ARTICLES

Prospects for Legal Regulation of Quantum Communication

Alexey Minbaleev,

**Kutafin Moscow State Law University (MSAL),
Institute of State and Law of the Russian Academy of Sciences
(Moscow, Russian Federation)**

Sergey Zenin,

University of Tyumen (Tyumen, Russian Federation)

Kirill Evsikov,

**Kutafin Moscow State Law University (MSAL),
Tula State University (Tula, Russian Federation)**

https://doi.org/10.21684/2412-2343-2024-11-2-11-54

Abstract. The leading countries across the world have entered the race to develop quantum technologies that will enable them to ensure their continued economic prosperity. Among these technologies, a special place is occupied by quantum communication, which is designed to ensure information security in an era where a quantum computer is capable of compromising a number of cryptography algorithms. In this article, this new digital technology includes quantum key distribution and encryption methods that are cryptographically resistant to a quantum computer. The study does not consider the regulation of the quantum communication sub-technology, the so-called "quantum internet," due to the technical limitations of the existing equipment. The authors note that their predictions about the cryptographic strength of encryption algorithms are based solely on modern knowledge about the capabilities of quantum computing and do not take into account its hidden potential, for example, in terms of cryptanalysis information systems based on a machine learning model generated by a quantum computer. Currently, the only data protection system that is not subject to quantum threats is the technology of quantum key distribution. In today's information and digital age,

information security systems are an important element of critical infrastructure. Given the importance of these technologies, different states use different methods to regulate this field. This article puts forward and substantiates the hypothesis that the implementation of a combination of regulatory legal acts could have a greater positive impact on the development of quantum communication and ensure an acceptable level of information security in the post-quantum era. The analysis showed that a significant number of states and interstate associations are conducting research in this area, relying only on investment growth. This strategy has prevented any country from achieving the competencies of the People's Republic of China. The authors also analyzed the methods of legal support used by China, Russia, and other countries in the field of quantum communication, which made it possible to identify a model of legal regulation of quantum communication that stimulates this technology's development.

Keywords: quantum computer; quantum threat; quantum communication; quantum cryptography; quantum key distribution; quantum random number generator; information security.

Recommended citation: Alexey Minbaleev et al., *Prospects for Legal Regulation of Quantum Communication*, 11(2) BRICS Law Journal 11–54 (2024).

Table of Contents

Introduction
1. Quantum Menace
2. BRICS Countries' Experience in Regulating Quantum Communications
2.1. China: Leader in Quantum Communications
2.2. Russia: Development of Quantum Technologies
2.3. Legal Regulation of Quantum Communications in Various Jurisdictions
2.3.1. Australia
2.3.2. United Kingdom
2.3.3. Denmark
2.3.4. United States
2.3.5. Europe
2.3.6. Japan
2.4. Conclusions Based on the Analysis of National Regulatory Experience
3. Features of Quantum Communication Technology Affecting its Legal Regulation
4. Concept of Legal Regulation of Quantum Communication
Conclusion

Introduction

The world is on the verge of an information revolution, the catalyst of which is digital technologies that are radically changing the methods of working with information. These technologies include big data analysis; virtual and augmented reality technologies; neurotechnology and artificial intelligence; distributed registry technologies; robotics and sensors; and quantum technologies.

The list of the most important digital technologies differs in different countries, but in the majority of countries, official documents in general include the term "quantum technologies." This term is commonly used to describe equipment that is capable of controlling complex quantum systems down to the level of individual particles, such as atoms and photons. Technologies for controlling individual quantum objects are used to solve problems in various fields, and accordingly, there are many varieties of them, which can be called subtechnologies. In Russia, the quantum subtechnologies receiving government support include quantum sensors, quantum communication, and quantum computers.[1] South Africa is highlighting similar sub-technologies.[2] While the importance of quantum sensors and quantum computing cannot be underestimated, the development of quantum communication has also emerged as a matter of national security. This point of view is reflected in Russian documents,[3] as well as those of the European Union,[4] the United States,[5] Japan,[6] and so on. Consequently, the security services of many countries have recognized this area as a subject of their competence. For example, in India, research in quantum communication is carried out by the Defense Research

---

1 Дорожная карта развития «сквозной» цифровой технологии «Квантовые технологии» (2019) // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации [Roadmap for the Development of End-to-End Digital Technology "Quantum Technologies" (2019), Ministry of Digital Development, Communications and Mass Communications of the Russian Federation] (May 20, 2022), available at https://digital.gov.ru/ru/documents/6650/.

2 Andrew Forbes et al., *Toward a Quantum Future for South Africa*, 3 AVS Quantum Sci. (Article 040501) (2021).

3 Постановление Президиума РАН от 18 мая 2021 г. № 79 «О состоянии и перспективах развития квантовых технологий в Российской Федерации» // СПС «КонсультантПлюс» [Resolution of the Presidium of the Russian Academy of Sciences No. 79 of 18 May 2021. On the State and Prospects for the Development of Quantum Technologies in the Russian Federation, SPS "ConsultantPlus"] (May 20, 2022), available at http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=776295#JRk455Tcn38fsb7f2.

4 European Commission, *2030 Digital Compass: The European Way for the Digital Decade* (2021) (May 20, 2022), available at https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118.

5 Information Security and Privacy Advisory Board, Meeting Minutes, 29, 30 and 31 March 2017, NIST Computer Security Resource Center (May 20, 2022), available at https://csrc.nist.gov/CSRC/media/Events/ISPAB-March-2017-Meeting/documents/ispab-meeting-minutes-march-2017.pdf.

6 SQAT® セキュリティレポート / 2019年9月号 (May 20, 2022), available at https://www.bbsec.co.jp/report/security_report.html.

and Development Organization, and research that is supported by the United States government confirms the importance of quantum key distribution technology within NATO.[7]

Considering the fact that quantum communications is still in its initial stages of development, the majority of countries have refrained from enacting laws to regulate legal relations in this area. The exception is China, which has become a leader in technology development and regulation. Our analysis shows that the experience of this industry leader can be used by other countries, and in some cases, it can also be improved. The purpose of this article is to model an effective legal mechanism that ensures the continued development of quantum communications. The research methodology used in this analysis consists of the following approaches:

• dialectical method of cognition, including analysis of opposing methods of legal regulation of information security in the conditions of the second quantum revolution;

• comparative legal method, including analysis of the current legislation of foreign countries;

• method of analogy of law and analogy of statute, including analysis of the possibility of applying legislation regulating similar social relations to legal relations in the field of quantum communication.

This topic under discussion is relevant, but there are practically no open publications on it. A few authors provide an analysis of the issues associated with the legal regulation of quantum communications.[8] However, without denying their importance and relevance, it should be noted that these publications lack a detailed elaboration of models of legal regulation. This appears to be due to the position of regulators in some countries, who recommend refraining from switching to new types of information security until they thoroughly explore several options for protecting against the quantum threat. To understand the reason for such caution, let us first consider what a quantum threat is within the framework of humanities without delving into the technical sphere, as well as encryption and cryptanalysis algorithms.

1. Quantum Menace

The "first quantum revolution" led to the advent of lasers, transistors, nuclear weapons, and the Internet, and its achievements are used in computers, mobile phones, communication systems, MRI scanners, etc. Today, there is reason to talk about a "second quantum revolution," which could have an even greater

---

7 Rupert A. Brandmeier et al., *Future Development of Quantum Computing and its Relevance to NATO*, 20(2) Connections: The Q.J. 89 (2021).

8 Simson L. Garfinkel & Chris J. Hoofnagle, *Quantum Communications*, in Law and Policy for the Quantum Age 257 (2022).

impact on the world. Its key difference from the "first quantum revolution," in which technologies and devices were built on the control of collective quantum phenomena, is a quantum device's ability to control complex quantum systems at the level of individual particles, such as atoms and photons.

In the European Union (EU), research in the field of quantum technologies is divided into five groups: quantum communications (QComm), quantum computing (QComp), quantum simulation (QSim), quantum metrology and sensing (QMS), and basic sciences (BSci). In Russia, however, they are divided into three groups as follows:

1. Quantum computing – a new class of computing devices that uses the principles of quantum mechanics to solve problems. It is predicted that in a great number of tasks, a quantum computer will be able to provide far greater acceleration compared to existing supercomputer technologies. Examples include the areas of cybersecurity, artificial intelligence, and the creation of new materials.

2. Quantum communications – technology used in cryptographic information protection that uses individual quantum particles to transfer keys. The main advantage of quantum communications is that the security of information is guaranteed by the laws of physics.

3. Quantum sensors and metrology – which comprise a set of high-precision measuring instruments based on quantum effects. A high degree of control over the state of individual microscopic systems makes it possible to create ultra-precise quantum sensors with spatial resolution comparable to the size of single atoms, as well as develop high-precision atomic clocks.[9]

The development of all these sub-technologies is accompanied by significant investments. For example, the United States is investing $20 billion towards the development of these technologies; Europe is investing more than €3 billion in the framework of the Quantum Flagship program; and China has set the budget of its National Quantum Laboratory at $12 billion. These are just the direct large public investments, and in addition to them, countries are actively using mechanisms of grants, public procurement, as well as tax support measures. Besides government programs, technology development is also promoted by venture funds and large information technology (IT) corporations (such as Google, Microsoft, Intel, IBM, etc.). All of these investments have yielded significant results, with several research groups publicly announcing their achievements, including the achievement of quantum supremacy.

In 2019, Google published the results of the Quantum Supremacy experiment, during which the Sycamore quantum processor performed calculations in 200 seconds that would take a conventional computer 10,000 years.[10] In 2021, a Chinese group of

---

[9] Roadmap for the Development of End-to-End Digital Technology, *supra* note 1.

[10] Frank Arute et al., *Quantum Supremacy Using a Programmable Superconducting Processor*, 574 Nature 505 (2019).

scientists introduced the Zuchongzhi processor, which is two to three times more powerful than Google.[11] In addition to these companies, there are a growing number of organizations in the world that are attracting significant investments to develop quantum computers.[12] It is important to note that work in this area is being carried out not only on hardware but also on software. Quantum simulators that simulate a quantum computer on a regular computer are already available to software developers, such as those offered by Microsoft,[13] Quirk,[14] and IBM applications.[15] Furthermore, the South African Quantum Technology Initiative (SA QuTI) is based on collaboration with IBM.[16] Wits University, the operator of this initiative, has received access to a 50-qubit IBM computer, which allows it to gain quantum competencies.

Advances in the field of quantum computing have renewed the debate about the quantum threat, which has become especially important in connection with widespread digitalization. As rightly noted by Yu. Kharitonova and L. Sannikova, it is necessary to strengthen legal mechanisms to protect citizens' rights and interests during the digitization of public services, particularly citizens' rights to data protection.[17]

Without delving into the encryption and decryption techniques, we can note that a quantum computer with a certain level of computing power is capable of breaking the data protection algorithms used today. Some authors predict that a quantum computer capable of hacking Bitcoin could be created by 2027, and RSA by 2031.[18] The

---

11 Yulin Wu et al., *Strong Quantum Computational Advantage Using a Superconducting Quantum Processor*, 127(18) Phys. Rev. Lett. 180501 (2021) (May 20, 2022), also available at https://physics.aps.org/featured-article-pdf/10.1103/PhysRevLett.127.180501.

12 Barney Cotton, *Quantum Computing Start-up Multiverse Computing Closes €10m Investment Round*, Business Leader (2021) (May 20, 2022), available at https://www.businessleader.co.uk/quantum-computing-start-up-multiverse-computing-closes-e10m-investment-round/; *PsiQuantum Closes $450 Million Funding Round to Build the World's First Commercially Viable Quantum Computer*, PsiQuantum, 27 July 2021 (May 20, 2022), available at https://psiquantum.com/news/psiquantum-closes-450-million-funding-round-to-build-the-worlds-first-commercially-viable-quantum-computer; *IonQ Becomes First Publicly Traded, Pure-Play Quantum Computing Company; Closes Business Combination with dMY Technology Group III*, IonQ, 1 October 2021 (May 20, 2022), available at https://ionq.com/news/october-01-2021-ionq-listed-on-nyse.

13 Квантовые симуляторы // Microsoft Learn [Quantum Simulators, Microsoft Learn] (May 20, 2022), available at https://docs.microsoft.com/ru-ru/azure/quantum/user-guide/machines/.

14 Quirk (May 20, 2022), available at https://algassert.com/quirk.

15 Build and Deploy Quantum Programs with Qiskit Runtime, IBM Cloud (May 20, 2022), available at https://cloud.ibm.com/quantum.

16 *Wits to Coordinate South Africa's National Quantum Initiative*, Wits University, 14 September 2021 (May 20, 2022), available at https://www.wits.ac.za/news/latest-news/research-news/2021/2021-09/wits-to-coordinate-south-africas-national-quantum-initiative.html.

