Journal of the Spanish Institute for Strategic Studies
ISSN-e: 2255-3479

Iván Soto Maciá
Computer engineer and Master in Intelligence. Expert in cybersecurity, strategy and foresight

Mail: adventt@protonmail.com

Quantum key distribution and its geopolitical impact

Abstract

Over the next few years, information security will face one of the most significant challenges in the history of modern cryptography, a profound change in the rules of the game: the advent of quantum computers. Positioning oneself before the problem of quantum key distribution will prove vital for the major global powers of our century. The United States and China represent the two prevailing positions: while the U.S. is cautiously skeptical, China has made a determined bid. The article explores the most relevant reasons behind one approach and the other, the challenges presented by the technology, the expectations for resolution and the main scientific advances. We then present the most important practical implementations to date, the strategy behind them and how the various players intend to project their vision of the future of secure communications. A future favorable to their interests.

Keywords

Quantum communications, quantum computing, supremacy, security, confidentiality, availability, resilience.

Cite this article:

Soto Maciá, I. (2025). Quantum key distribution and its geopolitical impact. *Journal of the Spanish Institute for Strategic Studies*. 25, pp. 501-520.

1 Introduction

It is safe to say that, with the advancement of quantum computing, over the next few years we will witness a significant and profound paradigm shift in secure communication protocols. One that will require adaptation time, great effort and investment, and a clear vision of the future. The outcome for the major geopolitical powers in the decades to come will depend on how accurate their foresight is, how they build that vision, how much effort they foresee necessary, and how well the various players prepare themselves.

Compared to classical computers, quantum computers offer exponentially faster resolution of mathematically complex problems and will therefore mean the end of the currently predominant algorithms in asymmetric cryptography (e.g. Diffie-Hellman key exchange, RSA or elliptic curve algorithms). In other words, they will force a rethinking of the current protocols for key exchange and asymmetric digital signature. The academic consensus is that it is not a question of whether or not it will be possible, but when. In other words, we are facing a fundamentally engineering challenge.

In view of this situation, efforts seem to be focused on the development of post-quantum cryptography, or *quantum-resistant* cryptography, with NIST leading the way in proposing new standards [1]. Since these cryptographic algorithms are designed for execution on classical computers, the problems to be overcome have to do with the increase in the demand for computational capacity, time consumed in communications and adoption/adaptation times by the actors involved.

This article, however, focuses on a potentially complementary line, quantum key distribution (QKD). First proposed in the work of G. Brassard and Charles H. Bennett between 1979 [2] and 1984 [3], and implemented by DARPA in 2002, QKD uses the fundamental properties of quantum mechanics to generate truly random keys of variable length[1] , and what is more relevant, to guarantee security (mainly confidentiality and integrity) in the distribution of cryptographic keys. It is this anchoring in fundamental properties that allows us to aspire to overcome not only present problems, but also definitely future ones, redefining de facto how we understand information security.

Although technological and economic barriers currently limit its large-scale implementation, the continued development of specific *hardware* could significantly reduce costs in the future, positioning it as a reliable and widespread solution, at least in the *backbone* of critical networks. We are, as in the case of quantum computers, facing a surmountable engineering problem.

1 The importance of quantum key generation, truly random and of sufficient length to implement ciphers such as OTP or one-time passbook, is not the subject of this article, although it should be considered as a further advantage of adopting QKD.

This article aims to explore the importance of QKD, the development and implementation efforts of major geopolitical powers, its potential to address quantum threats, and how future innovations could generalize its adoption.

2 Context and protocols

2.1 Context

Cryptography has historically been the mainstay of information security. In the digital age, modern cryptography guarantees the fundamental principles of secure communication: confidentiality, integrity and authenticity of messages. And this, in turn, is essential to maintaining our way of life. From e-commerce and banking to the security of military command and control communications, everything is based on modern cryptographic techniques.

These protocols are mostly based on symmetric encryption, which requires a prior exchange of keys. This key distribution problem is at the heart of the article, and the best solution we can offer today is asymmetric or public key cryptography.

As mentioned in the introduction, asymmetric cryptography bases its strength on mathematically complex problems, such as the factorization of prime numbers or the calculation of discrete logarithms, considered intractable for classical computers. However, quantum computers, whose distinctive feature is that they base their computation on elementary properties of matter, represent more than a mere leap in processing capacity, they represent a paradigm shift in algorithmic and programming possibilities. New and more efficient ways of tackling problems. Algorithms such as Shor's [4], designed specifically for these architectures, will be able to solve these hitherto intractable problems in minutes, rendering all current key distribution systems instantly obsolete.

Compared to the widely cited post-quantum cryptographic schemes published by NIST in 2024 (one of them allows key distribution or KEM [1]), QKD is a more disruptive solution, risky, but with the potential to go further, to be definitive.

What makes QKD unique is that it does not rely on mathematical algorithms, but on fundamental physical principles, so that, a priori, its validity will be independent of advances in computer theory. By using quantum particles as photons, QKD guarantees that any attempt to intercept the key to be shared (which will later be used in the symmetric encryption), i.e. any attempt to obtain information about the key, will alter it and will consequently be detectable: in the quantum world it is not possible to observe without leaving a trace.

Although this approach has many advantages, the West did not seem, to date, to bet on it, and signals intelligence agencies highlighted the problems and challenges presented by QKD in various publications [5]. These limitations have been widely discussed, highlighting for relevance, in my opinion: (i) the problem of source authentication (ii) the high cost of the necessary *hardware* (iii) the technical limitations

of current quantum networks, and (iv) denial of service problems. Nevertheless, the state of the art is advancing daily, and the investments of large states, primarily China, are evidence of what is at stake. At the same time, little by little, the West seems to be joining the race.

The history of technology shows that what we have previously referred to as engineering problems tend to become trivial over time. When that fog dissipates, what we will have on the table is a possible final solution to the problem of key generation and distribution.

