KONFERENSIYALAR.COM

ANJUMANLAR PLATFORMASI

O‘ZBEKISTON – 2030: INNOVATSIYA, FAN VA TA’LIM ISTIQBOLLARI

V RESPUBLIKA ILMIY-AMALIY KONFERENSIYA MATERIALLARI

AVGUST, 2025-YIL

O‘ZBEKISTON 2030

KONFERENSIYALAR.COM

ANJUMANLAR PLATFORMASI

O‘ZBEKISTON — 2030: INNOVATSIYA, FAN VA TA’LIM ISTIQBOLLARI

V RESPUBLIKA ILMIY-AMALIY KONFERENSIYASI MATERIALLARI

2025-yil, avgust

TOSHKENT-2025

ISBN 978-9910-09-280-0

O‘ZBEKISTON – 2030: INNOVATSIYA, FAN VA TA’LIM ISTIQBOLLARI. V Respublika ilmiy-amaliy konferensiyasi materiallari. – Toshkent: Scienceproblems team, 2025. – 96 bet.

Elektron nashr: https://konferensiyalar.com

Konferensiya tashkilotchisi: “Scienceproblems Team” MChJ

Konferensiya o‘tkazilgan sana: 2025-yil, 11-avgust

Mas’ul muharrir:
Isanova Feruza Tulqinovna

Annotatsiya
Mazkur nashrda “O‘zbekiston — 2030: innovatsiya, fan va ta’lim istiqbollari” nomli V Respublika ilmiy-amaliy konferensiyasi doirasida taqdim etilgan ilmiy maqolalar to‘plami jamlangan. Unda O‘zbekistonning turli oliy ta’lim va ilmiy-tadqiqot muassasalari, tarmoq tashkilotlari, mustaqil tadqiqotchilar tomonidan taqdim etilgan ijtimoiy-gumanitar, iqtisodiyot, huquq, biologiya, tibbiyot va boshqa sohalarga oid maqolalar kiritilgan. Maqolalarda ilm-fanning zamonaviy yo‘nalishlari, innovatsion texnologiyalar, ta’lim islohotlari hamda barqaror taraqqiyotga oid masalalar muhokama qilingan. To‘plam akademik izlanishlar, amaliy tajribalar va ilmiy xulosalarni birlashtirgan holda, fanlararo integratsiyani chuqurlashtirish va ilmiy hamkorlikni kuchaytirishga xizmat qiladi.

Kalit so‘zlar: ilmiy-amaliy konferensiya, innovatsiya, fan va ta’lim, O‘zbekiston 2030, barqaror rivojlanish, ilmiy izlanishlar, fanlararo integratsiya, ilmiy hamkorlik, texnologik taraqqiyot, zamonaviy ta’lim.

ISBN 978-9910-09-280-0

YURIDIK FANLAR

QUANTUM COMMUNICATION AND STATE SOVEREIGNTY IN CYBERSPACE

Abdikhakimov Islombek Bahodir ugli
Lecturer of Cyber Law Department, Tashkent State University of Law
E-mail:
islombekabduhakimov@gmail.com
Tel.: +998 94 423 12 98
Tashkent, Uzbekistan

Annotation. The emergence of quantum communication technologies represents a paradigm shift in how states conceptualize and exercise sovereignty in cyberspace. This article examines the intersection of quantum key distribution systems, satellite-based quantum networks, and evolving principles of digital sovereignty in international law. As nations race to develop quantum-secure communication infrastructures, fundamental questions arise about territorial control, jurisdictional authority, and the future of state power in the digital domain. Drawing on recent developments in China's Micius satellite program, the European Union's EuroQCI initiative, and the United States' DARPA quantum projects, this analysis explores how quantum technologies are reshaping sovereignty concepts while creating new geopolitical divides. The article argues that quantum communication is not merely a technological advancement but a sovereignty issue that will define the balance of power in the 21st century digital order.

Keywords: Quantum Communication, State Sovereignty, Digital Sovereignty.

