Winning the Race in Quantum Computing

ARTHUR HERMAN APRIL 18, 2018

Imagine a computer solving the mathematical problems that today's fastest supercomputers can't begin to unlock, in less than a blink of an eye. Imagine a technology that can enable an observer to see through walls, or see into the darkest depths of the world's oceans. Imagine a technology that can build essentially unhackable global networks, while rendering an antagonist's most secret data instantly transparent.

All these are characteristics of quantum computers and quantum technology, which will define the future of global information technology for decades, possibly centuries, to come. It represents a revolution as profound as any in modern history, and it's one on which we stand at the brink, with all its promise—and its perils.

The twentieth century saw humanity unleash and harness the almost unimaginable power of the atom, and so launch a new era in human history, the Nuclear Age. Now we are witnessing the birth of a new era in information technology based on the power of quanta. In the Quantum Age, computers will draw their computational capability from the complex and counterintuitive principles of quantum mechanics, which may transform the world almost as decisively as the Nuclear Age did.

Quantum computers won't look like today's computers. They won't have a keyboard or a monitor. They will be complex installations, impressive monuments to physics and engineering using cryogenics for cooling lasers in subzero temperatures, along with other solid-state and optical devices.

Today, more than twenty nations are competing to win the quantum future. One of those is the United States, whose major IT companies—Microsoft, Intel, Google, IBM—are currently leading efforts to develop the world's first fully functional quantum computer.

Another competitor is China, which recently announced that it will create an $11 billion, four-million-square-foot national quantum laboratory in the city of Hefei. This facility will be dedicated to making China a global leader in quantum technology, helping China achieve what experts call "quantum supremacy": the moment when a quantum computer can do tasks that a classical or digital computer, even today's most powerful supercomputers, cannot.

China has already shown its skill in developing quantum technological applications, such as the 2016 launch of the Micius quantum satellite, a crucial step in establishing a secure ground-to-space quantum communications network. The Chinese have also made key advancements in developing a similarly unhackable 2,000-kilometer quantum communications network from Shanghai to Beijing. Chinese military scientists even claim to have engineered a quantum-based "radar" capable of penetrating today's current stealth technologies—technologies that have served as the foundation of American military air supremacy since the Gulf War, as well as of the U.S. Navy's most advanced stealth submarines.[1]

Russia is also investing in quantum computing, spearheaded by the Russian Quantum Center (RQC). Scientists at the RQC announced in July 2017 that they had achieved a major breakthrough in creating a quantum computer that can do general computations—an important landmark on the road to "quantum supremacy."[2] Even North Korea has announced plans to become "a quantum power" in the twenty-first century.

As Representative Will Hurd of Texas, chairman of the congressional subcommittee on information technology, put it: "The impact of quantum on our national defense will be tremendous. The question is whether the United States and its allies will be ready" when the full quantum revolution takes hold.[3]

The implications of the quantum race are profound. The outcome will determine the twenty-first-century answer to an age-old question, the one posed in *Alice's Adventures in Wonderland*: "Who is to be master?"

That question was answered in the seventeenth and eighteenth centuries by the country which possessed the biggest navy and the most colonies: in that case, Great Britain was the master. In the nineteenth and twentieth centuries it was the country that had the most advanced military technologies and the biggest industrial base, including nuclear weapons. In the end, the United States emerged on top.

In the twenty-first century, supremacy will belong to the nation that controls the future of information technology, which is quantum. As we will see, it would be a mistake to assume that the United States is destined to be in this position. In the topsy-turvy, counterintuitive world of quantum

mechanics and quantum computing, decades-long dominance in IT doesn't automatically translate into dominance in the coming era. But strategy and commitment of resources, including funding, almost certainly will—and with it, the balance of the future.

What Quantum Can Do, and What It Can't

How does quantum computing work, and why are quantum computers destined to be superior to conventional digital computers?