2.2 Protocols

The QKD family of protocols is now more than 40 years old since the first standardizations, so publications about them, their mode of operation and underlying principles are numerous [6].

Thus, we do not intend to go into technical details at this point, but it is worth noting that they all share many common points. We will start from the need for the sender and receiver (by convention, Alice and Bob) to share a secret key that they will later use to encrypt symmetrically. For all QKD protocols accepted as standard, two phases are required: (i) the quantum transmission phase, where the sender and receiver send and/or measure quantum states, and (ii) the post-processing phase, where the secure key is generated.

In addition, in QKD protocols two channels are necessary, a quantum channel and a classical channel where the message exchange process takes place once the secret key has been agreed upon.

Based on these common points, we will distinguish two families of QKD protocols:

2.2.1 Based on a quantum transmitter-receiver channel (commonly known as "prepare and measure")

Those channels in which the transmission of the key is initiated by a photon beam encoded by the polarization method. In the reading, crystalline filters will be applied at which, similar to sunglasses, will filter or not the photon depending on its polarization. Thus, we highlight the following protocols:

– BB84: In 1984 the aforementioned G. Brassard and Charles H. Bennett proposed the first Quantum Key Distribution protocol, known as BB84 after their surnames and the year of its publication. Besides being the first, the rest of the "prepare and measure" protocols are variations of BB84 and are therefore applied in the same circumstances, and are subject to the same advantages and limitations.

The quantum transmission phase consists basically in that, starting from two polarization bases, rectilinear[2] and diagonal[3] , Alice will send the coded bits of the secret key choosing, for each one of them, one of the bases randomly. Bob, in turn, will measure the photons received by applying, likewise, one of the two bases, also randomly.

In the post-processing phase, Alice and Bob publicly share the bases they have used. Thus, in those bits where they have used the same base, the reading will be correct and will become part of the key, while those bits where the base of the sender and receiver differ will be discarded. Any attempt to obtain information from the quantum channel by a third party will modify the polarization of the photons, generating measurement errors by Bob, and consequently errors in the secret key generated. In such a case, Alice and Bob abort the communication.

– B92: published by Charles Bennett in 1992, it is a variant of the previous one in which the emitter uses only two non-orthogonal polarization states.

– SARG04: another variant of BB84, very similar, but especially robust against *photon-number splitting* attacks, which especially affect BB84 and B92.

2.2.2 Based on quantum entanglement

They base their operation on a different principle than the family of protocols derived from BB84: quantum entanglement. In the QKD domain, quantum entanglement means that, in the case of two entangled particles, any measurement applied to one of them instantaneously affects the state of the other. Thus, the particles are perfectly correlated, and it is possible to achieve directional synchronization in observations. This is true regardless of the distance between the entangled particles. However, it is impossible to predict before the measurement which state will be observed, so it is not possible to communicate across entangled particles without discussing the observations through a classical channel. We highlight the protocols:

– BBM92 and E91: published respectively by Charles Bennett, Gilles Brassard and David Mermin in '92; and Artur Ekert in '91. In these cases, there must be a reliable source emitting the entangled photons to Alice and Bob, as part of the quantum channel.

As we will see later in the case of the most important quantum network deployed to date, the Chinese network, both types of protocols have practical application, with protocols of the BB84 family being the most common in metropolitan and intercity (terrestrial) *backbones*, and protocols of the BBM92 and E91 family being used for global satellite communication.

2 It corresponds to measure the vertical component of the spin, with states 0 and 1.

3 Corresponds to measuring the horizontal component of the spin, with + and - states.

3 Challenges and resolution expectations

Any emerging technology faces a number of challenges that hinder its large-scale implementation. These problems, in my opinion, are not insurmountable, but require a coordinated effort from the scientific community, industry and governments, something that sounds unfeasible in today's race dynamics.

3.1 Source authentication

This is pointed out because it appears, recurrently, as one of the major problems of QKD, but it is not, in fact, a problem as such, but an essential limitation. In this sense, it is a false debate. QKD is a solution, as its name suggests, to the problem of key distribution (and, collaterally, to the problem of random key generation), not an "integral" cryptographic solution. It will continue to require support for the source authentication process (i.e. preloaded keys, or future post-quantum asymmetric cryptography), just as it will continue to require classical channels for the transmission of the message itself, via traditional symmetric cryptography.

It should be noted, however, that we are talking about the initial authentication of the source in a point-to-point channel (with little probability of third party intervention), since, once the first secret key has been generated and distributed, it can replace the preloaded keys and serve to authenticate the parties (and continue to update the process with each new key generated and distributed).

3.2 Hardware dependence

This is where we can find more encouraging prospects in the near future.

Regarding the cost of the *hardware*, it is true that to implement QKD requires specialized *hardware*, such as single photon sources, advanced detectors and dedicated fiber optic networks. Such equipment, besides being expensive, is not yet produced on a large scale, which makes it inaccessible for private initiative. This is even more pressing in the case of quantum satellite-based networks.

However, the history of technology has taught us that, over time, costs tend to decrease as advances in manufacturing occur and demand increases. In the case of QKD, miniaturization of components and production of more affordable *hardware* will be key factors. Integrated photonics technologies, for example, promise to significantly reduce cost by enabling many essential QKD components to be manufactured in an integrated fashion.

As for the *hardware* binding of QKD, i.e., the impossibility of emulating fundamental physical principles through *software*, this is a problem that, although it will persist, much progress can be made in mitigating it. In this regard, for example, the advances in *Device-independent Quantum Key Distribution* (DI-QKD), which

promises some decoupling from concrete *hardware* specifications [7], relaxing the need to physically model specific parameters, are noteworthy. Based on the Ekert 91 protocol, and dependent on high quality entanglement, several proofs of concept have been offered over the last few years. If it continues to advance, it could be a solution, collaterally, to all attacks exploiting technical vulnerabilities associated with currently operational QKD equipment.