17 Yulia Kharitonova & Larisa Sannikova, *Digital Platforms in China and Europe: Legal Challenges*, 8(3) BRICS L.J. 121 (2021).

18 Michele Mosca, *Cybersecurity in an Era with Quantum Computers: Will We Be Ready?*, 16(5) IEEE Sec. & Priv. 38 (2018).

UK regulator (the National Cyber Security Center – NCSC) in its 2020 recommendations predicts the emergence of a cryptographically significant quantum computer by 2030.[19] There are also forecasts for other dates, but they all agree on the following two points:

• a significant number of ciphers in use today will be compromised;

• the transition to new cryptography tools must begin today, because this is a long process.

It should be noted that the majority of predictions are based on open publications. Furthermore, in the context of geopolitical competition, there is a possibility that actual successes in building a working quantum computer will be confidential information, and this information can only be revealed after a significant amount of data has been compromised. This conclusion is confirmed by official documents issued by the public authorities of some countries, which, in addition to open data, also contain confidential information. For example, in October 2021, the U.S. Department of Homeland Security published a Post-Quantum Cryptography Preparation Memorandum, in which it noted that it faced national security challenges, including the protection of critical infrastructure data.[20] The reason for this was declared insufficient preparation for the transition to post-quantum cryptography.

Most countries across the world have recognized the presence of the quantum threat and have begun research in the field of quantum-safe cryptography. These are new methods of information protection, which include:

1. Post-Quantum Cryptographic Algorithms.
2. Quantum Key Distribution.

The given list of information security methods is not exhaustive. For instance, the UK regulator (NCSC) indicates the possibility of using ciphers based on a quantum random number generator (Quantum Random Number Generation). At the same time, the regulator notes that there are many scientific studies on the safety and effectiveness of various post-quantum cryptographic schemes, but at present, it is difficult to give precise recommendations on which one should be used.[21]

The distinction between the two designated post-quantum data protection methods exists in most countries. The analysis showed that some countries have chosen one of the methods of data protection in this era, while others are in an undecided state.

---

19 Quantum-Safe Cryptography (White Paper), National Cyber Security Centre (May 20, 2022), available at https://www.ncsc.gov.uk/whitepaper/quantum-safe-cryptography.

20 Memorandum on Preparing for Post-Quantum Cryptography, Homeland Security (May 20, 2022), available at https://www.dhs.gov/publication/memorandum-preparing-post-quantum-cryptography.

21 Quantum Security Technologies (White Paper), National Cyber Security Centre (May 20, 2022), available at https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies.

A technical report issued by the Joint Research Center (JRC), the European Commission's science and knowledge service in 2019, identified thirteen countries carrying out successful applied research in the field of quantum key distribution, including China, Russia, and South Africa.[22] However, such a report is incomplete; for example, it does not contain data on India, which has achieved significant success in this area.[23]

Since different countries have achieved different successes that are not comparable to their level of costs, we consider it necessary to put forward a hypothesis about the influence of related factors on the development of quantum communication, among which law occupies an important place. Let us consider foreign experience in the legal regulation of quantum communications in order to highlight the legal instruments used by different countries in this area.

2. BRICS Countries' Experience in Regulating Quantum Communications

2.1. China: Leader in Quantum Communications

China is a leader in quantum communications. In 2016, the country launched the world's first quantum communications satellite, which made it possible to create the longest mixed-type quantum key distribution network in 2021. The Chinese quantum network uses satellite-to-Earth technology, covers thirty-two nodes across four provinces and three cities, and integrates four quantum city networks in Beijing, Jinan, Hefei, and Shanghai. It has a length of 4,600 kilometers and over 150 users currently have access to quantum key distribution as a direct result of this network. Various entities, such as financial institutions, energy companies, and government agencies, are progressively adopting quantum communication services.

The country has come a long way in attaining this outcome. The People's Republic of China (PRC) first used quantum communication and quantum entanglement distribution in free space in 2005.

In 2010, the PRC successfully achieved the world's longest quantum teleportation, spanning 16 kilometers, and confirmed the possibility of quantum teleportation through the atmosphere for the first time, laying the foundation for a global quantum communication network based on satellite relays. This experiment required the creation of a free space quantum channel. In 2012, the world's first hundred-

---

[22] Martino Travagnin & Adam M. Lewis, *Quantum Key Distribution In-Field Implementations*, Technical Report by the Joint Research Centre (JRC), the European Commission's Science and Knowledge Service, European Commission (2019), at 46 (May 20, 2022), available at https://publications.jrc.ec.europa.eu/repository/bitstream/JRC118150/quantum_communication_state-of-the-art__review_4.0_final.pdf.

[23] Sushant Kulkarni, *Explained: What Is the Quantum Tech Demo by DRDO and IIT Delhi All About?*, The Indian Express, 25 February 2022 (May 20, 2022), available at https://indianexpress.com/article/explained/explained-what-is-quantum-tech-demo-by-drdo-and-iit-delhi-all-about-7789057/.

kilometer quantum transmission in free space over a distance of over 100 kilometers was realized.

On 7 January 2021, the leading international academic journal *Nature* published a paper titled "A 4,600 km Quantum Communications Network." It is noted by the scientific community to be the largest and most advanced quantum key distribution network on the planet, and is a "tremendous engineering achievement" in the field of quantum communications. The establishment of the Chinese network not only lays the scientific and technological foundation for the realization of a global "quantum network" in the future but also provides an unprecedented "world laboratory" for scientific research such as relativity and gravitational waves.

It should be noted that the network is divided into areas with trusted nodes. The 2,032-kilometer Beijing-Shanghai trunk line has thirty-two sites along the route using a "trusted relay" scheme, meaning information security at sites is ensured by means such as manual surveillance and network isolation. This kind of "trusted relay" uses classical technology to prevent intrusion into communication sites, but compared with the theoretically proven security of quantum communication, the relay station is still an area that has a high risk of data interception.

Given its high technical achievements, China is a pioneer in the systemic legal regulation of quantum cryptography. Among the problems that the PRC has sought to solve are:

- decentralization in cryptography regulation;
- creation of a cryptography market system based on the principles of non-discrimination and fair competition;
- reduction in the number of licenses;
- simplifying access to the cryptography equipment market.

These tasks were solved by making appropriate changes to the information law of China. Today, in the field of information protection in the PRC, there are seven main regulatory legal acts of the highest legal force:

- Personal Information Protection Law of the People's Republic of China (2021);
- Data Security Law of the People's Republic of China (2021);
- Security Regulations for the Protection of Critical Information Infrastructure (2021);
- Cryptography Law of the People's Republic of China (2019);
- Cybersecurity Law of the People's Republic of China (2016);
- Anti-Terrorism Law of the People's Republic of China (2015);
- Electronic Signature Law of the People's Republic of China (2004).

All of the listed regulatory legal acts influence the legal regulation of quantum cryptography. At the same time, direct legal regulation is carried out based on the Law of the People's Republic of China on Cryptography (hereinafter the Cryptography Law), which entered into force on 1 January 2020. The head of the State Administration of Cryptography, explaining the role of this source of law, noted the following as among the main objectives of the Law:

• development of cryptography;
• standardization and management of cryptography;
• development of the cryptographic industry;
• stimulating the creation of quality market products.[24]

The Cryptography Law consists of five chapters and forty-four articles. Chapter 1 "General Provisions" defines the legislative purpose of this law, the basic principles of cryptographic work, governance and management systems, and measures to promote and protect cryptographic development. Chapter 2 defines basic passwords and general passwords, specifies requirements for the use of these passwords and describes information security management systems. Chapter 3 is devoted to commercial cryptography and regulates the commercial cryptographic standardization system, the testing and certification system, the market access management system, the import and export management system, the electronic certification service management system, the commercial cryptography monitoring system, as well as a number of other issues. Chapter 4 provides the appropriate legal consequences for violating this law. Chapter 5 defines the rulemaking powers of the National Cryptographic Authority as well as the specifics of the entry into force of this law.[25]

A significant achievement of the Cryptography Law was the country's transition from strict regulation of relations in the field of cryptography to the liberalization of certain segments of the market, referred to as "commercial cryptography" in the legislation. Regulations on commercial encryption management in the PRC today focus on the sale of cryptographic products, the provision of encryption services, and the import and export of related technologies.

When it comes to regulating commercial cryptography, the Chinese regulator has switched from using administrative tools to market economic tools (such as standardization, testing, and certification). However, licensing and strict controls have not changed in terms of regulating cryptography issues related to national security and public safety. According to the Chinese regulator, these areas of public life are difficult to effectively control solely by using market mechanisms.

In continuation of these legislative initiatives, in the summer of 2021, the Ministry of Industry and Information Technology of the People's Republic of China approved three main standards for the equipment used in the quantum key distribution process:

• YD/T 3907.3-2021 Key Components and Modules for Quantum Key Distribution (QKD) Based on BB84 protocol, Part 3: Quantum Random Number Generator (QRNG);

---

[24] 维护国家密码安全 促进密码事业发展丨国家密码管理局负责人就《中华人民共和国密码法》答记者问 [Maintain National Cryptography Security and Promote the Development of the Cryptography Industry, *The Person in Charge of the State Cryptography Administration Answers Reporters' Questions on the Cryptozoology Law of the People's Republic of China*] (May 20, 2022), available at https://www.163.com/dy/article/G7PL4J0G0522LGCU.html.

[25] 中华人民共和国密码法 [Cryptozoology Law of the People's Republic of China] (May 20, 2022), available at http://www.oscca.gov.cn/sca/xxgk/2019-10/27/content_1057225.shtml.

• YD/T 3834.1-2021 Quantum Key Distribution System Specifications, Part 1: QKD System Based on BB84 Decoy State Protocol;

• YD/T 3835.1-2021 Quantum Key Distribution System Test Method, Part 1: QKD System Based on BB84 Decoy State Protocol.

These standards are among the best in the world, which is ensured not only by the date of their adoption but also by the fact that Chinese regulators have harmonized them with numerous international standard such as ICS 33.180 and ICS 33.180.01.

In addition to equipment standards, the Chinese regulator also approved cryptography standards in 2021. On 19 October 2021, the National Cryptography Authority published 16 cryptographic industry standards that became effective 1 May 2022:

• GM/T 0005-2021 – Randomness Testing Specifications;

• GM/T 0013-2021 – Trusted Computing Module Interface Compliance Test Specification;

• GM/T 0103-2021 – General Structure of a Random Number Generator;

• GM/T 0104-2021 – Technical Specification of Cloud Server Cryptographic Machine;

• GM/T 0105-2021 – Design Guide for Random Number Generation Software;

• GM /T0106-2021 – Requirements for Applications of Cryptographic Products Bank Card Terminal;

• GM/T 0107-2021 – Smart Card Key Management System Basic Technical Requirements;

• GM/T 0108-2021 – False State QKD BB84 Product Specifications;

• GM/T 0109-2021 – Cloud Based Electronic Signature Service Technical Requirements;

• GM/T 0110-2021 – Key Management Interoperability Protocol Specification;

• GM/T 0111-2021 – Technical Requirements for a Blockchain Cryptographic Application;

• GM/T 0112-2021 – PDF Document Technical Requirements for a Cryptographic Application;

• GM/T 0113-2021 – Fast Online Authentication Protocol;

• GM/T 0114-2021 – Bait Status BB84 Product Testing Specification of Quantum Key Distribution;

• GM/T 0115-2021 – Information System Requirements for Assessing Cryptographic Applications;

• GM/T 0116-202 – Information System Password Application Assessment Process Guide.[26]

As can be seen from the list, two of the 16 standards are entirely devoted to quantum key distribution: GM/T 0108-2021 and GM/T 0114-2021.

---

[26] 国家密码管理局公告（第43号 [Announcement of the State Cryptozoology Administration (No. 43)] (May 20, 2022), available at http://www.oscca.gov.cn/sca/xxgk/2021-10/19/content_1060880.shtml.

In addition to standardization, the State Cryptography Administration of the People's Republic of China implements educational and popularization projects, which involve the following:

• introduction of the basics of cryptography into the national education system;

• training civil servants in the basics of cryptography;

• popularization of cryptography in society through increasing awareness among citizens and legal entities about cryptographic security.

Thus, the above analysis allows us to identify several regulatory components of the Chinese "quantum miracle":

1. A regulatory framework for attracting scientific personnel from abroad and supporting research in this area

The state's attention to this area of knowledge stimulates research activities in this area. A significant number of theses in the field of quantum key distribution today are carried out by Chinese researchers, who specialize in this area of study both in their own country[27] and abroad.[28]

2. Government investment in infrastructure

The construction of backbone networks in China is carried out by the state, not the private sector. For instance, China is the only country that spent resources on the launch of the Mozi (Micous) satellite in 2016. The equipment of this space object made it possible in 2017 to ensure the quantum distribution of keys between Beijing and Vienna. In addition, China has consistently invested heavily in the creation of separate quantum communication lines, which were subsequently combined into a single quantum communication system.

