axonpartnersgroup.com

The Quantum Internet:
For the good of all?

Understanding the benefits.
Facing the challenges.
Managing the risks.

June 2024

Authors

Álvaro García
SENIOR MANAGER

Pablo Cámara
ASSOCIATE

Ignacio Ampuero
ASSOCIATE

AXON
CONSULTING

Contents

1.
Introduction

We are standing on the brink of a technological revolution. The quantum internet promises to transform data transmission and cybersecurity – and how we think about both.

But what exactly is the quantum internet – and the quantum technology from which it derives? How does it differ from our current digital infrastructure? And what new doors will it open? More importantly, as this technology becomes more widespread, how will it affect our existing security protocols?

This white paper begins by examining the emergence of the quantum internet. It analyses the situation today, the limitations of current technology, and whether, as many people believe, the quantum internet could overcome those limitations.

Looking much further ahead, this paper explores the potential future applications of this technology, and the hurdles that may need to be overcome to make them a reality. How, for instance, can long-distance data transmission be managed? And how will we ensure the integrity and reliability of information?

Finally, there is the question of cybersecurity. The cybersecurity potential of the quantum internet is, potentially, vast – but so are the risks. What challenges must be overcome to unlock this potential? What are the main risks associated with the development and implementation of quantum internet technology?

In short, how do we raise awareness and prepare people for an internet that can accomplish tasks unachievable today?

Let’s find out.

2.
Quantum internet: the basics

2.1.
The limitations of current technology

The world is moving towards an era of total interconnectivity. Can the current internet manage this? Once a revolutionary concept, today's internet faces structural and technological challenges that limit its ability to adapt to the escalating demands of the digital future. These challenges affect everything and everyone – from individuals to global operations. They include:

Security and privacy
Cryptography systems underpin internet security. They are under constant threat. Current algorithms, though robust, might eventually be inadequate to counter emerging threats, particularly with new hacking techniques and significant advances in computing capabilities on the horizon.

Data transmission capacity and speed
There has been an exponential increase in data production and the number of connected devices. This will continue. Limited capacity and latency could result – especially in areas with insufficient infrastructure. Both can compromise user experience and operational efficiency.

Figure 1: Limitations of the current internet [Source: Axon]

Scalability
The centralised structure of many internet networks creates bottlenecks that can hinder the expansion needed to support the growing number of users and devices. Networks should be able to accommodate new technologies and higher traffic loads. This isn't always the case.

Interoperability
This is a technologically diverse world. Different systems and applications must be able to work together efficiently. Differences in communications standards can limit interoperability. This in turn undermines the full functionality of global internet networks.

Energy consumption
Data centres and global network infrastructure require a significant amount of energy. Energy demand will grow with data volume. The search for ways to reduce energy consumption is becoming increasingly urgent.

Figure 1: Limitations of the current internet [Source: Axon]

Internet infrastructure and technology need to keep pace with these demands. It's not clear that they can. Could quantum internet be the answer? Before we respond to that question, let's look at how the quantum internet came into being.

2.2.
Understanding quantum concepts

The quantum internet is not unprecedented. It is based on a series of existing concepts and rules, many of which describe the behaviour of nature at and below the scale of atoms.

Starting small: quantum mechanics

The world we see around us obeys the laws of classical physics. But the microscopic realm of atoms and electrons plays by a very different set of rules. These rules are known as quantum mechanics.[1]

At the heart of the quantum internet are the basic units of quantum information; they are known as qubits. Unlike classical bits, which are either '0' or '1', qubits can exist in both states simultaneously due to a principle known as superposition. This unique ability allows them to hold more information than classical bits. It's not an easy concept to understand but a highly simplified way of looking at it is to imagine a coin spinning in the air; it's neither heads nor tails until it lands. It could even be said to be both. Qubits are similar, representing multiple possibilities at once.