KVANT ALOQA VA KIBERMAKONDA DAVLAT SUVERENITETI

Abdixakimov Islombek Bahodir o'g'li
Kiber huquq kafedrasi o'qituvchisi, Toshkent davlat yuridik universiteti

Annotatsiya. Kvant aloqa texnologiyalarining paydo bo'lishi davlatlarning kiber makondagi suverenitetni tushunish va amalga oshirish usullarida tub burilish yasamoqda. Ushbu maqola kvant kalitlarini taqsimlash tizimlari, sun'iy yo'ldosh asosidagi kvant tarmoqlari hamda xalqaro huquqda raqamli suverenitetning shakllanib borayotgan tamoyillari o'rtasidagi o'zaro bog'liqlikni tahlil qiladi. Davlatlar kvant xavfsiz aloqa infratuzilmasini yaratish poygasiga kirar ekan, hududiy nazorat, yurisdiksiya vakolati va raqamli sohada davlat hokimiyatining kelajagi bilan bog'liq asosiy savollar yuzaga kelmoqda. Maqolada Xitoyning Micius sun'iy yo'ldoshi dasturi, Yevropa Ittifoqining EuroQCI tashabbusi hamda AQShning DARPA kvant loyihalari misolida kvant texnologiyalari qanday qilib suverenitet tushunchalarini qayta shakllantirayotgani va yangi geosiyosiy tafovutlar yaratayotgani yoritilgan. Muallifning ta'kidlashicha, kvant aloqa oddiy texnologik yutuq emas, balki XXI asrning raqamli tartibida kuchlar muvozanatini belgilovchi suverenitet masalasidir.

Kalit so'zlar: Kvant aloqa, davlat suvereniteti, raqamli suverenitet

The concept of state sovereignty, traditionally rooted in territorial control and political independence, faces unprecedented challenges in the digital age. Cyberspace, characterized by its borderless nature and rapid information flows, has compelled scholars and policymakers to reconceptualize sovereignty beyond physical geography [1]. Now, quantum communication technologies introduce another transformative layer to this evolving landscape. These technologies, which exploit quantum mechanical properties to enable theoretically unbreakable encryption, are being framed by governments worldwide as essential to maintaining sovereignty in an interconnected digital world [2].

The significance of quantum communication for state sovereignty extends beyond technical capabilities. In 2017, China demonstrated the world's first satellite-based quantum key distribution using the Micius satellite, an achievement that governments globally recognized as establishing a new domain of strategic competition [3]. The European Union has characterized quantum technologies as "essential building blocks for Europe's technological sovereignty," while the United States views quantum capabilities as critical to national security [4][5]. This convergence of technological innovation and sovereignty discourse raises fundamental questions about how international law applies to quantum-enabled cyberspace and whether existing sovereignty frameworks remain adequate.

Quantum communication represents a fundamental departure from classical cryptographic methods. At its core lies quantum key distribution (QKD), a secure communication method that implements cryptographic protocols based on quantum mechanics principles, specifically quantum entanglement, the measurement-disturbance principle, and the no-cloning theorem [6]. Unlike traditional public key cryptography, which relies on computational difficulty, QKD provides information-theoretic security grounded in physical laws rather than mathematical assumptions [7].

The security of QKD stems from quantum mechanics' fundamental properties. The no-cloning theorem establishes that arbitrary unknown quantum states cannot be perfectly copied, preventing unauthorized duplication of encryption keys [8]. Furthermore, the Heisenberg uncertainty principle ensures that any attempt to measure or intercept quantum states necessarily disturbs the system, alerting legitimate parties to eavesdropping attempts [9]. These properties provide what researchers describe as "provable security" – security guaranteed by the laws of physics rather than assumptions about computational limitations [10].

Despite its theoretical elegance, QKD implementation faces significant practical challenges. Photon loss in optical fibers limits transmission distances to approximately 100-300 kilometers under ideal conditions [11]. Satellite-based quantum communication has emerged as a solution to distance limitations. China's Micius satellite, launched in 2016, pioneered this approach by achieving quantum entanglement distribution over 1,200 kilometers and enabling intercontinental quantum key distribution between China and Europe spanning 7,600 kilometers [12][13].

Sovereignty remains a cornerstone of international law, traditionally understood through two dimensions: internal supremacy within territorial boundaries and external independence from other states' authority [14]. The International Court of Justice has affirmed that "between independent States, respect for territorial sovereignty is an essential foundation of international relations" [15]. This principle grants states exclusive jurisdiction over territory, including the right to exercise legislative, adjudicative, and enforcement authority [16].

The United Nations Group of Governmental Experts on Cyber Security confirmed in consecutive reports that sovereignty and international norms flowing from sovereignty apply to cyber activities [17]. The Tallinn Manual 2.0 on International Law Applicable to Cyber Operations similarly affirms that existing international law applies to cyber operations, with sovereignty principles extending to cyber infrastructure located within state territories [18].

The exercise of sovereignty in cyberspace presents distinctive challenges absent in physical domains. Cyber operations can simultaneously involve multiple jurisdictions, with different components originating from or transiting through various countries [19]. Controversy persists regarding when cyber operations violate territorial sovereignty. The Tallinn Manual 2.0 experts unanimously agreed that cyber operations causing permanent functionality loss or physical damage violate sovereignty, but consensus eluded them regarding lower-intensity operations [20]. France has adopted a broad position, stating that any unauthorized cyber intrusion into French systems constitutes sovereignty violation [21].