3. Creation of a commercial cryptography market

Chinese cryptography was initially a highly regulated area of public life, which prevented sufficient competition from developing, as well as companies creating cryptographic equipment and providing services in this area. Nevertheless, even under such conditions, in 2018, the total sales of commercial cryptographic products reached 30 billion yuan. However, as noted by National Shield Quantum, which specializes in the field of quantum cryptography, when a consumer wants to use quantum-safe communications, he or she often faces problems with network availability and equipment compliance with national standards. In 2021, the issue with standards was resolved.

As of 2021, about 3,000 patent applications have been filed by leading countries (with China having filed 2,139 applications, the United States having filed 663, South

---

[27] 新型量子密钥分配协议的实际安全性分析及计算 [Practical Security Analysis and Calculation of a New Quantum Key Distribution Protocol] (May 20, 2022), available at http://www.ckcest.cn/default/es3/detail/1003/dw_thesis_copy/0655321f8e009a672fe55f6e67e5080f.

[28] Han Qin, *QKD and High-Speed Classical Data Hybrid Metropolitan Network*, Thesis, University of Cambridge Repository (2020) (May 20, 2022), available at https://doi.org/10.17863/CAM.62160.

Korea having filed 189, and Japan having filed 97 applications).[29] Effective government policy and law has allowed the PRC to gain four of the ten best global institutions, ahead of the United States, which ranks second and has only one institution in the international top ten. It is important to note that the competition between these countries shows that the size of investment does not always play a decisive role in digital leadership. The United States, United Kingdom, and Canada lead the way in venture capital (VC) investment and have cross-collaboration and data-sharing agreements. However, it is China that has the largest number of patents in the field of quantum communications and one of the best quantum computers in the world today.

According to research that was supported by the Institute of Information and Communications Technology Planning and Evaluation (IITP), (a South Korean government institution that manages research under the Ministry of Science and ICT (MSIT)), quantum key distribution networks (QKDNs) have also been identified as a means to allow for the effective use of data protection technology in 5G networks.[30]

2.2. Russia: Development of Quantum Technologies

In 2019, the Russian Federation approved the National Program for the Development of the Digital Economy.[31] One of the goals of the program is the creation of "end-to-end" digital technologies primarily based on domestic developments.[32] These included federal projects aimed at creating sustainable infrastructure for technologies such as distributed ledgers, artificial intelligence, quantum computing, quantum communications, etc.[33]

---

[29] Quantum communications (incl. quantum key distribution), Department of the Prime Minister and Cabinet (May 20, 2022), available at https://www.pmc.gov.au/resource-centre/domestic-policy/quantum-communications-incl-quantum-key-distribution.

[30] Taesang Choi et al., *Quantum Key Distribution Networks for Trusted 5G and Beyond: An ITU-T Standardization Perspective*, in International Telecommunication Union Kaleidoscope Academic Conference: Connecting Physical and Virtual Worlds, ITU K (2021).

[31] Паспорт национального проекта «Национальная программа «Цифровая экономика Российской Федерации»» (утвержден Президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 4 июня 2019 г. № 7) // СПС «КонсультантПлюс» [Passport of the National Program "Digital Economy of the Russian Federation," approved by the Presidium of the Council under the President of the Russian Federation for Strategic Development and National Projects, Protocol No. 7 of 6 June 2019, SPS "ConsultantPlus"] (May 20, 2022), available at http://www.consultant.ru/document/cons_doc_LAW_328854/.

[32] Паспорт федерального проекта «Цифровые технологии» (утвержден Президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности, протокол от 28 мая 2019 г. № 9) // СПС «КонсультантПлюс» [Passport of the Federal Project "Digital Technologies," approved by the Presidium of the Government Commission on Digital Development, the Use of Information Technologies to Improve the Quality of Life and Business Conditions, Protocol No. 9 of 28 May 2019, SPS "ConsultantPlus"] (May 20, 2022), available at http://www.consultant.ru/document/cons_doc_LAW_328937/.

[33] Постановление Правительства РФ от 29 марта 2019 г. № 377 «Об утверждении государственной программы Российской Федерации «Научно-технологическое развитие Российской Федерации»» // СПС «КонсультантПлюс» [Decree of the Government of the Russian Federation No. 377

Clause "m" of Article 71 of the Constitution of the Russian Federation stipulates that the federal authorities be in charge of ensuring the security of the individual, society, and the state in terms of the use of information technologies and the circulation of digital data.[34] For these purposes, the country has regulated the field of cryptography using methods of ensuring confidentiality (for example, preventing unauthorized access to information) and authenticity (for instance, the integrity and authenticity of authorship, as well as the impossibility of refusing authorship) of information.[35] In Russia, the regulatory framework regulating this area consists mainly of acts of executive authorities, for example, the procedure that is followed for approving means of cryptographic information security[36] and state encryption standards.[37] Public authorities now recognize that a number of ciphers may be unstable to a quantum computer, which means that the rules of law require changes. The importance of this issue is also noted in the federal project "Information Security."[38]

of 29 March 2019. On Approval of the State Program of the Russian Federation Scientific and Technological Development of the Russian Federation, SPS "ConsultantPlus"] (May 20, 2022), available at http://www.consultant.ru/document/cons_doc_LAW_322380/.

34 Конституция Российской Федерации // СПС «КонсультантПлюс» [Constitution of the Russian Federation, SPS "ConsultantPlus"] (May 20, 2022), available at http://www.consultant.ru/document/cons_doc_LAW_28399/.

35 ГОСТ Р 56875-2016. Национальный стандарт Российской Федерации. Информационные технологии системы безопасности комплексные и интегрированные. Типовые требования к архитектуре и технологиям интеллектуальных систем мониторинга для обеспечения безопасности предприятий и территорий (утвержден Приказом Росстандарта от 26 февраля 2016 г. № 81-ст) [GOST R 56875-2016. National Standard of the Russian Federation, Information Technology Security Systems Are Complex and Integrated, Standard Requirements for the Architecture and Technologies of Intelligent Monitoring Systems to Ensure the Safety of Enterprises and Territories, approved by Order of Rosstandart No. 81-st of 26 February 2016] (May 20, 2022), available at https://docs.cntd.ru/document/1200132478.

36 Приказ ФСБ Российской Федерации от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» // СПС «КонсультантПлюс» [Order of the FSB of the Russian Federation No. 66 of 2 September 2005. On Approval of the Regulations on the Development, Production, Sale and Operation of Encryption (Cryptographic) Information Security Means (Regulations PKZ-2005), SPS "ConsultantPlus"] (May 20, 2022), available at http://www.consultant.ru/document/cons_doc_LAW_52098/a0ddd10a21467c2c862799a191e13882eac2814f/.

37 ГОСТ Р 34.12-2015 Информационная технология. Криптографическая защита информации. Блочные шифры [GOST R 34.12-2015, Information Technology, Cryptographic Information Protection, and Block Ciphers] (May 20, 2022), available at https://docs.cntd.ru/document/1200121983.

38 План мероприятий по направлению «Информационная безопасность» программы «Цифровая экономика Российской Федерации» (утвержден Правительственной комиссией по использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности, протокол от 18 декабря 2017 г. № 2) // СПС «КонсультантПлюс» [The Action Plan in the Information Security Direction of the "Digital Economy of the Russian Federation" Program, approved by the Government Commission on the Use of Information Technologies to Improve the Quality of Life and Business Conditions, Protocol No. 2 of 18 December 2017, SPS "ConsultantPlus"] (May 20, 2022), available at http://www.consultant.ru/document/cons_doc_LAW_287996/.

These changes began with acts of a strategic nature. "The Roadmap for the Development of Quantum Technologies"[39] for instance, stipulates that the protection of distributed registries, blockchains, and critical production segments should be carried out using quantum cryptography and post-quantum algorithms. This means that the state is considering the feasibility of combined information protection in the post-quantum era. When speaking about terminology, it is important to note that in Russia, quantum communication is equated to quantum key distribution,[40] and a quantum-resistant encryption algorithm is called a post-quantum algorithm.

In Russia, there are no regulations containing recommendations on the choice of a specific encryption method by commercial companies. However, there are recommendations on assessing the risks of a quantum threat based on three parameters: the data storage period, the migration time to systems designed to protect against quantum attacks, and time remaining until quantum computers break security. At the same time, legal entities are actively involved in testing new technologies to protect their data. In 2016, a quantum communication line was put into operation in Russia, connecting two buildings of Gazprombank in Moscow, and in 2017, the world's first experimental demonstration of quantum blockchain technology was carried out.[41]

The Russian Federation has officially approved a development strategy for quantum technology in the form of a "Passport for the Road Map for the Development of High-Tech Field 'Quantum Communications' for the period until 2024."[42] This document defines the deadlines and targets that the project operators must achieve (Table 1), along with the persons responsible for their completion (Table 2).

---

39 Roadmap for the Development of End-to-End Digital Technology, *supra* note 1.

40 Указ Президента Российской Федерации от 17 декабря 2011 г. № 1661 «Об утверждении Списка товаров и технологий двойного назначения, которые могут быть использованы при создании вооружений и военной техники и в отношении которых осуществляется экспортный контроль» // СПС «КонсультантПлюс» [Decree of the President of the Russian Federation No. 1661 of 17 December 2011. On Approval of the List of Dual-Use Goods and Technologies That Can Be Used in the Creation of Weapons and Military Equipment and in Respect of Which Export Control Is Carried Out, SPS "ConsultantPlus"] (May 20, 2022), available at http://www.consultant.ru/document/cons_doc_LAW_124023/.

41 Информационная безопасность в эпоху квантовых технологий // Технологии Доверия [Information Security in the Era of Quantum Technologies, Technologies of Trust] (May 20, 2022), available at https://www.pwc.ru/ru/assets/pdf/quantim-cybersecurity-publication-rus.pdf.

42 Паспорт «дорожной карты» развития высокотехнологичной области «квантовые коммуникации» на период до 2024 года (утвержден Минцифры России 27 августа 2020 г. № 17) // СПС «КонсультантПлюс» [Passport of the Road Map for the Development of the High-Tech Field "Quantum Communications" for the Period Until 2024, approved by the Ministry of Digital Development of Russia on 27 August 2020 No. 17, SPS "ConsultantPlus"] (May 20, 2022), available at http://www.consultant.ru/document/cons_doc_LAW_384672/.

Table 1: **Target indicators for the development of quantum communications for 2021–2024**

Indicators	**2021**	**2024**
Total length of networks, km	1000	10000
Supported number of ports in point-to-multipoint networks	64	128
Maximum range outside the laboratory, km	200	250
Secret key generation speed, kbit/s at 25 km	100	5000
Equipment certification	+	+

Table 2: **Activities for the development of quantum communications for 2021–2024**

Necessary measures (actions) to solve a technological problem	**Expected result with characteristics**	**Implementation period**	**Suggested support tool**
Multiplexing Quantum and Classical Communications	The joint operation of the quantum channel with the classical one is ensured	2019–2021	Support of activity programs, Grant support for small businesses
Implementation of satellite quantum cryptography	Successful implementation of QKD in the "Earth-to-Satellite" mode	2019–2023	Grant support for small businesses Support for the development and implementation of industrial solutions
Realizing the export potential of solutions for QRK	Appearance in the Russian Federation of products for QKD with characteristics competitive for the global market	2020–2024	Support by subsidizing the interest rate on the loan Support for leading companies

One of the objectives mentioned in the strategic documents is the creation of an export product that is capable of competing in the international market. However, the Passport states that the export potential of quantum cryptography equipment may be limited under certain circumstances in which government interests may prevail over commercial ones. According to Appendix No. 1 to the Roadmap, the priority areas for the development of quantum communication include the following subtechnologies: quantum point-to-point key distribution; quantum networks based on trusted nodes; quantum networks based on untrusted nodes; quantum distribution of keys in open space for satellite solutions and unmanned vehicles; and post-quantum cryptography.

