

# Quantum Computing and Geopolitics

Tawhidur Rahman

BGD eGovt CIRT, Senior Technical Specialist (Digital Security & Diplomacy), Bangladesh Computer Council (BCC)

Quantum computing is one of those topics that people find very interesting yet quite intimidating at the same time. When people hear — or read — that the core of quantum computing is quantum physics and quantum mechanics, they often get intimidated by the topic and steer away from it. I will not deny that some aspects of quantum computing are incredibly puzzling and hard to wrap your mind around.

## The challenges of quantum mechanics

The fundamental properties of quantum mechanics have opened new opportunities for technology, but they can also pose some fundamental challenges. Elsa Kania, adjunct senior fellow at the Center for a New American Security, argues that a sober view of these challenges can help temper some of the hype around quantum information technologies: “While references to ‘the race for quantum computing’ do abound, it is important to recognize that this is not just a race, but rather more of a marathon.”

## Operational challenges

To begin with, there are some scientific challenges that are unique to quantum technology. For example, the very nature of quantum mechanics makes it impossible to “clone” or duplicate qubits, which are the quantum equivalent of a classical computer bit. This makes many common programming techniques that rely on copying the value of a variable impossible to use with quantum technology. For similar reasons, it’s impossible to read the same qubit twice. While this can be a great advantage for secure communications where you want to generate unforgeable cryptographic keys, it can create tremendous difficulties in computing as it complicates the techniques necessary to test or “debug” a program before running it.

## Engineering challenges

Along with these scientific and operational challenges to quantum, there are also significant engineering problems. As one might assume, the complicated nature of quantum science means developing quantum technology is very difficult. While research and development are

underway, most quantum systems exist only in a laboratory environment, with many challenges to be overcome before these systems can operate at scale.

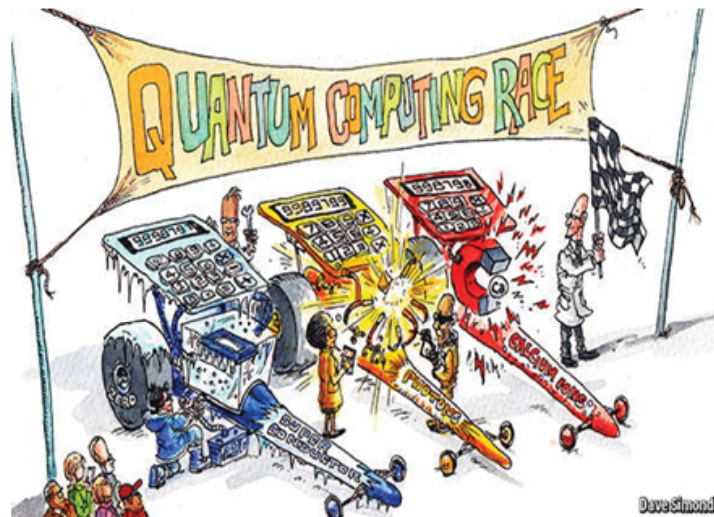
One major hurdle includes reducing “noise.” Noise is unwanted variations in data that interferes with computations and leads to errors. Noise is a problem for classical computers as well, but the sensitivity of qubits to external interference and their difficulty correcting errors that arise make it an especially difficult problem for quantum computers. Current attempts to overcome noise require laboratory settings that control for external

vibrations and electromagnetic waves, and maintain very precise temperatures near absolute zero. Without solving the problem of noise, quantum systems can’t reach their full potential.

Another challenge is increasing the number of qubits on a processor chip. Like a traditional computer’s bit processor (i.e., 32-bit or 64-bit processor), quantum computers need qubit processors with hundreds or even millions of qubits to complete complex computations accurately. Current

quantum computers possess roughly 50 qubits. However, according to Dr. Jonathan Dowling of Louisiana State University, current efforts to develop quantum computers are seeing the number of quantum bits on a quantum computer’s processor chips double every six months. “That is four times faster than Moore’s Law for classical chips, but the nature of quantum computers—[through] superposition and entanglement—means that their processing speed grows exponentially with the number of qubits. So, the processing power of quantum computers obeys double exponential growth,” Dowling noted. If this growth pattern continues, qubit processors could be capable of cracking one of the most widely used types of encryption, Rivest–Shamir–Adleman (RSA) encryption, and solving complex problems and simulations within the next decade.

