BIPSS Commentary
www.bipss.org.bd August -2023
BIPSS Towards a Secure World

Harnessing the Power of Quantum Technology: A New Weapon in National Security

Ifrita Nushin[1]

Source: Forbes.com

Introduction

Quantum Technology has developed in a gradual process from the 1980s to the present, which was mostly unnoticed by the general public. US politicians became aware of its potential for national and economic security in 2016 when the US intelligence community recognized the threat posed

[1]Ifrita Nushin is a Research Intern at the Bangladesh Institute of Peace and Security Studies (BIPSS). She completed her MSS (Masters) and BSS (honors) in the Department of International Relations from Bangladesh University of Professionals (BUP).

by quantum code-cracking computers, which led to an increase of funding various research programs in Quantum Technology.

Quantum computing is identified as a game-changing technology with the concept of 'quantum supremacy' suggesting that quantum computers could outperform classical computers in complex calculations. It operates differently from classical computers, using the principles of quantum mechanics to process information.

While China excels in quantum communication and computing, the US leads in quantum computing, emphasizing the vital role of investment and collaboration. The future lies in harnessing quantum's benefits, addressing vulnerabilities, and engaging diverse stakeholders for a secure and competitive quantum era. Investing in Quantum Technology is vital for national security to counter quantum-based threats to encryption and communication systems, improve intelligence capabilities, and strengthen defense strategies in an increasingly complex and interconnected world.

Why should governments invest in Quantum Technology?

While the practical applications of quantum supremacy may be debatable and initially limited, its implications are significant. Quantum computers demonstrate their ability to solve problems that are currently beyond the reach of classical computers. This achievement marks a significant step forward, showcasing that quantum computers have unique capabilities that classical computers lack.

However, it's crucial to understand that even with quantum supremacy, quantum computers cannot fully replace classical computers in the near future. Quantum computers will coexist with classical computers, playing an increasingly prominent role in the field of computing.[2] There are a number of reasons why more governments are investing in quantum technology.

i. **Strategic Advantage:** Command in quantum technology provides strategic advantage over adversaries in national security. Quantum sensing, quantum computing, and quantum communications could enhance military capabilities, improve intelligence gathering, and

[2] Herman, Arthur, and Idalia Friedson. "Quantum computing: how to address the national security risk." *Hudson Institute* (2018).

enable more efficient decision-making revolutionizing various aspects of military operations.

ii. **National Security threats:** Investing in quantum-resistant encryption is essential to protect national security interests. Quantum sensors could enhance surveillance capabilities, detect hidden threats, and provide critical information for military decision-making. Quantum computing could also be used to optimize military logistics, supply chain management, and resource allocation, leading to cost savings and improved operational efficiency.

iii. **Economic benefits:** Investment in quantum technology has the potential to drive innovation and create a quantum technology industry that can have broader economic benefits beyond defense and national security applications.