The answer lies in the bizarre world of quantum mechanics, where subatomic particles like electrons and photons can seemingly exist in multiple states (physicists call this superposition). All current computers, even supercomputers, process data in a linear sequence of ones and zeros. Every "bit," the smallest unit of data, has to be either a zero or a one. But a quantum bit or "qubit" can be a zero and a one at the same time, enabling multiple computations at once. So while a traditional computer has to sequentially explore the potential solutions to a mathematical problem, a quantum system is able to look at every potential solution simultaneously and generate answers—not just the single "best" but nearly ten thousand close alternatives as well—in less than a second: roughly the equivalent of being able to read every book in the Library of Congress at once, instead of one at a time, in order to find the one that answers a specific question.

Add more qubits and the quantum computing power actually grows exponentially—i.e. reading every book in the library at once happens faster and faster. So while conventional computers rely on huge numbers of transistors to achieve their computing speed, quantum computers use atoms

and subatomic particles as their physical system. No one can predict where the particles will end up, or what form they will eventually take. As MIT physicist Seth Lloyd put it to *Wired* magazine, "Quantum mechanics is just counterintuitive and we just have to suck it up."[4]

But the numbers work, as do the computations. For example, Google and NASA are currently using a quantum computing machine (the D-WaveX2) that can do certain computations at one hundred million times the speed of a traditional computer chip—and that operates 3,600 times faster than the world's fastest digital supercomputer.

There are, in fact, three types of quantum computers currently in use. The D-Wave system is an example of a quantum annealer and is used for solving sampling and optimization problems, such as finding the best route between two points—something classical computers have great difficulty doing. Quantum annealers do not try to manipulate the qubits while they are computing, and therefore they can do calculations using one thousand qubits, which become entangled (able to exhibit multiple states) more or less at random.

The second type of quantum computing model is that of an analog emulator, which can simulate physical processes. This might include, for example, simulating certain aspects of the earth's climate in a controlled experiment or simulating the best way for electricity to be transmitted without loss. These simulators have been built with up to fifty-one qubits.

A universal quantum computer—the Holy Grail of quantum computing (and what most commentators are referring to when they discuss quantum

computing)—would be able to run any type of algorithm and discover patterns in data sets that existing computers cannot analyze. The computing power needed for a universal quantum computer, however, requires entangling the qubits throughout the entire time of computing—a very difficult feat. At the moment, only twenty qubits have been effectively entangled in such a quantum computer.

Why is getting to the universal computer standard so difficult? Since subatomic particles are inherently unstable, keeping sufficient numbers of qubits entangled long enough to do calculations takes persistence, time, and resources.

The instability of qubits is called decoherence, and it is one of the chief engineering problems facing quantum scientists. When a qubit decoheres, it loses its superposition and can no longer act as both zero and one at the same time, but only one or the other, thus losing the ability to compute in a quantum manner. A qubit can decohere due to the slightest disturbance, which is why engineers are working on ways to mitigate the effects of minute disruptions of light, sound, and movement—and also why many quantum computers are built inside vacuums.

Nonetheless, a quantum computer capable of solving problems that would stump a classical computer is close at hand. Experts believe fifty qubits will be the formal threshold of "quantum supremacy." IBM recently claimed that its quantum computer had crossed the fifty-qubit threshold, but only for a few nanoseconds.[5] A breakthrough to genuine quantum supremacy is now a matter of applied engineering rather than scientific research—and only a matter of time.

Most experts agree that quantum computers will never completely displace conventional digital computers. Yet they will be deployed in an increasingly wide range of research activities and other complex tasks, bringing enormous improvements in performance and efficiency to areas such as weather forecasting, medical and genetic research, and tasks such as calculating traffic flows in the world's biggest cities—a task that D-Wave, a Canadian company, has already undertaken for China's capital Beijing.

And there is one thing quantum computers will be able to do that conventional computers cannot: hack conventional encryption systems around the world.

