

QUANTUM COMMUNICATION

Market applications

June 2025

MARKET APPLICATIONS REPORT

UNDERSTANDING
CONCRETE APPLICATIONS
OF KEY TRENDS &
TECHNOLOGIES



Funded by
the European Union



Agenda

01

Market size

A data-driven analysis of the current market size of quantum communication in Europe and worldwide, including projected growth and the present market share of active industry participants.

02

Market opportunities

Classification of the potential of quantum communication for companies by sectors through a heat map*.

03

Use cases

Real-world applications of quantum communication, showcasing its effectiveness, implementation scenarios, and outcomes.

04

Conclusion

05

Sources

*Scope & methodology

The heat map was developed to illustrate the potential impact of quantum technologies across various industry sectors. The sectors were identified based on a review of relevant literature and expert sources.

The opportunity level for each sector, categorized as low, medium, or high, was determined using qualitative criteria.

Specifically, the assessment considered how significantly each sector is expected to benefit from quantum technologies in the future. Two main factors guided this evaluation: the nature of the sector's core activities and their alignment with quantum capabilities and the critical importance of securing the data and information handled within the sector.

Quantum communication

Market size in Europe and the world

The **quantum communication market** refers to the segment of quantum technologies focused on enabling ultra-secure data transmission using the principles of quantum mechanics, particularly through **quantum key distribution (QKD)**.

What is the situation in Europe?

The **European quantum communication market** was valued at roughly **\$314 million in 2024** and is projected to grow at a robust **CAGR of ~31%**, reaching approximately **\$1.5 billion by 2030** ([source](#)). Germany is expected to lead regional growth, buoyed by national projects like the **QTF-Backbone**, which aims to build a dedicated fibre-based quantum and timing network over the next decade ([source](#)).

Europe is building a **continental quantum communication infrastructure** through the [EuroQCI initiative](#), launched with all 27 EU member states. Supported by programmes like **Digital Europe** and the **Connecting Europe Facility**, this initiative seeks to link critical institutions such as datacentres, hospitals and energy grids using quantum-secured channels.

European key metrics

According to [Horizon Grand View Research](#), the European quantum communication market generated a revenue of \$314M in 2024. It is expected to reach \$1,502M by 2030. A compound annual growth rate of 31.3% is expected from 2025 to 2030.



\$314.4M

Revenue in 2024



\$1,502.6M

Forecast revenue 2030



31.3%

CAGR 2025-2030

And on a worldwide level?

Worldwide key metrics

According to [McKinsey Digital](#).



\$0.9-1B

Revenue in 2023



\$10.5-14.9B

Forecast revenue 2035



23-25%

CAGR 2025-2035

The global quantum communication market is gathering pace as a strategic priority for national security and cybersecurity worldwide. **North America** currently leads with a +/-30% market share in 2024 ([source](#)). **China** remains the leader in **satellite-based QKD**, deploying major systems like the Micius satellite and integrated terrestrial networks ([source](#)).

Market-wide, revenues are projected to grow from around **\$0.9–1.1 billion** in 2023 to **\$10.5–14.9 billion by 2035** (CAGRs 23–25%), driven by national security demand, finance sector adoption and advances in photonic technologies.

Quantum Communication

Heat map of market opportunities

The heat map presented below offers a classification of quantum technologies' potential value by sectors. The other quantum technologies, computing and sensing, are presented for comparison purposes, as the focus of this report is quantum communication.

How to read this map?

As explained in our fact sheet on quantum communication (see our resources on our Knowledge Hub), the major potential of quantum communication lies in its ability to fundamentally secure our communications and data. The sectors most impacted will therefore be the ones that handles sensitive data.

<i>Quantum - 2025</i>				
	COMPUTING	COMMUNICATION	SENSING	
Application sectors	Banking, finance & insurance	High	High	Low
	Defence & government	Medium	High	High
	Telecom & IT	High	High	Medium
	Healthtech	High	Medium	High
	Energy & materials	Medium	Medium	High
	Transport & logistics	Medium	Medium	High
	Manufacturing	Medium	Low	Medium
	Space	Medium	Medium	High

High
 Medium
 Low

03

Use cases

In banking, finance & insurance

Quantum communication is set to revolutionise the banking, finance and insurance sectors by addressing one of their most critical challenges: **data security**. As quantum computers advance, traditional encryption methods are becoming increasingly vulnerable to being broken, exposing sensitive financial data and transactions to significant cyber risks.

Quantum communication, particularly through quantum key distribution, offers **unprecedented security**, for attacks happening now, but also for future attacks that quantum computers will make possible, and through that, ensures that **customer confidence remains**.

Key technologies:



- Quantum key distribution
- Quantum random number generators
- Quantum networks

Key applications:

- Secure interbank transactions:** QKD can be used to protect high-value or time-critical transactions between banks, ensuring confidentiality and integrity
- Fraud prevention and credit card security:** Quantum encryption can be applied to credit card data, dramatically reducing the risk of identity theft and fraud
- Two-factor authentication:** QKD can provide one-time passwords dispensed securely to mobile devices, improving authentication for online and in-person transactions
- Risk management and regulatory compliance:** Quantum-secure communication helps institutions comply with stringent data protection regulations and manage operational risks associated with data breaches

Concrete example: QKD by HSBC

A prominent example is [HSBC](#), which has successfully trialed QKD to secure a €30 million trading scenario involving the exchange of euros for US dollars, by integrating QKD into its infrastructure.