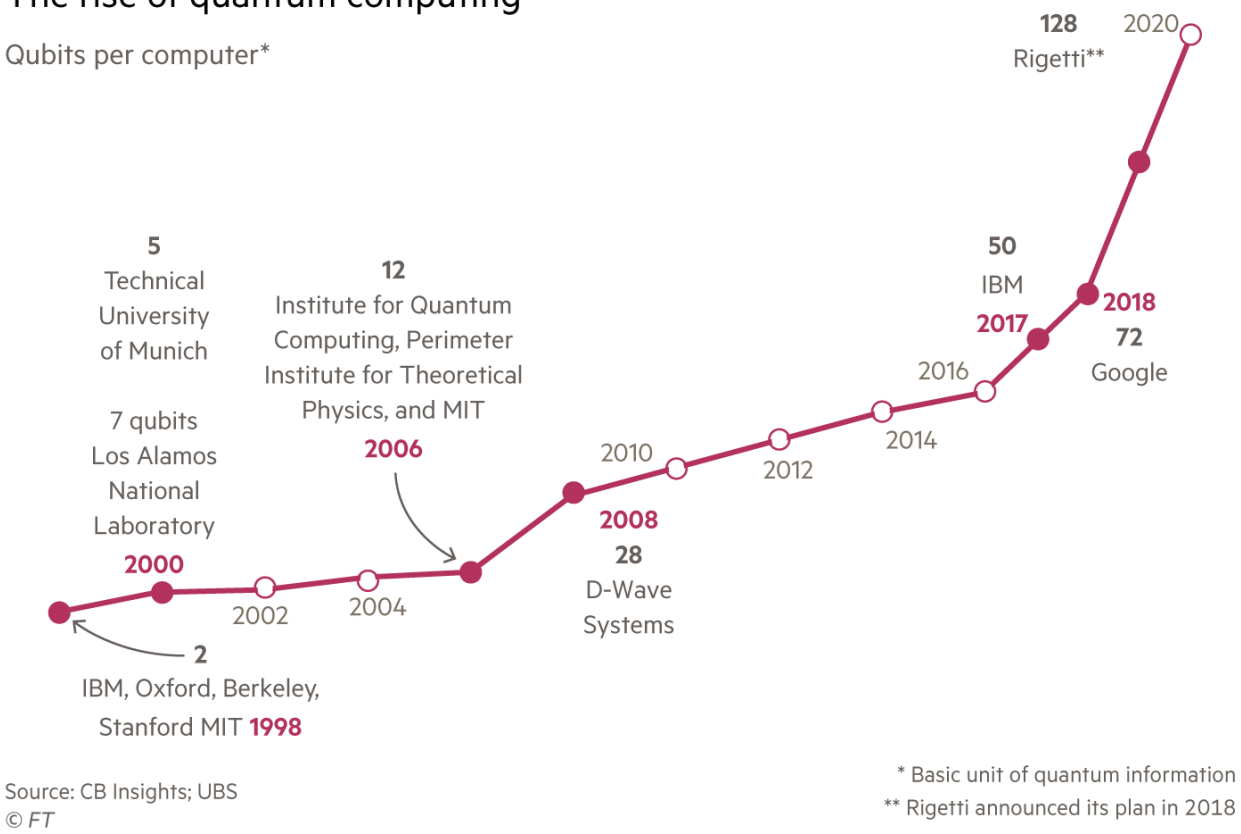
iv. **International Competition**: As quantum technology development becomes a global race, governments invest in quantum research to ensure they do not fall behind in this critical area of emerging technology. It also an impact on economic and geopolitics.[3]

For these reasons, governments seek to harness the advantages of quantum technology while safeguarding against its potential risks, ensuring a secure and competitive position in the future quantum era.

Major Players in quantum technology

The landscape of quantum technology in national security is guided by prominent entities spanning government research agencies like the U.S. National Quantum Initiative and the European Union Quantum Flagship, defense and intelligence agencies including the United States Department of Defense and the National Security Agency, industry leaders such as IBM, Google, Honeywell, and Rigetti Computing, as well as academic institutions like the National Institute of Standards and Technology and university research centers. This collective effort, underpinned by international collaboration, drives the evolution of quantum technology's vital role in safeguarding security interests.[4]

[3] Inglesant, Philip, Marina Jirotka, and Mark Hartswood. "Responsible Innovation in Quantum Technologies applied to Defence and National Security." *NQIT (Networked Quantum Information Technologies)* (2018).
[4] Parker, Edward. *Commercial and military applications and timelines for quantum technology*. Rand, 2021.



Source : The Financial Times

While there's no clear world leader, the United States, China, the European Union (EU), Canada, and the United Kingdom are investing significantly in quantum technology. Private-sector investment in quantum R&D has increased since around 2012, with Canada and the United States having notable private contributions. China has constructed a large quantum research facility, but no single country dominates this field.

However, United States is noticeably the dominant player in quantum computing. Major companies and organizations, such as Google, IBM, IonQ, Honeywell, Microsoft, Lockheed Martin, and NASA, are actively engaged in quantum computing research and development. The U.S. has built large quantum computers with 50 or more high-quality qubits. In contrast, China's investment primarily comes from the government, with Alibaba also investing in the field.[5]

[5] Parker, Edward. *Commercial and military applications and timelines for quantum technology*. Rand, 2021.