3.3 Technical limitations

Another major challenge is the limitation in the distance that QKD networks can cover. In optical fibers (the prevalent medium in inter-city networks) the photons carrying the information attenuate rapidly, causing the signal to lose strength after a few hundred kilometers. Although satellites have proven to be effective in overcoming this problem, their use is still experimental and extremely costly, so their mass adoption still faces significant barriers.

In this regard, one of the most promising solutions to overcome distance limitations are quantum repeaters. These devices, still under research, act like a regular signal repeater: they allow quantum signals to be retransmitted without losing their integrity. Although this technology is not yet ready for commercial deployment, the advances in this field are rapid and could have a major impact on the distribution distance.

Another technical limitation is the difficulty of integrating the QKD infrastructure into existing or *Legacy* infrastructures. As mentioned above, QKD requires completely new protocols and equipment, which complicates its adoption in an environment already stressed enough in the adaptation and implementation of post-quantum cryptography. This poses a dilemma for businesses and governments and is the likely cause of the prioritization of investments in post-quantum cryptography over QKD in the Western sphere.

In this regard, the focus is on the development of interoperability standards. QKD protocols, by definition, need to be interoperable with classical encryption protocols (they rely on classical symmetric encryption channels), but there is still a lot of work to be done on what is outside the QKD scope, such as channel authentication or digital signature protocols.

This is undoubtedly the area in which the third player in discord, Europe, can lead the way, as it continues to be a benchmark in any aspect related to standardization. The efforts of the European Committee for Standardization (CEN) and Electronic Standardization (CENELEC) in the field of quantum technology are particularly relevant. With regard to QKD, the role of the European Telecommunications Standards Institute (ETSI) and its working group dedicated to QKD standardization (ETSI ISG-QKD), or the International Telecommunications Union (ITU), which published in 2020 the standard *Overview on networks supporting quantum key distribution.* However, due to the maturity of the field, QKD has not yet gone through a rigorous standardization process, such as the one already referenced and carried out by NIST for post-quantum cryptography. It is yet to be determined who will be the hegemonic player in this regard.

3.4 Denial of service problems

The road to a resilient QKD is not going to be a simple one. As we have pointed out, the security of QKD lies in the impossibility of obtaining information about the distributed key without modifying it, and consequently generating measurement errors between the original sender and receiver (Alice and Bob). For this reason, it is relatively easy to carry out attacks that do not seek to decrypt the key, but rather to disrupt or degrade the system, making it inoperable or extremely slow. In critical systems, these denial-of-service (DoS) attacks often have a critical impact, and availability is often as important (sometimes more so) as confidentiality.

DoS attacks on QKD systems can take different forms. By saturating the quantum channel, an attacker floods the channel with unwanted signals, e.g. additional photons. This causes an increase in the quantum error rate (QBER) and Alice and Bob to constantly discard the generated keys, delaying or interrupting the exchange. Detector overload consists of sending pulses of light of higher intensity than expected, physically damaging this particularly sensitive equipment [8]. Finally, we have already mentioned that a communication involving QKD ultimately depends on a classical channel, so it is still susceptible to any attack on it, although these vulnerabilities are obviously not attributable to QKD technologies.

As specific solutions, it is worth highlighting the implementation of advanced optical filters for blocking unwanted signals before they reach the detectors, configured with Alice's feature pattern (although this makes the channel even more specific to a particular transmitter and receiver). However, the default response of these optical filters is to disconnect the channel, which prevents damage to the detectors, but in no way solves the original DoS target.

Faced with these types of attacks, building resilience, increasing physical protection and providing duplicity (alternative routes) when necessary, is even more relevant than in classic infrastructures, where practically all routes, distribution elements and protocols are interoperable. In addition, these alternative routes must be managed in real time and by virtue of quantum observations and the constancy of a DoS attack on them. In that sense, one of the most promising lines of research is the one that aims to incorporate the traditional management of *software-defined* networking[4] (SDN) to QKD protocols [9]. By incorporating the QKD optical network components as part of the SDN abstraction and management layer, and by establishing constant monitoring of QBER and secret key generation rate (SKR), it is possible to detect service degradations and quickly identify alternative routes to avoid or mitigate the effect of the DoS attack. All this, in much shorter times than those obtained by direct management of the QKD infrastructure. Ultimately, however, we are only dealing

4 IBM describes *software-defined* networking as an approach in which *software* is used to create and operate a series of virtual overlay networks that work in conjunction with an underlying physical network. SDNs provide the potential to minimize the hands-on time required to manage the network.

with the efficient construction and management of alternative routes and operational resilience.

Consequently, and for the time being, we can conclude that QKD channels are more exposed to DoS attacks than classical channels, and none of the current mitigation measures seem to be able to solve this point. Supporting the physical properties of particles takes its toll; what we gain in confidentiality in the channel, we must be willing to give up in availability. Alternatively, invest more in building resilience into an already expensive infrastructure.