And in Luxembourg?

The [INT-UQKD](#) project has established a terrestrial quantum key distribution (QKD) link between Luxembourg and Belgium ([Virgule](#)), specifically targeting use cases in regulated sectors with high security needs, most notably financial institutions in Luxembourg.

03

Use cases

In defence & government

Quantum communication is transformative for defence and government because these sectors require the highest levels of security for sensitive data, military operations and critical infrastructure. With the advent of quantum computers, traditional encryption methods are at risk of being broken, exposing classified communications and national secrets. Quantum communication provides **provably secure communication channels**, ensuring that any interception attempt is detectable and renders the information unusable. This technology offers **unbreakable security** and **resilience against future threats**.

Key technologies:



- Quantum key distribution
- Quantum networks
- (Quantum sensing and quantum cryptography)

Key applications:

- Secure classified communications:** QKD and quantum networks protect government and military data exchanges, ensuring confidentiality for everything from diplomatic cables to battlefield coordination
- Satellite and space-based communications:** Quantum satellites enable secure links between distant facilities, embassies or deployed units, overcoming terrestrial distance limitations
- Critical infrastructure protection:** Quantum communication safeguards vital systems from quantum-enabled cyberattacks

Concrete example: Altice Labs

In 2025, [Altice Labs](#) successfully demonstrated a quantum-secure network for military applications as part of the DISCRETION project (Disruptive SDN Secure Communications for European Defence).

A key component of the technology having allowed this secure communication is QKD, which offers unprecedented levels of protection.

And in Luxembourg?

Luxembourg is a key participant in the EuroQCI initiative, which aims to build a [pan-European quantum communication](#) network for government and defence.

03 Use cases




In telecom & IT

Quantum communication is poised to fundamentally transform the telecom and IT sectors by introducing **ultra-secure data transmission**, enabling the next generation of **network optimisation** and laying the groundwork for the **quantum internet**.




As quantum computers threaten classical cryptography, telecom operators must adopt quantum-safe solutions to protect their infrastructure and customer data. Quantum communication also promises operational efficiencies, smarter networks and new service models, such as Quantum-as-a-Service.

Key technologies:



-  Quantum key distribution
-  Quantum networks
-  Quantum random number generators

Key applications:

-  **Securing backbone and edge networks:** QKD and quantum cryptography protect sensitive data traversing national and international telecom infrastructures
-  **Quantum cloud services (QCaaS):** Telecom operators offer quantum resources via the cloud, enabling customers to run advanced computations on demand
-  **Quantum-enhanced datacentres:** Integration of quantum communication in datacentres for secure, high-speed data transfer and processing

Concrete example: Toshiba's world-first trial

In April 2025, [Toshiba](#) announced the success of its world-trial quantum communication technology. Quantum communication was deployed to standard telecoms infrastructure using semiconductors instead of complex cryptogenic components, paving the way for broader adoption.

Moreover, [NordVPN](#) is already proposing a post-quantum encryption VPN for enhanced cybersecurity.

And in Luxembourg?


POST Luxembourg participates in the EuroQCI initiative, aiming to deploy QKD-secured links for telecoms and IT networks.



The startup [LuxQuantum](#) is working on a solution for the compatibility between traditional and quantum cybersecurity tools.

03 Use cases

In healthtech

Quantum communication is set to transform the healthtech sector by providing **unprecedented security for sensitive medical data**, enabling **advanced diagnostics** and supporting the **digital transformation of healthcare**.

Key technologies: 


-  Quantum key distribution
-  Quantum random number generators


Key applications:

-  **Secure electronic health records:** QKD and quantum cryptography protect patient records
-  **Telemedicine and remote monitoring:** Quantum-secured channels ensure privacy during virtual consultations and real-time patient monitoring, even in rural or remote areas
-  **Collaborative research:** Quantum-secured networks facilitate data sharing between healthcare institutions, supporting collaborative diagnosis and drug discovery



In energy & materials

Quantum communication will enhance the **security and efficiency of systems**. Quantum technologies prevents cyberattacks that could disrupt energy supply and enables advanced **optimisation and simulation**, directly contributing to energy savings and reduced emissions.

Key technologies: 

-  Quantum key distribution


Key applications:


-  **Smart grid management:** QC secures and optimises smart grid operations, reducing losses and enabling efficient integration of renewables
-  **Greenhouse gas monitoring:** Quantum networks support secure, real-time data collection for emissions tracking and regulatory compliance

03 Use cases

In transport & logistics

Transport and logistics are complex, involving vast networks and dynamic scheduling. Quantum communication and quantum computing promise to help this sector by enabling **ultra-secure data exchange** and **real-time optimisation of routes and resources**.

