RSiS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

Science, Technology and Security

April 2025

Published by the Future Issues and Technology (FIT) Research Cluster, RSIS. This Bulletin comes as a series of articles on science and technology from the angle of national security.

Quantum Technologies, Global Supply Chain, and International Peace and Security | *Dongyoun Cho*

The intersection of quantum technologies, global supply chains, and international security presents challenges in understanding and regulating the quantum technology landscape. Without proactive policies, risks like technological fragmentation, supply chain instability, and geopolitical tensions could hinder quantum's potential. While quantum technologies are gaining attention in cybersecurity discussions, they remain broadly categorised under emerging technologies in major international frameworks. A strategic, domain-specific analysis is essential to inform policy solutions. Likewise, international frameworks must evolve to address quantum's dual-use nature and commercialisation, ensuring interoperability, stable supply chains, and ethical governance that foster peace, security, and equitable development.

Strategic Context of Quantum Technologies

On 7 June 2024, the United Nations (UN) declared 2025 as the International Year of Quantum Science and Technology. This global initiative highlights the pivotal role of quantum science in driving technological innovation, promoting sustainable development, and enhancing equitable access to education and economic opportunities. While acknowledging the potential of quantum technologies, the UN has expressed concerns regarding their security implications. In 2022, the UN Secretary-General addressed the General Assembly, cautioning against the risks posed by quantum computers, particularly their ability to "undermine cybersecurity and increase the risk of malfunctions in complex systems." Additionally, the Secretary-General underscored the absence of a "global framework to address these risks."

Governments worldwide are increasingly acknowledging the critical role of quantum technologies in driving future economic growth and promoting national security. Rapid advancements in quantum computing, cryptography, communications, and sensing have the potential to revolutionise these sectors, reshaping global economies, defence infrastructures, and scientific research. Although several applications remain in the

developmental stages, recent breakthroughs suggest substantial progress. Quantum technology, historically confined to academic research, has recently gained momentum through commercialisation, moving closer to widespread deployment.

Despite these advancements, the development, production, and deployment of quantum technologies rely on a highly sophisticated and complex global supply chain. While considerable attention has been devoted to the technical capabilities of quantum technologies, little attention has been directed toward the underlying global supply chains supporting their development. These supply chains, characterised by their high level of specialisation and geographical dispersion, are particularly vulnerable to geopolitical instability, reliance on critical materials, and technological bottlenecks, all of which could affect the pace of quantum innovation.

A key concern is the risk of technological fragmentation, wherein nations or companies develop proprietary quantum systems that are incompatible with one another. This fragmentation could create isolated technological ecosystems, undermining global cooperation and interoperability. Such a lack of integration not only limits the potential of quantum technologies but also heightens risks to global security, trade, and scientific collaboration.

Technological fragmentation also poses substantial challenges to international cooperation and security. Proprietary quantum ecosystems may hinder collaborative efforts as nations and companies become reluctant to share advancements owing to concerns about intellectual property protection or competitive disadvantages. This reluctance could decelerate the global development of quantum technology and limit its widespread applications.

Furthermore, incompatible quantum communication networks or cryptographic systems could introduce vulnerabilities into global security infrastructures. A lack of interoperability might aggravate geopolitical tensions, particularly as quantum technologies become more integral to defence and military systems.

Beyond security concerns, technological fragmentation introduces economic inefficiencies and stifles innovation. Companies may be compelled to develop multiple versions of quantum systems to meet diverse standards or platform requirements, diverting resources that could otherwise advance the field. This duplication of effort raises costs and impedes progress. Smaller nations or companies may find it particularly difficult to compete, exacerbating global inequalities and limiting broader participation in the emerging quantum revolution.

Fragmentation also threatens the stability of the global quantum supply chain. As countries or companies pursue proprietary systems, fluctuating demand for specific materials, components, or equipment may cause supply bottlenecks, raising manufacturing costs and inefficiencies. For instance, differing standards for quantum communication networks might necessitate the production of multiple versions of photonic components or quantum processors to serve distinct markets. The absence of

common standards could delay the global deployment of quantum technologies, further hindering international collaboration and innovation.

Challenges in the Current Understanding of the Quantum Supply Chain

The current understanding of the quantum technology supply chain is shaped by several key challenges, including the multifaceted nature of quantum technologies, the evolving structure of global supply chains, and the ever-changing landscape of export-control regimes.

