# International Overview of Quantum Security: Mapping Organizations, Technologies, and Use Cases in PQC and QKD

**Mabel Diz Marques Mota[1]*, João Carlos Passos[1], Alexandre de Santa Bárbara[1], Guilherme João Musse Neto[1], Gabrielly da Silva Roman[1], João Marcelo Silva Souza[1]**

*[1]SENAI CIMATEC University, Center of EMBRAPII CIMATEC in Quantic Technologies; Salvador, Bahia, Brazil*

**The article presents an international overview of the quantum security ecosystem, focusing on Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD). The methodology involved a systematic mapping of 85 active organizations, revealing the predominance of the private sector (84.7%), with the highest concentration in the United States (30.59%) and China (14.12%). The data indicate a strong presence in the development of hybrid solutions (65.88%), which can be attributed to the pursuit of greater implementation flexibility, particularly in contexts of technological transition. These solutions are directly associated with strategic sectors such as telecommunications (31 organizations), cloud computing (17), and finance/government (16). Use cases demonstrate applications in IoT, 5G networks, blockchain, and digital identity, with notable contributions from companies such as Infineon, Toshiba, ID Quantique, CryptoNext, Microsoft, and DigiCert. Additionally, the results suggest increasing maturity, commercial expansion, and the relevance of PQC and QKD for technological resilience and sovereignty, establishing these technologies as pillars of secure digital infrastructures in the era of quantum computing.**

**Keywords: Quantum Communication. Post-Quantum Cryptography. Quantum Key Distribution. PQC. QKD.**

The advancement of quantum computing threatens to compromise the main public-key algorithms currently in use, such as RSA (based on integer factorization) and ECC (elliptic curves), whose security relies on mathematical problems that quantum algorithms, such as Shor's, can solve in polynomial time [1]. In this context, two approaches are being explored: Post-Quantum Cryptography (PQC), which employs algorithms resistant to quantum attacks on classical systems [2], and Quantum Key Distribution (QKD), which ensures secure key generation and distribution based on physical principles, such as no-cloning and entanglement [3].

PQC is undergoing standardization by the National Institute of Standards and Technology (NIST) [2], while QKD already has commercial applications in optical networks and satellite-based systems [4]. Both are being adopted complementarily in sectors such as telecommunications, cloud computing, and financial services [5]. However, there is still a lack of studies that systematically analyze how these technologies are being applied globally, considering the nature of organizations, the sectors served, and implementation models.

This article presents a mapping of international initiatives in PQC and QKD, identifying their geographical distribution, implementation approaches, and use cases. The study is structured as follows: Section 2, theoretical foundations of PQC and QKD; Section 3, methodological aspects; Section 4, analysis of results; and Section 5, final considerations.

## Theoretical Framework

A Quantum Key Distribution (QKD) protocol enables two spatially separated parties (Alice and Bob) to share and generate random, secure sequences—secret keys [8]. Unconditional security is guaranteed by the laws of quantum mechanics, making it impossible for an eavesdropper (Eve) to interfere with the communication without being detected. A protocol can be divided into two main stages: the distribution of quantum states and post-

Received on 20 October 2025; revised 22 January 2026.

Address for correspondence: Mabel Diz Marques Mota. Av. Orlando Gomes, 1845 - Piatã, Salvador – BA – Brazil, Zipcode: 41650-010. E-mail: mabel.mota@fieb.org.br / mabeldizmarques@gmail.com.

J Bioeng. Tech. Health 2025;9(2):169-172

processing. Modern communication revolves around the Internet as a fundamental building block for interactions between parties, requiring data protection and privacy. QKD enables the construction of secure communication networks using infrastructures compatible with existing optical networks [8].

Post-Quantum Cryptography (PQC) is based on identifying mathematical problems that are difficult to solve even by fully operational quantum computers [5]. The security of these algorithms lies in the intrinsic difficulty of these problems, not in the computational limitations of classical computers. PQC emerges as a promising solution to protect future computer networks and machines in the era of quantum computing. Unlike QKD, which relies on quantum mechanical properties for symmetric key distribution, PQC encompasses a family of asymmetric key schemes (public-key cryptography) that are secure against both classical and quantum attacks. As an example, Amazon has introduced a hybrid KYBER mode for its AWS Key Management Service [9], demonstrating the adoption of PQC in cloud environments for key security.

Critical Infrastructures (CI) and Industrial Control Systems (ICS) are highly vulnerable to cyberattacks, with the potential for massive economic and social losses [5]. The transition to post-quantum cryptography in these environments is crucial [5].

The implementation of post-quantum cryptography (PQC) and quantum key distribution (QKD) is essential to secure future communications against the threat of fault-tolerant quantum computers [5]. Both technologies are considered the most promising for future quantum-secure cryptography [5].