No More Secrets: Quantum and Cybersecurity

Many experts agree that the new possibilities arising from advances in quantum computing will create a mortal threat to today's IT security. An algorithm formulated by mathematician Peter Shor in 1994 demonstrated that quantum computers will be able to factor large numbers far more efficiently than classical computers. As it happens, the difficulty of conducting large-number factoring is the foundation for most of today's encryption standards.

As a September 2017 article in the journal *Nature* warned: "Many commonly used cryptosystems will be completely broken once large quantum computers exist."[6] Most quantum experts believe that such a breakthrough may only be a decade away. Others are convinced it may come even sooner.

Either way, the coming years will witness the advent of a quantum computer powerful enough to break the encryption techniques currently used billions of times every day. Its first and foremost target could be the encryption system known as RSA, an algorithm that is the cryptographic method of choice for consumer bank transfers, credit card payments, online shopping, and email encryption.

The asymmetric encryption system currently used to protect credit card information and bank accounts relies on two keys. One key is the "private key" and consists of two large prime numbers known only to one's bank or to services such as PayPal. The other key, called the "public key," sits in cyberspace and is the product of multiplying together those two "private" prime numbers to create a semi-prime number. The only way a hacker could access encrypted credit card or bank information would be by factoring the large "public key" (often six hundred digits or more) back to the correct two numbers of the "private key"—a Herculean computation task that would take too long for a classical computer to solve.

A future quantum computer, however, will be able to do such a computation almost instantly. Even blockchain will not be able to withstand the first quantum attack if it relies on two-key encryption architecture—the architecture protecting nearly all digital information today.[7]

This includes our leading financial institutions, including Wall Street; our power grid and water systems; the nation's food supply and energy resources; as well as the entire federal government. As Jason Bloomberg of Intellyx concluded in a *Forbes* article, "Welcome to the cyber-battlefield of the 21st century"—a battlefield that will be dominated by quantum technology.[8]

Fortunately, as Dr. Aaron VanDevender, chief scientist at Founders Fund, observed during a conference at the Hudson Institute this past October, when it comes to quantum, the problem is also the solution. All over the world, research institutes, universities, and businesses are in a race against the clock to develop appropriate solutions and stopgaps to forestall a Quantum Pearl Harbor that overwhelms the world's leading encryption systems. For example, quantum-resistant algorithms (QRAs), which use grid-based, multivariate, code-based, and hash-based encryption techniques, are being developed. Theoretically, these cannot be undermined by quantum computers. Unfortunately, many of these cryptosystems will not be as effective for safely transmitting sensitive data such as financial information.

For that task, quantum technology itself is needed. Companies like SK Telecom are now using quantum technology to create random number generators (QRNGs) that, when coupled with quantum key distribution (QKD), can function as the equivalent of a cryptographer's one-time pad to protect communications between users. This allows two parties to produce a shared random secret key to encrypt and decrypt messages.

One of the advantages of QKD is that it can alert its users if someone else tries to gain access to the communication or know-ledge of the key. It can do this because of a fundamental property of quantum mechanics: trying to measure a quantum system actually disrupts the system. Therefore, a third party trying to eavesdrop on a QKD-protected communication will introduce anomalies that sever the connection—with both parties at either end instantly knowing what has happened.

Quantum key distribution can only produce and distribute a key; a second channel is needed to transmit any actual message data. Yet sending the key over long distances requires a quantum repeater, which has yet to be invented. Therefore, scientists are currently only able to create effective quantum communication networks over about 70–200 kilometers, usually made up of fiber optic cables. Quantum connectivity equaling a world wide web with multiple quantum channels is still years away. All the same, the Chinese are busy laying the foundations of such networks today, and these will become the secure information superhighways of tomorrow.

In the final analysis, the nation that takes the lead in quantum technology over the next decade will not only have enormous advantages in decrypting and exposing secrets—including the capacity to take over entire IT infrastructures in both the public and private sectors—but also the ability to render its own communications and networks largely hackproof.

