PakTech Today | Pakistan's Premier Technology Magazine
Vol. 01, Issue 14 • ISSN: 3136-2729

TECHNOLOGY FEATURE Industrial News / Technology Report / Research Communication

Quantum Internet: The Future of Secure Communication in a Cyber Warfare Era

As cyberattacks increasingly become the first strike in modern conflicts, a new kind of internet is emerging — one that could make hacking not just difficult, but physically impossible.

By **Muhammad Areeb** | Published: August, 2026
muhammadareeb4058@gmail.com | Position: Software Engineer

Introduction

In today's age, wars are no longer initiated through actual weapon attacks - wars are now initiated, often undetected, in cyberspace. Government websites crash, news sources are hijacked, vital systems are disabled long before the first physical engagement ever occurs. Cyber-attacks have become the opening shot of all modern wars.

Whether you're considering the banking sector or government databanks, none of the existing digital infrastructures are absolutely safe and hack-proof. With enough processing power, sophisticated techniques can even defeat a most protected network. This gives rise to a question: is it possible to make a system for communication that can be truly secure?

Quantum internet is a potential solution. It doesn't use sophisticated encryption to secure information but relies on physical principles. Such a development would not only change the ways in which countries guard their networks in a time of cyber war.

> ***" In a modern conflict, the first battle is the digital one — and the victor is the one who possesses or defends the information."***

Technology Overview

The quantum internet based on principles of quantum mechanics works quite differently to the classical internet we are all familiar with today. In place of the bits that are used in the classical internet it uses qubits which, due to the effect of Superposition can exist in more than one state at any given time.

The second core concept is quantum entanglement where two particles are intrinsically linked irrespective of distance. If an action is taken with one particle, the other is instantly altered allowing for a completely new mode of communication.

This allows the concept of **quantum teleportation** where we transfer the 'state of information' not the 'data'. Unlike classical networks it is not necessary to send data packets to the recipient in which they can be captured.

A typical quantum network includes:

- **Quantum nodes** for processing qubits
- **Communication channels** (fiber optics or satellites)
- **Quantum repeaters** to extend range
- **Quantum memory** to store quantum states

One practical use for such ideas is that of **Quantum Key Distribution (QKD)**. QKD is a method whereby two parties can establish and share the keys needed to encrypt and decrypt information. Any third-party trying to steal the key will be detected.