Digital sovereignty has emerged as a distinct policy concept, representing states' efforts to maintain control over digital infrastructure, data flows, and technological capabilities within the digital domain [22]. Quantum technologies fundamentally alter digital sovereignty's parameters. A robust quantum communication infrastructure enables states to secure their most sensitive communications against both current and future threats, including the anticipated capacity of quantum computers to break existing encryption methods [23].

The European Quantum Communication Infrastructure (EuroQCI) initiative exemplifies this sovereignty-technology nexus. Launched in 2019 with participation from all 27 EU member states, EuroQCI aims to build a quantum-secure communication network across Europe, combining terrestrial fiber networks with satellite components [24]. European Commission documentation explicitly characterizes the initiative as essential for "protecting European sovereignty and its economy in the face of increasing cybersecurity challenges" [25].

Several factors position quantum communication as a sovereignty issue. First, the technology directly affects states' ability to conduct secure communications – a fundamental attribute of independent statehood. Without quantum-secure channels, states face potential surveillance by adversaries who may intercept and store encrypted communications for future decryption [26]. This "harvest now, decrypt later" threat creates long-term vulnerability that undermines sovereignty's independence dimension.

Second, quantum communication infrastructure requires substantial physical components within state territory, including ground stations, fiber networks, satellites, and specialized equipment [27]. Control over this infrastructure translates directly to jurisdictional authority. Third, quantum communication capabilities create asymmetric advantages in intelligence gathering and information security, influencing power dynamics in international relations [28].

China has pursued quantum technologies with unprecedented ambition, viewing them as essential to achieving technological independence and strategic parity with Western powers [29]. The Micius satellite project represents China's most visible quantum achievement. Launched in August 2016, Micius demonstrated several world-first capabilities: satellite-based quantum key distribution over 2,500 kilometers, quantum entanglement distribution over 1,200 kilometers, and the first intercontinental quantum-secured video conference between Beijing and Vienna in 2017 [30][31].

Subsequent developments have extended China's quantum reach. In 2020, Pan's team achieved entanglement-based quantum key distribution via satellite without requiring the satellite itself to know the encryption keys [32]. More recently, China established quantum communication links with South Africa, marking the first such connection in the Southern Hemisphere and demonstrating China's intention to build quantum networks among BRICS nations [33]. China has also constructed a 2,000-kilometer fiber-optic quantum communication backbone connecting Beijing to Shanghai, with 32 trusted relay nodes enabling secure communications tested by government agencies and banks [34].

The United States has approached quantum technologies through multiple channels. The Defense Advanced Research Projects Agency (DARPA) established an early quantum key distribution network in Boston-Cambridge from 2003-2007 [35]. More recently, DARPA launched the Quantum-Augmented Network (QuANET) program, seeking to integrate quantum communication capabilities with classical network infrastructure to enhance security, privacy, and resilience [36][37]. QuANET differs from many international efforts by focusing beyond quantum key distribution to incorporate quantum time synchronization and quantum sensing data [38].

In 2024, QuANET performers demonstrated the first functioning quantum-augmented network, successfully transmitting messages across classical and quantum links with record-breaking speeds [39]. The European Union combines sovereignty concerns with scientific collaboration through its €1 billion Quantum Technologies Flagship, launched in 2018 [40]. The EuroQCI initiative constitutes the flagship's practical application to quantum communication infrastructure [41].

The concentration of quantum capabilities among technologically advanced states creates what scholars term a "quantum divide" paralleling historical digital divides [42]. Export controls on quantum-relevant technologies have expanded significantly since 2020. The United States imposed targeted bans on Chinese quantum companies in 2021, followed by comprehensive export license requirements for quantum hardware, software, and systems in late 2024 [43]. The European Union established a unified framework limiting exports of functional qubits exceeding 34 qubits [44]. China responded with export restrictions on germanium and gallium, materials essential for quantum production [45].

These restrictions create concentric circles of access: allied nations enjoy privileged technology exchange, competitors face increasing barriers, and nations in the Global South often find themselves excluded [46]. For countries lacking capital and research capacity, this exclusion creates a triple disadvantage: security infrastructure vulnerable to quantum computing threats, diminished economic competitiveness, and eroded technological sovereignty through dependence on external providers [47].

