz waves."[142] Terahertz waves, located on the electromagnetic spectrum between radio waves and infrared light, are significantly smaller than radio waves and allow larger quantities of data to be moved more rapidly than radio waves. Reducing the power consumption and quantum noise would allow less interference with quantum processors and could pave the way to large-scale quantum systems.[143]

Potential Impacts on Battlefield Dynamics and Applications

For the U.S. military application of quantum technology, the Defense Science Board (DSB), an independent DOD board of scientific advisors, has concluded that quantum sensing, quantum computing, and quantum communications are promising for the DOD.[144] Quantum sensing will significantly improve submarine detection, provide alternative positioning and navigation, enable military personnel to detect anything from underground structures to nuclear materials to electromagnetic emissions, and assist in locating adversary forces. Quantum computations will advance machine learning (ML), enhancing kinetic warfare systems by aiding the targeting algorithms of autonomous weapons, which would, consequently, revolutionize the battlespace.[145] The U.S. government could also make use of post-quantum encryption (PQE).[146] PQE remains a top priority for the NSA, developing quantum key distribution and cryptography to protect military and U.S. government communications and information.[147] PQE would be resistant to both traditional and quantum-enabled decrypting software. This could allow the private and public sectors to secure data. The British QC firm Majenta Solutions suggests that quantum decryption could be stalled by "sharding" data—dividing data into smaller, easier-to-manage portions.[148] Lastly, quantum communications will enable the secure networking of quantum military sensors, computers, and other systems, thus improving performance over a single quantum system or classical communications network.[149]

Michael Krelina, a researcher in the nuclear sciences and physical engineering faculty at the Czech Technical University in Prague, outlined an array of possible applications of quantum warfare in the future,[150] including:

- **Chemical and biological simulations and detection.** The ability to carry out extensive simulations using quantum simulations could play a role in the specialization and advancement of countermeasures of chemical warfare agents, such as cyanogen, phosgene, cyanogen chloride, sarin, or yperit.[151]

- **New material design.** Materials could theoretically be analyzed and simulated using quantum computation, allowing for the creation of potential new materials, room-temperature superconducting, and battery improvement. Additional defense materials, such as "better camouflage, stealth (electromagnetic absorption), ultra-hard armour, or high-temperature tolerance material design" could come to fruition.[152]

- **Cyberwarfare.** As mentioned, QKD has the potential to affect defense applications significantly and will need to overcome the weakness of endpoint vulnerabilities. Quantum applications could increase cyberwarfare vectors of attack on current encryptions while simultaneously seeing advancements in "quantum-resilient encryption algorithms" to counter future threats. Applying quantum computation to traditional computation to increase efficiencies and applying ML and AI in cybersecurity and warfare applications are likely outcomes.

- **Computing.** Computing capabilities will vastly improve between the coalition of stable quantum computations alongside classical operating systems. Capabilities will likely scale as part of hybrid cloud architectures with vast advances in optimization, ML and AI, and simulations. In terms of military applications, QC could include optimization for "logistics for abroad operations and deployment, mission planning, war games, systems validation and verification, new vehicle design, and their attributes such as stealth or agility."[153] To improve classical computations, QC could optimize and enhance "most classical ML/AI applications in defence, for example, automating cyberoperations, algorithmic targeting, situation awareness and understanding or automated mission planning."[154] For example, Lockheed Martin uses a quantum annealer from D-Wave Systems to validate and improve complex systems' software code.[155]

- **Positioning, navigation, and timing (PNT).** Quantum technology could create vast improvements within PNT structures. Inertial navigation using quantum capabilities could bring "100 times higher precisions than the classical counterpart" and could see advantages "manifested for GPS denied or challenging operational environment and enable precise operations [in] underwater and underground, or environments under the GPS jamming."[156] For example, the average submarine has an error of one mile per 72 hours. Quantum inertial navigation could have an error of "approximately hundreds of meters per month."[157] Recent reporting has signaled that quantum sensors for submarines and other vessels may be less than two years away in unacknowledged countries, and full navigation capabilities using such sensors is seven years to 10 years away for drones and small aircraft.[158] The Air Force recently awarded a research contract to SandboxAQ to evaluate its quantum sensor prototype "designed to complement the Global Positioning System (GPS) for accurate navigation in degraded, contested, or denied environments where the loss of precision GPS may negatively impact operations," on Air Force aircraft.[159]

- **Intelligence, surveillance, target acquisition, and reconnaissance (ISTAR).** Quantum improvements in ISTAR could dramatically improve situational awareness within multi-domain environments. Quantum sensing improvements will be seen in "individual land/sea/aerial vehicles and low-orbit satellites."[160] Seismology and magnetometry improvements will be seen in anomalies within the Earth's surface and the ability to observe submarines and mines in underwater environments.

- **Low-earth orbit (LEO) and space.** Quantum gravimeter and magnetic sensing could

  > detect camouflaged vehicles or aircraft; effective for searching for a fleet of ships or individual ships from LEO; detect underground structures such as caves, tunnels, underground bunkers, research facilities or missile silos; the localization of buried unexploded objects (landmines, underwater mines and improvised explosive devices); through-wall detection of rotating machinery.[161]

  With the increased traffic in LEO and beyond, quantum radar could vastly improve current capabilities to track extremely small debris, satellites, and meteorites.[162]

- **Imaging.** Quantum 3D cameras could "inspect and detect deviation or structural cracks on jets, satellites, and other sensitive military technology." Short-range imaging capabilities could improve "behind-the-corner or out of the line-of-sight visibility" and be used to "locate and recover trapped people, people in hostage situations or improved automated driving to detect incoming vehicles from around a corner." These improvements could also increase vision devices used to see in "cloudy water, fog, dust, smoke, jungle foliage in the nighttime"[163] and help helicopter pilots see in complex visual environments. Quantum rangefinders would remove the detectability of conventional rangefinders and would be indistinguishable from a target.[164]

- **Electronic warfare (EW).** Quantum capabilities could improve classical EW, radio frequency spectrum analyzers, and ML/AI techniques. Timing improvements can also enhance signals intelligence and counter-jammers.[165]

- **Light detection and ranging (Lidar).** Rampant speculation on the potential capabilities of quantum radar are at times overstated versus the cost and capabilities of conventional systems. That said, quantum technology may have an "advantageous environment" in space where radar could be established on a satellite to detect small satellites that are otherwise difficult to observe. Using quantum Lidar as an anti-drone capability to detect smaller and slower-moving drone systems and objects, short-range air defense systems could also improve.[166]

- **Underwater capabilities.** Submarines will likely be one of the first adopters of inertial navigation advantages brought by quantum capability. Larger submarines could onboard quantum devices and allow quantum magnetometers and gravimeters to help to map "undersea canyons, icebergs, or wrinkled sea bottom without using sonar that can be easily detected."[167] Additionally, a coastal array of superconducting quantum interference device (SQUID) quantum magnetometers could help anti-submarine warfare measures by detecting a submarine from 6 km away, with a conventional helicopter and plane having ranges of only hundreds of meters.[168]

- **Brain imaging and human-machine interface.** Although a speculative field, as many of these potential warfare applications mentioned above in proof of concept are in real applications, the possible use of quantum magnetic encephalography could allow increased capabilities for human-to-machine interface and data collection. For example, soldiers' helmets could be equipped with additional remote medical monitoring and detection, allowing further data input for battlefield commanders and medical support. Additionally, increased computational capabilities using quantum technology intermixed with conventional computing could enhance the human-machine interface with machines and autonomous systems on the battlefield.[169]

Time Is of the Essence

The United States has made strides in recent years with additional attention to advancing quantum capabilities and future possibilities. The Trump and Biden Administrations and Congress have prioritized quantum information sciences with the National Quantum Initiative and priority roles within the Office of Science and Technology Policy (OSTP) at the White House. Recent NDAAs have included various quantum reporting and benchmark requirements for agencies across the federal government, as well as initiatives to speed collaborative efforts with the private sector and allied partners.[170] While quantum technologies and applications will evolve along different timelines, the United States must strive to maintain current leads in some areas and rapidly advance, prepare for, and field quantum initiatives throughout the government and private sectors. To do so, the United States should:

Increase Access and Usage of Quantum Evaluative Test Beds for Federal Agencies and the DOD. Since the signing of the 2018 National Quantum Initiative Act, work on coordinating various quantum initiatives across the government and internationally has evolved. A garden variety of Department of Energy (DOE) laboratories is involved in multiple quantum evaluative test beds alongside academic and private-sector entities for research.[171] The Administration and Congress should reduce barriers to entry to these functions in different quantum research areas wherever possible. In recent years, the government has nearly doubled funding for quantum R&D. Still, the technical means of quantum information science and research talent will evolve into further applications.[172] DARPA, IARPA, the DOD, the Intelligence Community, the National Science Foundation (NSF), the NIST, and the DOE National Laboratories have various research programs. Duplicative and administrative spending should be reduced where possible while seeking broader buy-in from cross-spectrum agencies and the private sector to begin accessing and understanding quantum developments, including quantum applications beneficial to U.S. government core missions.