On the other hand, it is argued that China is the leader in quantum communication, having successfully deployed quantum communication satellites and built an extensive fiber optic network for Quantum Key Distribution (QKD). Chinese scientist Jian-Wei Pan has been instrumental in many of China's breakthroughs in this field.

The outlook of quantum technology's leadership is diverse, with various countries excelling in different subfields. Public and private investments have fueled progress, but there's no conclusive global leader in quantum technology due to specialization across different areas.[6]

Establishing Leadership in Quantum Arms Race

Although during the Cold War, the United States developed superiority in stealth technology as a response to the threat posed by radar-guided missile defenses in the USSR and other countries, China's recent advancements in quantum-inspired technologies are challenging the US's advantage in stealth warfare. In 2018, China's China Electronics Technology Group Corporation (CETC) introduced a radar prototype claiming to detect stealth aircraft using quantum physics principles.

This development is part of China's broader push to become a global leader in quantum technology. The country is heavily investing in quantum research centers and a national quantum science research center. China's People's Liberation Army (PLA) is recruiting quantum specialists, and defense companies like China Shipbuilding Industry Corporation (CSIC) are establishing quantum labs at universities. While the military applications of these efforts remain somewhat opaque, China's comprehensive strategy underscores its commitment to quantum technology.

In contrast, the US military is facing concerns that its competitive edge is diminishing. A congressional report highlighted the need for increased investment in new battlefield technologies. Quantum communication networks are a likely area of development. Chinese researchers have already established satellite-based quantum communication systems and terrestrial networks for encrypted messages. Quantum key distribution (QKD) forms the basis of these networks,

[6] Kania, Elsa B., and John K. Costello. "Quantum technologies, US-China strategic competition, and future dynamics of cyber stability." In *2017 International Conference on Cyber Conflict (CyCon US)*, pp. 89-96. IEEE, 2017.

enhancing communication security. However, challenges remain, particularly in securing ground networks against hacking.[7]