First, quantum technologies encompass a broad family of advanced systems with diverse applications, maturity levels, and associated security and economic implications. These technologies can be categorised into three primary domains: quantum computing, quantum sensing, and quantum communications. Each category exhibits distinct capabilities and developmental stages. Consequently, tailored approaches are required for assessment. While quantum sensing and communications are approaching commercial deployment, quantum computing remains largely experimental and demands unique frameworks for evaluating its progress and potential.[1]

Second, the global supply chain for quantum technologies remains in its formative stages, making it challenging to identify key actors, chokepoints, and particularly sensitive vulnerabilities. The evolving nature of these supply chains introduces challenges in controlling critical technologies, particularly given the varying technological maturity levels across quantum domains. A nuanced understanding of these differences is essential for determining priority areas in policy and governance.

Third, the increasing adoption of unilateral measures in quantum export controls highlights the limitations of traditional multilateral frameworks. Historically, export-control regimes were designed to address national security concerns, particularly the proliferation of nuclear, biological, and dual-use technologies. For instance, the Wassenaar Arrangement primarily focuses on controlling the export of dual-use goods and technologies, many of which were originally developed for military or governmental use before becoming commercially available. The Global Positioning System is a notable example. While still owned by the US military, it has become integral to civilian applications. These export controls have long aimed to strike a balance between limiting exports to nations of concern and mitigating national security threats.

In recent decades, however, the landscape of technological development has shifted dramatically. Private companies, rather than governments, have become the primary drivers of innovation, often introducing new technologies into the marketplace before regulatory frameworks can address their national security implications. This shift,

[1] While quantum sensing (e.g., magnetometers) has reached Technology Readiness Level (TRL) 9 and quantum communications (e.g., Quantum Key Distribution) is at TRL 7, universal quantum computing remains at TRL 3. For more information, please refer to OECD (2025), "A quantum technologies policy primer", OECD Digital Economy Papers, No. 371, OECD Publishing, Paris, https://doi.org/10.1787/fd1153c3-en.

wherein technologies developed for civilian use increasingly transition into military domains, presents new regulatory challenges. The rapid pace of innovation in emerging fields – for example, quantum technologies, artificial intelligence, and commercial drones – has outstripped the adaptation capacity of existing export-control regimes.

Beyond controlling dual-use technologies, export controls have increasingly been employed as tools for both national and economic security. This approach reflects a broader strategy aimed at maintaining technological leadership while restricting the advancement of potential adversaries. Consequently, export controls on quantum technologies have become integral to addressing these dual objectives.

In summary, the interplay among quantum technologies, the evolving global supply chain, and the limitations of traditional export-control regimes present notable challenges in understanding and regulating the quantum technology landscape. Addressing these issues demands targeted policy interventions and robust international cooperation.

Conclusion

The intersection of quantum technologies, global supply chains, and international security represents a critical frontier for governance and cooperation. Without proactive and inclusive policies, risks such as technological fragmentation, supply chain instability, and geopolitical tensions may undermine the transformative potential of quantum technologies.

Within the multilateral discourse on international peace and security, quantum technologies are beginning to gain traction in cybersecurity discussions owing to their potential to enhance and disrupt existing systems. Despite growing awareness, specific references to quantum technologies are notably absent from major international frameworks like the UN Pact for the Future, where they remain broadly categorised under the umbrella of emerging technologies. Analysing quantum technologies strategically across distinct domains is essential for understanding their implications and informing policy solutions proactively.

International frameworks need to evolve to effectively address the dual-use nature and rapid commercialisation of quantum technologies. By fostering interoperability, stabilising supply chains, and aligning governance with ethical and security considerations, the global community can shape a quantum future that promotes peace, security, and equitable development.

This article draws on material explored in greater detail in a forthcoming report from UNIDIR. Titled "Quantum Technologies, Global Supply Chain, and International Peace and Security: A Framework for Assessing Vulnerabilities in the Quantum Supply Chain," it provides further analysis of the field of quantum supply chains and their relevant implications for international security.

The designations and material presentation in this publication do not signify any opinion from the Secretariat of the United Nations regarding the legal status of any country, territory, city, or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries. The views expressed in this publication are solely those of the individual authors and do not necessarily represent the views or opinions of the United Nations, UNIDIR, its staff members, or sponsors.

About the Author

Dongyoun Cho, a former Major in the Republic of Korean Army, is a Senior Researcher in the Security & Technology Programme at the United Nations Institute for Disarmament Research (UNIDIR). She is also an Assistant Professor in the Department of Military Studies at Seokyeong University, Republic of Korea. She holds a Master's degree in Public Administration from Harvard University and was a World Fellow at Yale University. Her expertise lies in converging security and emerging technologies, including artificial intelligence, autonomy, cyber, and quantum.

S. Rajaratnam School of International Studies, NTU Singapore
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798
T: +65 6790 6982 | E: rsispublications@ntu.edu.sg | W: www.rsis.edu.sg