Distribución de claves mediante criptografía postcuántica frente a la distribución cuántica de claves

Característica	Criptografía postcuántica	Distribución cuántica de claves
Principio de funcionamiento	Algoritmos criptográficos basados en problemas matemáticos resistentes a ataques cuánticos	Propiedades fundamentales de la mecánica cuántica para garantizar la seguridad
Dependencia de *hardware* especializado	No presenta dependencias, y puede ejecutarse en infraestructuras digitales clásicas	Sí, requiere de equipos cuánticos especializados, aún no producidos a gran escala y de alto coste
Limitaciones técnicas	Moderadas, requiere análisis de interoperabilidad de protocolos dependientes de criptografía clásica	Relevantes, limitaciones asociadas a la distancia de distribución de claves por atenuación de la señal, y a la interoperabilidad con infraestructura clásica
Resiliencia	Ninguna debilidad intrínseca	Altamente vulnerable a ataques de denegación de servicio
Madurez tecnológica	Alta, con estándares publicados para el intercambio de claves (FIPS 203, ML-KEM) que han sido incluidos en paquetes de funciones criptográficas (OpenSSL 3.5, desde abril de 2025)	Baja, aún en desarrollo y con despliegues experimentales
Escalabilidad	Alta, fácilmente implementable en redes actuales	Baja a media, limitada por distancia, atenuación y necesidad de repetidores cuánticos
Complejidad y coste de implementación	Moderada, requiere de actualización de protocolos y *software/hardware,* pero no rediseño físico	Alta, requiere de nueva infraestructura física cuántica
Latencia y rendimiento	El proceso de intercambio de claves es rápido, a pesar de que las claves son del orden de 10 veces el tamaño de una clave clásica	Más lento que la criptografía postcuántica, depende del canal cuántico y el protocolo de intercambio
Detección de intrusión	No, protección basada en complejidad matemática	Sí, detección inherente

Figure 1. Source: own elaboration

4 Geopolitical positioning

4.1 Who is ahead in the quantum race?

With regard to the positioning of the major powers in quantum technology (QSI, which stands for *Quantum Information Science*, a concept that encompasses both quantum communications and quantum computing, among others), a superficial

analysis would force us to conclude that China is in the lead. By any quantitative metric, the distance is significant compared to its closest rival, the United States. However, as in quantum physics, the reading is not so trivial:

– Investment volume: if one thing can be said, it is that the major powers, particularly China an7d the United States, are devoting considerable efforts to QSI, although there are marked differences. For China, leadership in QSI is a far-reaching strategic issue, and this is reflected in its thirteenth (2016-2020) and fourteenth (2021-2025) five-year plans. Backing up its assertion with figures, it claims to have invested more than 15 trillion US dollars to date (2023), compared to the US estimate of 3.8 trillion [10] over the same period. However, it is difficult to pinpoint the true extent of China's investment due to the traditional opacity of its government spending. Some reports suggest that actual spending may be lower, reflecting a common pattern in which ambitious funding targets are not always fully met.

  Regardless of the details and based on empirical evidence, or, in other words, on the quantum infrastructures deployed on the ground, there is no doubt that Chinese investment is significantly higher than that of the United States, Europe, Japan, etc.

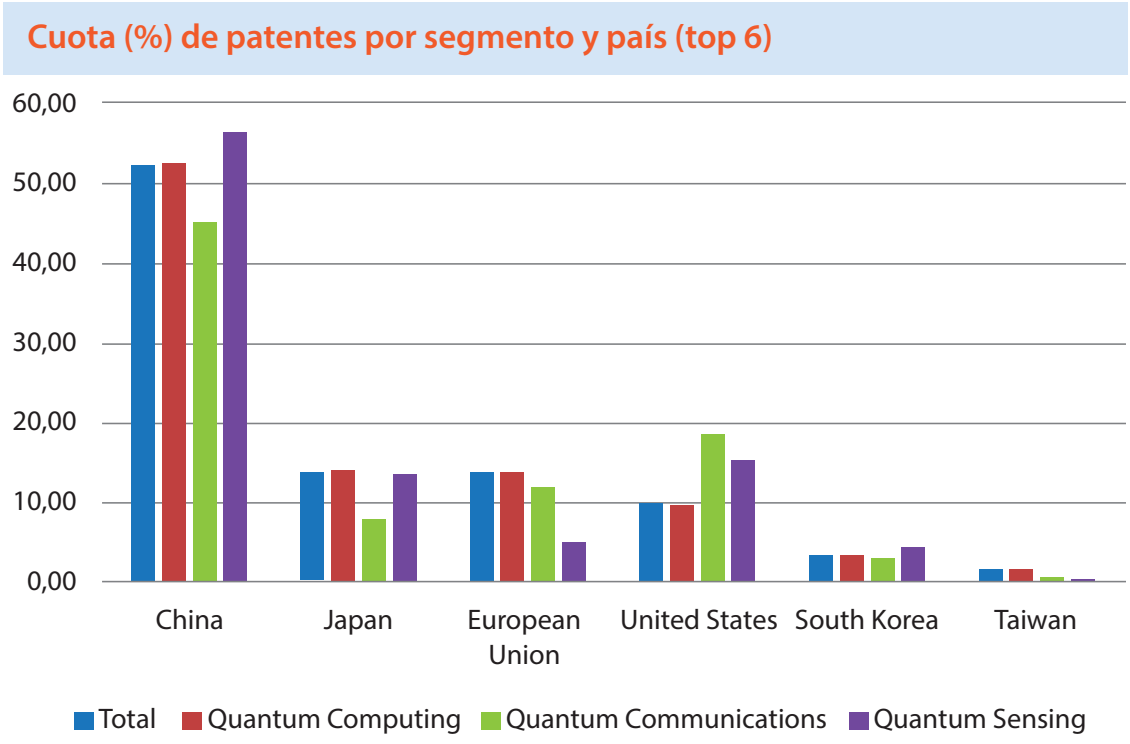

Figure 2. Source: McKinsey & Company Quantum Monitor 2023 [11]

– Nature of the investment: following the usual pattern, Chinese investment is fundamentally public, and the decision criterion is based on a single source, the party (which will prove to be relevant when determining the strategy). Of the entire Chinese business fabric, only 14 companies have contributed significantly, according to the criterion of patents and publications (Huawei,

Alibaba, QuantumCTek or Ruban Quantum Technology stand out, although the state participation in these companies casts doubt on the qualification of private investment). This contrasts sharply with the United States, where investment is mainly private in nature (driven by IBM, Google, Microsoft and Intel). In terms of *start-ups*, U.S. investment is 10 times higher than Chinese investment [10].

