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

Ponder the Improbable since 1996

IDSS Paper
Ponder. Analyse. Prepare. Engage. Refresh.

www.rsis.edu.sg

No. 089 – 15 December 2023

The authors' views are their own and do not represent the official position of the Institute of Defence and Strategic Studies of the S. Rajaratnam School of International Studies, NTU. These commentaries may be reproduced with prior permission from RSIS and due recognition to the authors and RSIS. Please email to Editor IDSS Paper at RSISPublications@ntu.edu.sg.

No. 089/2023 dated 15 December 2023

"Unhackable" Quantum Communication is a Myth

Michal Krelina and Manoj Harjani

SYNOPSIS

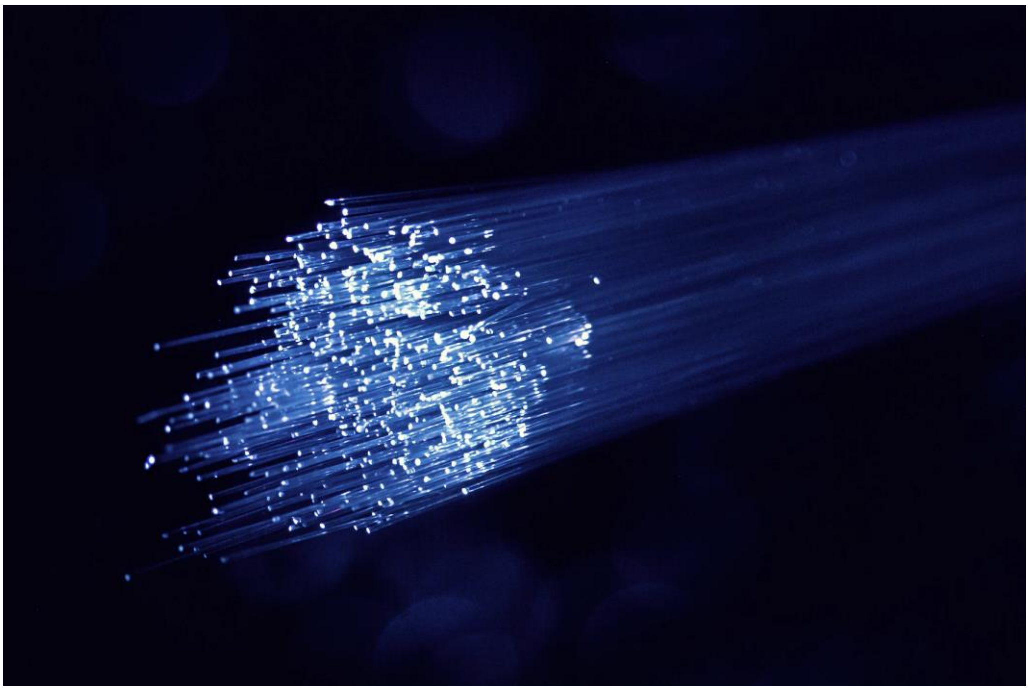
The threat posed by quantum computers to current encryption methods has motivated countries to find alternative ways to secure their communication networks. One method involves using quantum technologies itself, based on the common – but flawed – assumption that quantum communication is "unhackable" and therefore a superior approach to using new encryption methods that do not use quantum technologies. This view is driven by some properties of quantum information that give it a theoretical advantage against surveillance. ***MICHAL KRELINA*** *and* ***MANOJ HARJANI*** *point out that in practice there are several limitations that policymakers should consider when recommending quantum communication for use in networks supporting critical functions. They also highlight the countermeasures that could be taken to overcome those limitations.*

COMMENTARY

In recent years, countries have been working towards securing their communication networks using quantum technologies. A prominent example is China, which was the first country to launch a satellite for quantum communication in 2016. More recently in October 2023, researchers in the United Kingdom and Ireland successfully tested a quantum communication link via an underwater cable. Earlier this year, Singapore launched the National Quantum-Safe Network Plus initiative to partner local telcos in developing quantum communication infrastructure for critical sectors such as banking.

These efforts are motivated by the threat posed by quantum computers to current encryption methods that secure communication on the basis that certain mathematical problems cannot be easily solved by even the fastest "classical" supercomputers. Due to the different way they perform calculations compared to classical computers, quantum computers are theoretically capable of easily solving the mathematical problems that current encryption methods rely on. Although quantum computers with the capability to do this are nowhere close to being developed, this reality has not prevented hype building around the possibility of a “quantum apocalypse.”

Quantum communication is one of two ways to guard against the threat to encryption from quantum computers. The other is post-quantum cryptography (PQC), which uses new classical methods for encrypting data that can withstand potential attacks from quantum computers. However, PQC is not foolproof and faces a number of challenges for implementation. The main advantage that quantum communication is believed to have over PQC is that it is “unhackable”, but this is a flawed assumption. In fact, quantum communication has several limitations that should give policymakers cause for pause.