The moderator of the project is JSC Russian Railways, which has already achieved a few successes in this area, most notably, the launch of the first 700-kilometer quantum communication line between Moscow and St. Petersburg.[43] The country is also in the process of adopting regulations on the creation of specialized research centers, for example, the "Quantum Valley" technological hub in the Nizhny Novgorod region.[44]

So far, a clear legal framework for the regulation of quantum communication has not been formed in the country, which significantly complicates the implementation of technologies because in Russia, the circulation of cryptographic systems is a licensed activity.[45] However, the country has already created a legal mechanism for overcoming this legal impasse. Quantum communication is included in the list of technologies for which an experimental legal regime in the field of digital innovation can be established.[46] It is important to note that a special legal regime will

---

[43] Дмитрий Чернышенко запустил первую линию квантовой связи между Москвой и Санкт-Петербургом // Правительство России. 8 июня 2021 г. [*Dmitry Chernyshenko launched the first quantum communication line between Moscow and St. Petersburg*, Russian Government, 8 June 2021] (May 20, 2022), available at http://government.ru/news/42449/.

[44] Постановление Правительства Российской Федерации от 30 ноября 2021 г. № 2133 «О создании инновационного научно-технологического центра «Квантовая» долина» (вместе с «Правилами проекта по созданию и обеспечению функционирования инновационного научно-технологического центра «Квантовая долина»») // СПС «КонсультантПлюс» [Decree of the Government of the Russian Federation No. 2133 of 30 November 2021. On the Creation of the Innovative Scientific and Technological Center "Quantum Valley" (together with the "Rules of the Project for the Creation and Operation of the Innovative Scientific and Technological Center 'Quantum Valley'"), SPS "ConsultantPlus"] (May 20, 2022), available at http://www.consultant.ru/document/cons_doc_LAW_402228/.

[45] Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности» // СПС «КонсультантПлюс» [Federal Law No. 99-FZ of 5 April 2011. On Licensing of Certain Types of Activities, SPS "ConsultantPlus"], cl. 1, pt. 1, Art. 12 (May 20, 2022), available at http://www.consultant.ru/document/cons_doc_LAW_113658/.

[46] Постановление Правительства Российской Федерации от 28 октября 2020 г. № 1750 «Об утверждении перечня технологий, применяемых в рамках экспериментальных правовых режимов в сфере цифровых инноваций» // СПС «КонсультантПлюс» [Decree of the Government of the Russian Federation No. 1750 of 28 October 2020. On Approval of the List of Technologies Used within the Framework of Experimental Legal Regimes in the Field of Digital Innovation, SPS "ConsultantPlus"] (May 20, 2022), available at http://www.consultant.ru/document/cons_doc_LAW_366246/.

not replace full-fledged legal regulation because it is only limited to a specific period of time and mainly serves to develop, test, and implement a digital innovation.[47] However, it can serve as a connecting element for the harmonization of numerous requirements of regulatory legal acts in the field of communications and information and telecommunication technologies.

2.3. Legal Regulation of Quantum Communications in Various Jurisdictions

2.3.1. Australia

In 2020, CSIRO (Commonwealth Scientific and Industrial Research Organisation), Australia's national scientific research agency, published a roadmap for the country's quantum technology industry and made the following recommendations to the government:

1. Develop a national strategy for quantum technologies.
2. Explore effective and efficient financing mechanisms.
3. Attract, train, and retain the best talent.
4. Assess industry opportunities and infrastructure facilities.
5. Create multidisciplinary and multi-institutional projects.
6. Promote Australia's domestic capabilities in quantum technologies.
7. Provide clarity regarding the implementation of trade control provisions.
8. Encourage the active participation of local end users and the government in the Australian quantum ecosystem.[48]

The implementation of such recommendations led to the adoption of the following initiatives by Australian public authorities: the Quantum Technology Roadmap, the Australian Cyber Security Growth Network, the ARC Center of Excellence for Quantum Computation and Communication Technology, the Next Generation Technologies Fund, Silicon Quantum Computing, the Digital Economy and Technology Policy, and the Defense and Strategic Goods List 2021.

In November 2021, Australia and the United States published a joint statement on cooperation in the field of quantum science and technology,[49] which will take place within the framework of an agreement between the Government of the United States and the Government of Australia on cooperation in science and

---

[47] Федеральный закон от 31 июля 2020 г. № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» // СПС «КонсультантПлюс» [Federal Law No. 258-FZ of 31 July 2020. On Experimental Legal Regimes in the Field of Digital Innovation in the Russian Federation, SPS "ConsultantPlus"] (May 20, 2022), available at http://www.consultant.ru/document/cons_doc_LAW_358738/.

[48] Growing Australia's Quantum Technology Industry, CSIRO (May 20, 2022), available at https://www.csiro.au/en/work-with-us/services/consultancy-strategic-advice-services/CSIRO-futures/Future-Industries/Quantum.

[49] Joint Statement of the United States of America and Australia, U.S. Department of State, 17 November 2021 (May 20, 2022), available at https://www.state.gov/cooperation-in-quantum-science-and-technology-aus.

technology. The terms of the S&T Agreement and other related agreements govern this cooperation, including with regard to issues relating to financial arrangements, confidentiality, and the protection and allocation of intellectual property created, or furnished in the course of cooperative activities. The document calls for the establishment of standards for collaborative quantum technologies aimed at promoting interoperability, innovation, transparency, market diversity, and security in order to facilitate legal cooperation.

The United States attention to Australia is predictable due to the latter's success in the development of this area, and the number of startups by this country in the field of quantum technologies, particularly quantum communications, is growing. The advancement of this subtechnology in Australia includes devices and systems that transmit quantum information over a distance, including cryptographic keys.[50] Furthermore, it also includes applications for quantum communications, which allow the transfer of information between quantum computers and the exchange of cryptographic keys between individuals without the possibility of interception. The Australian defense, intelligence, communications, and banking and finance industries are just a few of the consumers of this sub-technology. In addition, Australian government has identified two use models as priority projects for the development of quantum communications, as follows:

- transfer of quantum information between remote sites;
- secure cryptographic key exchange between strangers.

The development of quantum communications is recognized by Australia as an important component for creating secure communications systems and maintaining national security. However, it should be noted that there are unresolved problems in this area. For example, Australian experts point to the possibility of interrupting satellite distribution of quantum keys because of the use of ground-based lasers, which could prevent the technology from being used in the defense sector.[51] Therefore, the government does not rule out the possibility that limited use cases may make quantum key distribution unsuitable for global purposes, and it eventually will be replaced by post-quantum cryptography.

2.3.2. United Kingdom

The United Kingdom became one of the first European countries to formulate a plan for the development of quantum technologies. The UK National Quantum Technology Program is valued at £315 million.[52] The country plans to create a quantum

---

50 Quantum communications, *supra* note 29.

51 David R. Gozzard et al., *Vulnerability of Satellite Quantum Key Distribution to Disruption from Ground-Based Lasers*, 21(23):7904 Sensors (Basel) (2021).

52 Budget 2018 Announcement on Quantum Technologies, Networked Quantum Information Technologies Hub, 30 October 2018 (May 20, 2022), available at https://nqit.ox.ac.uk/news/budget-2018-announcement-quantum-technologies.html.

computer by 2024.[53] Furthermore, an agreement similar to the one established with Australia has also been concluded between the United States and Great Britain.[54]

Central to the legal regulation of the quantum communications industry in the United Kingdom is investment legislation, in particular the National Security and Investment Act 2021 (NSIA).[55] It provides for mandatory notification and pre-approval for the acquisition of innovative technologies in seventeen sectors, including quantum. The following terminology used in the law deserves attention:

- quantum communication;
- quantum coupling;
- quantum imaging, sensing, timing, or navigation;
- quantum information processing, computation, or simulation;
- quantum-resistant cryptography.

The law understands "quantum communication" as:

- the transfer of information using the properties of quantum mechanics, in particular superposition, entanglement, single photon technology, the use of conjugate variable technologies, or a combination of these;
- using a communications network (quantum or otherwise) to propagate quantum states or information about a quantum state; or
- creating cryptographic keys or generating provably random numbers using a quantum physical process.

The term "quantum-resistant cryptography" in the context of law refers to methods of protecting information or data transmitted or stored in order to counteract an attack by a quantum computing or simulation device. Legal regulation of quantum communication in the United Kingdom, outside of financing issues, is reduced to advisory documents, for example, the white paper Quantum-Safe Cryptography, published in 2020.[56] This document suggests that citizens defer their decisions on which encryption algorithm should be used in the post-quantum era until the U.S. regulator provides further guidance.

---

53 Сколько денег страны мира тратят на квантовые технологии // РБК Тренды. 6 апреля 2021 г. [*How Much Money Do Countries Around the World Spend on Quantum Technologies?*, RBC Trends, 6 April 2021] (May 20, 2022), available at https://trends.rbc.ru/trends/industry/606ad5239a79474c50841023.

54 Joint Statement of the United States of America and the United Kingdom of Great Britain and Northern Ireland on Cooperation in Quantum Information Sciences and Technologies, U.S. Department of State (May 20, 2022), available at https://www.state.gov/cooperation-in-quantum-information-sciences-and-technologies-uk.

55 The National Security and Investment Act 2021 (Notifiable Acquisition) (Specification of Qualifying Entities) Regulations 2021 (May 20, 2022), available at https://www.legislation.gov.uk/uksi/2021/1264/contents/made?text=%22quantum%20technologies%22#match-1.

56 Preparing for Quantum-Safe Cryptography, National Cyber Security Centre (May 20, 2022), available at https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography.

2.3.3. Denmark

Control over investments in the quantum sector is becoming a trend. In Denmark, Act No. 842 of 10 May 2021, "On the Screening of Certain Types of Foreign Direct Investment (Investment Screening Act)" and the Danish Government Regulation No. 1491 of 25 June 2021 notification, "On Determining the Scope of the Law on the Screening of Certain Types of Foreign Direct Investment in Denmark,"[57] establish regulatory control over investments made in a number of technologies, including quantum communications. For instance, a foreign investor may request that the authorities evaluate whether a proposed foreign direct investment or a particular economic agreement relates to critical technology or critical infrastructure. Additionally, a Danish company that is the subject of a proposed foreign direct investment or a specific economic agreement may also request a similar assessment on behalf of the foreign investor.

2.3.4. United States

The National Quantum Initiative Act has been adopted in the United States.[58] This U.S. law introduces the new concept of "quantum information science" which refers to the use of the laws of quantum physics to store, transmit, process, calculate, or measure information. The document is programmatic in nature and is aimed at creating favorable conditions for the introduction of quantum technologies. Among the entities involved in the implementation of this law are the National Quantum Coordination Office, the Centers for Quantum Research and Education and the National Research Centers for Quantum Information Science, the Subcommittee on Quantum Information Science of the National Council on Science and Technology (SCQIC), the National Quantum Initiative Advisory Committee (NQIAC), and the National Institute of Standards and Technology (NIST).

In terms of legal regulation, the National Institute of Standards and Technology plays a significant role, by creating standards in this area, such as the following:

1. Standards in the field of quantum communications (Quantum Transport Measurements), specifically developing a core knowledge and measurement infrastructure that will facilitate the use of solid-state systems with emergent quantum properties in future electronic and quantum information science applications.

2. The Standards Quantum Communications and Networks. The project that aims to create quantum devices for use in quantum communications and networking applications.

---

[57] BEK nr 1491 af 25/06/2021 (May 20, 2022), available at https://www.retsinformation.dk/eli/lta/2021/1491.

[58] H.R.6227 – An Act to Provide for a Coordinated Federal Program to Accelerate Quantum Research and Development for the Economic and National Security of the United States (2018) (May 20, 2022), available at https://www.congress.gov/bill/115th-congress/house-bill/6227.

The NIST is today the world's leading center for the analysis of post-quantum cryptography algorithms, spurred by an open call launched in 2018 that invited groups of researchers to propose ciphers that a quantum computer could not crack. At the first stage, fifty ciphers were presented by various scientific organizations (such as Korea University, the Chinese Academy of Sciences, Sorbonne University, and the University of Waterloo, among others) and technology companies (including IBM Research, Microsoft, Philips Research, Intel, and others).[59] After a public discussion, algorithms were selected that advanced to the second stage and then to the final third round of the competition, after which the American regulator plans to certify a quantum-resistant encryption algorithm.[60] Furthermore, plans are also underway for new cryptography standards to be published before 2024.[61] However, currently, the regulator recommends taking into account "cryptographic flexibility," which ensures that encryption can be easily updated or replaced.

While U.S. authorities are still analyzing information security algorithms, American companies are already introducing them into their activities. Thus, IBM in 2022 provided users of cloud services with a "hybrid information security algorithm" that uses a combination of a quantum secure algorithm and classical key exchange algorithms.[62] This example concerns a single service, but the mass implementation of post-quantum encryption algorithms requires significant time and resources to update the cryptographic infrastructure.