## Materials and Methods

This study conducted systematic mapping, with manual collection of secondary data between May and July 2025. The data sources included the Quantum Insider platform, technical reports, institutional websites, and public documents from companies, research centers, and governmental initiatives.

A sample was prospected, consisting of organizations with identified activities in technologies based on PQC and/or QKD. The selection was based on public evidence of development, products, or technological applications. The variables considered for analysis were: country of origin, type of organization, adopted technology, implementation approach (software, hardware, or both), application sector, and use cases.

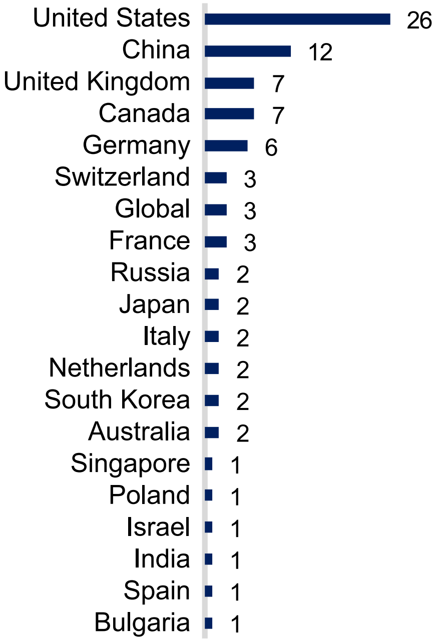
The data were organized and tabulated in a Microsoft Excel spreadsheet and subjected to descriptive analysis using relative frequency, with the aim of characterizing the global quantum security ecosystem.

## Results and Discussion

The data collection and analysis enabled the identification of 85 active initiatives involving technologies based on PQC and/or QKD. Figure 1 presents the geographical distribution of the mapped organizations.

The United States leads with 26 organizations (30.59%), followed by China with 12 (14.12%), forming a technological polarization axis that

**Figure 1.** Geographical distribution.



reflects the centrality of quantum security in digital sovereignty and industrial competitiveness agendas. The distributed presence in other countries demonstrates that, while concentrated, the technological race is already expanding to various markets and economic blocs.

The predominance of the private sector is highlighted in Figure 2. Fifty-four established companies and 18 startups account for 84.7% of the initiatives. This corporate leadership is complemented by 9 research centers, 3 cooperative initiatives, and 1 governmental body, forming a network that combines corporate innovation, academic research, and collaborative efforts.

This hybrid structure is typical of emerging technological fields [6,7], where knowledge transfer occurs through continuous interactions among universities, companies, governments, and society, enabling rapid translation of research into commercial applications.

Figure 3 indicates that 65.88% of solutions adopt hybrid hardware and software approaches, followed by 31.76% exclusively in software and 2.35% solely in hardware. The predominance of hybrid models signals a pursuit of flexibility, scalability, and robustness—essential attributes for integration into complex digital environments and for ensuring security against multiple attack vectors.

The sectoral analysis (Figure 4) shows that telecommunications concentrate the highest number of initiatives (31 organizations), followed by cloud computing (17), finance and government (16), IoT/automation (8), blockchain/fintech (7), and digital identity (6). This distribution highlights the prioritization of sectors critical to digital infrastructure and services.

The use cases underscore the maturity and strategic relevance of these technologies:

(i) IoT and Automation: Infineon integrates PQC into chips to secure data in smart factories, autonomous vehicles, and connected homes, ensuring resilience even in resource-constrained devices.

(ii) Telecommunications Networks: Toshiba, in partnership with BT, operates an urban quantum network in London, protecting financial, governmental, and healthcare communications, including satellite-based transmissions.

(iii) Finance and Government: ID Quantique secures transactions and governmental communi--cations on Orange's fiber network (France), complying with regulations such as GDPR.

(iv) Blockchain and Fintech: CryptoNext applies PQC to strengthen smart contracts and digital wallets, preventing quantum attacks and enhancing trust in decentralized platforms.

