International Relations and Diplomacy, Jan.-Feb. 2024, Vol. 12, No. 1, 26-33
doi: 10.17265/2328-2134/2024.01.003

Influence of Quantum Information Technology on International Security

ZHAO Dongqian
Nanjing University, Nanjing, China
Xi'an International Studies University, Xi'an, China

Humanity is currently undergoing the fourth industrial revolution, characterized by advancements in artificial intelligence, clean energy, quantum information technology, virtual reality, and biotechnology. This technological revolution is poised to have a profound impact on the world. Quantum information technology encompasses both quantum computing and the transmission of quantum information. This article aims to integrate quantum information technology with international security concerns, exploring its implications for international security and envisioning its groundbreaking significance.

Keywords: quantum information technology, quantum communication, quantum computing, international security

Introduction

Throughout the long history of humanity, efforts have been made to avoid wars. In 1648, the signing of the Treaty of Westphalia solidified the concept of sovereign states, attempting to establish an international order where all nations are relatively equal. However, in this international system lacking top-level constraints, the question of how each country can attain security remains eternal. American scholar Arnold Wolfers pointed out: "Security is a type of peace. It is a condition in which the state's most vital interests are protected by measures that ward off threats and guard against surprise attacks." (Li, 2002, p. 150). Hence, it can be seen that security is not purely an objective state but also a psychological one, characterized by uncertainty and relativity. For nations, the content and scope of security are constantly evolving. The primary concern for national security is to safeguard territorial integrity and protect against threats of war from other countries. However, with the advancement and development of human technology, the behavior patterns and survival conditions of the entire human race have also changed, leading to profound transformations in the propositions covered by national security. The fourth industrial revolution, characterized by advancements in artificial intelligence, clean energy, quantum information technology, virtual reality, and biotechnology, is underway. This technological revolution is bound to bring unprecedented changes to various domains of human life. This article aims to integrate quantum information technology with security concerns, exploring the significance and impact of quantum information technology on international security.

ZHAO Dongqian, Ph.D. Candidate, the Institute of International Relations, School of History, Nanjing University, Nanjing; lecturer, School of International Relations, Xi'an International Studies University, Xi'an, China.

The Significance of Quantum Information Technology for International Security

Due to the distinct laws of quantum mechanics compared to classical mechanics, the unique physical properties of quantum phenomena have brought about significant changes in the processing and transmission of information.

Currently, commonly used classical cryptographic communication and numerous digital signature schemes in computer software are based on the RSA public-key cryptographic protocol proposed in 1978. The foundation of the RSA protocol lies in the problem of large number factorization, and the key to breaking the RSA protocol lies in whether one can successfully factorize large numbers into suitable factors. Despite the continuous increase in computational speed of computers, the number of calculations required by classical algorithms increases exponentially with the increase in the size of large numbers. In other words, by appropriately increasing the size of large numbers, it is possible to surpass the highest level of development achieved by classical computers during the same period. Therefore, the RSA protocol has long been considered secure. On the other hand, quantum algorithms such as Deutsch, Shor, and Grover fundamentally construct superposition states to simultaneously represent all possible input values, and then achieve parallel computation of all inputs through unitary transformations. Taking the Shor algorithm as an example, while the classical algorithm takes approximately 10^{17} seconds to complete large number factorization, the Shor algorithm can solve it in just 10^{-6} seconds. Due to the potential for accelerated encryption cracking by quantum computing, the development of quantum computers may pose a threat to the security of currently widely used encryption algorithms. The European Policy Centre predicts that by 2031, as many as 50% of commonly used encryption systems will be vulnerable to being cracked by quantum computers (Fu, Jia, & Lv, 2024).

The quantum computing technology poses a disruptive threat to existing cryptographic techniques. Once a country achieves a breakthrough in quantum computing technology, it would have the ability to easily crack the core secrets of other nations, leading to a devastating blow to the information security of those countries.

On the other hand, quantum cryptography can provide stronger security than traditional cryptography. For example, quantum key distribution protocols exhibit exceptionally high resistance to eavesdropping and theoretically enable the realization of absolutely secure key exchange. Hence, this feature can be applied to communication domains involving national secrets and security. Sectors such as core financial communications, intergovernmental secrets, and military communications, which require utmost confidentiality, can leverage this technology. This is crucial for secure communication in the international security domain as it helps prevent eavesdropping and information leakage. Quantum communication networks facilitate absolutely secure communication, thereby contributing to the protection of sensitive information transmission in the realm of international security.