Vol. 01, Issue 14 • ISSN: 3136-2729

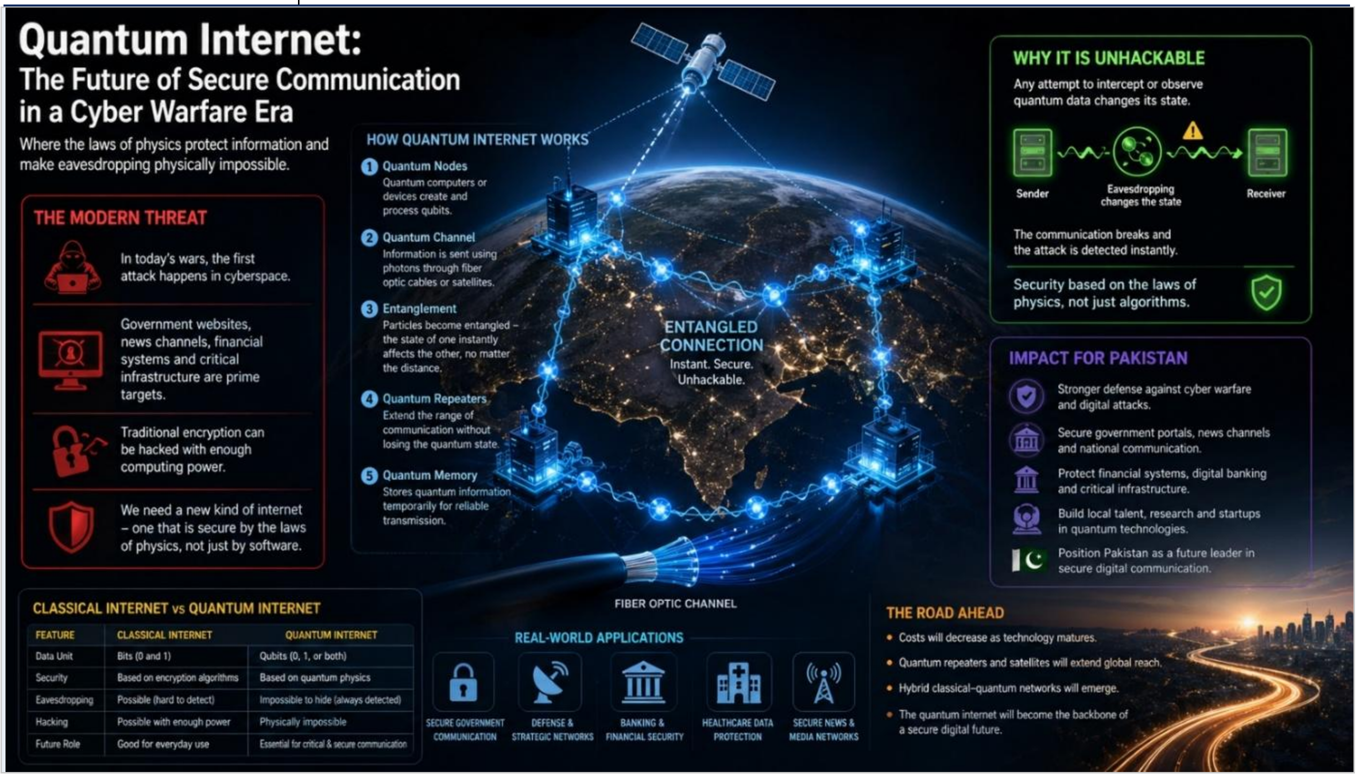

Figure 1: *Conceptual model of a quantum internet showing secure communication through entangled particles. Credit: Author*

Key Findings & Impact

In terms of cybersecurity and global conflict, the necessity for a quantum internet becomes more transparent. Cyber-attacks on governmental websites, financial systems, and news organizations have become more common during geopolitical conflicts. They disrupt the flow of communication and knowledge, and contribute to the vulnerability of a nation.

Quantum communication changes this equation entirely.

Based on the Heisenberg Uncertainty Principle, any attempt to observe or intercept quantum data alters its state. This means that hacking is not just difficult — it is instantly detectable.

Recent experiments have already demonstrated:

- Secure quantum communication over fiber networks
- Successful quantum key distribution in real-world conditions
- Early-stage quantum networks connecting multiple nodes

The influence of this technology includes:

- **National Security:** Protecting national security from cyber warfare
- **Media Integrity:** Hacking prevention of news channels, information spread **Financial Systems:** Secured digital banking, secure online transactions
- **Critical Infrastructure:** Power grid protection, defense systems protection, communication networks protection

It is critical for Pakistan as it undergoes rapid digital transition. Increased dependence on online systems also brings increased threat from cyber-attacks. Using quantum secure communication could help boost national resilience.

What's Next?

Though quantum internet is highly powerful, it is a nascent technology. Before its widespread usage, many hurdles need to be overcome. High cost of components, fragile nature of quantum states, and distance of transmission are few to name.

Despite this, progress is being made both governments and organisations are putting investment into quantum research around the globe and acknowledging its value in areas such as innovation and national security.

The near future will bring hybrid networks which are essentially a merge between classical and quantum networks; speed with unmatched security.

It is imperative that developers, researchers, scientists and innovators start to educate themselves about quantum computing today to form the solutions for tomorrow. It can't be more apparent with cyber-warfare now the common tactic of fighting against each other. The quantum internet isn't about faster communications. It's about ensuring that even when conflicts arise, truth and information are always safe.

About the Author
Muhammad Areeb loves to tinker with Software engineering and has a great curiosity toward new and upcoming technologies like artificial intelligence and quantum computing. The core idea is to make these difficult topics easily digestible for future generations of developers. He can be reached at muhammadareeb4058@gmail.com.

Keywords: Quantum Internet; Cybersecurity; Cyber Warfare; Quantum Computing; Pakistan Tech

References

[1] Wehner, S., Elkouss, D., & Hanson, R. (2018) Quantum internet: A vision for the road ahead, Science, 362(6412).
[2] Kimble, H.J (2008) The quantum internet, *Nature*, 453, pp. 1023–1030.
[3] Pirandola, S. et al. (2020) Advances in quantum cryptography, *Advances in Optics and Photonics*, 12(4), pp. 1012–123