**Figure 3.** Type of technological implementation.

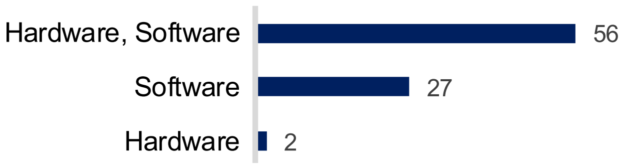


**Figure 2.** Organizational profile.

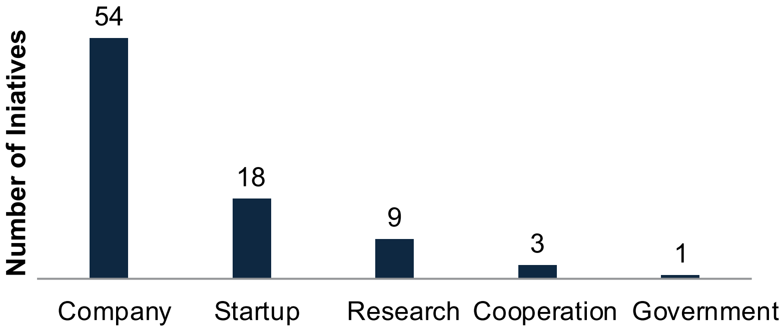
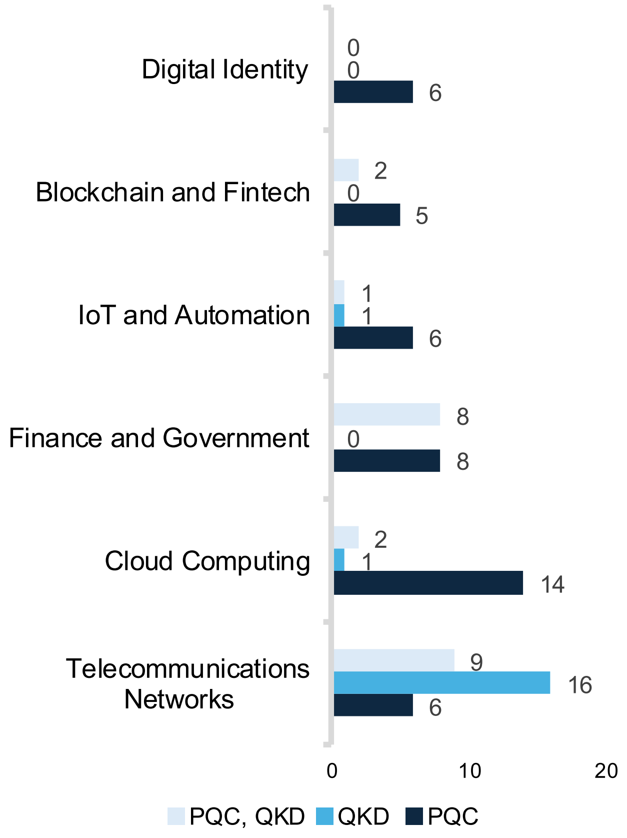


**Figure 4.** Sectoral applications.



(v) Cloud Computing: Microsoft incorporates PQC into Azure with Post-Quantum TLS and researches QKD for secure networks, protecting sensitive data in scalable environments.

(vi) Digital Identity: DigiCert provides quantum-resistant certificates, used by Panasonic in India, and combats deepfakes with signed metadata for secure authentication.

In this context, the results reveal a global ecosystem concentrated in strategic hubs, with corporate leadership and hybrid solutions targeting critical sectors. PQC and QKD are advancing toward commercial maturity, becoming essential for secure communication and digital sovereignty.

## Conclusion

This study revealed the maturity and strategic impact of PQC/QKD within a dynamic global ecosystem, with 85 mapped organizations, led by technological hubs such as the United States (30.59%) and China (14.12%). The predominance of hybrid solutions (65.88%) and the strong presence of the private sector (72 organizations) highlight the pursuit of flexibility and innovation in response to the threats posed by quantum computing. Additionally, they demonstrate maturity in critical sectors, with practical applications led by companies such as Infineon, Toshiba, ID Quantique, CryptoNext, Microsoft, and DigiCert, addressing specific demands in areas such as 5G network protection, cloud security, digital authentication, and decentralized financial transactions. These advancements reinforce quantum security as a cornerstone for resilient digital infrastructures, aligned with regulatory requirements and technological sovereignty.

## References

1. P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," Proceedings 35th Annual Symposium on Foundations of Computer Science, 1994.
2. NIST, “Post-Quantum Cryptography Standardization,” [Online]. Available: https://csrc.nist.gov/projects/post-quantum- cryptography
3. V. Scarani et al., “The security of practical quantum key distribution,” Rev. Mod. Phys., vol. 81, no. 3, pp. 1301–1350, 2009.
4. Y. Zhang et al., “Continuous-variable quantum key distribution system: past, present, and future,” arXiv preprint arXiv:2310.04831, 2023.
5. Del Moral JO et al. Cybersecurity in critica l infrastructures: A post-quantum cryptography perspective. IEEE Internet of Things Journal, v. 11, n. 18, p. 30217-30244, 2024.
6. Cai Y et al. Triple helix or quadruple helix: which model of innovation to choose for empirical studies?. Minerva, v. 60, n. 2, p. 257-280, 2022.
7. Roman M, Fellnhofer K. Facilitating the participation of civil society in regional planning: Implementing quadruple helix model in Finnish regions. Land use policy, v. 112, p. 105864, 2022.
8. Dias MA et al. Distribuição quântica de chaves com modulação não gaussiana: protocolos, desempenho e segurança. 2023.
9. BAavdekar R et al. Post quantum cryptography: Techniques, challenges, standardization, and directions for future research. arXiv preprint arXiv:2202.02826, 2022.