Despite remarkable progress, quantum communication faces persistent technical obstacles. Distance limitations, though ameliorated by satellite systems, still constrain terrestrial networks. Quantum repeaters, which could extend fiber-based networks indefinitely, remain immature and difficult to implement at scale [48]. Detector imperfections and environmental interference create security vulnerabilities [49]. Integration with existing infrastructure presents another challenge, as current quantum systems require specialized equipment incompatible with standard network architectures [50].

The international legal framework governing quantum communication remains underdeveloped. Questions arise regarding the legal status of quantum-encrypted communications crossing borders, the applicability of interception and surveillance laws to quantum channels, and the obligations of states hosting quantum network infrastructure [51]. The Tallinn Manual 2.0 provides some guidance on cyberspace sovereignty generally but does not specifically address quantum communication technologies [52]. International cooperation mechanisms for quantum technologies remain limited, with increasing securitization limiting knowledge sharing [53].

The quantum race's trajectory will significantly influence international power dynamics. States achieving quantum communication superiority may leverage this advantage to enhance their global influence and secure their decision-making autonomy [54]. The concentration of quantum capabilities among a few states could create a multipolar quantum order, with distinct spheres of influence around Chinese, American, and European quantum networks. States excluded from quantum development may increasingly view the technology gap as threatening their sovereignty [55].

The international legal framework governing sovereignty in cyberspace provides foundational principles but requires adaptation to address quantum-specific questions. Ambiguities in applying sovereignty to cyber operations become more acute with quantum technologies, where physical infrastructure, quantum states, and information flows intersect in novel ways.

Looking forward, the quantum race will likely accelerate as states recognize the technology's strategic significance. Whether this acceleration produces collaborative frameworks or intensified competition will shape not only global security but also fundamental questions about sovereignty's future in an increasingly digitized world. The principle is clear: technological capabilities increasingly define sovereignty's practical exercise in the 21st century. As quantum technologies mature and deploy at scale, sovereignty in cyberspace will be measured not only by legal principles and political independence but by concrete technological capabilities to secure communications, protect data, and maintain autonomy in an interconnected digital realm.

Adabiyotlar/Литература/References:

1. Couture, S., & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? New Media & Society, 21(10), 2305-2322.
2. Eslam, H., & Tiwari, G. (2025). Cyberspace: Reimagining Cybersecurity and Its Impact on State Sovereignty. In M. Chawki & A. Abraham (Eds.), Cybercrime Unveiled: Technologies for Analysing Legal Complexity. Springer.
3. E-International Relations. (2025, September 29). The Quantum Race: How Emerging Technologies Reshape Global Security Governance.
4. Mazzucato, M. (2023). Digital sovereignty, digital infrastructures, and quantum horizons. AI & Society, 38, 1-19.
5. Liman, T., & Weber, R. (2023). Quantum Computing: Bridging the National Security–Digital Sovereignty Divide. European Journal of Risk Regulation, 14(3), 476-483.
6. Wikipedia. (2025, November 9). Quantum key distribution.
7. TechTarget. (n.d.). What is Quantum Key Distribution? QKD Explained.
8. Quside. (2025, March 13). How does Quantum Key Distribution (QKD) work?
9. Sabani, M., Savvas, I., Poulakis, D., & Makris, G. (2022). Quantum Key Distribution: Basic Protocols and Threats. In 26th Pan-Hellenic Conference on Informatics (PCI 2022). ACM.
10. ID Quantique. (2025, November 5). Quantum Key Distribution | QKD | Quantum Cryptography.
11. Quantum Xchange. (2025, June 30). How Does Quantum Key Distribution (QKD) Work?
12. Pan, J.-W., et al. (2022). Micius quantum experiments in space. Reviews of Modern Physics, 94, 035001.
13. Phys.org. (2018, January 19). Real-world intercontinental quantum communications enabled by the Micius satellite.
14. von Heinegg, W. H. (2012). Legal Implications of Territorial Sovereignty in Cyberspace. In 4th International Conference on Cyber Conflict Proceedings 2012. NATO CCD COE.
15. International Court of Justice. (1949). Corfu Channel Case.
16. NATO CCD COE. (2025, September 24). Sovereignty - International cyber law: interactive toolkit.
17. Chircop, L. (2019). Territorial Sovereignty in Cyberspace After Tallinn Manual 2.0. Melbourne Journal of International Law, 20(2), 349.
18. Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press.
19. von Heinegg, W. H. (2013). Territorial Sovereignty and Neutrality in Cyberspace. International Law Studies, 89, 123-156.
20. Chircop, L. (2019). Territorial Sovereignty in Cyberspace After Tallinn Manual 2.0. Melbourne Journal of International Law, 20(2), 349.
21. Just Security. (2021, March 12). The Application of International Law to Cyberspace: Sovereignty and Non-intervention.
22. Mazzucato, M. (2023). Digital sovereignty, digital infrastructures, and quantum horizons. AI & Society, 38, 1-19.
23. Defense Magazine. (2025, July 25). Quantum independence: State sovereignty between lasers, chips, and geopolitics.
24. European Commission. (n.d.). European Quantum Communication Infrastructure - EuroQCI.
25. Mazzucato, M. (2023). Digital sovereignty, digital infrastructures, and quantum horizons. AI & Society, 38, 1-19.
26. Defense Magazine. (2025, July 25). Quantum independence: State sovereignty between lasers, chips, and geopolitics.
27. Mazzucato, M. (2023). Digital sovereignty, digital infrastructures, and quantum horizons. AI & Society, 38, 1-19.