Legislative initiatives on these matters include the QUEST Act of 2021, which was integrated into the recently passed CHIPS and Science Act of 2022. The act seeks to carry out the Quantum User Expansion for Science and Technology Program through the DOE (recently codified by the National Quantum Initiative Act) to "encourage and facilitate access to U.S. quantum computing hardware and quantum computing clouds for research purposes."[173] While the government should build further access points for researchers and the private sector to DOE laboratories for quantum research, the federal government should avoid resourcing for commercialization. Any future funds should come from existing basic science research appropriations.

As outlined in previous recommendations on DOE lab reforms and the interest of the private sector and venture capital in quantum research, Congress should consider allowing labs to use flexible pricing for user facilities and unique capabilities, including charging a market rate for proprietary research and operation of technical facilities. Additionally, the DOE should allow labs autonomy in nonfederal funding partnership agreements, allowing lab managers to collaborate with third parties for analysis within the U.S. with proper security protocols.[174]

Expedite Post-Quantum Cryptography Playbooks, Beginning with Rapidly Identifying Public-Key Cryptography and How It Is Used Within Government Agencies. The Biden Administration's recently released National Security Memorandum on quantum technology set a goal of "mitigating as much of the quantum risk as is feasible by 2035."[175] While experts do not have a consensus on when the cryptanalytically relevant quantum computer (CRQC) will be able to break public-key cryptography, China or another adversary may reach these capabilities before the United States, and advance further pilfering of the U.S. government and citizen data. Recent Chinese research on this matter and potential breakthroughs, while disputed and unlikely to be revealed if proven, show an eagerness by the CCP to reach this milestone first.

The U.S. goal should be to quickly assess, catalog, and build prioritized playbooks for federal agencies to deploy post-quantum cryptology algorithms to protect data as soon as feasible, and before 2035. The potential for a "Q-Day," the hypothetical date when a quantum computer could crack current cryptographic standards, should be at the forefront of national security leaders' minds.[176] China recently surprised the U.S. government with a weapons test of hypersonic capabilities ahead of the pace of intelligence assessments. General John Hyten, the prior Vice Chairman of the Joint Chiefs of Staff, called it "stunning."[177]

President Joe Biden recently signed bipartisan legislation, the Quantum Computing Cybersecurity Preparedness Act, to evaluate the federal agency prioritization parameters and funding needs of post-quantum cryptography standards through the Office of Management and Budget (OMB) after the NIST completes its algorithmic standards, which must withstand the rigor of AI advances.[178] Congress should continue to put pressure on the Administration to better position the government's future encryption needs in the commercial community, as 5G/6G capabilities, rapid AI advances, and the Internet of Things (IoT) are further developed, no matter the unknown timelines in which these quantum capabilities are reached.

Build Education Incentives For 21st-Century Science, Technology, Engineering, and Math (STEM); Cyberspace; and Quantum and Information Science Technology (QIST) Needs, Not for Woke Ideology and Economically Unattractive Fields. The Subcommittee on Quantum Information Science of the National Science and Technology Council released a report in February 2022 outlining workforce development issues in the quantum field.[179] The report outlines various strategic needs and challenges in developing a future QIST-capable workforce. These STEM-related workforce issues are not unique to the area of quantum technology; the United States will continue to need significant development within talent pools in other fields, such as cyberspace, computer science, and AI. This speaks to higher education's need to develop additional pathways in these fields and to include these fields in K–12 education.

Giving parents choices in their children's education while creating educational systems geared toward the future needs of the American economy and national security is vital. States should enact legislation that increases curriculum transparency for parents to transform outcomes from elementary school to higher education. For example, Governor Ron DeSantis (R–FL) signed H.B. 1467, which requires school districts to be transparent in the selection of instructional materials as well as establishing fixed term limits for school board members.

Governor DeSantis also signed S.B. 7044, which stripped power from accrediting agencies that had removed objectivity from the process. This bill will require Florida's public colleges and universities to seek accreditation from different accreditors in consecutive accreditation cycles. The bill will require enhanced transparency of costs associated with Florida's public colleges and universities. This is in stark contrast to the pursuit of critical race theory (CRT) and many accredited degree paths that lead students toward careers with inadequate market needs and incomes. It is telling that the Biden Administration's Department of Education has targeted[180] Florida's innovative approach to accreditation reform as it hopes to maintain the "iron triangle"[181]—regional accreditation organizations, the schools, and federal bureaucrats—that exists to prevent innovation in higher education while keeping the federal government's tentacles in institutions that fear losing accreditation. States should introduce and pass model legislation[182] to prevent CRT from being taught in K–12 schools and look for additional opportunities to provide school choice, educational savings accounts (ESAs), and comprehensive parental rights while providing transparency on educational opportunities in STEM fields.

Congress should reintroduce S. 2339, the Higher Education Reform and Opportunity (HERO) Act, sponsored by Senator Mike Lee (R–UT) in the 116th Congress, which would require institutions of higher education to publish information on student success, to provide fiscal accountability, and to provide school accountability for student loans. This would demonstrate the need for more STEM students and outline the pitfalls of pursuing a degree with a limited investment return. The HERO Act and broader efforts at accreditation reform would enable industry to collaborate with colleges to provide quality assurance and enable students to learn directly from prospective employers in the STEM space.

Additionally, partnerships between private-sector research entities in the quantum field and academia have increased. IBM recently partnered with Howard University and 12 other historically black colleges and universities (HBCUs) to offer multi-year investments and access to quantum computers to further develop talent in quantum and other STEM fields.[183] Opportunities like these, which allow students and parents to gain greater transparency of possible outcomes related to STEM degrees and pipeline opportunities from corporations to explore quantum-related fields, are essential for ensuring an advanced and educated workforce prepared for the future of quantum technologies. Educating the next generation about the national security challenges connected to the adoption of quantum technology should be at the forefront of education and national security policymakers.

Expand International Collaboration. In recent years, the Biden and Trump Administrations have made significant inroads toward international collaboration with partners in areas such as quantum technology and cyberspace. Many partners throughout Europe and Asia continue to develop practical quantum science programs in different fields that can assist with the future development of quantum technology and its potential applications. While these collaborations present a massive advantage over Chinese and Russian actions, they must see follow-through after the joint statements and declarations. China is seeking to collaborate with Austria, Canada, Italy, and Russia. The U.S. should be at the forefront of securing secure, cooperative research efforts with Austria, Canada, and Italy while sharing dual-threat security concerns of joint Chinese research.

Collaboration should include existing security arrangements. For example, NATO's 2022 summit in Madrid discussed further commitments to developing emerging technologies, such as "quantum computing, artificial intelligence, and space tech" through its recently established Defence Innovation Accelerator for the North Atlantic (DIANA), which models DARPA with technology fusion centers across NATO.[184] DIANA includes more than $1 billion in funding, access to dozens of accelerator sites and test centers across 20 allied countries, and a new investment fund focused on deep, emerging, and disruptive technologies, including AI, big-data processing, quantum-enabled technologies, autonomy, biotech, novel materials, and space.[185] For example, the U.S. should consider concrete concepts with partners, such as Quad members.