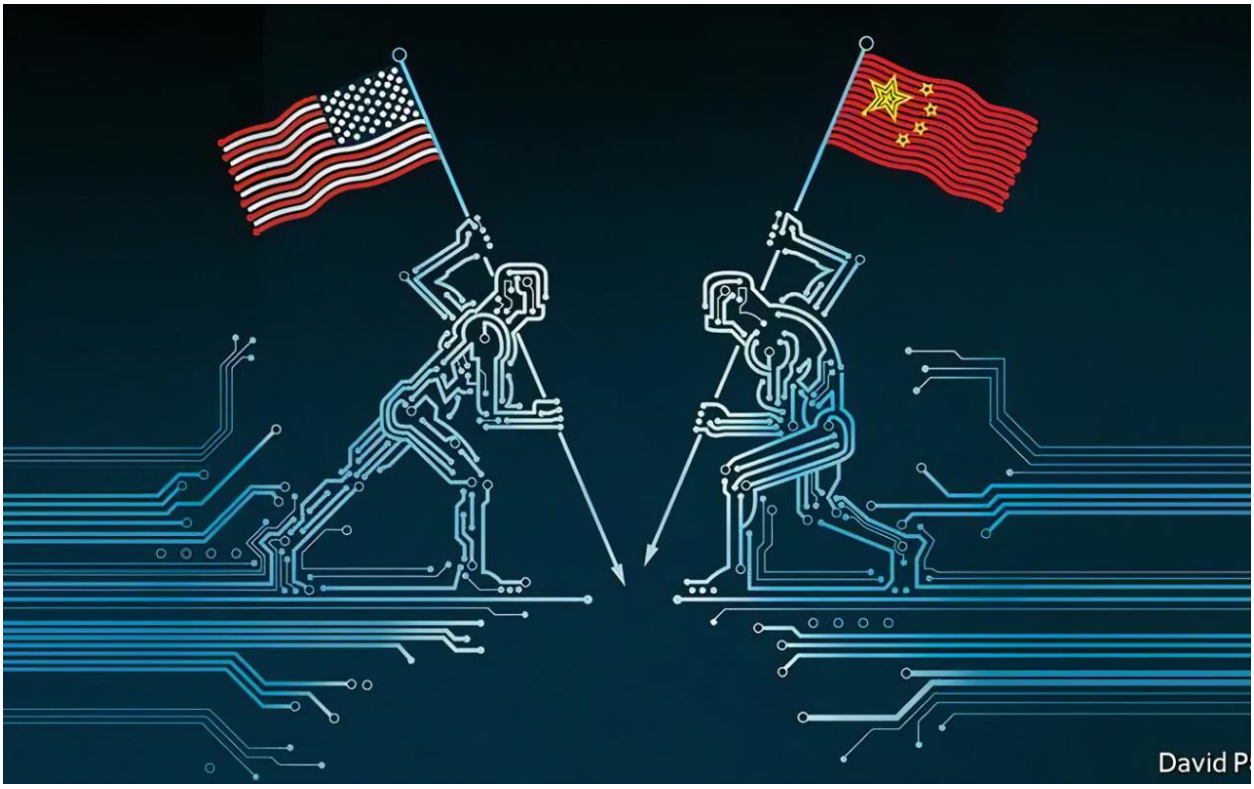
Source: Wonderful Engineering

Moreover, China has surged ahead of the US in the race for quantum computing, with recent breakthroughs including the unveiling of the world's fastest programmable quantum computer. President Joe Biden's recent actions seek to boost America's quantum capabilities for both offense and defense. Quantum computing's potential threatens current encryption methods, and its advancement by adversaries like China could lead to a catastrophic cyber security breach.[8]

The US, initially investing around $500 million in 2015, saw its funding expand to almost $2.1 billion by 2021. In contrast, China's investment surged from $300 million to an estimated $13 billion during the same period. While US integrates quantum cooperation into alliances like NATO and strategic pacts such as AUKUS and the Quad, China is likely to collaborate with Russia in technological domains, including potential quantum cooperation.[9]

---

[7] Giles, M. (2019) *The US and China are in a quantum arms race that will transform warfare ...* Available at: https://www.crows.org/news/432997/The-US-and-China-are-in-a-quantum-arms-race-that-will-transform-warfare.htm.
[8] Payton, T. (2022) *America is losing the quantum race with China, Newsweek.* Available at: https://www.newsweek.com/america-losing-quantum-race-china-opinion-1705642.
[9] Pao, J. (2023) *Rising specter of a quantum computing arms race, Asia Times.* Available at: https://asiatimes.com/2023/02/rising-specter-of-a-quantum-computing-arms-race/.



Source: The Telegraph

Therefore, while US has a head start in quantum research, China's focused investment and collaborative approach between government, academia, and industry are rapidly closing the gap. The US military has advantages in experience and international collaboration, yet China's determination and strategic vision could reshape the future of warfare. As both nations continue to explore the potential of quantum-inspired technologies, the global military balance may be further influenced by these quantum advancements.

Post-quantum Era Implications and Challenges

Quantum technology has the potential to revolutionize various aspects of national security, from sensing to communication and computing. However, challenges such as technological readiness, security vulnerabilities, and the development of countermeasures need to be addressed as these technologies progress. Some of them are disused as follows:

1. **Enhanced Capabilities**: Quantum technologies offer the potential to significantly enhance military capabilities, such as precise navigation, secure communication, advanced computing, and intelligence, surveillance, target acquisition, and reconnaissance (ISTAR) systems. These advancements could lead to updates, modifications, or even the creation of new military doctrines, strategies, and plans.[10]
2. **Technology Policies and Strategies**: National technology policies and strategies are essential for responding to the strategic ambitions of different actors. These policies should encompass research of national quantum technology resources, development and feasibility studies, and assessments of military and security threats and potential.
3. **Monitoring and Adaptation**: Keeping track of quantum technology evolution and adaptation is crucial to prevent technological surprises from neighboring or potentially hostile countries. Even if certain countries lack the immediate capabilities for quantum warfare, monitoring is essential for maintaining a balanced power structure.
4. **Trade and Export Policies**: National trade and export policies play a role in regulating the dissemination of quantum technologies. Some countries may restrict access to emerging technologies due to their strategic importance, while others might implement export controls to mitigate proliferation risks.[11]
5. **Communication and Security**: Effective communication of quantum advantages among allies, especially in the fields of quantum ISTAR and quantum cyber capabilities, needs to be balanced with security considerations. Sharing significant quantum advancements could potentially compromise military secrets and upset the balance of power.
6. **Peace, Ethics, and Challenges**: Ethical concerns related to quantum technologies in military applications are emerging, with calls for guidelines to address potential issues like human DNA manipulation, new materials for war, and intrusive AI. The faster decision-making capabilities offered by quantum technologies could potentially increase the likelihood of conflict, prompting discussions about arms control and proliferation.
7. **Technical Challenges**: The transition from laboratory proofs of concept to practical applications introduces technical challenges, including miniaturization, operability, and

