Quantum Communications
Enhancing Network Security and Resilience in a Geopolitical Context

SERENTSCHY.COM
SERENTSCHY ADVISORY SERVICES GMBH

Innovation and Telecommunications Policy: Shaping Tech, Markets & Networks
May 21, 2025, Ivey Donald K. Johnson Centre,
130 King St W, Toronto

Quantum Communications
Network Security and Resilience in a Geopolitical Context

Roadmap

- Introduction
- Quantum Communications
- Network Security and Resilience
- Geopolitical Implications
- What is "Digital Strategic Autonomy"?
- Key Applications for Quantum Communications
- Prospects and Recommendations
- Conclusions

Quantum Communications
Network Security and Resilience in a Geopolitical Context

Criminal Court: Microsoft's email block a wake-up call for digital sovereignty

Microsoft blocked the email account of Chief Prosecutor of the International Court of Justice after Trump's sanctions. Critics: "We urgently need alternatives."

The International Criminal Court in The Hague. (Image: ICC)

Microsoft blocked the email account of the Chief Prosecutor of the International Criminal Court (ICC), Karim Khan. The court is nearly paralyzed in its operations, according to the Associated Press news agency.

This example is intended solely to illustrate the need for more digital sovereignty.

Quantum Communications
Network Security and Resilience in a Geopolitical Context

1. Introduction

Background and Context: The geopolitical landscape is increasingly complex, with technological advancements playing a crucial role in national security and economic competitiveness. Quantum communications, with its promise of unbreakable encryption, is at the forefront of this technological race.

Message: In my talk, I will discuss the potential of quantum communication to improve network security and resilience, particularly in the context of digital sovereignty and strategic autonomy against the backdrop of the massive tectonic shifts in the geopolitical landscape.

2. Quantum Communications - An Overview (1)

- **Definition and Importance**: Quantum communications leverage the principles of quantum mechanics to provide secure communication channels. It is essential for protecting sensitive data in various sectors.
- **Key Technologies**: Post-quantum cryptography (PQC), a new mathematically based cryptography, and quantum key distribution (QKD), which is based on the laws of physics, are the solutions for quantum-secure encryption.

Quantum Communications
Network Security and Resilience in a Geopolitical Context

2. Quantum Communications - An Overview (2)

Current State of Quantum Communications: Canada is making significant strides in quantum communications, based on the **National Canadian Quantum Strategy** to build a full-stack quantum ecosystem and equip Canada with a national secure quantum communications network and quantum cryptography capabilities.

3. Network Security and Resilience (1)

- **Importance of Network Security**: Network security is critical for protecting sensitive data and infrastructure from cyber threats.
- **Challenges in Network Security**: Current challenges include the increasing sophistication of cyber threats, in particular the use of AI-based tools.

3. Network Security and Resilience (2)

- **Resilience in Network Infrastructure**: Network resilience is the ability to maintain operational continuity in the face of disruptions
- **Quantum Communications for Enhanced Security**: Quantum communications provide unbreakable encryption, making it an ideal solution for enhancing network security.

4. Geopolitical Implications (1)

Geopolitical Landscape: The geopolitical landscape is characterized by competition among major powers like the U.S., China, and Europe. The latest geopolitical disruptions present both Canada and Europe with a new kind of dilemma: the long-standing boundary between "like-minded" and "non-likeminded countries" appears to be blurring, and confidence in a constellation known as the "Western Alliance" has been eroded.

4. Geopolitical Implications (2)

- **Digital Sovereignty and Strategic Autonomy** involves the ability of a nation to control and protect its critical technologies and infrastructures.
- **Global Competition**: The global competition in quantum technologies is intense, with major players investing heavily in research and development.

4. Geopolitical Implications (3)

- **Policy and Regulatory Frameworks** govern the development and deployment of quantum communications. These frameworks ensure that quantum technologies are used responsibly and ethically, aligning with Canada's geopolitical interests.

A digression on Digital Strategic Autonomy (1)

Strategic Autonomy is defined here as the ability of a given country to decide and act upon the future in economy, society and democracy.
It is the means to realize and safeguard (digital) sovereignty.

Strategic Autonomy is built on **3 Cs: capabilities, capacities, and control**.

Quantum Communications
Network Security and Resilience in a Geopolitical Context

Digital Strategic Autonomy (2)

Capabilities *are about what is available in the country, as relevant for strategic autonomy.*

Quantum Communications
Network Security and Resilience in a Geopolitical Context

Digital Strategic Autonomy (3)

Capacities *are about how much a country can do, as relevant for strategic autonomy.*

Quantum Communications
Network Security and Resilience in a Geopolitical Context

Digital Strategic Autonomy (4)

Control *is about the actual ability of a country to control and protect its critical technologies and infrastructures*

5. Key Applications and Examples for Quantum Communication (1)

Critical infrastructures facing a massive increase from more and more sophisticated attacks, with new technologies like AI and quantum playing a major role.

Banking: Quantum communications enhance the security of financial transactions, protect sensitive customer data and preventing fraud.

Quantum Communications
Network Security and Resilience in a Geopolitical Context

5. Key Applications and Examples for Quantum Communication (2)

Defense: Quantum communications are crucial for securing national defense infrastructures, protecting against cyber threats and espionage.

Logistics and Transportation are critical sectors that rely heavily on secure and efficient communication networks.