But quantum technology's impact on strategic balance isn't just limited to encryption. Quantum sensing, the use of quantum technology to measure tiny variations in gravitational fields even at great distances, and quantum optics, will dramatically change the landscape of military technologies in the coming years. Through quantum metrology technologies, objects that are invisible to the most advanced sensors will become "visible" to quantum sensors, even objects behind steel walls or at the bottom of the ocean. Developments in this arena will have a profound effect on today's militaries, including the ability to detect submarines or subterranean weapons systems normally considered hidden from view.[9]

America's current advantage in stealth technology, for example, would almost instantly vanish, and the electromagnetic stealth technologies deployed as part of the $1 trillion F-35 Joint Strike Fighter program, intended to give the United States and its allies air dominance well into the twenty-first century, would become virtually obsolete.

This is why Congressman Hurd's warning stands: the impact of quantum technology on our national defense will be tremendous. The question is whether the United States will be ready when the full quantum revolution takes hold, in a decade or less.

There are in fact two critically important aspects of quantum readiness—and of winning the quantum race. The first and most obvious need is for the United States to achieve quantum supremacy through developments in the field of quantum computing. The second, equally if not more important, is making our nation's infrastructure, including government and financial institutions, secure from quantum attack.

How Ready Is the United States?

In terms of quantum computing, no one doubts that the American private sector leads the way. Google, Microsoft, Intel, and IBM have been actively engaged in quantum computing research for almost a decade.

Google announced in 2017 that it would achieve "quantum supremacy" by the end of the year—although that breakthrough will now probably come sometime in 2018.[10] IBM has successfully built and measured an operational prototype fifty-qubit processor with similar performance

metrics. This new processor expands upon the twenty-qubit quantum computing system accessible to third-party users through their cloud computing platform, and which will be made available in the next-generation IBM Q systems. Intel announced the creation of its seventeen-qubit chip for quantum computing in October, and, even more recently, Microsoft announced that it would release a free preview version of its Quantum Development Kit, which includes the Q# programming language.

Start-up Rigetti Computing—a company that proves quantum computing research is not limited to the megafirms—is also developing software for future quantum computers, including its own, as is IBM.

Other start-up quantum computing companies are attached to universities, such as IonQ, a company formed by the University of Maryland in order to commercialize quantum technologies created in their laboratories. Another is Quantum Circuits, which sprang out of the Yale Quantum Institute. Quantum communication technology has also drawn attention from large and midsize American firms including AT&T, Raytheon, and HRL Laboratories.

But how close is the United States to becoming "quantum secure"? That depends on whom you ask. Government officials, particularly at the National Security Agency and the National Institute for Standards and Technology, which oversee the government's efforts in quantum cyber protection, tend to give a relatively optimistic answer. Others, particularly quantum cybersecurity experts in the private sector, are gloomier.

For one thing, the number of American firms offering quantum cybersecurity solutions is practically nonexistent, with research still located inside academic and government laboratories. By contrast, countries such as Canada, Australia, Switzerland, and Germany are home to industry leaders who offer a growing suite of commercial products.

Among the IT giants, only Google has shown an interest in quantum cybersecurity. The rest are focused on developing computers for commercial applications. Important as these applications may be, the private sector's neglect of quantum cryptography is significant and alarming.

There is a tendency to assume that once the IT giants have built their quantum computers to their satisfaction, their investment and expertise will naturally shift to quantum cybersecurity. Yet this is by no means a given. The field of quantum computing is populated by people with backgrounds in physics, particularly quantum physics. Cybersecurity, on the other hand, is a field that attracts mathematicians or people with a computer science background. This creates a conceptual gap that cannot be easily bridged, even within the same company. Or, rather, it is a gap that will require government leadership to overcome.