Increase Vigilance to Space-Based Quantum Applications, Opportunities, and Threats. The space domain continues to expand in both options and threat vectors with an explosion of commercially based and nation-state facilitators and increasing threats from adversaries, such as China and Russia. China's 2016 entry with quantum satellite Micius is a prime example of technological innovation that focuses on building quantum communication networks and ground relay systems. Last year's cyberattack on Viasat and its European impacts as part of the Russian war on Ukraine and advancements in commercial broadband capabilities with SpaceX's Starlink is just the beginning of a crowded atmosphere where nations will seek the advantage.

Space-based quantum sensing and computing capabilities could further revolutionize everything from intelligence, including geospatial intelligence (GEOINT) and signals intelligence (SIGINT) collection, to predicting earthquakes, droughts, and floods.[186] The U.S. must expand capabilities within the National Aeronautics and Space Administration (NASA) and the Space Force for future quantum technologies while outlining policies to protect commercial capabilities.[187]

Protect Quantum IP. While many elements of QIS are in nascent stages and many advocate worldwide cooperation with few boundaries, the United States and many of its closest allies must wake up to the threats emanating from joint quantum research with China. In several other technology fields, including semiconductors, hypersonics, and AI, Chinese technology transfers, both legal and illegal, continue to compound the ability of the United States to protect its homegrown IP. The CHIPS and Science Act of 2022 calls for various research security guardrails for billions of dollars of U.S. taxpayer-backed technology research funding. Still, massive gaps and security concerns remain unaddressed or unfairly criticized and maligned by detractors from research and academia.[188] Congress must address these remaining research security concerns, including further consideration of proposals such as former Senator Rob Portman's (R–OH) S. 3997, the Safeguarding American Innovation Act, and placing additional restrictions on U.S. stakeholders that receive funding from the CHIPS and Science Act from making specific investments and undertaking specific research collaborations with China.

Task the House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party with Assessing the Effectiveness of Current U.S. Export-Control Mechanisms and Potential Outbound Investment Controls Related to Strategic Technologies. The select committee should seek insights from government, business, and academic research communities on the effectiveness of current export-control mechanisms, the Department of Commerce's entity list, the Federal Communications Commission, and the Committee on Foreign Investment in the United States, as well as on concerns about particular outbound investments that could affect national security and technology. The committee should quickly make legislative recommendations to the appropriate authorizing committees, which the committees should debate and consider in haste. Priorities should include frameworks that will not involve vast expansions of the federal regulatory state but are focused on economic levers and functional tools without loopholes to counter China's capabilities and protect America's innovations.

The Department of Commerce has yet to finalize definitions related to emerging and foundational technologies, as called for by recent reforms in the Foreign Investment Risk Review Modernization Act (FIRRMA) of 2018 and the Export Control Reform Act (ECRA) of 2018. Although this definitions debate is highly technical and should be considered carefully, private-sector stakeholders are blind to which areas they should be concerned about within their businesses. The National Counterintelligence and Security Center has released a list of emerging and foundational technologies of concern.

Still, the Commerce Department, the current primary stakeholder, should work toward final recommendations and expediently consider industry and academic feedback. The effectiveness of the United States' current entity list restrictions is unclear, and FIRRMA's and ECRA's export-control mechanisms need to be addressed further. Due to the nascent nature of the field, technical specifications relating to quantum technology are very complicated to quantify from a threat standpoint. The select committee should analyze and discuss with stakeholders, including governmental laboratories, the Intelligence Community, and the DOD, the fundamental question: What does the U.S. need to do to protect itself?

Further cyberespionage protections should be established within quantum-based industries and research facilities. China will likely continue to target vast swaths of data that could be used to feed quantum simulations and run parallel to Chinese economic espionage goals. These include "quantum similar-relevant biology fields like genomics, biopharmaceuticals, and vaccines, as well as crops, livestock, and agricultural microorganisms."[189]

Accelerate the DOD's Work to Understand Vulnerabilities and Opportunities in Current and Future Systems Using Quantum Technologies. While the DOD is making strides in resourcing and understanding possible uses of quantum technology, the department must break down the silos in these approaches that have been seen similarly ongoing and it should streamline broader department uses of AI capabilities. The DOD should work, program by program, with stakeholders on understanding how QC could advance warfighting abilities in data; sensory technologies; intelligence, surveillance, and reconnaissance (ISR); and communication. This understanding will be vital to all domains. The domains will include air-, sea-, land-, and space-based capabilities and vulnerabilities that the U.S. must understand and address as China advances its technology in this space and diminishes or targets U.S. defense strengths.

U.S. Response to a Post-Quantum World

How the United States postures itself for success in the era of quantum computing, sensing, and encryption will have reverberating ramifications for everything from the future of manufacturing to the development of future medical cures to the national security needs of the military and the ability to protect information.

In addition, when QC is fully developed and mobilized, who reaches quantum supremacy first will determine global power dynamics. The United States cannot allow power to be centralized in the hands of one actor, especially the CCP. For the U.S. to lead in the quantum realm, it must take a whole-of-government and whole-of-industry approach alongside foreign allies and partners.[190]

While many challenges remain in bringing quantum technology to scale, the scientific race and outcome amongst nations, militaries, academia, and technology companies will define the 21st century.