[10] Krelina, Michal. "Quantum technology for military applications." *EPJ Quantum Technology* 8, no. 1 (2021): 24.
[11] Parker, Edward. *Commercial and military applications and timelines for quantum technology*. Rand, 2021.

maintaining sensitivity and resolution. Building a skilled quantum workforce is also important, requiring education and training in quantum information science.

8. **Data and Standardization**: Quantum technologies will generate vast amounts of classical and quantum data, necessitating robust data transmission, processing, and evaluation capabilities. Standardization is crucial for ensuring interoperability among devices produced by different manufacturers within a quantum network.[12]

The Pathway Forward

Developing a quantum strategy for military applications involves careful consideration of investments and timing. Establishing a national quantum ecosystem that combines industry and academic institutions, backed by government support and funding, is crucial. The strategy should encompass three phases: Identification of advantageous quantum technologies, Development through research and prototyping, and Implementation and deployment with integration into military doctrines and scenarios.

Additionally, it is significant for quantum technology countermeasures to address potential vulnerabilities, particularly in the context of spoofing, disabling, or disrupting quantum systems. Decision makers must anticipate the emergence of countermeasures and assess their potential impact on the effectiveness of deployed quantum technologies.[13]

Furthermore, to harness the benefits of quantum technologies, collaboration should extend beyond big technology companies to include start-ups, universities, and research institutes. Allies can contribute by providing testing infrastructure and involving end-user military operators in early experimentation. This not only furthers technology development but also familiarizes the military with quantum capabilities. Active participation in the quantum ecosystem enhances understanding of potential risks, particularly in the cyber domain. [14]

---

[12] Kania, Elsa B., and John K. Costello. "Quantum technologies, US-China strategic competition, and future dynamics of cyber stability." In *2017 International Conference on Cyber Conflict (CyCon US)*, pp. 89-96. IEEE, 2017.

[13] Inglesant, Philip, Marina Jirotka, and Mark Hartswood. "Responsible Innovation in Quantum Technologies applied to Defence and National Security." *NQIT (Networked Quantum Information Technologies)* (2018).

[14] Amerongen, M. van (2021a) *Quantum Technologies in Defence & Security*, *NATO Review*. Available at: https://www.nato.int/docu/review/articles/2021/06/03/quantum-technologies-in-defence-security/index.html.

Source: The Telegraph

As funding and interest in quantum technologies continue to grow, it is anticipated that the technology will mature over the next five to ten years, emphasizing the importance of proactive engagement to fully capitalize on quantum's potential in defense and security.

Conclusion

The near-term impacts of quantum technology may not live up to some of the exaggerated claims, particularly in terms of quantum computers' immediate relevance for cryptography. However, the field holds tremendous promise. Quantum computers, once scaled up significantly, could revolutionize scientific simulations, offering substantial economic benefits. Looking ahead, the development of more advanced quantum communication technologies, though in early stages, could connect quantum computers and sensors in groundbreaking ways.

While no single country has a clear lead in quantum technology overall, it's evident that quantum information science is a fiercely contested arena of "close competition" between the United States and China, as characterized by the U.S.-China Economic and Security Review Commission.

Leading the global race are countries like the United States, Canada, the United Kingdom, and the European Union, with China distinguishing itself in quantum communication

As quantum capabilities continue to mature and innovative applications emerge, the world stands on the brink of a new technological era, where quantum advancements have the power to reshape various industries and domains.