At the heart of the quantum internet are the basic units of quantum information: they are known as qubits

1 "Quantum Internet, The Internet's next big step ", https://filelist.tudelft.nl/Websections/Vision teams/Quantum computing/quantum magazine june 2019.pdf

But qubits are just the start. The following concepts are also essential for exploring the working mechanisms of the quantum internet[2]:

- **Superposition principle:** In quantum mechanics, objects can exist in multiple states at the same time – this is called superposition. For example, a qubit, which is the basic unit of quantum computing, can be both '0' and '1' at the same time, which is a bit like being in two places at once

- **Quantum measurements:** Measuring a quantum state, like checking the position of our spinning coin, causes it to "collapse" into a specific state. Once the state of a qubit is measured (for example as "0"), it remains in that state. Thus the measurement not only reveals the state, but also fixes it.

- **Quantum entanglement:** This is where things get even stranger... If two qubits are entangled (very roughly, a form of interaction), knowing the state of one instantly tells you the state of the other, no matter how far apart they are, we can say they are 'maximally entangled'. It's like having two dice that, when rolled, always land on matching numbers, even if one is in New York and the other in Tokyo.

  Entanglement has two important features relevant to quantum networks:

  - **Entangled states are highly correlated.** Even though the outcomes of measurements seem random, if you compare the results from two entangled qubits, you will find they always match up. This coordination happens regardless of how far apart the qubits are.

  - **Entanglement cannot be shared with a third party.** According to the laws of quantum mechanics, if two qubits are what is known as 'maximally entangled', a third qubit cannot be equally entangled with either of them.[3]

2 "Quantum Internet: Networking Challenges in Distributed Quantum Computing", https://arxiv.org/pdf/1810.08421v1

Besides the concepts directly linked to qubits, there are additional fundamental principles crucial to understanding quantum mechanics:

- **No-cloning theorem:** Unlike classical information, which can be copied easily, the no-cloning theorem in quantum mechanics says it's impossible to make an exact copy of an unknown quantum state. This implies that qubits cannot be copied and any attempt to do so can be detected, due to the measurement principle. This principle is crucial for secure communications, as it means that any interference is detectable.[3]

- **Quantum teleportation:** Quantum teleportation is a fascinating process that allows the instantaneous transfer of quantum information from a sender to a distant receiver without moving the physical system in which it is encoded. For this to occur, the two parties must have established a classical communication link and share a maximally entangled state. This integration of classical and quantum resources is essential for the functionality of quantum networks. During teleportation, the quantum state disappears at the original location and reappears at another, without physically traversing the space between them. Importantly, the original quantum state is destroyed during this process, ensuring that the information cannot be duplicated or intercepted without detection. This mechanism highlights the unique non-cloning property of quantum information and represents a new –and important – way in which information might be transmitted in future quantum networks.[4]

Quantum teleportation is a fascinating process that allows instantaneous transfer of quantum information

3 "Quantum NETwork: from theory to practice", https://ar5iv.labs.arxiv.org/html/2212.01226

4 "Quantum internet The internet's next big step", https://filelist.tudelft.nl/Websections/Vision teams/Quantum computing/quantum magazine june 2019.pdf

AXON CONSULTING

2.3.
What is the quantum internet?

The (related) concept of quantum computing emerges from applying fundamental quantum mechanics principles to modern computation. Classical computers operate with bits, which, again, are simple switches that can be either '0' or '1'. In contrast, as we have seen, quantum computers use qubits, which can be both '0' and '1' simultaneously thanks to quantum superposition. This means quantum computers can harness the unique properties of quantum mechanics, enabling them to process information in fundamentally different ways from traditional computing. Simply put, this ability allows quantum computers to tackle complex problems relatively quickly – even, it has been argued, problems that today's most advanced supercomputers would need decades to solve.

The computational power of quantum computers depends on the number of qubits they can process. It increases exponentially with each high-quality qubit added. However, building a quantum computer with many interacting qubits is a formidable technological challenge.

To address these limitations, a practical solution has been developed: linking multiple smaller-scale quantum computers through a network. This approach would amplify the combined computational power of these interconnected quantum computers far beyond what each could achieve alone. The name of this network? The quantum internet.

...even an early-stage quantum internet with just a few qubits can provide security superior to the classical internet

The quantum internet can be enabled using current technology. However, this network of quantum computers would still rely on the classical internet infrastructure for operational purposes because it utilises its devices. Despite this dependency, even an early-stage quantum internet with just a few qubits can provide security superior to the classical internet.