– Patents: if we look at the number of domestic patents, China stands out with a much higher volume than the United States [11]. The patent typology reflects the Chinese focus on communications, particularly QKD, as we will see in later sections. The United States, however, leads in the number of international patents [10], underscoring its vocation to set standards beyond its borders. In the case of China, the nature of research and knowledge sharing is asymmetric, closed to the outside.

– Publications: again, China significantly leads the ranking of publications [10]. It is usual, in other technological fields such as Artificial Intelligence, to mention that quantity is not quality, and in terms of quality (citations, references, *H-index*) and impact, the United States remains ahead. This is not the case for QSI, where the quality of Chinese publications is also (slightly) ahead of the US. Again, the distribution of QSI publications by type shows that the Chinese strategy is different from that of the US, which will be discussed below.

4.2 Different strategies for quantum supremacy

The truth is that, based on the criteria mentioned above (investment, nature of the investment, publications and patents), it can be seen that the strategy of the two major powers is markedly different.

Let us take as a starting point a taxonomy of the most promising QSI fields of study that differentiates between quantum computing, quantum communications and sensor/sensor technology. For all the above criteria, the Chinese leadership is overwhelming in quantum communications [10], [11] and [12], in sensing the situation is even, while in quantum computing, the United States leads by a wide margin.

As an illustrative example, in terms of publications associated with quantum communication (mainly QKD), China leads with 38% overall, compared to 12.5% for the United States, with an H-index of 48 vs. 43. In the case of quantum computing, the volume of publications is similar (23% Chinese share vs. 21% US), but the US H-index is much higher (52 Chinese vs. 92 US).

In terms of international patents, during the period 2016-2021, China published 3,601 patents in quantum communication compared to 551 for the United States, while in relation to quantum computing the situation is the opposite, with 1,408 patents by China and 2,509 by the United States [12].

China's determination to lead in quantum technology by 2035 is strong and a central part of Xi Jinping's plan to improve the country's competitiveness. What is an anomaly is that, unlike other players (not all), research and deployment of quantum communications infrastructure remains a priority within its medium- and long-term strategy. In this regard, no one has been as ambitious as the Chinese.

4.3 QKD, state of the art

China has established itself as the undisputed leader in QKD, both in terms of investment and practical implementation, in a bet that can already be considered long-standing: since 2008, long before the tangible reflection in the five-year plans, the statements of physicists such as Chen Zengbing [13] pointed in that direction. But, perhaps, the big boost at the investment level came in 2013, after the Snowden leaks, which generated a great impact and sense of insecurity in the politburo.

China's plan involves building a QKD network covering the major communication *backbones*, applying different technologies depending on capillarity [14]. Fundamentally:

- Quantum communication in metropolitan *backbones* using optical fiber and miniaturized receiver emitters.
- Quantum communication in intercity *backbones* where quantum repeaters would play a key role.
- Global quantum communication, between different inter-city *backbones* via satellite relay.

They reached the first milestone, urban quantum communication between 2011 and 2013, when the Hefei and Jinan metropolitan networks were fully operational. These were followed by the Beijing and Shanghai metropolitan networks, and finally, they reached the second milestone: since 2017, the world's largest terrestrial QKD network can be considered functional, with an extension of more than 2,000 kilometers on the main *backbone*, linking Beijing, Jinan, Hefei and Shanghai.

Regarding the third milestone, a global quantum communication, its most significant breakthrough was the launch of the first quantum satellite, "Micius", in 2016, which enabled the first QKD transmissions on a global scale: i.e. QKD transmissions capable of distributing keys between, for example, Asia and Europe. With this, China was showing that another global network, a quantum internet, was possible. A first step beyond local and inter-city networks. "Micius" was followed in 2022 by a second satellite, "Jinan-1", with a remarkable degree of miniaturization and two to three times faster in key generation. The period between 2025 and 2027 will be key, with the planned launch of several low- and medium-Earth orbit satellites, which will complement the functions of the previous ones [15].

In other words, the commitment to achieve a complete QKD (*satellite-to-ground*) network will be maintained over time. Currently, the combination of the 3 levels

mentioned above, i.e., from "Micius" to the nodes of the Beijing-Shanghai *backbone*, already allows the distribution of keys in communications over 4,600 km [16].

Clearly the network is not fully autonomous. To achieve point-to-point communication, it still requires access and distribution layers based on traditional technologies, and it was never intended to be otherwise. It is a matter of protecting sensitive communications between the most relevant nodes in the network. The remaining steps to achieve secure point-to-point communication will depend on the confidentiality of the communication: the first beneficiaries of the quantum communications network will be the military and government agencies, extending later to critical sectors of the economy, such as the financial sector, which is intensive in the use of highly sensitive communications.

China's leadership in QKD gives it a key strategic advantage in security and communications. This capability allows China to secure its critical networks (currently military, government and financial) against possible future quantum computing attacks, something that few other countries can claim. Moreover, its ability to export quantum infrastructure to other countries could consolidate its geopolitical influence, especially in the Digital Silk Road arena.

The state of the art is clear: China leads the advances in QKD and maintains a solid position in the rest of the fields; while the United States focuses its efforts on quantum computing and sensing, and in cryptography, mainly on post-quantum cryptography.

In QKD, most global players are a step ahead of the United States. Among the most noteworthy developments are:

– Europe (with the EuroQCI project [17]), has as its declared goal the construction of a secure quantum communication infrastructure that will cover the entire EU, including its overseas territories. Like many other countries, the starting point is also the construction of a *backbone* linking government institutions and critical infrastructures, complementing the traditional network (which will continue to provide the greatest capillarity and reach). This goal is ambitious, and the scheduled timelines show commitment and foresight, but also the usual EU slowness. 2019 was the program launch year and the initiatives related to the terrestrial segment kicked off in 2023 and those associated with the space segment will do so with the launch of the first satellite scheduled for 2025/2026.