Besides its crucial role in information confidentiality, quantum mechanics inherently features entanglement, which can be exploited for long-distance quantum transmission. Bennett proposed quantum teleportation in 1993, enabling the establishment of a series of quantum relay stations between communicating parties when their distance exceeds the permissible range due to optical fiber loss. This allows for long-distance transmission, overcoming the barrier of distance. The advancement of quantum technology will reshape communication methods and strategic layouts in the international security domain.

In addition to quantum information transmission, the potential of quantum computers capable of executing quantum algorithms is immense. Computers equipped with quantum computing technology not only possess superior computational power compared to classical computers but also represent a revolutionary breakthrough.

They are true analog computers capable of reproducing the realities of nature. Quantum computers can wield tremendous power in fields such as advanced materials, drug design, and genetic engineering, including the exploration of the universe's mysteries such as quantum field theory (Qi, 2018). The significance of quantum computers in this regard is profound, and nations achieving breakthroughs in this field will hold a leadership advantage.

The International Security Competition Landscape of Quantum Information Technology

The importance of quantum computing technology and quantum communication is gradually becoming evident. Currently, breakthroughs in quantum computing, quantum communication, quantum radar, and other technologies have driven the expansion of quantum technology applications in the military domain, catalyzing global military transformations and changes in the nature of warfare (Zhang, Li, & Hao, 2022). But not all countries have the research and development capabilities in quantum information technology. Therefore, countries and regions with scientific research capabilities are vigorously conducting research in the field of quantum information, engaging in fierce competition with the aim of gaining a leading advantage over other nations.

In order to maintain its technological leadership, the United States is taking multiple approaches in the field of quantum research. On one hand, it is vigorously pursuing the development of quantum computers and communications, while on the other hand, actively preparing for post-quantum cryptography.

As a leading technological power, the United States has been investing in quantum technology research as early as 2002 when the National Science Foundation allocated $50 million for the purpose. To enhance coordination of research and development projects and foster collaboration among various departments, the National Science and Technology Council of the United States established a cross-agency working group in October 2014 to engage in the study of study quantum information science (Lv, Liu, & Jia, 2022). This interdepartmental working group, led by the Department of Energy, the National Institute of Standards and Technology, and the National Science Foundation, also involved other departments such as the Office of the Director of National Intelligence, the Department of Defense, and the White House Office of Science and Technology Policy. In 2016, this working group released a report titled *Advancing Quantum Information Science: National Challenges and Opportunities*. The report underscored the significance of foundational research in quantum science, with focal points on areas such as quantum communication, quantum sensing and metrology, quantum simulation and quantum computing. It also highlighted the challenges faced in these domains (Qiao, 2017). Ever since 2013, both the White House and the Pentagon have installed and operationalized quantum communication systems (Wang, 2013).

The United States government, research institutions, and businesses are actively driving research and development in quantum information technology. In February 2020, the White House website published the *United States Quantum Network Strategy*, outlining the initiative to establish a quantum internet and ensure the accessibility of quantum information science to the public (Wang, 2020). In May 2022, Florida Atlantic University in the United States collaborated with Qubitekk Corporation and L3 Harris Corporation to jointly develop the first mobile quantum network based on unmanned aerial vehicles (UAVs), capable of rapidly adapting to changing battlefield environments and enabling secure quantum information sharing (Defense Bulletin, 2022). Companies such as IBM, Google, Microsoft, and others are developing quantum computers and achieving significant milestones such as increasing the number of quantum bits and reducing error rates. In

November 2017, IBM announced the successful development of a 20-qubit quantum computer and a 50-qubit prototype. The quantum state duration of the 20-qubit quantum computer was increased from the previous 50 microseconds to 90 microseconds. The 50-qubit prototype laid the foundation for the development of next-generation quantum computer systems. In 2019, Google in the United States developed a quantum computer named 'Sycamore' with 53 qubits, achieving quantum supremacy for the first time globally (Xu, Guo, He, & Huang, 2023).