The, as yet unrealised, vision for the quantum internet is a globally interconnected network of quantum computers, enhancing the way we send, receive and compute information using the unique advantages of quantum technology. Its purpose is to facilitate applications that are beyond the capabilities of the classical internet, supplementing or even supplanting today's internet. In fact, using the quantum features we have described, the quantum internet could significantly enhance information-processing capabilities, boost transmission security, ensure precise information synchronisation, and accomplish tasks unattainable in classical networks.

In particular, the development of a fully-fledged quantum internet is expected to support a wide range of exciting applications, such as quantum key distribution (QKD). QKD is a cryptographic protocol that uses the principles of quantum mechanics to create a shared, unbreakable key, a feature unachievable with classical internet technology.

Thus a quantum internet will complement the existing classical internet infrastructure. However, it will require additional quantum components to support new applications and services. These components mainly consist of various types of quantum nodes and the communication links connecting them. These nodes and links, illustrated in Figure 2, are:

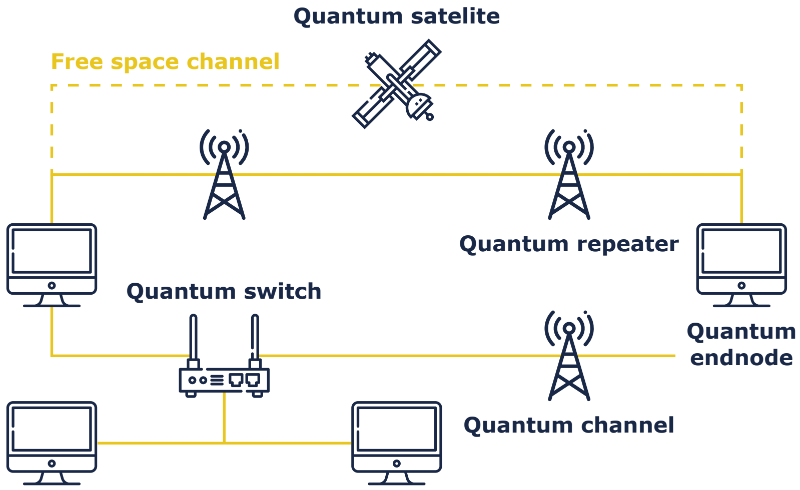

Figure 2: Quantum internet infrastructure components [Source: Axon]

- **Quantum channels:** These are the physical connections that allow qubits to move between nodes. Unlike regular network channels that transmit classical messages, quantum channels specifically handle the transmission of quantum information. Telecom fibers, already used for regular data transmission, can also serve as quantum channels under certain conditions .

- **Quantum repeater:** In quantum networks, unlike classical networks where signals can be copied and amplified, the no-cloning theorem prevents qubits from being duplicated. Therefore, for long-distance communication, quantum repeaters are employed. These devices use entangled photon pairs to extend the transmission distance of qubits – or, rather, they will. Fully functioning models are not yet a reality.[5]

5 "Quantum repeaters: From quantum networks to the quantum internet", https://ar5iv.labs.arxiv.org/html/2212.10820

- **Quantum end node:** A quantum end node acts as a user or client that sends or receives quantum information, or as a cloud server providing quantum computing services. These nodes typically handle service requests. While the quantum internet enhances classical communication with quantum capabilities, it requires nodes to also support classical communication (through the regular internet, for example), for exchanging control information.[5]

- **Quantum switch/router:** Like a switch in classical internet networks, a quantum switch facilitates connections within quantum networks by linking multiple users and managing multipartite quantum connections.[6]

- **Quantum satellite:** While ground-based quantum repeaters can extend communication distances to a few thousand kilometers, creating a truly global quantum internet will require the use of quantum satellites and space-based links. In space, photon paths mostly run through a vacuum, resulting in significantly less photon loss and quantum decoherence6 (the loss of information from a system into the environment).

While ground quantum repeaters can extend communication distances to a few thousand kilometers, creating a truly global quantum internet will require the use of quantum satellites and space-based links

As mentioned earlier, the quantum internet is expected to greatly improve on the current internet in areas like cryptography, computing, and sensing. Of course we can't predict all its uses. However, we have identified several key applications, which we will discuss in the next section.