So where is the U.S. government on the issue of quantum cybersecurity? Today it spends roughly $200 million a year on all areas of quantum research, not just quantum and post-quantum cryptography.[11] That money is spread over multiple agencies including the Department of Energy, the National Security Agency (NSA), the Air Force Research Lab, darpa and iarpa, the National Science Foundation, and the National Institute for Standards and Technology (NIST). NIST has made post-quantum

cryptography its particular bailiwick, and over the past several years has hosted a series of conferences on setting standards for quantum-resistant algorithms, the next taking place this spring.

NIST has publicly stated that federal government agencies should be ready to switch to what it calls "post-quantum" encryption by 2025—a timeline that looks very slow compared to the gathering threat of quantum computer assaults, particularly from China.

In sum, despite the significant work being done at Los Alamos, other national labs, and the Department of Energy, the evidence hardly suggests a concerted national effort, certainly not compared to other countries that, with a much smaller resource base, have made investing in quantum technology a national priority.

We can contrast our lack of national priority on quantum with what is happening in China. The level of Chinese investment and effort in the quantum sector is staggering: more than thirty times that of the United States. Chinese quantum research dates back to 2004, when scientists proved a five-photon entanglement experimentally. In 2013 Chinese technicians successfully set up a quantum communications experiment covering a distance of over one hundred kilometers, and in 2015 China's main quantum research group teamed up with Alibaba to found a designated research lab for quantum computing.[12]

China made global headlines in August 2016 when it launched the world's first quantum communications satellite to test long-range entanglement and QKD. Beijing plans to launch another quantum satellite in the next year,

with the goal of laying the foundations of a "global quantum internet" under Chinese control, and establishing quantum secure communications, including for China's armed forces.

But the biggest step came with the creation of the massive (91-acre) quantum research facility, the National Laboratory for Quantum Information Science, at Hefei in Anhui province. The facility will have a budget of $11.4 billion over two and a half years. Its agenda is more than simply scientific research. As China's leading quantum expert Pan Jianwei announced, it will also develop quantum technology "of immediate use to the [Chinese] armed forces." These include quantum metrology to improve stealth operations for submarines, as well as the first large-scale Chinese quantum computer which can penetrate the West's encryption systems.[13]

Even more alarming from a national security standpoint is that China has found ready collaborators on important quantum technology in Western countries, including the United States. The 2013 breakthrough in using quantum computing to solve linear equations, for example, was done with the help of scientists from Canada and Singapore. Indeed, an Australian study of Chinese intellectual property theft found that scientists from multiple nations, including the United States, have routinely cooperated with Chinese quantum research funded by the National Natural Science Foundation of China, the Chinese Academy of Sciences, and the Ministry of Science and Technology.[14]

Together with Google's recently announced decision to open an artificial intelligence research facility in China, the level of cooperation on quantum with China should raise national security concerns, both for the United

States and its allies. Yet as Anton Zeilinger—a physicist at the Austrian Academy of Sciences in Vienna who tried but failed to raise funds for a European quantum satellite—has warned, the lack of robust quantum investment strategies in the West and slow decision-making processes will tempt more American and Western scientists to solicit support from China.[15]

Creating a National Quantum Technology Strategy

What do we need to do? Last October I published an op-ed in the *Wall Street Journal* calling for a Manhattan Project–style investment in a National Quantum Initiative: an investment not solely in terms of funding, but in terms of creating a coordinated national effort that harnesses the energies, experience, and innovative instincts of the private sector to a coherent and comprehensive national strategy. "Like its atomic predecessor," I suggested, "the new program should marshal federal government money, the efficiencies of private industry, and the intellectual capital of the nation's laboratories and universities, while keeping everyone focused on the essential mission: winning the quantum race."[16]

Such a National Quantum Technology Security Strategy would for the first time establish clear strategic objectives for America's quantum efforts. It would determine technological priorities (e.g. quantum and post-quantum cryptography versus quantum computing), and set realistic timelines for crucial technological development. It will then outline a roadmap for achieving those established strategic objectives, as well as propose a desired budget (the National Photonics Initiative, for example, has called for an additional $500 million of federal funding over five years for such a

Quantum Initiative—a fraction of what the Manhattan Project would cost in today's dollars).