  The infrastructure will have a set of main nodes (i.e. Madrid, Vienna, Berlin and Poznan) and, from these, branches to the other member countries. Although these links currently go no further than proofs of concept, the degree of progress within of the main nodes is remarkable. Particularly Madrid, whose metropolitan quantum network (MadQCI) is the largest in Europe, and in constant growth since 2009. It currently has 26 QKD modules in 9 nodes, connected by 110 kilometers of optical fiber. For its management, MadQCI uses SDN, a growing option due to, among other advantages, those already mentioned in this article regarding management, administration and resilience

building. Its development is the result of a public-private collaboration initiative, with contributions from the Polytechnic University of Madrid, Huawei and Toshiba, among others.

- The United Kingdom, for its part, has followed a path very similar to that of continental Europe. The London metropolitan network has been operational since 2022 [18]. In this case, although backed by the government, the initiative is fundamentally private, with BT and Toshiba leading the way, and unlike other quantum networks it could be considered the first "commercial" network, given that, since it went into production, it has been open to the integration of any paying customer, whether or not it is a critical infrastructure for the state. Since then, the metropolitan network has grown, integrating customers such as HSBC [19], with connections between data centers over distances of up to 62 kilometers.
- Japan is perhaps the country where the private initiative in QKD is the strongest. Toshiba and NEC are the first and third companies by number of international QKD patents, with NTT, Fujitsu and Hitachi also as relevant players. Tokyo has, since 2010 [20], its own metropolitan QKD network, and it is expected that, by 2035, the quantum network will have been extended to the rest of the country, constituting a nationwide network. Arguably, apart from China, they are the first to face practical implementation problems, which has led them to rethink and even "rebuild" their networks on several occasions. On the other hand, the influence of their companies at the international level is prevalent (for example, Toshiba's involvement in European networks).
- South Korea, with private companies such as Swiss ID Quantique[5] , SK Telecom, LG, and public initiatives such as ETRI at the forefront, has deployed the second largest quantum network in the world, after China. It is a nationwide QKD *backbone*, connecting 48 government departments over more than 800 kilometers of fiber [21]. In its sights is to convert the network, in the near future, into a commercial service (in the same sense as the United Kingdom), allowing the entry of private companies in "Quantum as a Service" mode, i.e., leasing the service. Likewise, and without decommissioning the current quantum network (based on quantum transmitter-receiver channels), 2025 should be the year in which the first 100 kilometers of network operated with entanglement-based protocols are added.
- India has metropolitan networks, such as Delhi, of approximately 200 kilometers. Over the past few years, it has taken a more aggressive and militaristic approach to its QKD deployment, channeling most projects through the *Innovations for Defence Excellence* (iDEX) initiative [22].

5 Founded in 2001 as a *spin-off* from the University of Geneva, it is considered the first company to commercialize QKD products (since 2007), and collaborated, together with the University of Geneva, in the first European deployments, proofs of concept and experimental QKD networks in the first decade of the 21st century.

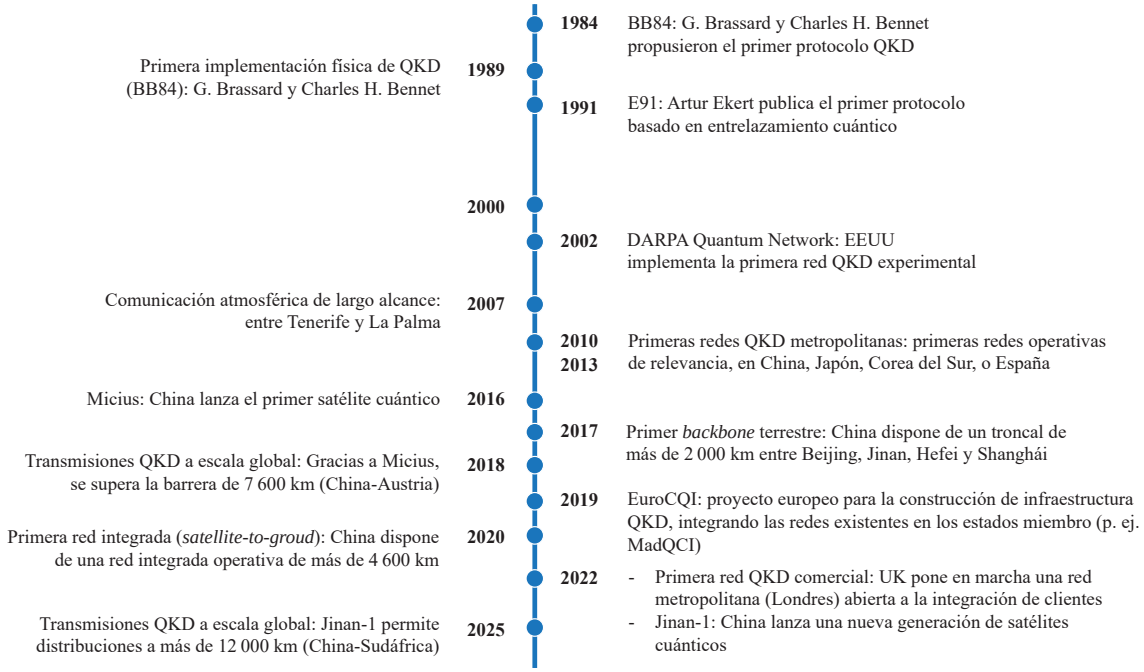

Figure 3. Most relevant milestones in the article. Source: own elaboration

4.4 QKD, two strikingly different approaches

Faced with this situation, as we have already mentioned, the position of the U.S. government is summarized in the official position of the NSA [5]:

> "In summary, NSA views quantum-resistant (or post-quantum) cryptography as a more cost effective and easily maintained solution than quantum key distribution. For all of these reasons, NSA does not support the usage of QKD or QC to protect communications (...)".

