SCIENCEZONE | ONLINE SCIENTIFIC CONFERENCES

GOVERNING THE UNKNOWN: LEGAL REGULATION OF QUANTUM COMPUTING THREATS

Islombek Abdikhakimov
Lectuer of Cyber Law Department, Tashkent State University of Law
islombekabduhakimov@gmail.com

Abstract: Quantum computing, while offering transformative potential in science, communication, and cryptography, simultaneously presents unprecedented risks to cybersecurity, privacy, and global security. Current legal frameworks remain inadequate to address the threats posed by quantum technologies, particularly the ability to undermine widely used encryption systems. This article examines the legal regulation of quantum computing threats, identifying gaps in international law, national legislation, and export control regimes. Using a qualitative analysis of existing norms, treaties, and proposals, the study highlights the urgent need for adaptive, anticipatory, and globally harmonized regulation. Recommendations include updating cybersecurity law, strengthening international cooperation, and developing quantum-specific legal frameworks to mitigate risks while enabling responsible innovation.

Keywords: quantum computing, cybersecurity, legal regulation, encryption, international law, export control

Introduction

Quantum computing represents a paradigm shift in information processing, leveraging quantum mechanics to perform calculations beyond the reach of classical computers (Arute et al., 2019). While the benefits range from advances in drug discovery to optimization problems, the most immediate legal and security concern lies in its ability to break existing cryptographic protocols (Mosca, 2018). This capability threatens the foundation of global digital infrastructure, including banking, e-commerce, and secure communications.

Despite the urgency, legal responses remain fragmented. International cybersecurity frameworks such as the Budapest Convention on Cybercrime (2001) do not explicitly address quantum computing threats. Similarly, export control laws focus on conventional dual-use technologies but lack clarity on quantum algorithms and hardware (Horowitz, 2022). This paper investigates the legal regulation of quantum computing threats, analyzing gaps and proposing pathways for reform.

Methodology

This study employs a qualitative doctrinal legal research approach, supplemented by comparative analysis. Primary sources include treaties, conventions, national legislations, and policy papers. Secondary sources include peer-reviewed articles and reports from institutions such as the World Economic Forum and the European Union Agency for Cybersecurity (ENISA). The research focuses on three key areas:

1. **Cryptographic vulnerability** and cybersecurity regulation.

2. **International legal instruments** addressing quantum threats.

3. **Export control frameworks** governing sensitive quantum technologies.

Results

1. Cryptographic Vulnerability and Legal Gaps

Shor's algorithm demonstrates that a sufficiently powerful quantum computer could efficiently factor large numbers, rendering RSA and ECC cryptography obsolete (Shor, 1997). While post-quantum cryptography (PQC) is under development, legal frameworks mandating its adoption remain absent. For instance, the EU's Cybersecurity Act (2019) enhances digital resilience but does not specify quantum readiness (ENISA, 2021). The U.S. National Institute of Standards and Technology (NIST) is standardizing PQC algorithms, yet no federal law compels their adoption across critical infrastructure (Chen et al., 2022).

2. International Legal Instruments

International law is largely silent on quantum threats. The Tallinn Manual on the International Law Applicable to Cyber Operations (2017) acknowledges cyber risks but lacks provisions on quantum-enabled attacks. The UN Group of Governmental Experts (GGE) has promoted norms of responsible state behavior in cyberspace, but quantum computing remains outside its explicit scope (UNODA, 2021). This omission creates uncertainty in attributing liability for quantum-enabled cyberattacks or espionage.

3. Export Control and Dual-Use Regulation

Quantum technologies fall within the scope of "dual-use" items regulated by export control regimes such as the Wassenaar Arrangement. However, guidelines remain vague, focusing on hardware (e.g., cryogenic systems, quantum sensors) but not on algorithms or cloud-based quantum computing services (Horowitz, 2022). This creates loopholes for proliferation risks, particularly where hostile actors could access foreign quantum capabilities through remote platforms.

Discussion

The findings indicate a **triple regulatory gap**: cybersecurity law lags behind technological advances, international law lacks explicit provisions, and export control frameworks inadequately capture software-based threats. The consequences include:

- **Erosion of trust in digital systems**: Without mandatory PQC, governments and corporations risk catastrophic breaches once scalable quantum computers emerge.
- **Legal uncertainty in state responsibility**: International law's silence on quantum-enabled attacks leaves ambiguity regarding retaliation, proportionality, and liability.
- **Weak export controls**: Absence of harmonized rules on quantum algorithms undermines non-proliferation efforts.

To address these challenges, anticipatory regulation is required. Legal scholars advocate for "technology-neutral yet forward-looking" frameworks that integrate quantum considerations into cybersecurity and arms control treaties (Fischer, 2021). Moreover, states must cooperate to establish global standards on PQC adoption, liability in quantum cyber incidents, and monitoring of dual-use quantum exports.

Conclusion

Quantum computing threatens to disrupt the legal foundations of cybersecurity and international security. Current laws are insufficient to address risks such as the breaking of encryption, cross-border quantum cyberattacks, and proliferation of dual-use technologies. Effective regulation requires a threefold strategy: (1) enacting national laws mandating post-quantum cryptography, (2) integrating quantum risks into international cybersecurity treaties and norms, and (3) updating export control frameworks to include algorithms and cloud-based services. Proactive and harmonized governance will be essential to mitigate the dangers of quantum computing while fostering its responsible development.

References

1. Arute, F., et al. (2019). Quantum supremacy using a programmable superconducting processor. *Nature, 574*(7779), 505–510. https://doi.org/10.1038/s41586-019-1666-5

2. Budapest Convention on Cybercrime. (2001). Council of Europe.

3. Chen, L. K., et al. (2022). Post-quantum cryptography standardization: Current status and future directions. *NIST Journal of Research, 127,* 1–20.

4. ENISA. (2021). *Post-Quantum Cryptography: Current state and quantum mitigation.* European Union Agency for Cybersecurity.

5. Fischer, E. (2021). *Quantum technologies and cybersecurity: Policy implications.* Congressional Research Service.

6. Horowitz, M. C. (2022). The politics of emerging technologies: The case of quantum computing. *Journal of Strategic Studies, 45*(6), 931–952.

7. Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy, 16*(5), 38–41.

8. Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing, 26*(5), 1484–1509.

9. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. (2017). Cambridge University Press.

10. UNODA. (2021). *Developments in the field of information and telecommunications in the context of international security.* United Nations Office for Disarmament Affairs.