Endnotes

1. Jacob Fromer, "12 More Chinese Companies Are Placed on US Export Blacklist," *South China Morning Post*, November 25, 2021, https://www.scmp.com/news/china/article/3157288/12-more-chinese-companies-are-placed-us-export-blacklist?module=perpetual_scroll_0&pgtype=article&campaign=3157288 (accessed June 13, 2022), and The White House, "Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems," January 19, 2022, https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/ (accessed June 13, 2022).
2. Alexandra Kelley, "Push for More Quantum Tech Investment Reaches World Economic Forum," Nextgov, January 18, 2023, https://www.nextgov.com/emerging-tech/2023/01/push-more-quantum-tech-investment-reaches-world-economic-forum/381906/ (accessed January 23, 2023).
3. Mark Lapedus, "The Great Quantum Computing Race," *Semiconductor Engineering*, July 26, 2021, https://semiengineering.com/the-great-quantum-computing-race/#:~:text=Quantum%20computing%20is%20heating%20up,developers%20aren't%20far%20behind (accessed June 13, 2022).
4. Cem Dilmegani, "In-Depth Guide to Quantum Artificial Intelligence in 2022," *AI Multiple*, May 24, 2022, https://research.aimultiple.com/quantum-ai/ (accessed June 13, 2022).
5. Chris Jay Hoofnagle and Simson Garfinkel, "Quantum Cryptanalysis: Hype and Reality," *Lawfare* blog, February 16, 2022, https://www.lawfareblog.com/quantum-cryptanalysis-hype-and-reality (accessed June 13, 2022).
6. Amit Malewar, "Breakthrough Leads to Photonic Sensing at the Ultimate Quantum Limit," *Tech Explorist*, June 7, 2022, https://www.techexplorist.com/breakthrough-leads-photonic-sensing-ultimate-quantum-limit/47967/ (accessed June 13, 2022).
7. John Clarke and Frank K. Wilhelm, "Superconducting Quantum Bits," *Nature*, June 18, 2008, https://www.nature.com/articles/nature07128#:~:text=Superconducting%20quantum%20bits%20(qubits)%20form,inductance%20and%20no%20energy%20dissipation (accessed September 29, 2022).
8. Mikko Möttönen and Valtteri Lahtinen, "Why Superconducting Qubits Might Be the Path to Quantum Advantage," Quanscient, May 2, 2022, https://quanscient.com/blog/2022/05/02/why-superconducting-qubits-might-be-the-path-to-quantum-advantage/#superconducting-qubits (accessed September 30, 2022).
9. S. G. J. Philips et al., "Universal Control of a Six-Qubit Quantum Processor in Silicon," *Nature*, Vol. 609 (2022), pp. 919–924, https://doi.org/10.1038/s41586-022-05117-x (accessed September 30, 2022).
10. Elizabeth Gibney, "Quantum Computer Race Intensifies as Alternative Technology Gains Steam," *Nature*, November 17, 2020, https://www.nature.com/articles/d41586-020-03237-w (accessed September 30, 2022).
11. John Russell, "Quantum Watch: Neutral Atoms Draw Growing Attention as Promising Qubit Technology," HPC Wire, January 25, 2022, https://www.hpcwire.com/2022/01/25/quantum-watch-neutral-atoms-draw-growing-attention-as-promising-qubit-technology/ (accessed September 30, 2022).
12. Marric Stephens, "A New Option for Neutral-Atom Quantum Computing," *Physics*, Vol. 15, No. 55 (May 3, 2022), https://physics.aps.org/articles/v15/s55 (accessed September 30, 2022).
13. Ibid.
14. James Dargan, "6 Companies Working with Photonic Quantum Computing Technology in 2022," *The Quantum Insider*, March 24, 2022, https://thequantuminsider.com/2022/03/24/6-quantum-computing-companies-working-with-photonic-technology/#:~:text=Photonic%20quantum%20computing%20is%20a,along%20with%20the%20scattering%20unit (accessed September 30, 2022).
15. Charles Q. Choi, "In the Race to Hundreds of Qubits, Photons May Have 'Quantum Advantage,'" *IEEE Spectrum*, March 5, 2021, https://spectrum.ieee.org/race-to-hundreds-of-photonic-qubits-xanadu-scalable-photon (accessed October 3, 2022).
16. Ibid.
17. Philip Ball, "Major Quantum Computing Strategy Suffers Serious Setbacks," *Quantumagazine*, September 29, 2021, https://www.quantamagazine.org/major-quantum-computing-strategy-suffers-serious-setbacks-20210929/ (accessed October 3, 2022).
18. Jennifer Langston, "In a Historic Milestone, Azure Quantum Demonstrates Formerly Elusive Physics Needed to Build Scalable Topological Qubits," *Microsoft Innovation Stories*, March 14, 2022, https://news.microsoft.com/innovation-stories/azure-quantum-majorana-topological-qubit/#:~:text=The%20ability%20to%20create%20and,information%2C%20called%20a%20topological%20qubit (accessed October 3, 2022).
19. Rich Miller, "Inside Google's Quantum Computing Data Center," Data Center Frontier, November 22, 2021, https://datacenterfrontier.com/inside-googles-quantum-computing-data-center/ (accessed June 13, 2022).
20. News release, "How Quantum Computing Can Help Keep Things Cool," Honeywell, May 2022, https://www.honeywell.com/us/en/news/2022/05/how-quantum-computing-can-help-keep-things-cool (accessed June 13, 2022).
21. News release, "IBM Unveils New Roadmap to Practical Quantum Computing Era; Plans to Deliver 4,000+ Qubit System," IBM, May 10, 2022, https://newsroom.ibm.com/2022-05-10-IBM-Unveils-New-Roadmap-to-Practical-Quantum-Computing-Era-Plans-to-Deliver-4,000-Qubit-System (accessed June 13, 2022).

22. Leah Hesla, "Amazon Web Services Joins Q-NEXT Quantum Center," Argonne National Laboratory, May 18, 2022, https://www.anl.gov/article/amazon-web-services-joins-qnext-quantum-center (accessed June 13, 2022).

23. News release, "Intel Introduces Project Amber for Cloud-to-Edge and On-Premises Trust Assurance," Intel, May 11, 2022, https://www.intc.com/news-events/press-releases/detail/1545/intel-introduces-project-amber-for-cloud-to-edge-and (accessed June 13, 2022).

24. "Lockheed Martin Invests in Quantum Computing," *Digital Engineering 247*, December 4, 2021, https://www.digitalengineering247.com/article/lockheed-martin-invests-in-quantum-computing/ (accessed June 13, 2022).

25. Jennifer Langston, "In a Historic Milestone, Azure Quantum Demonstrates Formerly Elusive Physics Needed to Build Scalable Topological Qubits," Microsoft, March 14, 2022, https://news.microsoft.com/innovation-stories/azure-quantum-majorana-topological-qubit/ (accessed June 13, 2022).

26. Kelly McSweeney, "Disruptive Concepts and Technologies: Quantum Technology," Northrop Grumman, https://www.northropgrumman.com/what-we-do/disruptive-concepts-and-technologies-quantum-technology/ (accessed June 13, 2022).

27. Jane Lanhee Lee, "D-Wave Sets Up Latest Quantum Computer in California," Reuters, May 12, 2022, https://www.reuters.com/technology/d-wave-sets-up-latest-quantum-computer-california-2022-05-12/ (accessed June 13, 2022).

28. Stephen Shankland, "Quantum Computing's Impact Could Come Sooner Than You Think," CNET, September 16, 2022, https://www.cnet.com/tech/computing/quantum-computings-impact-could-come-sooner-than-you-think/ (accessed September 22, 2022).

29. Corinne Reichert, "Google Reportedly Attains 'Quantum Supremacy,'" CNET, September 25, 2019, https://www.cnet.com/tech/computing/google-reportedly-attains-quantum-supremacy/ (accessed June 13, 2022).

30. Jerry Chow, Oliver Dial, and Jay Gambetta, "IBM Quantum Breaks the 100-Qubit Processor Barrier," IBM, November 16, 2021, https://research.ibm.com/blog/127-qubit-quantum-processor-eagle (accessed June 13, 2022).

31. News release, "IBM Unveils Breakthrough 127-Qubit Quantum Processor," IBM, November 16, 2021, https://newsroom.ibm.com/2021-11-16-IBM-Unveils-Breakthrough-127-Qubit-Quantum-Processor (accessed June 24, 2022).

32. Charles Q. Choi, "An IBM Quantum Computer Will Soon Pass the 1,000-Qubit Mark," *IEEE Spectrum*, December 24, 2022, https://spectrum.ieee.org/ibm-condor (accessed February 9, 2023).

33. Qureca, "Overview on Quantum Initiatives Worldwide," September 7, 2020, https://www.qureca.com/overview-on-quantum-initiatives-worldwide/ (accessed June 21, 2022).

34. The White House, "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems," May 4, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/ (accessed June 24, 2022).

35. "Rigetti Computing Selected to Deliver Technology for Phase 2 of DARPA ONISQ Program," Global Newswire, January 27, 2022, https://www.globenewswire.com/news-release/2022/01/27/2374396/0/en/Rigetti-Computing-Selected-to-Deliver-Technology-for-Phase-2-of-DARPA-ONISQ-Program.html (accessed June 22, 2022).

36. Quantum.gov, "Quantum in the CHIPS and Science Act of 2022," August 9, 2022, https://www.quantum.gov/quantum-in-the-chips-and-science-act-of-2022/ (accessed September 23, 2022).

37. Quantum Computing Report, "U.S. CHIPS and Science Act: How Does It Impact Quantum?" August 9, 2022, https://quantumcomputingreport.com/u-s-chips-and-science-act-how-does-it-impact-quantum/ (accessed February 24, 2023).

38. Quantum annealing (which also includes adiabatic quantum computation) is a quantum computing method used to find the optimal solution of problems involving a large number of solutions, by taking advantage of properties specific to quantum physics, such as quantum tunneling, entanglement, and superposition.

39. News release, "USC to Lead IARPA Quantum Computing Project," University of Southern California, June 26, 2017, https://www.eurekalert.org/news-releases/465854 (accessed June 27, 2022), and Cem Dilmegani, "Quantum Annealing in 2022: Practical Quantum Computing," AI Multiple, June 14, 2022, https://research.aimultiple.com/quantum-annealing/ (accessed June 27, 2022).

40. Intelligence Advanced Research Project Activity, "LogiQ: Logical Qubits," https://www.iarpa.gov/research-programs/logiq (accessed February 24, 2023).