In 2021, the U.S. Government Accountability Office prepared a report including a brief overview of the legal regulation of quantum technologies.[63] The analysis shows that the legal regulation of quantum communications in the United States will consist of mandatory and non-binding legal documents, accompanied by various legal means including certification, quality labeling, auditing, and regulatory sandboxes. An interesting aspect of the U.S. legal regulation model is the activity of the state in concluding international documents on cooperation with countries occupying leadership positions in the development of quantum technologies, for example, with

---

59 First PQC Standardization Conference, NIST Computer Security Resource Center (May 20, 2022), available at https://csrc.nist.gov/Events/2018/first-pqc-standardization-conference.

60 Post-Quantum Cryptography, Round 3 Submissions, NIST Computer Security Resource Center (May 20, 2022), available at https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions.

61 U.S. Department of Homeland Security, *Post-Quantum Cryptography Frequently Asked Questions* (October 2021) (May 20, 2022), available at https://www.dhs.gov/sites/default/files/publications/post_quantum_cryptography_faq_3_seals_october_2021_508.pdf.

62 Introduction to Quantum-Safe Cryptography in TLS, IBM Cloud (May 20, 2022), available at https://cloud.ibm.com/docs/key-protect?topic=key-protect-quantum-safe-cryptography-tls-introduction.

63 Quantum Computing and Communications: Status and Prospects, U.S. Accounting Chamber, 19 October 2019 (May 20, 2022), available at https://www.gao.gov/products/gao-22-104422.

Japan, as demonstrated by the Tokyo Statement on Quantum Cooperation.[64] In the context of the quantum threat, we can say that such documents form the legal basis for identifying the moment of creation of a quantum computer by another state.

2.3.5. Europe

Europe is one of the leaders in the development of quantum communications. For example, Switzerland was the first in the world to create a commercial quantum cryptography line for electronic voting,[65] and since 2007 it has been used to secure the network linking the ballot counting center in Geneva to government storage to ensure the integrity of election results data.[66] Quantum cryptography combines 256-bit AES Ethernet encryption with quantum key distribution (QKD). QKD uses the inherent properties of quantum mechanics to ensure that the key that is used to encrypt data is truly unique and has not been intercepted by any attacker. The solution provides a point-to-point Gigabit Ethernet link that can be used to send ballot information for federal and cantonal elections from the central counting station to the government data center in Geneva. Typically, sealed ballot boxes are transported from polling places to a central counting station, where they are opened and counted along with mail-in votes that have already been delivered. The counting process is carried out manually in accordance with a set of strict procedural rules. Geneva law stipulates that any citizen can be present during the counting of votes to ensure the accuracy of the results. However, in the modern world, this principle has been rethought: the election commission closely monitors the counting of votes and data entry, but the authenticity and integrity of any subsequent data transmission are now guaranteed by the highest level of encryption. Although this system has shown good results, quantum communication was able to ensure information security only in a certain section of the electronic voting chain.[67] This fact does not allow us to fully assess the effectiveness of quantum communication in the electoral process, yet the long period of its use indicates the high efficiency of this digital technology.

The European Telecommunications Standards Institute (ETSI) published a report in 2016 on the potential compromise of a number of algorithms utilized for

---

64 The Tokyo Statement on Quantum Cooperation, 19 December 2019, U.S. Department of State (May 20, 2022), available at https://www.state.gov/tokyo-statement-on-quantum-cooperation/.

65 Peng Xue & Xin Zhang, *A Simple Quantum Voting Scheme with Multi-Qubit Entanglement*, 7 Sci. Rep. (Article 7586) (2017).

66 *IDQ Celebrates 10-Year Anniversary of the World's First Real-Life Quantum Cryptography Installation*, IDQ, 23 November 2017 (May 20, 2022), available at https://www.idquantique.com/idq-celebrates-10-year-anniversary-of-the-worlds-first-real-life-quantum-cryptography-installation.

67 Paul Marks, *Quantum Cryptography to Protect Swiss Election*, New Scientist, 15 October 2007 (May 20, 2022), available at https://www.newscientist.com/article/dn12786-quantum-cryptography-to-protect-swiss-election.

protecting confidential data when a quantum computer is developed.[68] In 2018, the EU launched the Quantum Flagship,[69] based on the Quantum Technology Support program.[70] This document aims to support quantum researchers for ten years, and within the framework of quantum communications, the EU has allocated funding for ten projects.[71] The legal regulation of quantum technologies in the EU is implemented by the European Commission; to this end, it has created a Strategic Advisory Board (SAB), which is an advisory body to the Commission in the implementation of existing EU legislation, programs, and policies. The selected members comprise a high-level group of representatives, including independent experts from academia, research and technology institutes, and organizations from the industrial sector specializing in the field of quantum communications.

Furthermore, the EU has issued a declaration aimed at creating a quantum communications infrastructure (QCI) throughout the EU over the next ten years. The development of this technology is supported by Digital Europe programs[72] and Horizon Europe.[73] At the same time, the quantum communication infrastructure – EuroQCI, is considered the basis of the future "quantum Internet," potentially connecting quantum computers, simulators, and sensors to radically improve their performance and enable a new technological revolution.[74] It is assumed that the following actions will take place within the framework of EuroQCI:

• create a European industrial ecosystem for the safe operation of QCI technologies and systems;

• deploy advanced national QCI systems and networks;

• coordinate the first deployments of national EuroQCI projects and create a large-scale quantum key distribution testing and certification infrastructure (QKD);

---

68 ETSI, Quantum Computing Impact on Security of ICT Systems; Recommendations on Business Continuity and Algorithm Selection, ETSI – EG 203 310, 1 June 2016 (May 20, 2022), available at https://standards.globalspec.com/std/10026941/EG%20203%20310.

69 Homepage of Quantum Flagship (May 20, 2022), available at https://qt.eu/.

70 Supporting Quantum Technologies Beyond H2020, Quantum Support Action (QSA) – Version 1.1, Quantum Flagship, 7 May 2018 (May 20, 2022), available at https://qt.eu/about-quantum-flagship/newsroom/working-paper-v1-1/.

71 *See* Перечень отобранных проектов [List of Selected Projects]: The Launch of the Quantum Flagship (May 20, 2022), available at https://qt.eu/about-quantum-flagship/newsroom/quantum-flagship-launch-press-release/.

72 The Digital Europe Programme, European Union (May 20, 2022), available at https://digital-strategy.ec.europa.eu/en/activities/digital-programme.

73 What Is Horizon Europe?, European Commission (May 20, 2022), available at https://ec.europa.eu/info/research-and-innovation/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en.

74 European Commission, *Digital Europe Work Programme 2021–2022*, 10 November 2021 (May 20, 2022), available at https://ec.europa.eu/newsroom/repository/document/2021-46/C_2021_7914_1_EN_annexe_acte_autonome_cp_part1_v3_x3qnsqH6g4B4JabSGBy9UatCRc8_81099.pdf.

• deploy a large-scale infrastructure for testing and certification of QKD devices, technologies, and systems, allowing them to be accredited and implemented in EuroQCI.

Today, the European Quantum Industry Consortium (QuIC) plays a significant role in developing policy in the field of regulation of quantum communications in the EU. Its objectives are as follows:

• to identify gaps in the quantum technology sector in terms of supply chain, components and technologies, productivity, intellectual property, standards, and personnel;

• to identify applications and use cases of quantum technologies in various fields;

• to promote coordination between quantum technology industries;

• to promote the needs of the quantum technology industry to public stakeholders; and

• to create a fair and sustainable quantum technology business environment in Europe.[75]

Furthermore, discussions are taking place at the European Union level on a number of technical acts in the field of quantum technologies, for example, on issues of photonic integration in general and quantum photonic integrated circuits (QPICs) as a tool to promote the development of quantum technology. Moreover, quantum photonics receives significant attention in the QPIC Draft Position Paper.[76]

The standardization of quantum communications in the EU is carried out by the European Telecommunications Standards Institute. Additionally, the European Standards Organization (ESO) is the recognized regional body for standards involving telecommunications, broadcasting, and other electronic communications networks and services. The organization publishes recommendations and standards[77] for quantum key distribution[78] and for quantum-safe cryptography.[79] The EU uses exactly this terminology, which cannot be considered justified. In 2021, ETSI published the following documents:

---

[75] European Quantum Industry Consortium, *Statutes European Quantum Industry Consortium e.V.*, version 04.02.2021, 13 December 2021 (May 20, 2022), available at https://www.euroquic.org/wp-content/uploads/2022/01/Statutes-Quantum-Industry-Consortium-2021-dec-13-EN-final.pdf.

[76] Quantum Flagship & Photonics21 ETP, *Quantum PIC Position Paper (Draft)*, 19 March 2021 (May 20, 2022), available at https://www.photonics21.org/download/events/2021/QPIC_position_paper_07-04-2021_finaldraft.pdf.

[77] ETSI Standards, ETSI (May 20, 2022), available at https://www.etsi.org/standards-search#page=1&search=&title=1&etsiNumber=1&content=0&version=0&onApproval=1&published=1&historical=1&startDate=1988-01-15&endDate=2022-05-04&harmonized=0&keyword=&TB=856,,836&stdType=&frequency=&mandate=&collection=&sort=1.

[78] Industry Specification Group (ISG) on Quantum Key Distribution for Users (QKD), ETSI (May 20, 2022), available at https://www.etsi.org/committee/1430-qkd.

[79] Quantum-Safe Cryptography (QSC), ETSI (May 20, 2022), available at https://www.etsi.org/technologies/quantum-safe-cryptography.

• ETSI TR 103 616 V1.1.1 (2021-09) "Quantum-Safe Signatures";[80]

• ETSI TR 103 823 V1.1.1 (2021-09) "Quantum-Safe Public Key Encryption and Key Encapsulation."[81]

In addition to pan-European regulation, quantum communication is also regulated by the national legislation of the respective EU countries. For instance, in the Netherlands, the "National Strategy in the Field of Quantum Technologies" was adopted in 2019, which provides for the creation of a legal and public council on the basis of the Quantum Software Consortium to discuss and resolve legal problems that quantum technologies pose.[82]

2.3.6. Japan

Japan is implementing various projects in the field of quantum technologies, mainly within the framework of research cooperation with the United States, in connection with which a list of topics for joint research is being determined.[83] The country also has its own programs for the development of quantum technologies, for example, "Research Advanced Technologies" (ERATO) of the Japan Science and Technology Agency (JST),[84] as well as programs for the development of quantum communications and cryptography of the National Institute of Information and Communication Technologies (NICT), and projects of the Ministry of Internal Affairs and Communications (for e.g. satellite quantum cryptotechnology).[85]

Japan's quantum communications development strategy includes the following activities: development of a roadmap; creation of quantum innovation centers to connect universities and research institutes and industry; creation of venture capital companies through investments from public financial institutions or the Japan Innovation Network Corporation; start-up support programs; government procurement; etc.

In addition to these countries, other states are also involved in the development of quantum communications. For example, in Korea, research that is supported by the

---

80 ETSI, *CYBER; Quantum-Safe Signatures*, Technical Report, ETSI TR 103 616 V1.1.1 (2021-09) (2021) (May 20, 2022), available at https://www.etsi.org/deliver/etsi_tr/103600_103699/103616/01.01.01_60/tr_103616v010101p.pdf.

81 *Id*.

82 *National Agenda on Quantum Technology: the Netherlands as an International Center for Quantum Technology*, Qutech, 16 September 2019 (May 20, 2022), available at https://qutech.nl/2019/09/16/national-agenda-on-quantum-technology-the-netherlands-as-an-international-centre-for-quantum-technology/.

83 Japanese Ongoing Projects in the Field of Quantum Science (FY2021), Japan Science and Technology Agency (May 20, 2022), available at https://www.jst.go.jp/inter/washington/quantumdcl2021.html.

84 ERATO (May 20, 2022), available at https://www.jst.go.jp/erato/en/index.html.

85 Yoshihisa Yamamoto et al., *Quantum Information Science and Technology in Japan*, 4(2) Quantum Sci. & Tech. (2019) (May 20, 2022), available at https://iopscience.iop.org/issue/2058-9565/4/2.

Institute of Information and Communications Technology Planning and Evaluation (IITP) grant funded by the Korean government's Ministry of Science and ICT (MSIT), analyzes the potential of using Quantum Key Distribution Networks (QKDNs) for data protection in 5G networks.[86] However, these states do not pay significant attention to legal methods of stimulating quantum communication, so the analysis of their achievements is not analyzed in this article.

2.4. Conclusions Based on the Analysis of National Regulatory Experience

An analysis of the regulatory frameworks that govern the quantum communications industry around the world reveals that the top priority in this process is the regulation of the programs implemented at the strategic and development levels. An important mechanism for government regulation of the development of quantum communications is government funding to support projects in the field of quantum communications. At the same time, countries in the process of establishing legal regulations focus on one of two types of quantum communication. The first is based on the priority of quantum key distribution technologies in protecting information from the threat of violating the cryptographic strength of encryption algorithms emanating from a quantum computer. This approach, which is based on the laws of quantum physics, provides a high level of information security. The leader in this direction is the People's Republic of China, which currently has the longest quantum communication line, including fiber optic communication lines and satellites.