5. Key Applications and Examples for Quantum Communication (3)

Electricity Generation and Transport is a critical infrastructure that requires secure and resilient communication networks to ensure the reliable and efficient delivery of power. Key applications are **Secure Grid Management**, **Real-Time Monitoring and Control** of the power grid, **Smart Grid Technologies** (protection from hacking and other cyber threats).

Quantum Communications
Network Security and Resilience in a Geopolitical Context

6. Prospects and Recommendations (1)

- **Future Trends** in quantum communications include the development of more advanced quantum encryption methods, the integration of quantum technologies with AI, and the expansion of quantum networks.

- **Policy Makers** should invest in research and development and building of **full-stack ecosystems**, foster international collaboration, and create regulatory frameworks that support the adoption of quantum communications.

Quantum Communications
Network Security and Resilience in a Geopolitical Context

6. Prospects and Recommendations (2)

- **Industry** is called upon to leverage quantum technologies as a pathway to new business opportunities, to test applications together with customers using testbeds, and thus to deploy quantum communications for greater security and resilience.

7. Conclusions (1)

- **Geopolitical developments** over the past two to three years, and particularly the course taken by the new US administration, have led to a complete paradigm shift. **Digital Sovereignty and Strategic Autonomy are now at the top of the agenda for all actors.**
- **Quantum communications** offer significant potential for enhancing network security and resilience. They are crucial for achieving strategic sovereignty and protecting critical infrastructures.
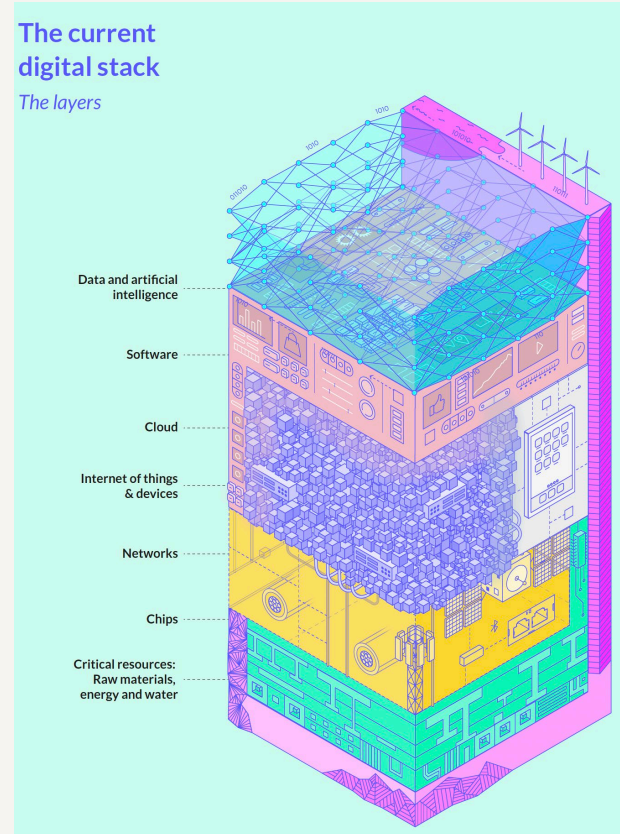
7. Conclusions (2)

Call to Action: The adoption and integration of quantum communications are essential for ensuring a secure and resilient digital future against the backdrop of the geopolitical disruptions. To tap into this potential, further policy research, **consideration of the entire digital stack** (see EuroStack), and increased cooperation and investment are needed.

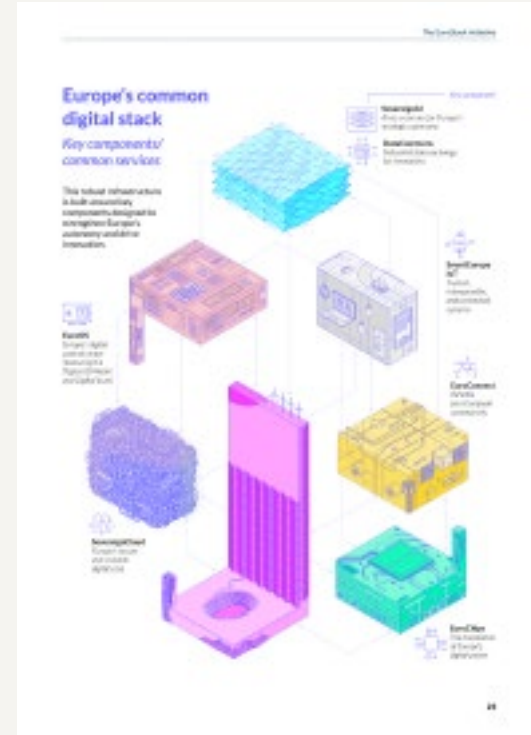Source: https://www.euro-stack.info/docs/EuroStack_2025.pdf

The current digital stack
The layers

Data and artificial intelligence

Software

Cloud

Internet of things & devices

Networks

Chips

Critical resources: Raw materials, energy and water

22

Quantum Communications
Network Security and Resilience in a Geopolitical Context

7. EuroStack as a model for more digital sovereignty

Seven guiding principles:

- Sovereignty and security: Guaranteeing that Europe's critical digital infrastructure remains under European jurisdiction
- Interoperability
- Sustainability
- Data as a common good
- Decentralized sovereign infrastructure
- Inclusive governance
- Strong democracy

Source: https://www.euro-stack.info/docs/EuroStack_2025.pdf