This contrasts sharply with what is happening in the field, in academia. Although the level of QKD infrastructure deployment in the United States is modest (comparatively speaking), and the same could be said of the volume of publications and patents, those advances that make it into the media are scientifically notorious and show that they have not lagged behind in terms of research. For example, in May 2024, a joint initiative of Harvard University and Amazon succeeded in transmitting interlaced photons in 35-kilometer networks [23] (in the same sense that South Korea intends to do in 2025). It remains to be resolved whether the apparent misalignment between the position of the US government and that of its academic and private sectors, which may not be interested in the present QKD (which would explain the volume of patents and publications), but are interested in its future possibilities, is real.

It could be argued, however, that the United States plays in a different light, being a strong advocate of NATO's favorable stance on QKD [24]. We therefore consider that the US position is best described as "cautious skepticism".

Notwithstanding the above nuances, this divergence in the analysis of the future of QKD has aroused the curiosity of many analysts. Why is China investing such

large amounts of money in the deployment of QKD infrastructure, while the United States, at least in its public statements, considers the technology a dead end? There are more than a few who point out that The U.S., in this case, has been overly prescriptive in its stance, and a similar approach to the Korean one would have been more prudent. They have bet big that QKD will have no future practical application, or even a relevant place in a future post-quantum communications infrastructure.

In certain areas, such as military communications, availability (remember the DoS problem in QKD) is as important as confidentiality. Perhaps this is why investments in military communications disruption are steadily increasing in the U.S. sphere. They are fully confident that the denial problem is insurmountable.

5 The future of QKD

The development of QKD is already transforming geopolitical dynamics, marking a new era in the competition for national sovereignty and the security of critical communications. If QKD becomes established as a standard, the powers that master this technology will not only secure their own communications, but will also have the ability to influence the global communications infrastructure, redefining alliances and the balance of power in the 21st century.

The future of QKD is also intrinsically linked to the possibilities of developing a "quantum internet", a network that uses the properties of quantum mechanics to transmit information in a way that is not only secure (an aspect in which QKD would be key), but also efficient and comparatively superior to the classical internet by orders of magnitude that are difficult to anticipate. This opens the door to new forms of distributed and ultra-fast computing and would have an evident reflection in those processes in which the intensive use of computing capacity is fundamental: the example that comes to mind is that of Artificial Intelligence.

Whether the scenario described above materializes will depend on multiple factors, which could be summarized in the capacity of the scientific community to overcome the challenges currently presented by the field.

On the one hand, what we have called engineering issues. On the one hand, the integration of the QKD infrastructure with the traditional infrastructure, which will ensure that quantum communication becomes more than just point-to-point communication on a set of relevant *backbones*, leaving the rest of the network vulnerable, will be critical. Day by day, researchers push the attenuation limit, increasing the distances over which QKD communication is possible. Another focus of progress is the development of more efficient protocols, such as MDI-QKD, which eliminates the need for so many reliable measurement elements.

On the other hand, problems that can only be mitigated, such as denial of service. The success of the practical implementation of QKD will depend, to a large extent, on how well it is mitigated.

The pace of scientific progress (measured, for example, in number of patents or publications), the quality of such progress, the evolution in the investment of the different States, or the commitment in the deployment of costly infrastructure by practically all relevant actors reveals the thinking of their decision-makers in this regard: QKD will be an important piece in the era of post-quantum computing, and for some actors, the fundamental piece.

6 Conclusion

There is a widespread sense of urgency in governments to push quantum initiatives, confident that quantum supremacy will provide a differential advantage in the fields of computing, sensing and communications. And this is as much as to say an essential strategic advantage.

What makes quantum communication particularly interesting is the fact that there is no consensus on the subject. In contrast to other research fields such as Artificial Intelligence or quantum computing itself, where there are no major differences of opinion regarding the need to master them, and the career dynamics are fully established, in the case of, for example, QKD, we find two differentiated positions between the two most significant global players, China and the United States.

Inevitably and depending on how the next few years/decades play out, these unhedged bets will mark a different future for both players and, consequently, deserve special attention and monitoring.

Regardless of the quality of the research centers, in the case of a technology such as QKD, which requires the deployment of massive, high-cost infrastructure, there is no such thing as a *fast-follower*. If QKD ultimately proves to be a critical piece of the post-quantum landscape, the United States will be at a distinct disadvantage, with a long way to go in terms of investment and time if it is to catch up. To give up on QKD's present is to tacitly give up on its future.

In this future scenario, the imbalance in its adoption will foreseeably generate ethical and geopolitical consequences. China, with years of monopoly ahead of it, will control a significant part of the global flow of secure information, while the rest of the players will be vulnerable to interception.

Beyond this first interpretation, this mismatch could redefine the global map in other, more subtle ways. China will be in a position to export quantum infrastructure to other countries, and more importantly, to offer its strategic allies access to its quantum network as an incentive, displacing traditional Western technological supremacy and allowing them to manipulate, de facto, whatever information their allies can process. Countries in the Global South, in search of digital sovereignty, could be strongly attracted by this possibility, provided it is offered at the right cost. From an ethical point of view, the monopoly of quantum communication could give rise to a new form of technological colonialism, where China could extend its authoritarian model beyond its borders, controlling and manipulating information according to its interests.

All these factors would have the potential to consolidate its geopolitical influence based on technology, its *sharp power*, and this influence would prove to be key to imposing performance and interoperability standards that would, in turn, cement more years of leadership in quantum communications. This virtuous circle is something that we in the West have experienced with classical computing and is extremely difficult to destabilize. A paradigm shift such as quantum communication offers that possibility, and it is vital to get the strategy right.