The second is based on the idea of prioritizing the use of new ciphers that will not lose cryptographic strength in the long term. This method is based on mathematical problems, the solution to which is considered inaccessible to a high-power quantum computer. The country that is leading the way in this direction is the United States, which has been analyzing various cryptography algorithms for a long time in order to approve a post-quantum encryption standard. The effectiveness of the standard planned for adoption is determined by the U.S. regulatory experts, who make their decisions based on existing knowledge in the field of quantum technologies. The cryptographic stability of the algorithm they have chosen will be tested under the conditions of the existence of a quantum computer and artificial intelligence developed with its help. In this regard, the risk involved in decrypting the post-quantum encryption algorithm can be assessed as significant. This is compounded by the lack of significant alternative research conducted on post-quantum encryption in other countries. For example, the United Kingdom recommends that information holders delay the migration of data until the U.S. regulator has issued a standard.

Both of the described approaches to information protection have advantages and disadvantages that must be taken into account in the process of legal regulation

[86] Choi et al. 2021.

of quantum communication. Thus, quantum key distribution comprises the following features:

1. This method of information protection is not susceptible to classical attacks based on cryptanalysis and allows for the remote transfer of an encryption key without human intervention.

2. Quantum key distribution is carried out in two ways: via fiber-optic communication channels and via atmospheric channels, including the use of satellites.

3. The existing technologies for transmitting photons via fiber optic communication channels have limitations on the data transmission range.

4. The level of information security during quantum key distribution depends on the physical security of technical equipment.

5. Quantum key distribution requires new communications infrastructure and additional equipment.

An encryption algorithm that has cryptographic strength when compared to a quantum computer has the following disadvantages:

1. Data migration requires the expenditure of fewer resources from the information owner.

2. So far, no state has defined an unconditionally secure post-quantum encryption algorithm.

3. Selecting a post-quantum encryption algorithm in the absence of an accurate understanding of the capabilities of a quantum computer in the field of machine learning for decrypting information is highly risky.

4. The cryptographic strength of the encryption algorithm is ensured by the absence of an effective decryption method, i.e. it will be subject to constant attacks and cryptanalysis.

5. A new encryption algorithm requires time to change the infrastructure that ensures information security.

This allows us to conclude that during legal regulation it is necessary to ensure the availability of all quantum encryption methods and that, in order to protect critical infrastructure, it is advisable to simultaneously use several methods of information protection that are cryptographically resistant to attacks from a quantum computer.

Regulation of a quantum-safe encryption algorithm does not require complex legal structures and can be limited to the introduction of an appropriate standard and recommendations for data migration. Regulating quantum key distribution, on the other hand, requires a more complex legal framework.

3. Features of Quantum Communication Technology Affecting its Legal Regulation

When it comes to the legal regulation of new digital technology, it is necessary to take into account its architectural features. Let us therefore consider the technical properties of quantum key distribution that can influence its legal regulation.

1. Quantum communication is a technology for transmitting information using single quantum objects

This allows us to assert that quantum key distribution equipment can be classified as communication equipment, and quantum key transmission lines can be classified as a special type of telecommunication lines. Based on this, it is advisable to initiate the legal regulation of quantum key distribution with its inclusion in national communications legislation. The implementation of such a proposal will make it possible not to mix similar categories and take into account in legislation the potential possibility of the emergence of a quantum Internet.

2. Quantum communication is not a homogeneous technology, but a combination of several data transfer methods

Based on the method of information transfer employed, quantum communication can be divided into the following categories:

• quantum internet – a technology for transmitting information in qubits;

• quantum key distribution – a technology for transmitting the key for encrypting messages with quantum objects;

• quantum-safe encryption algorithm – a technology for encrypting messages in a way that is crypto-resistant under the conditions of the existence of a quantum computer.

The authors understand that a quantum-safe encryption algorithm is not a method for transmitting data by single quantum objects, but rather it depends on the level of development of the quantum computer. Thus, it would be reasonable to recognize this method of data transmission as dynamic (i.e. it is subject to change in the process of gaining knowledge about quantum computing) and attributed to quantum communication. Consequently, the proposed legal structure will facilitate harmonious modification or integration with other methods of data protection.

Based on the information transmission channel used, quantum communication can be divided into two categories:

• quantum communication via a fiber optic communication channel;

• quantum communication in free space, including the transfer of quantum objects through air or water.

It should be noted that while quantum communication over the air or through a fiber optic link is well established in technology, the transmission of data using quantum objects underwater is a new area of research[87] that has the potential to establish communications with submarines.

Currently, the technology of quantum key distribution via a fiber optic communication channel has reached commercial potential all over the world. However, the legislator should design the framework of the legal institution in

[87] Mario Mastriani et al., *Bidirectional Teleportation for Underwater Quantum Communications*, 20 Quantum Info. Processing 22 (2021).

such a way as to allow the harmonious inclusion of developing types of quantum communication. Accordingly, the possibility of commercial exploitation of other methods of quantum communication must be taken into account during the legal regulation of the industry.

3. Quantum cryptography protocols implemented today are conditionally secure

Quantum cryptography is based on quantum key distribution, which, under proven protocols such as the BB84 protocol, is an unconditionally crack-resistant encryption method. The current level of development of special equipment and communication lines does not allow the technical ability to fully comply with secure protocols for single-photon information encoding. This makes quantum key distribution vulnerable to attacks. Taking into account that quantum encryption equipment can also be subject to attacks, it is advisable when establishing standards for quantum communication to require the re-design of redundant methods of information protection.

When considering the issues pertaining to information encryption in the era of quantum computing, most scientists assume that there are two alternative and conditionally secure encryption methods, namely quantum key distribution and post-quantum encryption. Considering that the capabilities of quantum computers are not known but only predicted, public authorities are obliged to recommend a combination of several encryption methods, either in the form of a mandatory or advisory regulatory legal act.

4. Quantum key distribution is limited by the transmission range of the photon

Quantum key distribution relies on the creation, transmission, and detection of signals at the quantum level. This is difficult to achieve if the network used for transmission is also in use with classical signals, which are much more powerful. On the other hand, quantum transmission can be neither amplified nor regenerated – at least not without quantum repeaters, which are not feasible with current technology – implying a limited reach for quantum communications and the need to resort to trusted repeaters to increase the distance. In order to optimize the transmission of quantum signals together with classical communications over a network, whether they share the same physical media or not, and to effectively manage the key relay required for longer distances, it is necessary to integrate the QKD systems such that they can communicate with the network control and also receive commands from it.[88]

The transmission of photons via fiber optic communication channels is limited by the network range and, on average, does not exceed 100 kilometers. However, Chinese scientists announced in 2020 that they had achieved a distance of over

[88] ETSI, *Quantum Key Distribution (QKD); Control Interface for Software Defined Networks*, ETSI GS QKD 015 V1.1.1 (2021–03) (2021) (May 20, 2022), available at https://www.etsi.org/deliver/etsi_gs/QKD/001_099/015/01.01.01_60/gs_QKD015v010101p.pdf.

500 kilometers.[89] Nevertheless, even this distance poses a significant limitation on the practical application of quantum cryptography for countries with expansive territories.

Given these conditions, it is advisable to proceed with the possibility of transitioning from point-to-point solutions to a star architecture, which should lead to a reduction in connection costs and the prevalence of solutions without the requirement to trust the intermediate node. An example of quantum network infrastructure in Russia is shown in Figure 1 below. This network cannot be considered flawless. The authors agree with the opinion that the optimal quantum key distribution network should be built on satellite communication.[90]

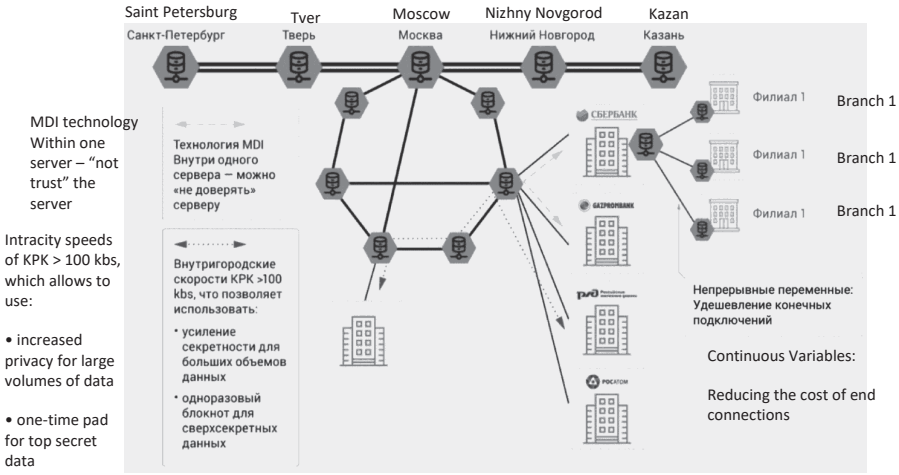

Fig. 1: **An example of quantum network infrastructure in Russia**

The star scheme uses several integrated communication channels, including trunk communication lines and city communication lines. In the process of formulating legal regulations, it is necessary to take this specificity into account. This would entail either determining the subject of a natural monopoly that manages communication lines or establishing a transparent control scheme over the distribution of quantum keys in areas of responsibility that are difficult to define, along with legal guarantees for the protection of the rights of key recipients. It seems promising to create a self-

[89] Jiu-Peng Chen et al., *Sending-Or-Not-Sending with Independent Lasers: Secure Twin-Field Quantum Key Distribution over 509 km*, 124(7) Phys. Rev. Lett. (Article 070501) (2020); Xiao-Tian Fang et al., *Implementation of Quantum Key Distribution Surpassing the Linear Rate-Transmittance Bound*, 14 Nat. Photonics 422 (2020).

[90] Veenu Yadav & Deepshikha Agarwal, *Analysis of Quantum Cryptography for Secure Satellite Communication*, 9(5) Int'l J. Sci. & Tech. Res. 120 (2020).

regulatory organization and use it to insure against the risks of information security violations. The establishment of a single guarantor for the protection of property rights of users of the quantum key distribution system would enable the building of market confidence in its functioning. A self-regulatory organization that has satisfied a user's complaint should have the right, by way of subrogation, to appeal to the person who violated the security protocol.

5. Quantum key distribution makes it possible to detect an attack

Quantum key distribution typically ceases when an attack is detected as it is deemed intercepted. In such a scenario, there may not be a real attack on the quantum network. Photon delivery may be hindered by external factors, including weather (as seen in atmospheric key distribution), imperfect communication equipment, etc. Putting a stop to key generation in the classical version should lead to a temporary interruption of the communication channel, which is fraught with negative consequences in systems with continuous data transfer. For example, in traffic management systems, a failure of a communication channel can create emergency situations. Based on this, it would be advisable if the legal regulation of quantum key distribution in practice normatively established the obligation of the quantum communication network operator to duplicate communication channels.

At the same time, it should be noted that there is another way to protect the quantum communication channel. Some researchers propose an enhanced measure of security for a quantum key distribution protocol, in which we require that the adversary not only obtains no information about the key but also remains unaware that a key generation protocol has been executed. When the adversary applies the same quantum channel independently to each quantum-transmitted state, akin to a collective attack in the quantum key distribution literature, we come up with a protocol that achieves cover and secret key expansion under mild restrictions.[91]

6. The state should support not only the creation of equipment for quantum key distribution but also for post-quantum cryptography

"Inside Quantum's Post-Quantum Cryptography Report Pegs PQC Market at $9.5 billion in 2029," according to a press release.[92] The report's authors estimate that more than 80 percent of PQC (post-quantum cryptography) revenue will come from web browsers, Internet of Things (IoT), and machine tools. A boom in equipment sales is expected after NIST's decision to complete the competition to select the most secure information security algorithm in the quantum era. It is important to note that the majority of citizens may not have the ability to access quantum key distribution, just as they currently do not have access to expensive encryptors. However, public

---

[91] Mehrdad Tahmasbi & Matthieu R. Bloch, *Covert and Secret Key Expansion over Quantum Channels under Collective Attacks*, 66(11) IEEE Trans. Info. Theory 7113 (2020).

[92] Post-Quantum Cryptography (PQC): A Revenue Assessment, Report IQT-PQC-0620, 1 June 2020, Inside Quantum Technology (May 20, 2022), available at https://www.insidequantumtechnology.com/product/post-quantum-cryptography-pqc-a-revenue-assessment/.

authorities cannot afford to leave them without even minimal protection in the face of the emergence of a quantum computer. This allows us to say that the state is obliged to create a market with the availability of conditionally secure cryptography algorithms that are suitable for mass use, as well as control the availability of these algorithms to citizens of all income levels.