But just as with classical computers, the chip is not the only important component. New quantum computers and other such technologies also require ecosystems of



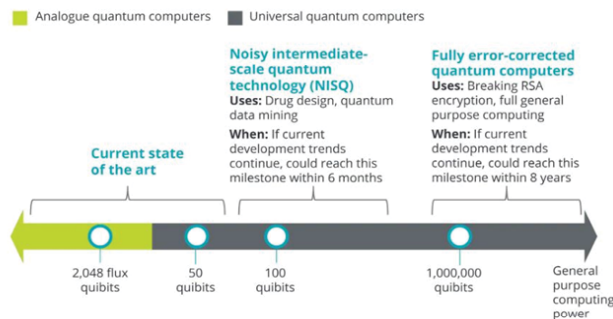
supporting software, hardware, and algorithms, just as traditional computers, encryption, communications, and other technologies do. Developing these additional items will undoubtedly come with their own scientific and engineering challenges. It is important to note that quantum technologies are still in the early stages of development, which means that as these technologies mature, new problems requiring new solutions will likely come up.

### Types of quantum computing systems

Not all quantum information technologies are the same. There are a few different approaches to creating qubits and using them to store, process, and output information. Those different approaches have varied strengths and limitations that make them suitable for different uses and influence their transition from the lab to the market (figure 2).

FIGURE 2

Quantum computers vary in how they can be used



**Analogue quantum computers:** Most associated with adiabatic quantum computers, quantum annealers, and direct quantum simulators, these types of quantum systems are some of the most developed systems to date. Because they are less capable of reducing noise, which impairs qubit quality, their functionality is currently limited to simpler and more specific use cases.

**Noisy intermediate-scale quantum technology (NISQ):** NISQ has been described as the next evolution in quantum computing. Although NISQ is unlikely to completely replace analogue quantum computers, NISQ systems are more capable of tolerating noise, meaning they may require fewer qubits before being commercially viable. While improvements against noise are a design feature of NISQ systems, noise will still impose limitations on these systems.

**Fully error-corrected quantum computers:** By using specially designed algorithms and additional qubits, these computers emulate a noiseless system. Because they require additional qubits to correct errors produced by noise, these systems are even more challenging to develop and may take longer to make commercially viable than analogue or NISQ systems. A fully error-corrected system would be able to solve a variety of complex problems and simulations.

### Quantum's uses in national security

The possibilities afforded by advanced quantum information technologies may affect some of the most important national security tools and tasks, such as intelligence collection, solution optimization, encryption, stealth technology, computer processing, and communications. Indeed, the diversity of quantum applications across the national security domain warrants

some immediate concern, both for how we can harness quantum systems and for how those quantum systems may undercut our security. But the pursuit of quantum systems necessitates advancing an ecosystem of quantum hardware, software, and algorithms, all of which have their own unique scientific, operational, and engineering challenges. So, while some concern is appropriate, too many scientific and technological challenges remain to expect radical change due to quantum technology in the near term. Still, government leaders should be aware of the emerging opportunities, challenges, and threats posed by quantum technology and begin taking steps to prepare for the coming change.

### What can this mean for national security?

With uses ranging from code-breaking to code-making, and imaging to navigation, quantum information science has clear military and intelligence applications. Moreover, with developed countries such as the United States, China, Russia, Austria, Australia, Canada, the United Kingdom, and commercial companies around the globe investing in quantum research, these defense applications could have significant impact on relative national security.<sup>30</sup> Government leaders, even those in nontechnical positions, should have a basic understanding of quantum systems and the emerging national security challenges so they can take steps to protect information and prepare their organizations, teams, and business practices for the quantum world. Here are some problem areas in national security matters where quantum science can be applied.

### Loss of secrets

Information security is one of the most fundamental elements of national security. Whether it be military plans, advanced technology information, diplomatic cables, personal data, or company data, critical details related to state and business security are embedded in data being shared through public and private networks. If we can't protect this data, we can't expect any reasonable sense of national security. Cryptography is one way in which governments and private companies secure information.

The most immediately evident application of quantum computing is in national security. Quantum computers have the potential to disrupt current security protocols that protect global financial markets, render many of today's sophisticated encryption systems inoperable and upend secret government intelligence. International competition is of grave concern because one of these machines could in theory crack the encryption that protects sensitive information inside governments and businesses around the world. Quantum communications and cryptography would also offer a distinct tactical advantage to any actor that employs them on the battlefield.

Using quantum communications for the purposes of transmitting classified data is appealing to military planners across the world, as these transmissions are impossible to tap clandestinely thanks to the fundamental properties of matter. This poses an opportunity for a veritable "quantum leap" forward in military communication. Take a moment to imagine a global leak, an explosion of data unlike anything the planet has yet seen, where the innermost secrets of virtually every government, corporation, and entity on the planet become publicly available. Then combine this with