Though quantum communication can theoretically transmit information in a manner that is believed to be unconditionally secure, there are several limitations that policymakers should consider when recommending its use in networks supporting critical functions. *Image by Unsplash.*

What is Quantum Communication?

In classical communication, a binary bit is used to represent information using either 0s or 1s. Quantum communication harnesses the principles of quantum mechanics to represent information, using quantum bits or qubits. Unlike classical bits, which can only be either 0 or 1, qubits can be in a “superposition” of 0 and 1 simultaneously. This allows qubits to store more information than classical bits. Furthermore, when qubits are measured, their superposition is disturbed irrevocably, which is a helpful property to detect eavesdropping. It is also impossible to create an exact copy of a qubit, which is a further advantage against surveillance. Quantum communication protocols such as quantum key distribution (QKD) make use of these advantageous properties of qubits to transmit information in a manner that is believed to be unconditionally secure.

Limitations

Nevertheless, when we move from theory to practice, the apparently unconditional security of quantum communication comes up against significant limitations. Foremost is the fact that it requires purpose-built equipment and infrastructure. Not only is this costly, but it also reduces the ability of quantum communication networks to be upgraded easily to counter evolving security threats. Furthermore, it introduces the risk of insider threats as the basis for security is provided by hardware which can be manipulated.

Free-space quantum communication using satellites and drones aims to overcome this limitation related to physical infrastructure while facilitating long-distance quantum communication. Other than China, the European Union has emerged as a player in this field, with a quantum communication satellite launch planned for 2024 as part of the broader EuroQCI initiative to build a regional infrastructure for quantum communication. Singapore-based startup SpeQtral is also aiming to launch a quantum communication satellite in 2024, the first by a private company.

However, free-space quantum communication infrastructure is vulnerable to denial-of-service (DoS) attacks, which pose a significant challenge due to the ease with which such attacks can be carried out. One type of DoS attack involves using a laser to "dazzle" a receiver for quantum communication, overwhelming it in the same way that jamming would for a radio receiver. If a malign actor can trace the position of a quantum communication satellite, a successful DoS attack can be executed with a relatively low-powered laser.

Both terrestrial and free-space quantum communication are also vulnerable when the density of the network is low and the options for rerouting network traffic are either costly or infeasible. In such a scenario, a DoS attack targeting a single element of a network can have an outsized impact, potentially causing a significant reduction in functionality. This would be untenable if the network infrastructure is supporting time-sensitive operations or critical decision-making processes. DoS attacks involving dazzling would also be difficult to attribute, which makes it harder to respond effectively to them. Without clear identification of the responsible party, retaliatory or deterrent measures become riskier, which potentially leaves the targeted quantum communication network vulnerable to further attacks.

Countermeasures

Assessing risks and vulnerabilities is an important first step. The vulnerability of a quantum communication receiver to DoS attacks hinges on its specific design, so it is critical to gauge this experimentally during the security certification process and develop mitigation measures. Such measures often focus on hardening the security of the quantum communication receiver, but they are not a silver bullet. A more advanced mitigation measure would be to increase the density of the quantum communication network itself, thereby enabling rerouting of information. The alternative routes in the network can use classical communication secured with PQC to increase the overall resilience to DoS attacks tailored specifically for a quantum communication network.

To support a security certification process, countries will need to invest in infrastructure for testing and verification. As part of the EuroQCI initiative, the European Union called for a tender in July 2023 worth €16 million (~S$23.4 million) to develop such infrastructure. But it is not yet clear how this will be operationalised and whether there will be capabilities to also discover new vulnerabilities. How the certification process connects with the larger effort on standardisation for quantum communication will be critical to ensure interoperability. The International Standards Organisation (ISO) released standards for QKD security in August 2023, but the extent of their adoption is unclear.

The main takeaway for all countries considering the implementation of quantum communication networks is that they should proceed with caution, particularly where the technology is intended to be deployed to support critical functions, including in the military domain. Alongside investments in testing and verification, more attention will be needed for R&D to discover future vulnerabilities and potential mitigation measures. Nevertheless, as with traditional cybersecurity, humans remain the weakest link. “Unhackable” networks therefore remain a pipe dream, and countries should continue to be circumspect in their assessments of how secure their communication networks will be even as quantum communication is increasingly adopted.

Michal KRELINA *is a research scientist at the Czech Technical University in Prague and a quantum security consultant at the European Union Agency for the Space Programme;* ***Manoj HARJANI*** *is a Research Fellow with the Military Transformations Programme at the S. Rajaratnam School of International Studies.*