4. Concept of Legal Regulation of Quantum Communication

When discussing the model of legal regulation of quantum communication, it should be remembered that different states have different legal systems and use different legal instruments. In order to ensure terminological accuracy, the following definitions will be used in this section:

• normative legal act – a binding act adopted by a legislative or executive body of state power;

• strategic normative act – a document adopted by a government body that is advisory in nature, i.e. not mandatory.

Our analysis made it possible to identify the following minimum set of legal means that states should use to stimulate the development of quantum communication:

1. Legal regulation of investments in quantum communications

We believe that the potential bottlenecks in trade and investment can be overcome largely through the exchange of experiences to mitigate the lack of knowledge on national laws and regulations and by the creation of cooperative mechanisms that facilitate the economic flow among them.[93] However, data protection technologies are of strategic importance; therefore, it is necessary to limit the access of representatives of foreign investors to this area in the form of a law. It is important to note that similar laws that restrict foreign investors' access to this field have already been adopted in the United Kingdom and Denmark, which indicates the possibility of their harmonization with the liberal economic model.

The authors do not proceed from the advisability of a ban on attracting foreign capital but only recommend creating legal mechanisms to insure against adverse consequences, for example, limiting the possibility of registering patents for non-residents. These rules must be adopted only in the form of a normative legal act since they affect the issue of private property and business activity, i.e. an area sensitive to the stability of work rules.

2. Distribution of competencies in the field of regulation of quantum communications

Nearly every country across the world has identified the authorities or legal entities that are authorized to regulate the field of quantum communications. It is important to note that a monopoly in this area does not always benefit the industry.

---

[93] Emílio M.D. Silva & Bruce R.S. Campos, *Possible Legal Cooperation for a BRICS Perspective on International and Transnational Economic Law*, 8(4) BRICS L.J. 31 (2021).

For example, when the regulator determines the authority responsible for security, the state may be faced with a trend to restrain the market; conversely, transferring the functions of the regulator to the economic bloc may lead to damage to the interests of national security. Thus, it appears that there must be a balance of interests in this issue. It is advisable to divide competence between several subjects of legal relations, as well as to divide financing between several business entities. The legal mechanism of fair competition in this area will allow for the achievement of better results with a limited amount of resources.

3. Consolidation of the principles of regulation of quantum communication in regulatory legal acts

At the time of the formation of the industry, it is important to prevent law enforcement measures that limit its development. At the same time, the level of information security cannot be reduced. The principles of legal regulation are capable of combining these bipolar goals. The authors propose to establish these principles in the form of a normative legal act, which will allow the subjects of law to protect their interests in court in the absence of a specific rule of conduct by drawing an analogy with law, providing for the following two possibilities:

1. If the relations are not directly regulated by the legislation or agreement of the parties and there is no custom applicable to them, the legislation regulating similar relations (analogy of law) is applied to such relations, unless this contradicts their essence.

2. If it is impossible to use an analogy of law, the rights and obligations of the parties are determined based on the general principles enshrined in the legislation.

The authors highlight the following principles of legal regulation of quantum communication:

• priority of human rights and freedoms – legal regulation of quantum communications is based on a human-oriented approach, stipulating that their ultimate goal is to ensure the protection of human rights and freedoms guaranteed by national and international legislation, as well as improving the well-being and quality of life of citizens;

• the right to data protection is absolute – the legal regulation of quantum communications provides for the right of all people to use any method of protecting information, except for methods the use of which is prohibited by law;

• multiple methods of protecting information – in the event that there are mandatory requirements for the protection of information established by regulatory legal acts, it is allowed to use other methods of protecting information as duplicating methods, if the obligation of duplication is not provided for by law;

• risk-oriented approach to regulation – legal regulation of quantum communications is carried out on the basis of a risk-oriented approach, providing for the adoption of mandatory norms in the event that the use of other regulators carries a significant risk to the information security of the state, individuals, and

organizations, including through the establishment of experimental legal regimes in the field of digital innovation;

• stimulation of self-regulation – legal regulation of quantum communications stimulates the use of tools, self-regulation, and the formation of codes (sets) of ethical rules for the use of quantum communications;

• scientific validity – legal regulation of quantum communications is allowed only after a mandatory multiple scientific examination of their impact on information security and other areas of human life, society, and the state, carried out by at least two independent assessment entities not affiliated with any of the market participants;

• ensuring a balance of interests of subjects of legal relations – legal regulation of quantum communications ensures compliance with the interests of owners of quantum communication technologies, consumers of quantum communication services, and other persons involved in the field of quantum communications;

• delimitation of responsibilities of subjects of legal relations – legal regulation of quantum communications ensures a clear delimitation of responsibility for the protection of information between all participants in legal relations and provides for the possibility of bringing legal entities and individuals to different types of liability for possible negative consequences of the use of quantum communications;

• technological sovereignty – legal regulation of quantum communications ensures the achievement of the necessary level of state independence in this area;

• support for competition – legal regulation of quantum communications ensures equal opportunities for everyone, including small and medium-sized businesses, to develop quantum communication technologies and access to quantum key distribution services.

4. Creation of interconnected quantum communication standards, including standards for quantum key distribution and quantum-safe cryptography

Today, many countries around the world are creating quantum communication standards that make it possible to certify equipment and communication lines. The Chinese experience was discussed in detail in Section 2.1. In addition, we can highlight the work of ETSI, where the Industry Specification Group (ISG) on quantum key distribution for users was created. During the course of 2021, work progressed on six new Group Specifications (GS), which are outlined below:

1. GS QKD 010 addresses the design, construction, characterization, and operation of QKD systems that are intended to protect against Trojan horse attacks.

2. GS QKD 013 defines procedures for characterizing specific properties of complete QKD transmitter modules.

3. GS QKD 016 describes a common criteria protection profile for complete QKD systems, involving point-to-point devices from the physical implementation up to the output of final secret keys.

4. GS QKD 018 provides a definition of orchestration interfaces between SDN orchestrator(s) and SDN controller(s) of QKD networks.

5. GS QKD 020 specifies an interface to meet the most urgent interoperability requirements between key management systems in QKD networks.[94]

A number of countries are of the opinion that post-quantum cryptography will free us from the threat to information security in the quantum era. However, the cryptographic strength of new algorithms is assessed by experts, who may make mistakes. For example, in the United States, the MD5 and the SHA-1 algorithms were used, which, according to experts, provided a sufficient level of information security. However, a Chinese woman, Wang Xiaoyun, successfully cracked the MD5 in 2004 and the SHA-1 ciphers in 2005.[95] It is important to note that random individual countries around the world may have the competence to find vulnerabilities in ciphers. There is no doubt that the creation of a quantum computer and the development of machine learning based on it will be able to change the methodology of cryptanalysis to a state that is currently unpredictable. It has been experimentally proven that artificial intelligence systems are already achieving successes in various fields that were not predicted by their creators.[96] Therefore, the authors point out that there is a risk of error when choosing a post-quantum encryption algorithm. This allows the public authority to use combined methods of protecting critical information in the initial stages of the development of a quantum computer.

Researchers in the field of quantum key distribution also talk about the advisability of using several types of cryptography. For example, research scholars L.-J. Wang, K.-Y. Zhang, and J.-Y. Wang note that with the help of mature public key infrastructure and post-quantum cryptography with quantum-resistant security, each user only needs to apply for one digital certificate from a certificate authority to achieve efficient and secure authentication for quantum key distribution.[97] The scientists experimentally tested the feasibility, efficiency, and stability of a post-quantum cryptography algorithm for authenticating quantum key distribution and demonstrated the benefits that occur when new users join a quantum network using a public key infrastructure. In this case, nodes must mutually trust only the certification authority in order to authenticate each other.

5. A comprehensive change in legislation to harmonize quantum communication with existing social relations

---

94 Contributions for QKD, ETSI (May 20, 2022), available at https://portal.etsi.org/Contribution.aspx?Tb_Id=723&searchText=&IncludeSubTb=False&sort=pk_contribution&sortorder=DESC&NbItemsPerPage=50&Year=2022.

95 王小云：连破两套美国顶级密码，获711万国家奖金，美国不淡定了 [Net Ease, *Wang Xiaoyun: He broke two top American passwords in a row and won a national bonus of 7.11 million: The United States is no longer calm*] (May 20, 2022), available at https://www.163.com/dy/article/GO4UUA6A0543IDAW.html.

96 Alexey V. Minbaleev & Kirill S. Evsikov, *Anti-Corruption Information Technologies*, 14(11) J. Siberian Fed. U. Human. & Social Sci. (2021).

97 Liu-Jun Wang et al., *Experimental Authentication of Quantum Key Distribution with Post-Quantum Cryptography*, 7 npj Quantum Info. 67 (2021).

In the process of introducing quantum communication, it is not enough to limit oneself to fragmentary changes in the legal system. This analysis made it possible to identify several priority measures in the field of lawmaking that promote the introduction of quantum communication technologies, which can conventionally be called the "Concept of the Legal Regulation of Quantum Communication" (hereinafter the Concept). It is advisable to systematize the law-making process in order to approve the concept by means of a normative legal act. This will also facilitate the coordination of the activities of different public authorities. Often, a state has different government bodies that are authorized to regulate a particular area of public life. At the same time, their corporate interests often contradict the interests of other government bodies, which creates competition that is acceptable under normal conditions but destructive in the area of complex changes in legislation in order to develop a specific industry. The analysis showed that the best option to overcome this administrative barrier is the adoption of a document defining the general goals for the concept, the tasks of a specific government body, and the time frame for their implementation. Therefore, to develop quantum communication within such a concept, it is advisable to incorporate the following elements.

1. Creation of mechanisms for the simplified implementation of quantum communications

At the initial stage, it is advisable to create a legal mechanism for testing, trial operations, and implementation of solutions in the field of quantum communications. This framework should allow for the timely and effective implementation of new developments without excessive administrative procedures or changes to a significant amount of legislation and ensure the necessary level of security and controllability by government agencies.

The legal means of creating such a mechanism are experimental legal regimes in the field of digital innovation (known as regulatory sandboxes). Using the regulatory sandbox as an experimental legal regime is one of the ways to test the creation, production, and realization of digital innovation. Having been first applied in 2016 in the United Kingdom, this model is currently successfully implemented in countries such as Singapore, Australia, and the United Arab Emirates.[98] The use of experimental legal regimes in quantum communication is proposed as a means to introduce quantum key distribution in the fields of unmanned vehicles, the Internet of Things, and industrial robotics. This can stimulate the development of quantum communications in general as well as individual elements that make up digital technology, for example, a quantum random number generator. It is important to note that the technological possibilities of such an application are already being analyzed by the scientific community.[99]

---

98 Elizaveta Gromova & Tjaša Ivanc, *Regulatory Sandboxes (Experimental Legal Regimes) for Digital Innovations in BRICS*, 7(2) BRICS L.J. (2020).

99 Basman K. Mohammed & Mohammed M. Abdulmajeed, *Performance Evaluation for Deterministic Six State Quantum Protocol (6DP) Using Quantum*, in Proceedings of the 5th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), I-SMAC 1404 (2021).

2. Legal liability of subjects of legal relations in the field of quantum communication

Emerging social relations in the field of quantum communication involve a complex multi-subject composition, which is further complicated by a number of factors, including the following:

• the presence of a competitive global market for equipment for quantum cryptography, complicated by the classification of goods as dual-use;

• the formation of a competitive national market for equipment for quantum communications, complicated by the presence of national restrictions on the civil circulation of certain types of goods;

• the formation of a market for the provision of services in the field of quantum communications with a plurality of economic entities that have signs of a natural monopoly;

• the formation of a market for certification of equipment and communication lines for quantum communications;

• the emergence of a space constellation that provides quantum communication over a considerable distance.

The integrity of the actions of each of the subjects of legal relations must be ensured by institutions of legal responsibility, which require improvement in connection with the development of quantum communication. The Concept provides for improving the mechanisms of civil, administrative, and criminal liability in the event of harm to information security by entities involved in legal relations in the field of quantum communications.

Furthermore, the Concept provides for the creation of legal mechanisms for the prevention of offenses in the field of quantum communications, including preventive remedies for the rights of individuals and legal entities. Taking into account the legal properties of information, the Concept involves the creation in the field of quantum communication of mechanisms that provide compensation for material damage to information security, aimed at the effective and fair functioning of institutions for the distribution of responsibility in the event of harm to public authorities, legal entities, and individuals.