References

Alferov, S. V., Bugai, K. E. y Pargachev, I. A. (2022). Study of the Vulnerability of Neutral Optical Filters Used in Quantum Key Distribution Systems against Laser Damage Attack. *JETP Letters*. 116, pp. 123-127. [Accessed: 2025]. Available at: https://doi.org/10.1134/S0021364022601117

Bennett, C. y Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*. 560, pp. 175-179. [Accessed: 2025]. Available at: https://doi.org/10.48550/arXiv.2003.06557

Brassard, G. (2005). Brief history of quantum cryptography: a personal perspective. *IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security*. Awaji, pp. 19-23. DOI: 10.1109/ITWTPI.2005.1543949.

Chen, Y. A., Zhang, Q., Chen, T. Y. *et al.* (2021). An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature*. 589, pp. 214-219.

Comisión Europea. (s. f.). Iniciativa sobre la Infraestructura Europea de Comunicación Cuántica (EuroQCI). [Accessed: 2025]. Available at: https://digital-strategy.ec.europa.eu/es/policies/european-quantum-communication-infrastructure-euroqci

EQIC. (2024). A Portrait of the Global Patent Landscape in Quantum Technologies. European Quantum Industry Consortium. [Accessed: 3 enero 2025]. Available at: https://www.euroquic.org/wp-content/uploads/2024/03/QuIC-White-Paper-IPT-January-2024.pdf

Express Defence. (2024). Indian Army signs quantum key distribution contract under iDEX. *Financial Express*. [Accessed: 2025]. Available at: https://www.financialexpress.com/business/defence-indian-army-signs-quantum-key-distribution-contract-under-idex-3627043/

HSBC. (2023). HSBC becomes first bank to join the UK's pioneering commercial quantum secure metro network. *HSBC*. [Accessed: 2025]. Available at: https://www.hsbc.com/news-and-views/news/media-releases/2023/hsbc-becomes-first-bank-to-join-the-uks-pioneering-commercial-quantum-secure-metro-network

Hugues-Salas, E. *et al.* (2018). Experimental Demonstration of DDoS Mitigation over a Quantum Key Distribution (QKD) Network Using Software Defined

Networking (SDN). *Optical Fiber Communications Conference and Exposition (OFC)*. San Diego, pp. 1-3.

IDQ. (2022). IDQ and SK Broadband complete phase one of nation-wide Korean QKD Network. *IDQ*. [Accessed: 2025]. Available at: https://www.idquantique.com/idq-and-sk-broadband-complete-phase-one-of-nation-wide-korean-qkd-network/

Jones, A. (2024). China to launch new quantum communications satellites in 2025. *SpaceNews*. [Accessed: 3 enero 2025]. Available at: https://spacenews.com/china-to-launch-new-quantum-communications-satellites-in-2025/

Lord, A., Woodward, R., Murai, S., Sato, H., Dynes, J., Wright, P., White, C., Davey, R., Wilkinson, M., Clinton-Tarestad, P., Hawkins, I., Farrington, K. y Shields, A. (2023). London Quantum-Secured Metro Network. *Optical Fiber Communication Conference (OFC)*. Optica Publishing Group, paper W4K.4.

McKinsey & Company. (2023). Quantum technology patent share from 2000 to 2022, by segment and country [Graph]. *Statista*. [Accessed: 3 enero 2025]. Available at: https://www.statista.com/statistics/1318009/quantum-technology-patent-share-segment-country/

National Security Agency. (2025). Post-Quantum Cybersecurity Resources, Quantum key distribution and quantum key cryptography. National Security Agency. [Accessed: 2025]. Available at: https://www.nsa.gov/Cybersecurity/Post-Quantum-Cybersecurity-Resources/

NATO. (s. f.). Quantum Technologies and the Science for Peace and Security Programme. NATO. [Accessed: 2025]. Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/2023/11/pdf/231130-SPS-Quantum-1487-23.pdf

NIST. (s. f.). Post-Quantum Cryptography, Computer Security Resource Center. NIST. [Accessed: 2025]. Available at: https://www.nist.gov/pqcrypto

Omaar, H. y Makaryan, M. (2024). How Innovative Is China in Quantum? *ITIF*. [Accessed: 5 enero 2025]. Available at: https://itif.org/publications/2024/09/09/how-innovative-is-china-in-quantum/

Qi, C. (2024). China's Quantum Ambitions: A Multi-Decade Focus on Quantum Communications. *Yale Journal of International Affairs*. [Accessed: 3 enero 2025]. Available at: https://www.yalejournal.org/publications/chinas-quantum-ambitions

Sabani, M., Savvas, I., Poulakis, D. y Makris, G. (2023). Quantum Key Distribution: Basic Protocols and Threats. *Proceedings of the 26th Pan-Hellenic Conference on Informatics (PCI '22)*. Nueva York, Association for Computing Machinery, pp. 383-388. [Accessed: 2025]. Available at: https://doi.org/10.1145/3575879.3576022

Sasaki, M. *et al.* (2011). Field test of quantum key distribution in the Tokyo QKD Network. *Opt. Express*. 19(11), pp. 10387-10409.

Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. *Proceedings 35th Annual Symposium on Foundations of Computer Science*. Santa Fe, pp. 124-134. DOI:10.1109/sfcs.1994.365700.

Xi, G. (2008). Interview with Chen Zengbing of the University of Science and Technology of China: Interpretation of Quantum Communication That 'Will Not Be Stolen. *Beijing Science and Technology Daily*.

Zapatero, V., Leent, Tim van, Arnon-Friedman, R. *et al*. (2023). Advances in device-independent quantum key distribution. *npj Quantum Information*. 9, p. 10. [Accessed: 2025]. Available at: https://doi.org/10.1038/s41534-023-00684-x

Zhang, M. (2024). Harvard Researchers and Amazon Collaborate to Launch Boston's First Quantum Network. *The Harvard Crimson*. [Accessed: 2025]. Available at: https://www.thecrimson.com/article/2024/5/28/quantum-network-boston-cambridge/

Article received: January 8, 2025
Article accepted: June 4, 2025