41. Intelligence Advanced Research Project Activity, "ELQ: Entangled Logical Qubits," https://www.iarpa.gov/research-programs/elq (accessed February 24, 2023).

42. Kelley M. Sayler, "Defense Primer: Quantum Technology," Congressional Research Service *Report for Congress*, updated May 6, 2022, https://crsreports.congress.gov/product/pdf/IF/IF11836 (accessed June 22, 2022).

43. Check Point, "What is a Zero-Day Attack?" https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-zero-day-attack/ (accessed June 22, 2022).

44. News release, "NIST Announces First Four Quantum-Resistant Cryptographic Algorithms," National Institute of Standards and Technology, July 5, 2022, https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms (accessed February 24, 2023).

45. Alexandra Kelley, "NIST Identifies 4 Quantum-Resistant Encryption Algorithms," Nextgov.com, July 5, 2022, https://www.nextgov.com/cybersecurity/2022/07/nist-identifies-four-quantum-resistant-encryption-algorithms/368954/ (accessed July 5, 2022).

46. News release, "NCCoE Announces Technology Collaborators for the Migration to Post-Quantum Cryptography Project," National Institute of Standards and Technology, July 15, 2022, https://content.govdelivery.com/accounts/USNIST/bulletins/31f0b39 (accessed July 19, 2022).

47. Alexandra Kelley, "NSA Releases Post-Quantum Algorithms, Aims for Full Implementation by 2035," Nextgov.com, September 8, 2022, https://www.nextgov.com/cybersecurity/2022/09/nsa-releases-post-quantum-algorithms-aims-full-implementation-2035/376880/ (accessed September 23, 2022).

48. Kevin Townsend, "AI Helps Crack NIST-Recommended Post-Quantum Encryption Algorithm," *Security Week*, February 21, 2023, https://www-securityweek-com.cdn.ampproject.org/c/s/www.securityweek.com/ai-helps-crack-a-nist-recommended-post-quantum-encryption-algorithm/amp/ (accessed March 6, 2023).

49. Mariam Baksh, "NIST Selects 12 Companies for Implementing Post-Quantum Cryptography," Nextgov.com, July 18, 2022, https://www.nextgov.com/cybersecurity/2022/07/nist-selects-12-companies-implementing-post-quantum-cryptography/374601/ (accessed July 19, 2022).

50. News release, "The Launch of the Quantum Flagship," Quantum Flagship, October 29, 2018, https://qt.eu/about-quantum-flagship/newsroom/quantum-flagship-launch-press-release/ (accessed July 11, 2022).

51. Keith Cowing, "Thales Alenia Space and Partners Sign Contract With European Space Agency for TeQuantS Quantum Satellite Communications Project," SpaceRef, January 23, 2023, https://spaceref.com/newspace-and-tech/thales-alenia-space-and-partners-sign-contract-with-european-space-agency-for-tequants-quantum-satellite-communications-project/ (accessed January 23, 2023).

52. News release, "EU Innovation Moves One Step Closer to the World's First Compact Quantum Computer," Quantum Flagship, October 26, 2021, https://qt.eu/about-quantum-flagship/newsroom/first-eu-compact-quantum-computer/ (accessed June 22, 2022).

53. Dashveenjit Kaur, "Where Does EU Stand in the Quantum Computing Race with China and US?" T_HQ Technology and Business, December 3, 2021, https://techhq.com/2021/12/where-does-eu-stand-in-the-quantum-computing-race-with-china-and-us/ (accessed June 22, 2022).

54. S. L. N. Hermans et al., "Qubit Teleportation Between Non-Neighboring Nodes in a Quantum Network," *Nature*, No. 605 (May 25, 2022), pp. 663–668, https://doi.org/10.1038/s41586-022-04697-y (accessed June 22, 2022).

55. Brian Greene, "Spooky Action at a Distance" *NOVA*, September 22, 2011, https://www.pbs.org/wgbh/nova/article/spooky-action-distance/ (accessed June 22, 2022); Cade Metz, "'Quantum Internet' Inches Closer with Advance in Data Teleportation," *The New York Times*, May 25, 2022, https://www.nytimes.com/2022/05/25/technology/quantum-internet-teleportation.html (accessed June 22, 2022); and Martijn Boerkamp, "Quantum Teleportation Expands Beyond Neighbouring Nodes," *Physics World*, May 25, 2022, https://physicsworld.com/a/quantum-teleportation-expands-beyond-neighbouring-nodes/ (accessed July 6, 2022).

56. "Germany to Support Quantum Computing with 2 Billion Euros," Reuters, May 11, 2021, https://www.reuters.com/article/us-germany-quantumcomputer-idUSKBN2CS0W9 (accessed July 11, 2022).

57. UK Research and Innovation, "UK National Quantum Technologies Programme," https://uknqt.ukri.org/ (accessed February 27, 2023).

58. News release, "Russia Sets Up Lab to Create Quantum Computer," XinhuaNET, November 25, 2020, http://www.xinhuanet.com/english/2020-11/25/c_139542572.htm (accessed February 27, 2023).

59. "Russia: Moscow Divvies Up 5G and Quantum Development Among Its Proxies," RANE Worldview, July 10, 2019, https://worldview.stratfor.com/article/russia-moscow-charts-state-course-5g-quantum-emerging-tech-development (accessed July 11, 2022).

60. Dan O'Shea, "Russia Reaches Milestone On Quantum Computing Roadmap," *Inside Quantum Technology News*, December 30, 2021, https://www.insidequantumtechnology.com/news-archive/russia-reaches-milestone-on-quantum-computing-roadmap/ (accessed June 22, 2022).

61. Mariana Iriarte, "Russia Invests $750 M into Its Quantum Future," HPC Wire, January 6, 2020, https://www.hpcwire.com/2020/01/06/russia-invests-790m-into-its-quantum-future/ (accessed June 22, 2022).

62. Yun Sun, "China's Strategic Assessment of Russia: More Complicated Than You Think," *War on the Rocks*, March 4, 2022, https://warontherocks.com/2022/03/chinas-strategic-assessment-of-russia-more-complicated-than-you-think/ (accessed July 5, 2022).

63. Matt Swayne, "How Will the Ukraine–Russia Crisis Affect Quantum?" *The Quantum Insider*, March 10, 2022, https://thequantuminsider.com/2022/03/10/how-will-the-ukraine-russia-crisis-affect-quantum/ (accessed, July 5, 2022).

64. Christopher Weidacher Hsiung, "China's Technology Cooperation with Russia: Geopolitics, Economics, and Regime Security," *The Chinese Journal of International Politics*, Vol. 14, No. 3 (2021), pp. 447–479, https://doi.org/10.1093/cjip/poab009 (accessed February 21, 2023).

65. Mateusz Masiowski et al., "Quantum Computing Funding Remains Strong, But Talent Gap Raises Concern," McKinsey Digital, June 2022, https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/quantum-computing-funding-remains-strong-but-talent-gap-raises-concern (accessed March 2, 2023).

66. Dashveenjit Kaur, "China Has Quantum Computers that Are 1 Million Times More Powerful than Google's," T_HQ Technology and Business, October 28, 2021, https://techhq.com/2021/10/china-has-quantum-computers-that-are-a-million-times-more-powerful-than-googles/ (accessed June 22, 2022).

67. Patrick Tucker, "Is China About to Destroy Encryption As We Know It? Maybe," *Defense One*, January 20, 2023, https://www.defenseone.com/technology/2023/01/china-about-destroy-encryption-we-know-it-maybe/382041/ (accessed January 23, 2023).

68. Bao Yan et al., "Factoring Integers with Sublinear Resources on a Superconducting Quantum Processor," arXiv, December 23, 2022, https://www.researchgate.net/publication/366587622_Factoring_integers_with_sublinear_resources_on_a_superconducting_quantum_processor (accessed January 23, 2023).

69. Simon Sharwood, "Warning: China Planning to Swipe a Bunch of Data Soon So Quantum Computers Can Decrypt It Later," *The Register*, November 29, 2021, https://www.theregister.com/2021/11/29/china_quantum_ai_offensive/ (accessed June 22, 2022).