28. Liman, T., & Weber, R. (2023). Quantum Computing: Bridging the National Security–Digital Sovereignty Divide. European Journal of Risk Regulation, 14(3), 476-483.
29. E-International Relations. (2025, September 29). The Quantum Race: How Emerging Technologies Reshape Global Security Governance.
30. Wikipedia. (2025, October 8). Quantum Experiments at Space Scale.
31. Science. (n.d.). China's quantum satellite achieves 'spooky action' at record distance.
32. Scientific American. (2024, February 20). China Reaches New Milestone in Space-Based Quantum Communications.
33. The Quantum Insider. (2025, March 14). China Establishes Quantum-Secure Communication Links With South Africa.
34. Phys.org. (2018, January 19). Real-world intercontinental quantum communications enabled by the Micius satellite.
35. Wikipedia. (2025, September 30). DARPA Quantum Network.
36. DARPA. (n.d.). A Network Security Revolution Enhanced by Quantum Communication.
37. DARPA. (n.d.). QuANET: Quantum-Augmented Network.
38. Nextgov/FCW. (2025, August 18). DARPA aims for interoperability between classic and quantum communication.
39. Executive Gov. (2025, August 8). DARPA Demos First Functioning Quantum-Augmented Network.
40. E-International Relations. (2025, September 29). The Quantum Race: How Emerging Technologies Reshape Global Security Governance.
41. European Commission. (n.d.). European Quantum Communication Infrastructure - EuroQCI.
42. Just Security. (2025, May 6). The Digital Divide Meets the Quantum Divide.
43. Just Security. (2025, May 6). The Digital Divide Meets the Quantum Divide.
44. Just Security. (2025, May 6). The Digital Divide Meets the Quantum Divide.
45. Defense Magazine. (2025, July 25). Quantum independence: State sovereignty between lasers, chips, and geopolitics.
46. Just Security. (2025, May 6). The Digital Divide Meets the Quantum Divide.
47. The Quantum Insider. (2025, May 5). 'Qubits For Peace': Researchers Warn Quantum Technology Is Deepening The Global Divide.
48. Science. (n.d.). China's quantum satellite achieves 'spooky action' at record distance.
49. ID Quantique. (2025, November 5). Quantum Key Distribution | QKD | Quantum Cryptography.
50. Wikipedia. (2025, October 8). Quantum Experiments at Space Scale.
51. Mazzucato, M. (2023). Digital sovereignty, digital infrastructures, and quantum horizons. AI & Society, 38, 1-19.
52. Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press.
53. E-International Relations. (2025, September 29). The Quantum Race: How Emerging Technologies Reshape Global Security Governance.
54. Liman, T., & Weber, R. (2023). Quantum Computing: Bridging the National Security–Digital Sovereignty Divide. European Journal of Risk Regulation, 14(3), 476-483.
55. Just Security. (2025, May 6). The Digital Divide Meets the Quantum Divide.

O'ZBEKISTON — 2030: INNOVATSIYA, FAN VA TA'LIM ISTIQBOLLARI

V RESPUBLIKA ILMIY-AMALIY KONFERENSIYASI MATERIALLARI

2025-yil, 11-avgust

Mas'ul muharrir: *F.T.Isanova*
Texnik muharrir: *N.Bahodirova*
Diszayner: *I.Abdihakimov*

O'ZBEKISTON — 2030: INNOVATSIYA, FAN VA TA'LIM ISTIQBOLLARI. V Respublika ilmiy-amaliy konferensiyasi materiallari. – Toshkent: Scienceproblems team, 2025. – 96 bet.

Elektron nashr: https://konferensiyalar.com

Konferensiya tashkilotchisi: Scienceproblems Team

Konferensiya o'tkazilgan sana: 2025-yil, 11-avgust

ISBN 978-9910-09-280-0