The most crucial component in quantum computers is the quantum chip. Quantum chips harness the ability of quantum superposition, a physical property that enables parallel computation, far surpassing traditional electronic chips. Intel, an American company, has been achieving notable advancements in quantum chip development. They released a 17-qubit quantum chip in 2017 and announced the production of a 49-qubit quantum chip in January 2018. Similarly, the research team at Google, also based in the United States, has made remarkable progress. Although their quantum chip only has six qubits, they utilized a bump-bonding technique. This technique significantly enhances the scalability of quantum chips while reducing the control lines within the chip, thereby greatly minimizing electronic interference with the quantum bits (Chen, 2018). Mitigating interference has been a longstanding challenge in quantum research, making Google’s breakthrough highly significant.

To address the growing threat of quantum computers in decrypting sensitive information, the report *Quantum Computing: Development and Prospects* from the United States emphasizes the need to design and deploy algorithms and infrastructure to counter quantum decryption before the first quantum computer goes online (Lv et al., 2022). During the post-quantum encryption phase, new standards for algorithms are formulated, approved, and integrated into encryption formats. Vendors update hardware and software, re-encrypt sensitive data, and reissue public key certificates. All official documents are re-signed, and software code is upgraded, verified, and redistributed. (Chen, 2019). In order to address the challenges of transitioning into the post-quantum cryptography era, the United States has already made comprehensive deployment and planning arrangements.

The European Union has been actively promoting the construction of quantum communication networks since the early years of this century to achieve more secure communication. In 2008, the EU published a report on strategies for quantum information processing and communication. Twelve member states within the EU have established engineering teams for secure communication based on quantum cryptography. This represented another major research project collaboration among European countries following cooperation in nuclear center and international space station projects (Lu et al., 2018). In 2016, the EU launched the Quantum Technology Flagship initiative, with a total investment of 1 billion euros, focusing on quantum sensing, quantum communication, quantum computing, and quantum simulation. The European Union has initiated the “Quantum Key Industrial System” to build quantum communication infrastructure. Some laboratories and research institutions in the EU have successfully established networks based on quantum key distribution and conducted pilot applications in cities and regions (Qiao, 2017). In September 2022, a coalition led by SES Corporation designed, developed, and operated an end-to-end secure quantum key distribution system based on the EAGLE-I satellite, aiming to demonstrate and validate next-generation network security for Europe in orbit (Xian, 2022).

As a global normative force, the European Union is driving the establishment of standards and specifications for quantum secure communication to ensure the security and interoperability of quantum communication networks. The EU is also actively promoting international cooperation projects, such as Quantum Flagship collaborating with other countries and regions to advance quantum information technology (Quantum Flagship, 2023). Several research institutions and companies in Europe are conducting research and development in quantum computing. They are dedicated to building more stable and reliable quantum bits and quantum computers to address complex computational problems. The EU hopes to have the capability in quantum research and become a major player in quantum research worldwide.

Other countries are also unwilling to fall behind. The Japanese government has unveiled a strategic plan focused on researching next-generation quantum communication technology, aiming to establish a highly secure and secret high-speed quantum communication network by 2030. On January 7, 2019, India announced a $525 million investment in research on artificial intelligence, machine learning, the Internet of Things, and quantum computing. In August 2022, QNu Labs, an Indian company, provided the army with a quantum key distribution system, breaking the distance record for quantum key distribution transmission in India and achieving innovative secure communication (Zhang et al., 2022). Israel, known for its competitive edge in high technology, revealed on December 3, 2019, plans to invest approximately 2.43 billion RMB over six years in quantum computing research (Dong & Ma, 2020).

Compared to the EU and the United States, China initially lagged behind, but later caught up and has achieved remarkable success in the field of quantum communication. On August 16, 2016, at the Jiuquan Satellite Launch Center, China successfully launched the world's first quantum science experimental satellite, "Micius" using the Long March 2D carrier rocket. Four months later, this quantum satellite successfully completed its in-orbit testing mission and was officially handed over for user operations. This marked the first time globally that thousand-kilometer-level space-to-ground bidirectional quantum entanglement distribution, thousand-kilometer-level ground-to-space quantum teleportation, and thousand-kilometer-level space-to-ground high-speed quantum key distribution was achieved. In 2017, the world's first long-distance quantum secure communication backbone network, the "Beijing-Shanghai Trunk Line", was opened. This long-distance quantum secure communication backbone network covers Beijing, Shanghai, Jinan, and Hefei, with a length of over two thousand kilometers and a key rate exceeding 20 kbps along the entire line, capable of meeting the business needs of distributing keys to tens of thousands of users (Hai, 2018). The "Beijing-Shanghai Trunk Line" provides quantum secure communication services to financial institutions, government departments, and other institutions along the route that require high security levels. The further development of quantum communication technology will extend from protecting specific sectors to safeguarding the entire national security.