3. Improving the regime for the export and import of technologies and services in the field of quantum communications

The relevance of this section is confirmed by international practice, for example, BRICS recently announced a developmental breakthrough in quantum communications. The Russian technological company Shvabe and the BRICS nations intend to create an intercontinental satellite quantum communication channel using the latest elements of macro-and fiber optics, which will cover a distance of more than 10,000 kilometers.[100] This is a great advancement for communications globally.

[100] BRICS International Quantum Communications Research Underway, Space in Africa (May 20, 2022), available at https://africanews.space/brics-international-quantum-communications-research-underway/.

In order to develop quantum communications technologies, it is necessary to create a favorable regime for their import and export. Export restrictions should only apply to technologies that affect national security interests. Quantum communication technologies are subject to export and import controls due to their dual-use nature, which can potentially be used in the creation of weapons and military equipment. This list does not contain exceptions and is not subject to revision. At the same time, certain elements of quantum communication are in high demand in the global market as a means to ensure information security in civilian goods. A scientific assessment of the admissibility of simplifying the circulation of certain types of quantum communication technologies should thus be provided for by current legislation.

There are two options for resolving this area, which include the following:

• moving away from a general restriction on the circulation of quantum key distribution technologies along with a transition to a description of specific quantum communication equipment, the export and import of which could lead to damage to national security;

• individual expert assessment of the admissibility of exporting equipment for quantum communications.

To implement the latter approach, the Concept involves adjusting the certification system, which will allow for an expert assessment of the admissibility of exporting each model of equipment based on the principle of scientific validity. Furthermore, exporting any technology or equipment model requires a mandated evaluation, which must be conducted at least once every two years. However, the owner of the technology (the creator of the equipment) may appeal the conclusion that export is impossible.

4. Development and clarification of terms and definitions in the field of quantum communications

A number of definitions have different interpretations in different countries, for example, "post-quantum cryptography algorithm" in the United States and "quantum-safe cryptography algorithm" in the EU. There is also no generally accepted definition of "quantum communication." It seems that the solution to these issues should be the first stage of legal regulation of quantum communication, where legal boundaries should be established for these concepts, as well as for the "fiber optic quantum communication channel," "free space quantum communication channel," and "trusted quantum communication node."

5. Improving the system of technical regulation and conformity assessment

Currently, the majority of countries have a number of established technical standards in the fields of photonics, communications, and information security, but except for China, regulatory and technical regulation in the field of quantum communications is still at an early stage of formation. In order to ensure, the reliability, security, and interoperability of solutions in the field of quantum communications,

it is necessary to create a modern system of regulatory and technical regulation in this area.

The Concept allows for the existing technical standards and regulations to be adapted for certain areas of application of quantum communications technologies. However, for commercial use, it is necessary to form a full-fledged, comprehensive system of technical standards containing mandatory standards for quantum key distribution equipment and quantum and post-quantum cryptography algorithms. This is necessary for the creation of a certification system.

6. Related tasks of legal regulation of quantum communication

Finally, for the successful development of digital technology, it is necessary to create an accompanying ecosystem, which is regulated by various branches of law that have an auxiliary nature, such as the following:

• migration legislation – to facilitate international cooperation and access of high-level foreign specialists to national research centers;

• legislation in the field of education – the creation of educational standards for higher education for training specialists in the field of quantum communications and support for the creation and promotion of educational programs for different categories of citizens that contribute to the formation of basic digital literacy competencies, including an understanding of the fundamentals and importance of quantum-safe communication;

• labor legislation – when forming strategic documents regulating relations in the field of employment, it is necessary to take into account the impact of quantum communications technologies on the labor market, including changes in the demand for certain professions;

• antimonopoly legislation – if the state has chosen a model of quantum communication with a single operator of the quantum key distribution network, then it is subject to inclusion in the list of natural monopolies. This classification should be determined by a regulatory legal act that establishes the rules for providing quantum communication services and connecting to quantum communication networks. It would also be advisable to establish regulations for tariffs regarding quantum communications.

Conclusion

The quantum communication system is a conditionally safe technology capable of providing protection in the face of a quantum threat. Its development is ensured only through the coordinated actions of public authorities, acting within the framework of a single Concept, an example of which is given in the article. A regulatory act of a strategic nature contributes to a comprehensive change in existing legal norms, and therefore plays an important role in creating an information security system for society, the state, and business. The content of the Concepts may differ depending on

the data protection technology preferred by a particular state; however, the article provides several key features of the quantum communication architecture that must be taken into account by any state when developing its regulations.

The study made it possible to identify risks that could hinder the effective legal regulation of quantum communication. These risks include:

• risk of terminological uncertainty;

• the risk of a decrease in the level of information security when transitioning from existing methods of information security and quantum communication;

• the risk of not transitioning to quantum communication due to the problem of a lack of cryptographic flexibility in the equipment used and created;

• the risk of an erroneous definition of the subject and boundaries of regulation of quantum communication due to a lack of experience in the use of quantum technologies;

• the risk of irresponsibility for causing harm when using quantum communications due to the multi-subjectivity of participants in legal relations.

These risks must be taken into account in the process of creating a quantum communications market.

In order to protect the fundamental human rights pertaining to information access and privacy, as guaranteed by international treaties, the authors recommend that the general population be publicly informed about the presence of a quantum threat. Based on the principle that ignorance of the law does not exempt one from liability due to its publication in the public domain, the state should publish official recommendations on data protection in the context of the creation of a quantum computer and on its migration to information systems with quantum-safe data protection technologies. Furthermore, it appears that these recommendations should be non-binding, except in cases of state protection of critical infrastructure.

Such recommendations can help the state fulfill its obligation to society and business to ensure information security in the face of difficult-to-predict threats that can be created by a quantum computer and a cryptanalysis information system built by a quantum computer using machine learning methods.

In their analysis of the legal framework for promoting the quantum communication market, the authors considered the resource-intensive infrastructure required for quantum key distribution, both in the presence and absence of a natural monopoly company. Both options seem to be effective for obtaining a quantum key distribution network, to which government and commercial companies can connect to ensure a guaranteed level of information security. This is especially important in the context of the development of the digital economy.

The study also provided an overview of the standards of quantum-safe cryptography that currently exist in different countries. This analysis allows any country to use these standards as a basis for creating a national standardization and certification system. The authors note that the standardization process must take into

account the fact that quantum communication lines and equipment have a wide range of uses, for example, the transfer of quantum objects by air or by water. These aspects must be taken into account in the certification process in order to allow for the creation of suitable standards for hybrid quantum communication channels.

Taking into account the significance of quantum communications, their regulation should not be limited to normative legal acts but should be accompanied by official acts of a recommendatory nature as well as acts of an informal normative nature that are adopted within the framework of self-regulation. The authors do not allow for the possibility of adopting optional regulatory acts in the field of protecting critical information. The use of quantum communications that pose a threat to the defense of the country and state security should also be prohibited.

The authors especially note that the legal regulation of quantum communication is a highly dynamic process. Legislation in this area should provide mechanisms that enable the prompt revision of mandatory rules based on the results of analysis carried out by the authorized authority on an ongoing basis. It would be advisable to consolidate the obligation of such analysis at the legislative level by identifying the government body responsible for maintaining the cryptographic strength of encryption algorithms in the context of the development of quantum computers and artificial intelligence.

Acknowledgements

The research was funded by the Russian Science Foundation (project No. 24-18-00950 "Problems and Prospects of Regulation of Quantum Communications in a Data Economy").

References

Arute F. et al. *Quantum Supremacy Using a Programmable Superconducting Processor*, 574 Nature 505 (2019). https://doi.org/10.1038/s41586-019-1666-5

Brandmeier R.A. et al. *Future Development of Quantum Computing and its Relevance to NATO*, 20(2) Connections: The Quarterly Journal 89 (2021).

Chen J.-P. et al. *Sending-Or-Not-Sending with Independent Lasers: Secure Twin-Field Quantum Key Distribution over 509 km*, 124(7) Physical Review Letters (Article 070501) (2020). https://doi.org/10.1103/PhysRevLett.124.070501

Chen Y.-A. et al. *An Integrated Space-to-Ground Quantum Communication Network over 4,600 Kilometres*, 589 Nature 214 (2021). https://doi.org/10.1038/s41586-020-03093-8

Choi T. et al. *Quantum Key Distribution Networks for Trusted 5G and Beyond: An ITU-T Standardization Perspective*, in International Telecommunication Union Kaleidoscope Academic Conference: Connecting Physical and Virtual Worlds, ITU K (2021). https://doi.org/10.23919/ITUK53220.2021.9662098

Fang X.-T. et al. *Implementation of Quantum Key Distribution Surpassing the Linear Rate-Transmittance Bound*, 14 Nature Photonics 422 (2020). https://doi.org/10.1038/s41566-020-0599-8

Forbes A. et al. *Toward a Quantum Future for South Africa*, 3 AVS Quantum Science (Article 040501) (2021). https://doi.org/10.1116/5.0060426.

Gozzard D.R. et al. *Vulnerability of Satellite Quantum Key Distribution to Disruption from Ground-Based Lasers*, 21(23):7904 Sensors (Basel) (2021). https://doi.org/10.3390/s21237904

Gromova E. & Ivanc T. *Regulatory Sandboxes (Experimental Legal Regimes) for Digital Innovations in BRICS*, 7(2) BRICS Law Journal 10 (2020). https://doi.org/10.21684/2412-2343-2020-7-2-10-36

Hoofnagle C. & Garfinkel S. *Quantum Communications*, in Law and Policy for the Quantum Age 257 (2022). https://doi.org/10.1017/9781108883719.011

Kharitonova Yu. & Sannikova L. *Digital Platforms in China and Europe: Legal Challenges*, 8(3) BRICS Law Journal 121 (2021). https://doi.org/10.21684/2412-2343-2021-8-3-121-147

Minbaleev A.V. & Evsikov K.S. *Anti-Corruption Information Technologies*, 14(11) Journal of Siberian Federal University, Humanities & Social Sciences 1674 (2021).

Mosca M. *Cybersecurity in an Era with Quantum Computers: Will We Be Ready?*, 16(5) IEEE Security & Privacy 38 (2018). https://doi.org/10.1109/MSP.2018.3761723

Polyakova T.A. et al. *Development of the Science of Information Law and Legal Provision of Information Security: Formation of the Scientific School of Information Law (Past and Future)*, 12 Gosudarstvo i pravo 97 (2021). https://doi.org/10.31857/S102694520017761-8

Silva E.M.D. & Campos B.R.S. *Possible Legal Cooperation for a BRICS Perspective on International and Transnational Economic Law*, 8(4) BRICS Law Journal 31 (2021). https://doi.org/10.21684/2412-2343-2021-8-4-31-37

Tahmasbi M. & Bloch M.R. *Covert and Secret Key Expansion over Quantum Channels under Collective Attacks*, 66(11) IEEE Transactions on Information Theory 7113 (2020).

Wang L.-J. et al. *Experimental Authentication of Quantum Key Distribution with Post-Quantum Cryptography*, 7 npj Quantum Information (Article 67) (2021). https://doi.org/10.1038/s41534-021-00400-7

Wang M. & Li H.-S. *Bidirectional Quantum Teleportation Using a Five-Qubit Cluster State as a Quantum Channel*, 21 Quantum Information Processing 44 (2022). https://doi.org/10.1007/s11128-021-03389-2

Wu Y. et al. *Strong Quantum Computational Advantage Using a Superconducting Quantum Processor*, 127(18) Physical Review Letters 180501 (2021).

Xue P. & Zhang X. *A Simple Quantum Voting Scheme with Multi-Qubit Entanglement*, 7 Scientific Reports (Article 7586) (2017). https://doi.org/10.1038/s41598-017-07976-1

Yadav V. & Agarwal D. *Analysis of Quantum Cryptography for Secure Satellite Communication*, 9(5) International Journal of Scientific and Technology Research 120 (2020).

Information about the authors

Alexey Minbaleev (Moscow, Russian Federation) – Head, Department of Information Law and Digital Technologies, Kutafin Moscow State Law University (MSAL), Expert, Institute of State and Law, Russian Academy of Sciences (9 Sadovaia-Kudrinskaia St., Moscow, 125993, Russian Federation; e-mail: avminbaleev@msal.ru).

Sergey Zenin (Tyumen, Russian Federation) – Associate Professor, Vice-Rector, Director, Institute of State and Law, University of Tyumen (16 Lenina St., Tyumen, 625003, Russian Federation, e-mail: s.s.zenin@utmn.ru) **– corresponding author**.

Kirill Evsikov (Tula, Russian Federation) – Associate Professor, Department of Information Law and Digital Technologies, Kutafin Moscow State Law University (MSAL), Head, Department of State and Administrative Law, Tula State University (155 Friedrich Engels St., Tula, 30001, Russian Federation; e-mail: ksevsikov@msal.ru).