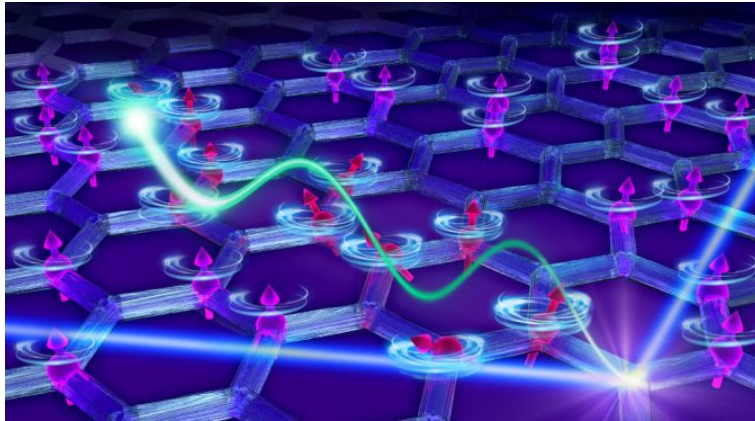
the collapse of all trust on the internet. What would result is an undeniable destabilization of cyberspace and geopolitical stability.

### How Real Is the Threat of Hijacked Machines?

Following the demands of the market for Omni channel presence, traditional business making is being digitally transformed. Big enterprises, medium and even micro businesses are embracing digital technology—such as cloud computing environments, IoT devices, mobility, microservices and DevOps—to deliver enhanced quality products and services at an increasing pace. Machines and machine identities are the core of this transformation.

Healthcare, water supply, electricity, oil and refinery, law enforcement, traffic management, airports and airplanes, all depend more and more on interconnected devices that need to authenticate themselves to ensure the proper functioning of highly critical infrastructure. Small or bigger scale incidents on critical infrastructure have significant physical and societal impact.

Machine authentication relies heavily on encryption algorithms. What could happen if an adversary could develop and use quantum computers to reverse engineer machine identities? The scenario of “Mortal Engines” will become a frightening reality. That actor would have the ability to wreak havoc. Hijacked machines could be turned against states, communities and cause deaths, not by physically killing people, but by, for example, contaminating the water supply. It could cause chaos in motorways and in air traffic control.



### Geopolitical Implications of Quantum Computing

While at the microphysical level everything about quantum computing is very small, at the geopolitical level it’s just the opposite: the implications are very large indeed. Quantum computing will bring seismic geopolitical implications, especially in the critical domains of information security and cyberwarfare.

When China launched in 2016 Micius, the world’s first quantum communications enabled satellite, some remembered of the launch of the Soviet Union’s Sputnik satellite in 1957, which caught the United States off guard and spurred a decades-long contest to regain and maintain global technological and military supremacy. This parallel was also pinned by Jian-Wei Pan, the lead researcher on the Micius project, who hailed the start of “a worldwide quantum space race.”

Quantum computing is an emblematic battleground. Mastering such state-of-the-art technology is not a matter of prestige, it is a vital issue of determining the global status quo. Quantum computing is this century’s moonshot—and now (as then), its outcome is about far more than national

pride. It’s nothing less than a matter of national security.

For militaries, the potential gains of quantum-enabled computing networks are clear. If the QUESS project is a success, China could gain an upper-hand in its space-based intelligence operations, including surveillance, reconnaissance, navigation, environmental monitoring, communications and attack assessment. If technology functions according to the laws of quantum theory, cyberattacks on satellites would become impossible, meaning that adversaries would not be able to interfere with military communications, for example by providing false coordinates or jamming signals. Strengthening these services would bolster China’s geopolitical power-projection and increase its presence as a leading player in space technology. Quantum-enabled military communications could thus present China with an opportunity to reduce U.S. dominance in international affairs.


The U.S. National Academy of Sciences has published the report Quantum Computing: Progress and Prospects where in the findings it is mentioned that “Although the feasibility of a large-scale quantum

computer is not yet certain.... Quantum computing research has clear implications for national security. Even if the probability of creating a working quantum computer was low, given the interest and progress in this area, it seems likely this technology will be developed further by some nation-states.

Thus, all nations must plan for a future of increased QC capability. The threat to current asymmetric cryptography is obvious and is driving efforts toward transitioning to post-quantum cryptography... But the national security implications transcend these issues. A larger, strategic question is about future economic and technological leadership....”

In 1919, Halford John Mackinder wrote in Democratic Ideals and Reality: A Study in the Politics of Reconstruction an influential theory for a route to world domination, writing:

**“Who rules East Europe commands the Heartland:  
Who rules the Heartland commands the World-Island:  
Who rules the World-Island commands the World”.**

In the post WWII world, nuclear weapons determined the world balance and defined conventional warfare. QIS seems to be destined to redraw the rules of cyberwarfare. Whoever masters it, will cement their supremacy across almost every key technological domain. Given the dire consequences of falling behind, no country nor high-tech company can afford lagging in the quantum race, or even worse, ignoring it. Is quantum computing the new “World-Island”? 

Feedback: [pialfg@gmail.com](mailto:pialfg@gmail.com)