China is actively developing in the field of quantum computing technology, frequently achieving new breakthroughs. On May 3, 2017, the Chinese Academy of Sciences announced the birth of the world's first optical quantum computer. Professor Pan Jianwei's team at the University of Science and Technology of China independently developed a 10-qubit superconducting quantum circuit sample. Through high-precision pulse control and global entanglement operations, they successfully achieved the largest number of entangled superconducting qubits in the world to date and fully characterized a 10-qubit quantum state through tomographic measurement methods. At the same time, the research team further demonstrated the feasibility of accelerating the solution of linear equations through quantum computing parallelism using superconducting quantum circuits to implement a quantum algorithm for solving linear equation systems. Alibaba's DAMO Academy Quantum Laboratory in China announced in May 2018 that it had successfully simulated an 81-qubit, 40-layer Google random quantum circuit, known as "Tai Zhang", which used to be the most powerful quantum circuit simulator in the world. On October 11, 2023, the University of Science and Technology of China announced the development of the “Jiuzhang III”, a quantum computing prototype capable of manipulating 255 photons. The “Jiuzhang III” achieved the ability to manipulate 255 photons for the first time, greatly enhancing computational complexity. The most complex sample that this computer can compute in 1 microsecond would take the current fastest supercomputer in the world approximately 200 billion years to complete (Xu, Guo, He, & Huang, 2023). China also attaches importance to the independent research and development of the physical foundation and key technologies of quantum computers. On June 10, 2022, Huawei publicly announced a patent for “a quantum chip and quantum computer”, which helped to address issues such as the difficulty of quantum chip fabrication and low yield (Ji, 2023). Recently, a Chinese research team has for the first time utilized common semiconductor material gallium nitride (GaN) to create quantum light sources (Tianjidiaochaju, 2024). This achievement provides new impetus for the development of quantum computing.

Overall, globally the current level of quantum computing remains primarily in the stages of fundamental theoretical research and prototype product development and verification. Achieving greater advancements requires breakthroughs in multiple key technologies. There are various technological pathways for realizing quantum computing, including semiconductor, superconducting, ion trap, optical, diamond vacancy, cold atom, and nuclear magnetic resonance technologies. A common challenge faced by all pathways is decoherence, or the error problem of quantum states. In terms of the current experimental manipulation technology level, none of the pathways can fully achieve the realization of a truly impactful quantum computer. However, we should note that the first classical computer, ENIAC, occupied an area of 170 square meters and weighed 30 tons at the time of its manufacture, and at that time, it was also unimaginable of the epoch-making significance that computers would bring to humanity. The potential of quantum computing technology should not be underestimated, and countries with research capabilities are eagerly investing significant funds and intellectual support in related research and development. Based on the secret properties and transmission advantages of quantum communication technology, countries with research capabilities will further invest in research funding in this field, accelerate research progress and intensity, thereby ensuring national security.

Although there are still many critical areas in quantum computing technology that require further research and breakthroughs, scientific research progress has not halted for the sake of national security. Internationally, countries with the capability to conduct research on quantum computing have different overall layouts and advantages. Nevertheless, the momentum of research in each nation is driven by a fear of lagging behind, shaping a competitive environment in the realm of international security.

Conclusion

In the new wave of technological revolution, quantum information technology has a dual impact on international security, as it can both enhance communication and information security levels and potentially challenge traditional security paradigms. Every country is concerned about falling behind in development and being vulnerable to attacks from other nations. Therefore, each one hopes to gain an absolute security advantage, leading to a competitive dynamic in the development of quantum information technology at the national level. There are several points that need to be highlighted:

Firstly, it is essential to deeply understand the impact of quantum information technology in our era. With the advancement of quantum information technology, it no longer remains confined to topics in cryptography and computing. We can foresee that the integration of quantum information technology with artificial intelligence, virtual reality, and biotechnology will bring about a disruptive revolution. When new technologies can process complex data at speeds beyond human reach and make decisions, humanity will face an entirely new ecosystem challenging themselves.