70. John Keller, "China Launches Cloud-Based Quantum Computing Operating System Software to Challenge U.S. in Technology," Military Aerospace Electronics, February 23, 2021, https://www.militaryaerospace.com/computers/article/14198004/operating-system-quantum-computing-software (accessed June 22, 2022).

71. Liu Zhen, "China's Latest Quantum Radar Won't Just Track Stealth Bombers, But Ballistic Missiles in Space Too," *South China Morning Post*, June 15, 2018, https://www.scmp.com/news/china/diplomacy-defence/article/2151086/chinas-latest-quantum-radar-wont-just-track-stealth (accessed June 21, 2022), and Michael J. Biercuk, "Read Before Pontificating on Quantum Technology," *War on the Rocks*, July 13, 2020, https://warontherocks.com/2020/07/read-before-pontificating-on-quantum-technology/ (accessed June 21, 2022).

72. Cloud Security Alliance, "What Is Quantum Key Distribution?" Quantum-Safe Security Working Group, August 2015, https://www.quintessencelabs.com/wp-content/uploads/2015/08/CSA-What-is-Quantum-Key-Distribution-QKD-1.pdf (accessed July 13, 2022).

73. Ibid.

74. Hamish Johnston, "Quantum Cryptography Network Spans 4600 km in China," *PhysicsWorld*, January 7, 2021, https://physicsworld.com/a/quantum-cryptography-network-spans-4600-km-in-china/#:~:text=A%20network%20for%20quantum%20key%20distribution%20%28QKD%29%20spanning,location%20in%20the%20far%20west%20of%20the%20country (accessed, July 5, 2022).

75. Ibid.

76. Elsa B. Kania and John K. Costello, "Quantum Hegemony? China's Ambitions and the Challenge to U.S. Innovation Leadership," Center for a New American Security, 2018, p. 14, https://www.7tunnels.com/wp-content/uploads/2019/10/CNASReport-Quantum-Tech_FINAL.pdf (accessed February 27, 2023).

77. Ibid., p. 15.

78. Ibid., p. 22.

79. Ibid.

80. Ibid.

81. National Quantum Coordination Office, "Enhancing Competitiveness," https://www.quantum.gov/competitiveness/#INTERNATIONAL-COOPERATION (accessed July 11, 2022).

82. Alexandra Kelley, "More International Quantum Partnerships Likely as U.S. Stakes Claim in Field," Nextgov, April 14, 2022, https://www.nextgov.com/emerging-tech/2022/04/more-international-quantum-partnerships-likely-us-stakes-claim-field/365664/ (accessed September 23, 2022).

83. News release, "DRDO and IIT Delhi Scientists Demonstrate Quantum Key Distribution Between Two Cities 100 Kilometres Apart," Indian Ministry of Defense, February 23, 2022, https://pib.gov.in/PressReleasePage.aspx?PRID=1800648 (accessed June 30, 2022).

84. Jaspreet Gill, "'Disruptive Impact': India's Military Starts Investing in Quantum Key Distribution," *Breaking Defense*, September 1, 2022, https://breakingdefense.com/2022/09/disruptive-impact-indias-military-starts-investing-in-quantum-key-distribution/ (accessed January 23, 2023).

85. "Quantum Technology Can Add $310 Billion to Indian Economy by 2030," *Economy India*, February 9, 2022, https://economyindia.in/quantum-technology-can-add-310-billion-to-indian-economy-by-2030/ (accessed June 28, 2022).

86. Romita Majumdar, "Quantum Technology Can Add $310 Billion to Indian Economy by 2030," *The Economic Times*, February 8, 2022, https://economictimes.indiatimes.com/tech/tech-bytes/quantum-technology-can-add-310-billion-to-indian-economy-by-2030/articleshow/89416916.cms?from=mdr (accessed September 26, 2022).

87. Dustin Carmack et al., "India–U.S. Relations, Priorities in the Next Decade," Observer Research Foundation and The Heritage Foundation, June 2022, https://www.orfonline.org/wp-content/uploads/2022/06/ORF-Heritage_India-US-Priorities.pdf (accessed July 6, 2022).

88. Campbell Kawn, "Australia Prioritises 63 Critical Technologies Including Quantum and Blockchain," ZDNet, November 16, 2021, https://www.zdnet.com/article/australia-priorities-63-critical-technologies-including-quantum-and-blockchain/ (accessed June 27, 2022).

89. U.S. Department of State, "Cooperation in Quantum Science and Technology," joint statement by the United States and Australia, November 17, 2021, https://www.state.gov/cooperation-in-quantum-science-and-technology-aus (accessed February 27, 2023).

90. The White House, "Fact Sheet: Implementation of the Australia–United Kingdom–United States Partnership (AUKUS)," April 5, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/05/fact-sheet-implementation-of-the-australia-united-kingdom-united-states-partnership-aukus/ (accessed January 23, 2023).

91. Alexandra Kelley, "The Future of Quantum Security Will Be Encoded in Light, Researchers Hope," NextGov, January 20, 2023, https://www.nextgov.com/cybersecurity/2023/01/future-quantum-security-will-be-encoded-light-researchers-hope/382037/ (accessed January 23, 2023).

92. Dashveenjit Kaur, "Japan's First Domestic Quantum Computer Targets 10m Users by 2030," TechWire Asia, April 18, 2022, https://techwireasia.com/2022/04/japans-first-domestic-quantum-computer-targets-10m-users-by-2030/ (accessed July 7, 2022).
93. Ibid.
94. Ibid.
95. Baichun Zhang, Jiuchun Zhang, and Fang Yao, "Technology Transfer from the Soviet Union to the People's Republic of China 1949–1966," *Comparative Technology Transfer and Society*, Vol. 4, No. 2 (August 2006), pp. 105–171, http://english.ihns.cas.cn/Publications_new/Ra/201310/W020131015378079814609.pdf (accessed March 6, 2023).
96. Christopher Weidacher Hsiung, "China's Technology Cooperation with Russia: Geopolitics, Economics, and Regime Security," *The Chinese Journal of International Politics*, Vol. 14, No. 3 (2021), pp. 447–479, https://doi.org/10.1093/cjip/poab009 (accessed June 28, 2022).
97. Ibid., p. 451.
98. Ibid., p. 454.
99. Ibid.
100. Ibid.
101. Ibid.
102. Ibid., p. 455.
103. Ibid.
104. Sun, "China's Strategic Assessment of Russia: More Complicated Than You Think."
105. Ibid.
106. Ibid.
107. Sayler, "Defense Primer: Quantum Technology," p. 2.
108. Alex Rossino, "Planned DOD Quantum Information Sciences Investment," GovWin Deltek, February 9, 2022, https://iq.govwin.com/neo/marketAnalysis/view/Planned-DOD-Quantum-Information-Sciences-Investment/6397?researchTypeId=1&researchMarket= (accessed June 22, 2022).
109. Sayler, "Defense Primer: Quantum Technology," p. 2.
110. The White House, "Fact Sheet: President Biden Announces Two Presidential Directives Advancing Quantum Technologies," May 4, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/fact-sheet-president-biden-announces-two-presidential-directives-advancing-quantum-technologies/ (accessed June 22, 2022).
111. The White House, "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems," May 4, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/ (accessed June 29, 2022).
112. Ibid.
113. The National Quantum Initiative, "QIS Centers," 2022, https://www.quantum.gov/action/ (accessed June 22, 2022), and U.S. Department of State, "Joint Statement of the United States of America and Switzerland on Cooperation in Quantum Information Science and Technology," October 21, 2022, https://www.state.gov/joint-statement-of-the-united-states-of-america-and-switzerland-on-cooperation-in-quantum-information-science-and-technology/ (accessed January 23, 2023).
114. Rebecca Pifer, "How Close Is Quantum Computing in Healthcare?" Healthcare Dive, July 19, 2021, https://www.healthcaredive.com/news/how-close-quantum-computing-in-healthcare-clinical-trials-payers-providers/600554/ (accessed June 21, 2022).
115. Tim Bowler, "How Quantum Sensing Is Changing the Way We See the World," BBC News, March 8, 2019, https://www.bbc.com/news/business-47294704 (accessed June 22, 2022).
116. Wusheng Wang et al., "Quantum Blockchain Based on Asymmetric Quantum Encryption and a Stake Vote Consensus Algorithm," *Nature Scientific Reports*, No. 12 (2022), p. 8606, https://doi.org/10.1038/s41598-022-12412-0 (accessed June 22, 2022).
117. Chris Jaikaran, "Preparing Secrets for a Post-Quantum World—National Security Memorandum 10," Congressional Research Service *Report for Congress*, May 9, 2022, https://crsreports.congress.gov/product/pdf/IF/IF11836 (accessed June 22, 2022).
118. Brandi Vincent, "China May Steal Encrypted Government Data Now to Decrypt with Quantum Computers Later," Nextgov.com, November 22, 2021, https://www.nextgov.com/emerging-tech/2021/11/report-china-may-steal-encrypted-government-data-now-decrypt-quantum-computers-later/187020/ (accessed June 22, 2022), and Booz Allen Hamilton, "Chinese Threats in the Quantum Era," https://www.boozallen.com/expertise/analytics/quantum-computing/chinese-cyber-threats-in-the-quantum-era.html (accessed July 12, 2022).
119. Akira Oikawa, Yuki Okoshi, and Yuki Misum, "China Emerges as Quantum Tech Leader While Biden Vows to Catch Up," Nikkei Asia, March 14, 2021, https://asia.nikkei.com/Spotlight/Datawatch/China-emerges-as-quantum-tech-leader-while-Biden-vows-to-catch-up (accessed September 26, 2022).