The strategy would also target key physical assets in need of quantum security, such as power plants and distribution facilities, communication systems, data centers, transportation infrastructure systems (including transportation vehicles critical for the food supply), and water supply systems, as well as the nation's governmental and financial infrastructure.

In addition, an executive order calling for a National Quantum Strategy would also establish a National Quantum Security Council. Such a council would be co-chaired by the director of the National Institute of Standards and Technology and deputy director of U.S. Strategic Cyber Command, with the commander of the Air Force Research Laboratory and the senior director for cybersecurity on the National Security Council serving as vice-chairs. Other members would include representatives from NIST, and representatives from leading universities and research labs such as Livermore and Los Alamos.

In the end, the goal of a National Quantum Technology Security Strategy would be to focus on the development of quantum technology by effectively assisting the private sector, while taking into consideration that private sector goals might not fully align with national security priorities. At the same time, given that the United States currently lags in the quantum cryptography field, it is important for lawmakers to realize that America can't achieve this strategy entirely on its own. Winning the quantum race will also require the help of our closest allies.

Creating a U.S.-Led Quantum Alliance

Therefore, the second step for making America quantum secure is the formation of a Quantum Alliance. The essence of progress in any new science is collaboration and information sharing. Unfortunately, in quantum computing and in quantum cybersecurity, the general pattern of U.S. cooperation, even with close allies, has largely been at the basic research and university level, with very little or none at the government-to-government or government-to-corporate level.

For example, this has been the pattern with America's closest quantum neighbor, Canada. As the former director of the Canadian Institute for Quantum Computing (IQC) at the University of Waterloo remarked in an interview, there has not been much systematic cooperation at all between the U.S. and Canadian governments. "Quantum Canada" has worked with the University of Maryland and its quantum computing start-up IonQ; IQC has also done contract work with darpa and with iarpa on specific projects—but only at the research level.[17]

Likewise, when the University of Southern California launched a quantum initiative with a $95 million budget, IQC was able to obtain some of that money for research work conducted in Waterloo, but no larger collaborative enterprise emerged from the project. The same was true when IQC and Canadian Quantum Valley Investments joined together with Lockheed Martin, Schlumberger, and Sunny Brook on specific quantum technology projects.

In the case of the private sector, Canada's D-Wave has had several contracts with American companies and with the U.S. government, including NASA. On the quantum cybersecurity side, isara Corporation has some clients in the United States although the bulk of its business is still in Canada. But as of today, it's hard to find any evidence of systematic cooperation between Canada and the U.S. government on quantum cybersecurity, or with any U.S. cybersecurity firms.

The same pattern applies in the case of U.S. cooperation with another ally, namely Australia. When asked about Australian collaboration with the U.S. quantum sector, Dr. Jane Melia of Quintessence Labs, one of Australia's largest and most innovative companies in quantum cybersecurity, replied that "There exist collaborations between Australian and other international research institutions. There are also international QKD conferences (such as QCrypt, typically in September each year) attended by scientists from both countries." She went on to add, "and of course we read each other's papers!" But more deliberate bilateral quantum cooperation remains a long way off.

In the case of the UK, U.S. companies such as Google, IBM, Lockheed Martin, Raytheon, Northrop Grumman, and QuSpin have partnered with the Birmingham University Information Tech nologies Hub, the largest of the UK hubs which is working to build a quantum computer demonstrator to present a "networked, hybrid light-matter approach to quantum information processing."[18]

Otherwise, any strategic planning for sharing quantum research or technology seems to be largely lacking. Notably, the UK Quantum Technology Hub in Sensors and Metrology issued a call to work with U.S.

companies, but it is targeted at potential American end users, rather than at collaborative up-front research and development.

On the U.S. side, the Department of Energy (DoE), which has organized an interagency working group on quantum information technology, is an exception. Perhaps its tradition of cooperation on nuclear research has spilled over into the quantum computing arena. All the same, one of the leading labs in quantum communications research, DoE's Los Alamos National Labs, has no funds to work outside the United States.