Key technologies: 


-  Quantum key distribution




Key applications:

-  **Secure supply chain communications:** QKD secures communications between manufacturers, suppliers and logistics providers, reducing the risk of data breaches and counterfeit goods
-  **Autonomous and connected vehicles:** Quantum communication facilitates secure, real-time coordination between autonomous vehicles, improving traffic flow and safety




In space

Space communications is vulnerable to interception and attacks due to the long distances. Quantum communication enables fundamentally **secure data transmission**, **improves navigation** and supports the **next generation of satellite networks**.

Key technologies: 

-  Quantum key distribution
-  Quantum clock synchronisation
-  Quantum entanglement distribution

Key applications:

-  **Secure satellite communications:** QKD protects command, control and data links for commercial, scientific and defence satellites, preventing interception and spoofing
-  **Inter-satellite quantum networks:** Quantum links between satellites enable secure, global data relay and distributed quantum computing in space
-  **Secure earth observation:** Quantum communication ensures the integrity and confidentiality of sensitive Earth observation data

The quantum communication market is accelerating rapidly, driven by growing concern over **the security of data and the threat posed by future quantum computers to classical cryptography**. Europe is investing robustly, with market revenue expected to grow from €314 million in 2024 to €1.5 billion by 2030, at an estimated compound annual growth rate (CAGR) of 31%. **Key projects like EuroQCI are establishing secure quantum networks** for governments, finance, defence, and telecoms, solidifying the strategic importance of quantum communication infrastructure across the continent.

Quantum key distribution (QKD) is the market's cornerstone technology, offering unprecedented levels of security for sectors where data confidentiality is paramount, including banking, insurance, defence, healthtech, energy, and transport. Real-world demonstrations, such as HSBC's use of QKD in finance, quantum-secure military networks in Europe, and Toshiba's successful telecom trials, underscore the technology's readiness and competitive advantage.

In Luxembourg, participation in the EuroQCI initiative, and pioneering efforts such as the INT-UQKD project signal a commitment to building quantum-secure infrastructure for critical sectors and positioning the nation as a digital sovereignty leader.

In conclusion, quantum communication is evolving from experimental deployments to mature, sector-wide adoption. The market's growth is propelled by operational needs for ultra-secure data transmission, regulatory compliance, and future-proofing against quantum-era threats. The next decade should see quantum-secure networks transition from strategic pilots into the backbone of Europe's and Luxembourg's confidentiality, resilience, and competitiveness in the digital age.

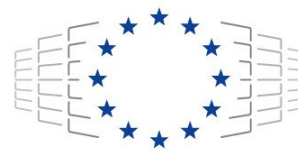
Explore [our Technologies at a Glance report](#) on our knowledge hub for more insights on the technology.

Quantum technologies

- [CSIS](#), “Quantum Technology: Applications and Implications”, May 2023
- [Quantum Flagship](#), “Quantum Technologies in a nutshell”
- [IBM](#), “What is quantum computing?”
- [Innovation News Network](#), “Why quantum computing is advancing rapidly – but adoption remains slow”, June 2025
- [Techtarget](#), “9 quantum computing challenges IT leaders should know”, April 2025
- [IBM](#), “What is quantum cryptography?”
- [Fortune Business Insights](#), “Quantum Cryptography Market”, June 2025
- [McKinsey Digital](#), “Quantum sensing: Poised to realize immense potential in many sectors”

Quantum communication

- [McKinsey Digital](#), “Quantum Communication: Trends and outlook”, February 2025
- [McKinsey Digital](#), “Quantum communication growth drivers: Cybersecurity and quantum computing”, February 2025
- [MIT Technology Review](#), “What is quantum communication?”, February 2019
- [Restena.lu](#), “Luxembourg Experimental Network for Quantum Communication Infrastructure (LuxQCI)”
- [Nasa](#), “Quantum Communication 101”
- [The Business Research Company](#), “Quantum Communication Global Market Report 2025”
- [BBG.com](#), “Are you ready for Quantum Communications?”, March 2023
- [Market Research Future](#), “Quantum Communication Companies”
- [Markets and Markets](#), “Quantum Communication Market”, November 2024
- [Grand View Research](#), “Quantum Communication Market Summary”
- [Quside](#), “Quantum Random Number Generator (QRNG) Everything You Need to Know”



EuroHPC
Joint Undertaking

EuroCC 2 has received funding from the European High-Performance Computing Joint Undertaking (JU) under grant agreement No 101191697. The JU receives support from the European Union's Digital Europe Programme and Germany, Bulgaria, Austria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Greece, Hungary, Ireland, Italy, Lithuania, Latvia, Poland, Portugal, Romania, Slovenia, Spain, Sweden, France, Netherlands, Belgium, Luxembourg, Slovakia, Norway, Iceland.

LUXINNOVATION MARKET APPLICATIONS REPORT

Discover more insightful content at www.luxinnovation.lu/knowledge-hub

Luxinnovation knowledge digest contributors

Research & writing: Tiffany Devresse

Analysis support: Samira Bouzid

Editing & review: Sara Bouchon, Lena Mårtensson



LUXINNOVATION
#MakingInnovationHappen