120. Stephen Shankland, "US Blocks Export of Quantum Computing Tech to Chinese Organizations," CNET, November 24, 2022, https://www.cnet.com/tech/computing/us-blocks-export-of-quantum-computing-tech-to-chinese-organizations/ (accessed June 22, 2022).

121. Brian Liu and Raquel Leslie, "U.S.–China Tech Decoupling Accelerates with New Export Controls on Chinese Quantum Computing Companies," *Lawfare*, December 1, 2021, https://www.lawfareblog.com/us-china-tech-decoupling-accelerates-new-export-controls-chinese-quantum-computing-companies (accessed June 22, 2022).

122. Kate O'Keeffe, "Export Controls Against Russia Add to Uncertainty for Business," *The Wall Street Journal*, March 2, 2022, https://www.wsj.com/articles/export-controls-against-russia-add-to-uncertainty-for-business-11646245942 (accessed June 22, 2022), and The White House, "Fact Sheet: United States Takes Further Actions to Counter Sanctions Evasion by Russia," June 2, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/06/02/fact-sheet-united-states-takes-further-actions-to-counter-sanctions-evasion-by-russia/ (accessed June 22, 2022).

123. John D. McKinnon and Asa Fitch, "U.S. Restricts Semiconductor Exports in Bid to Slow China's Military Advance," *The Wall Street Journal*, October 7, 2022, https://www.wsj.com/articles/u-s-restricts-semiconductor-exports-in-bid-to-slow-chinas-military-advance-11665155702 (accessed January 23, 2023), and Asa Fitch and John D. McKinnon, "U.S. Seeks to Further Restrict Cutting-Edge Chip Exports to China," *The Wall Street Journal*, October 3, 2022, https://www.wsj.com/articles/u-s-seeks-to-further-restrict-cutting-edge-chip-exports-to-china-11664846407?st=o4l2djez7morzq6&reflink=desktopwebshare_permalink (accessed October 5, 2022).

124. University of New South Wales, "Hot Qubits Break One of the Biggest Constraints to Practical Quantum Computers," *ScienceDaily*, April 15, 2020, http://www.sciencedaily.com/releases/2020/04/200415110453.htm (accessed June 22, 2022).

125. Sebastian Moss, "Cooling Quantum Computers," Data Center Dynamics, January 27, 2021, https://www.datacenterdynamics.com/en/analysis/cooling-quantum-computers/#:~:text=Cooling%20quantum%20computers%201%20Keeping%20things%20cool.%20To,3%20Quantum%20computing%20comes%20to%20the%20cloud.%20 (accessed June 22, 2022).

126. Pat Brans, "Finland Brings Cryostats and Other Cool Things to Quantum Computing," *Tech Target ComputerWeekly*, February 2, 2022, https://www.computerweekly.com/feature/Finland-brings-cryostats-and-other-cool-things-to-quantum-computing (accessed June 22, 2022).

127. Ibid.

128. Meredith Roaten, "Algorithmic Warfare: DARPA Probing Quantum Computing Capabilities (UPDATED)," *National Defense*, June 6, 2023, https://www.nationaldefensemagazine.org/articles/2022/6/23/darpa-probing-quantum-computing-capabilities (accessed June 24, 2022).

129. Ibid.

130. Ibid.

131. Yen Nee Lee, "China's Rare Earth Exports Fell in May Amid Trade War with the US," CNBC, June 10, 2019, https://www.cnbc.com/2019/06/10/china-exports-of-rare-earths-fell-in-may-amid-trade-war-with-the-us.html (accessed June 22, 2022).

132. Ibid.

133. Earth.org, "How Rare-Earth Mining Has Devastated China's Environment," July 14, 2020, https://earth.org/rare-earth-mining-has-devastated-chinas-environment/ (accessed July 13, 2022).

134. Ibid.

135. Yen Nee Lee, "China's Rare Earths Exports Fell in May Amid Trade War with the US," CNBC, July 10, 2019, https://www.cnbc.com/2019/06/10/china-exports-of-rare-earths-fell-in-may-amid-trade-war-with-the-us.html (accessed July 13, 2022).

136. Samantha Subin, "The New U.S. Plan to Rival China and End Cornering of Market in Rare Earth Metals," CNBC, April 19, 2021, https://www.cnbc.com/2021/04/17/the-new-us-plan-to-rival-chinas-dominance-in-rare-earth-metals.html (accessed July 6, 2022).

137. Doug Palmer, "U.S. Decides Against National Security Tariffs on Rare Earth Magnets from China, Japan, EU," *Politico*, September 21, 2022, https://www.politico.com/news/2022/09/21/biden-national-security-tariffs-earth-magnets-china-japan-eu-00057920 (accessed September 26, 2022).

138. Matt Swayne, "Researchers See Path to Quantum Computing at Room Temperature," *The Quantum Insider*, May 5, 2020, https://thequantuminsider.com/2020/05/05/researchers-see-path-to-quantum-computing-at-room-temperature/ (accessed June 24, 2022).

139. U.S. Army CCDC Army Research Laboratory Public Affairs, "Army Researchers See Path to Quantum Computing at Room Temperature," April 30, 2020, https://www.army.mil/article/235127/army_researchers_see_path_to_quantum_computing_at_room_temperature (accessed June 29, 2022).

140. Ibid.

141. Ibid.

142. Adam Zewe, "A New Way for Quantum Computing Systems to Keep Their Cool," *MIT News Office*, February 21, 2023, https://news.mit.edu/2023/new-way-quantum-computing-systems-keep-their-cool-0221 (accessed March 6, 2023).