Secondly, this is a competition for future dominance. It is not merely a war in the field of science and technology but a contest for leadership in various aspects of politics, economics, and military affairs. This competitive situation will only intensify within the international landscape dominated by nation-states. If a country gains an absolute advantage in quantum information technology, it can rapidly establish comprehensive dominance in various fields, leading to profound changes in the international landscape.

Lastly, we should recognize that technology itself does not possess value judgment. The essence of humanity lies in our ethical judgments and value choices. It is through these that we imbue technological advancements with human values. China's first quantum communication satellite is named "Micius", reflecting China's technological development embedded with deep-seated values of "universal love" and "non-aggression", as well as hopes and visions for humanity's future. It is often said that technology is a double-edged sword. Whether the technological revolution precipitates a bloodless war or fosters decentralized development and progress for all humanity hinges on their own choices.

References

Chen, J. (2019). Interpretation of the US Report *Quantum Computing: Development and Prospects*. *Dual-Use Technologies and Products, 32*(1), 20-23.

Chen, Q. (2018). Breakthroughs in US quantum computing research. *Shanghai Informatization, 15*(3), 79-81.

Defense Bulletin. (2022, June 4). US Department of Defense develops first mobile quantum network based on drones. Retrieved January 6, 2023 from https://mp.weixin.qq.com/s/ND0ZC4QJsyVBTZybWMfd9A

Diankexiaoshan. (2022, September 28). Europe to develop eagle-I quantum encryption satellite system. Retrieved January 6, 2023 from https://mp.weixin.qq.com/s/AjFOMr-b-29lvIsenKZNVw

Dong, L., & Ma, S. (2020). Major countries worldwide vigorously promote the development of quantum information technology. Military Digest, 16-19.

Fu, G., Jia, R., & Lv, W. (2024). Overview of cyber security technology hotspots in 2023. *Information Security and Communications Privacy, 1*, 16-25.

Hai, C. (2018). Seizing the heights of quantum technology development. *New Economic Guide*, 17-21.

Ji, W. (2023, February 23). Laying out the "contested land" to create the "southern heights". *Shenzhen Business Daily*, p. A04.

Li, F. (2022). International quantum cryptography patent development trend and hot spot analysis. *World Sci-Tech R&D, 44*(1), 69-80.

Li, S. (2002). *Introduction to international political science*. Shanghai: Shanghai People's Publishing House.

Lu, J., Zhang, X., Luan, T., Zhang, X., & Fu, Y. (2018). Discussion on the development of quantum information systems. *Journal of China Academy of Electronics and Information Technology, 13*(5), 498.

Lv, F., Liu, X., & Jia, X. (2022). Policy deployment and important progress of basic research in American quantum information science strategy in recent two decades. *World Sci-Tech R&D, 44*(1), 12-24.

Qi, M. (2018). Proof beyond the riemann hypothesis: Internet security faces greater threats. *Internet Weekly, 21*, 17.

Qiao, J. (2017). Latest trends in quantum information science and American responses. *Global Science and Technology Outlook, 32*(Z1), 17.

Quantum Flagship. (2023, March 13). Project launch—QKISS: Developing ready-to-deploy European quantum key distribution (QKD) Systems. Retrieved January 2, 2024 from https://qt.eu/news/2023/2023-03-13_project-launch-qkiss-developing-ready-to-deploy-european-quantum-key-distribution-qkd-systems

Tianjidiaochaju. (2024, April 21). A quantum leap in chip design by Chinese teams. Retrieved April 22, 2024 from https://new.qq.com/rain/a/20240421A01W9N00

Wang, C. (2020). Progress and implications of global quantum internet. *China Informatization, 11*, 7-9.

Xu, H., Guo, X., He, X., & Huang, Z. (2023, October 11). Jiuzhang III is here: China advances further in developing quantum computers. Retrieved January 3, 2024 from http://www.news.cn/tech/2023-10/11/c_1129910485.htm

Wang, Q. R. (2013). *Outlook on quantum communication technology and applications*. Beijing: National Defense Industry Press.

Zhang, X., Li, Q., & Hao, Z. (2023). Research on the progress and trend of emerging technologies of foreign cyber security in 2022. *Information Security and Communications Privacy, 4*, 12-18.