Additionally, the oversight of information sharing with foreign entities, even allies such as Britain and Australia, constantly runs into difficulties with export controls of sensitive technology, making it difficult for researchers to decide what to share and what not to share. Most, it seems, choose to avoid future trouble by not sharing at all.

In still other instances, a U.S. company will partner with a foreign university engaged in quantum research, as when IBM recently announced that it was making Oxford University a member of its newly formed IBM Q Network, a collaboration of Fortune 500 companies, academic institutions, and national research labs aimed at exploring practical applications for quantum computing systems.

Yet in none of these examples do we see either the U.S. government or its allies directing or supervising the resultant multinational effort. This can lead to unfortunate results, as when the Russian Quantum Center was able to get Mikhail Lukin, a Harvard professor and director of Harvard's Quantum Optics Center, to join its international advisory board. Another

respected figure in the field, Eugene Polzik of the Quantum Optics Lab at the Niels Bohr Institute in Copenhagen, is a member of the RQC's executive committee and the principal contact for RQC applicants. He said, "We are very enthusiastic about trying to make Russia a part of the international scientific community."[19]

Likewise, in November 2017, a joint team consisting of researchers at the University of Sydney and Microsoft, in collaboration with Stanford University, made a groundbreaking discovery that is key to scaling up quantum computers. The team miniaturized a device called a microwave circulator and its findings were published in *Nature Communications*. The team is led by Professor David Reilly, who is director of the University of Sydney's Microsoft Quantum Laboratory, based out of the Sydney Nanoscience Hub, and funded by organizations which include Microsoft Research, the U.S. Department of Energy, darpa, and the Australian Research Council Centre of Excellence Scheme. One of the coauthors of the paper, however, Dr. Xufeng Kou, also happens to be a tenure-track professor in China. Though he began working on the project while a student at UCLA, he was working at ShanghaiTech when the project was completed.[20]

Additionally, Australia's University of Technology in Sydney (whose participating organizations include Lockheed Martin, Microsoft, Dartmouth College, UCLA Berkley) set up the Centre for Quantum Software and Information in December 2016, which is focused on developing crucial software and algorithmic components for the fields of quantum cryptography and quantum information. Yet the Centre's Research Director is Mingsheng Ying, who not only studied at Fuzhou Teachers College in Jiangxi, China, but is also currently professor at the State Key

Laboratory of Intelligent Technology and Systems in the Department of Computer Science and Technology at Tsinghua University, Beijing.

Sharing of basic research information on quantum with Chinese scientists may not always be a national security risk, but China's willingness to use foreign research on advanced technologies (acquired either legally or illegally) to advance its own national security strategy, including its military posture, is well known. In fact, alarm bells are starting to go off in Australia, as their Department of Defence has recently been accused of ignoring universities that shared military technology with China illegally. An article from the Australian Broadcasting Corporation authored by Tom Iggulden noted that "Australian universities conduct world-leading research in areas such as artificial intelligence [and] supercomputing," and that the Defence Department has traditionally relied on self-assessment from universities to monitor their own information-sharing practices.

Recently, the U.S. House Committee on Science, Space, and Technology and its Subcommittees on Research and Technology and Energy voiced concerns that the quantum sector in the United States was falling behind countries that are ramping up research and development in this area. China is outspending the federal government thirtyfold in quantum technology. When viewed in combination with China's heavy investment in artificial intelligence and other key fields, this disparity is even more alarming. In artificial intelligence, for example, Google is actively cooperating with China. Eric Schmidt, former chairman of Alphabet (Google's parent), has warned that China will overtake the United States in this area by 2025.[21] And with its forthcoming satellite-navigation system modeled on our own GPS, the government in Beijing is sending a clear signal that it understands

the stakes involved in dominating the world's information technology future, while others may be taking that future for granted.