143. Ibid.

144. Sayler, "Defense Primer: Quantum Technology."

145. Katie Kline, Marco Salvo, and Donyae Johnson, "How Artificial Intelligence and Quantum Computing Are Evolving Cyber Warfare," The Institute of World Politics, March 27, 2019, https://www.iwp.edu/cyber-intelligence-initiative/2019/03/27/how-artificial-intelligence-and-quantum-computing-are-evolving-cyber-warfare/ (accessed July 11, 2022).
146. The National Institute of Standards and Technology, "Post Quantum Cryptography (PQC)," https://csrc.nist.gov/Projects/post-quantum-cryptography (accessed June 22, 2022).
147. National Security Agency, Central Security Service, "Post-Quantum Cybersecurity Resources," 2022, https://www.nsa.gov/Cybersecurity/Post-Quantum-Cybersecurity-Resources/ (accessed June 22, 2022).
148. Kevin Townsend, "British Firm Tackles 'Harvest Now, Decrypt Later' Problem with Sharding Technology," *Security Week*, March 3, 2022, https://www.securityweek.com/british-firm-tackles-harvest-now-decrypt-later-problem-sharding-technology (accessed June 21, 2022).
149. Sayler, "Defense Primer: Quantum Technology," p. 1.
150. Michal Krelina, "Quantum Warfare: Definitions, Overview and Challenges," *EPJ Quantum Technology*, Vol. 8, Article 24 (November 6, 2021), https://doi.org/10.1140/epjqt/s40507-021-00113-y (accessed January 25, 2023).
151. Ibid.
152. Ibid.
153. Ibid.
154. Ibid.
155. Ibid.
156. Ibid.
157. Ibid.
158. Yonah Jeremy Bob, "Will Rafael's Quantum Research Change the Face of Submarine, Aerial, and Networked Warfare?" *The Jerusalem Post*, January 20, 2022, https://www.jpost.com/israel-news/article-694108?utm_source=newsletter&utm_medium=email&utm_campaign=newsletter_axioswhatsnext&stream=science (accessed February 21, 2023).
159. "SandboxAQ Awarded U.S. Air Force Contract for Quantum Navigation Research," PR Newswire, January 30, 2023, https://www.prnewswire.com/news-releases/sandboxaq-awarded-us-air-force-contract-for-quantum-navigation-research-301732942.html?utm_source=newsletter&utm_medium=email&utm_campaign=newsletter_axioswhatsnext&stream=science (accessed February 21, 2023).
160. Ibid.
161. Krelina, "Quantum Warfare: Definitions, Overview and Challenges."
162. "SandboxAQ Awarded U.S. Air Force Contract for Quantum Navigation Research," PR Newswire.
163. Krelina, "Quantum Warfare: Definitions, Overview and Challenges."
164. "SandboxAQ Awarded U.S. Air Force Contract for Quantum Navigation Research," PR Newswire.
165. Ibid.
166. Ibid.
167. Krelina, "Quantum Warfare: Definitions, Overview and Challenges."
168. "SandboxAQ Awarded U.S. Air Force Contract for Quantum Navigation Research," PR Newswire.
169. Ibid.
170. Sayler, "Defense Primer: Quantum Technology."
171. U.S. Department of Energy, "The State of the DOE National Laboratories 2020 Edition," https://www.energy.gov/sites/default/files/2021/01/f82/DOE%20National%20Labs%20Report%20FINAL.pdf (accessed July 12, 2022).
172. Mateusz Masiowski et al., "Quantum Computing Funding Remains Strong, But Talent Gap Raises Concerns," McKinsey Digital, June 15, 2022, https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/quantum-computing-funding-remains-strong-but-talent-gap-raises-concern (accessed July 12, 2022).
173. H.R. 1837, Quantum User Expansion for Science and Technology (QUEST) Act of 2021, https://www.congress.gov/bill/117th-congress/house-bill/1837?r=5&s=2 (accessed July 13, 2022).
174. Matthew Stepp et al., "Turning the Page: Reimagining the National Labs in the 21st Century Innovation Economy," The Information Technology and Innovation Foundation, The Center for American Progress, and The Heritage Foundation, June 2013, https://www2.itif.org/2013-turning-page-national-lab-innovation-economy.pdf (accessed July 13, 2022).
175. The White House, "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems," https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/ (accessed July 12, 2022).

176. Kania and Costello, "Quantum Hegemony? China's Ambitions and the Challenge to U.S. Innovation Leadership," p. 29, and Zhanna L. Malekos Smith, "What China's Targeting of US Telecoms Means for Post-Quantum Security," *The Hill*, June 14, 2022, https://thehill.com/opinion/cybersecurity/3520574-what-chinas-targeting-of-us-telecoms-means-for-post-quantum-security/ (accessed July 13, 2022).
177. Chandelis Duster, "Top Military Leader Says China's Hypersonic Missile Test 'Went around the World,'" CNN, November 18, 2021, https://www.cnn.com/2021/11/17/politics/john-hyten-china-hypersonic-weapons-test/index.html (accessed March 1, 2023).
178. H.R. 7535, Quantum Computing Cybersecurity Preparedness Act, 117th Congress, https://www.congress.gov/bill/117th-congress/house-bill/7535?q=%7B%22search%22%3A%5B%22Quantum+Computing+Cybersecurity+Preparedness+Act%22%2C%22Quantum%22%2C%22Computing%22%2C%22Cybersecurity%22%2C%22Preparedness%22%2C%22Act%22%5D%7D&r=1&s=1 (accessed July 13, 2022).
179. Subcommittee on Quantum Information Science, Committee on Science, "Quantum Information Science and Technology Workforce Development National Strategic Plan," White House National Science and Technology Council, February 2022, https://www.quantum.gov/wp-content/uploads/2022/02/QIST-Natl-Workforce-Plan.pdf (accessed July 15, 2022).
180. Stanley Kurtz, "Biden vs. DeSantis: The Unknown Clash," *National Review*, August 9, 2022, https://www.nationalreview.com/corner/biden-vs-desantis-the-unknown-clash/ (accessed September 28, 2022).
181. Lindsey M. Burke, "Lee's College Accreditation Legislation Could Drive Down College Costs," The Daily Signal, January 10, 2014, https://www.dailysignal.com/2014/01/10/lees-college-accreditation-legislation-drive-college-costs/ (accessed September 28, 2022).
182. The Heritage Foundation, "Protecting K–12 Students from Discrimination," June 18, 2021, https://www.heritage.org/article/protecting-k-12-students-discrimination (accessed July 15, 2022).
183. Office of the President, Howard University, "Howard University to Lead IBM's First Quantum Education and Research Initiative for Historically Black Colleges and Universities," October 5, 2020, https://president.howard.edu/from-the-president/viewpoints/howard-university-lead-ibms-first-quantum-education-and-research (accessed July 15, 2022).
184. Antoaneta Roussi and Laurens Cerulus, "NATO Aims to Take on Russia with Its Own Cyber Military-Industrial Complex," PoliticoPro Cybersecurity, June 29, 2022, https://subscriber.politicopro.com/article/2022/06/nato-aims-to-take-on-russia-with-its-own-cyber-military-industrial-complex-00043088 (accessed July 15, 2022).
185. News release, "NATO Sharpens Technological Edge with Innovation Initiatives," North Atlantic Treaty Organization, April 7, 2022, https://www.nato.int/cps/en/natohq/news_194587.htm (accessed March 1, 2023).
186. The Physics arXiv Blog, "The Future of Space-Based Quantum Technology," *Discover*, July 22, 2021, https://www.discovermagazine.com/technology/the-future-of-space-based-quantum-technology (accessed July 12, 2022).
187. Dustin Carmack, "U.S. Must Implement Lessons on 'Hybrid' Conflict from Ukraine War," Heritage Foundation *Backgrounder* No. 3704, April 28, 2022, https://www.heritage.org/cybersecurity/report/us-must-implement-lessons-hybrid-conflict-ukraine-war.
188. Dustin Carmack, "CHIPS Is a Missed Opportunity for Real Security," The Daily Signal, August 1, 2022, https://www.dailysignal.com/2022/08/01/chips-is-a-missed-opportunity-for-real-security?_gl=1*uh78gp*_ga*MTYyMDE5NTc1OS4xNjYwNjYwMDAx*_ga_W14BT6YQ87*MTY2NDQ2OTQwMi41Ni4xLjE2NjQ0Njk0MTcuNDUuMC4w.
189. Booz Allen Hamilton, "Chinese Threats in the Quantum Era."
190. The National Quantum Initiative, "QIS Centers."

The Heritage Foundation
214 Massachusetts Ave., NE | Washington, DC 20002
(202) 546-4400 | heritage.org