Nonetheless, simply spending more money is *not* the answer. If the United States and its quantum-capable allies don't mobilize and coordinate their effort to secure leadership in this sector, someone else will. That someone else will almost certainly be China.

China has already taken the lead in quantum communications, with its quantum satellite and its two-thousand-kilometer long quantum communication pathway from Beijing to Shanghai. Given its heavy investment in future quantum technology, including quantum computers, and its commitment to gaining quantum supremacy as a national strategy priority, it seems inevitable that China will move into the lead as this technology becomes more widespread. This is true not only in the realm of weaponization of quantum as discussed above, but also in establishing global standards and practices for future quantum networks and communications. The gains in terms of economic and geopolitical leverage for China in achieving this leadership position could be incalculable—just as the losses in terms of economic growth and opportunity for the United States and the West, not to mention losses in the realm of national security, could be equally egregious.

It is time for our leaders, and the public, to understand the stakes of quantum computing. What is unfolding every day at corporate, university, and government laboratories around the world is more than a scientific advance of enormous proportions and consequences. It will also determine the geopolitics of the future.

In the end, the Manhattan Project didn't just win a world war; it secured the future for American leadership and the security of the free world in the atomic age. In the quantum age, the stakes will be at least as vital—and the consequences of losing the quantum race, nearly as catastrophic.

This article originally appeared in American Affairs *Volume II, Number 2 (Summer 2018): 96–113.*

Notes

[1] Thomas E. Ricks, "The Quantum Gap with China," *Foreign Policy*, November 28, 2017.

[2] Dom Galeon, "Scientists Build a 51-Qubit Quantum Simulator and It's the Largest One Yet," *Futurism*, July 21, 2017.

[3] Will Hurd, "Quantum Computing Is the Next Big Security Risk," *Wired*, December 7, 2017.

[4] Natalie Wolchover, "Have We Been Interpreting Quantum Mechanics Wrong This Whole Time?," *Wired*, June 30, 2014.

[5] Dom Galeon, "IBM Just Announced a 50-Qubit Quantum Computer," *Futurism*, November 10, 2017.

[6] Arthur Herman, "The Computer That Could Rule the World," *Wall Street Journal*, October 27, 2017.

[7] Idalia Friedson, "How Quantum Computing Threatens Blockchain," *National Review*, February 28, 2018.

[8] Jason Bloomberg, "This Is Why Quantum Computing Is More Dangerous Than You Realize," *Forbes*, August 11, 2017.

[9] Jason Palmer, "Here, There, and Everywhere: Quantum Technology Is Beginning to Come into Its Own," *Economist*, March 9, 2017.

[10] Jack Nicas, "How Google's Quantum Computer Could Change the World," *Wall Street Journal*, October 16, 2017.

[11] Interagency Working Group on Quantum Information Science of the Subcommittee on Physical Sciences, "Advancing Quantum Information Science: National Challenges and Opportunities," National Science and Technology Council, July 22, 2016.

[12] Barb Darrow, "Alibaba's Cloud Unit Teams with Chinese Researchers on Quantum Computing," *Fortune*, July 30, 2015.

[13] Stephen Chen, "China Building World's Biggest Quantum Research Facility," *South China Morning Post*, September 11, 2017.

[14] Mara Hvistendahl, "China's Theft of U.S. Trade Secrets under Scrutiny," *Science*, February 28, 2017.

[15] Eanna Kelly, "EU to Unveil Ten-Year €1B Quantum Technology Programme," *Science Business*, May 10, 2016.

[16] Arthur Herman, "The Computer That Could Rule the World," *Wall Street Journal*, October 27, 2017.

[19] R. Colin Johnson, "Russia Pioneering Quantum Technologies," *EE Times,* July 22, 2013.

[20] "Xufeng Kou," ShanghaiTech University, accessed April 18, 2018.

[21] Patrick Tucker, "China Will Surpass US in AI Around 2025, Says Google's Eric Schmidt," *Defense One*, November 1, 2017.