5 "Quantum repeaters: From quantum networks to the quantum internet", https://ar5iv.labs.arxiv.org/html/2212.10820

6 "The quantum internet, explained", https://news.uchicago.edu/explainer/quantum-internet-explained

3.
What will the quantum internet do?

The fully formed quantum internet is still some way off. However, there are already several beneficial applications relevant to the quantum internet in use or in development. These applications demonstrate the potential of quantum internet technologies, not only in improving communication, but also in areas such as computing, sensing, and fundamental scientific research. Current and developing applications include:

Figure 3: Current applications of quantum internet [Source: Axon]

- **Ultra-secure communications:** Leveraging quantum key distribution (QKD), the quantum internet could provide a level of communication security that would be, theoretically, unbreakable. The inherent properties of quantum mechanics ensure that any interception attempt would alter the transmitted information, thereby exposing the presence of an eavesdropper.

- **Quantum cloud computing:** By connecting multiple quantum computers, the quantum internet could facilitate remote access to the power of quantum computing. Users could then perform complex calculations requiring high computational power remotely and transmit the results securely.

- **Enhanced sensor networks:** The extreme sensitivity of quantum devices could be used to develop sensor networks with far greater capabilities than today, allowing them to detect subtle variations in environmental signals or even gravitational waves. Such advances could have profound implications in fields such as physics and astronomy.

What about the even longer term? Again it depends on advances in technology but a number of other specific applications are on the horizon, including:

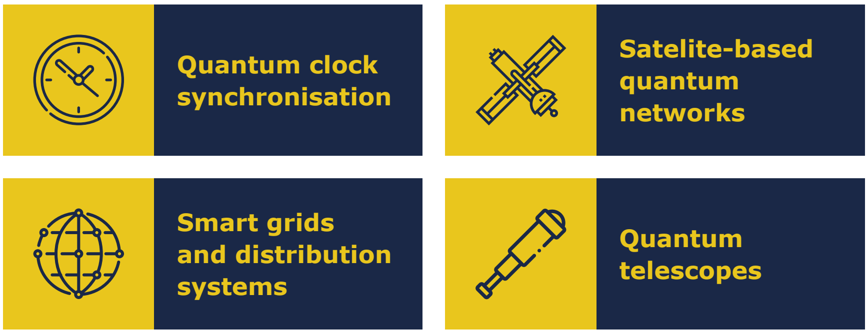

Figure 4: Potential applications of quantum internet [Source: Axon]

- **Quantum clock synchronisation:** This application uses quantum entanglement to synchronise clocks with extremely high precision, measured in picoseconds.[7] It's more accurate and secure than traditional methods, and is especially useful in quantum communication networks, where synchronisation requirements are much more stringent.

- **Satellite-based quantum networks:** By integrating satellites with ground stations, these networks can escape the limitations of optical fibre. This hybrid infrastructure supports protocols like teleportation and QKD across intercontinental distances, paving the way for a truly global quantum communication network.

- **Smart grids and distribution systems:** The quantum internet can handle and transmit information with high levels of security and efficiency. This could be crucial for the next generation of smart grids and smart distribution systems, facilitating more efficient and secure management of energy resources.

- **Quantum telescopes:** Using quantum entanglement, quantum telescopes could revolutionise astronomy by enabling observations with unprecedented resolution. This technology would provide clarity and detail far beyond current limits, and potentially revolutionise our understanding of the cosmos.

7 "Quantum Clock Synchronization for Future NASA Deep Space Quantum Links and Fundamental Science", https://smd-cms.nasa.gov/wp-content/uploads/2023/05/89_9b25ced0bed15ec3326b7d75829fbd88_TroupeJamesE.pdf

4.

What is holding it back?

The quantum internet promises some revolutionary applications; it also faces significant challenges. Some of these challenges relate to the deployment of the quantum internet – and in particular to its core components. These include:

Scalability
Difficulty in scaling up infrastructure to meet growing demand.

Qubit fabrication and control
Difficulty to manufacture qubits with high precision and to control them in large quantities.

Qubit stability
Difficulty in maintaining qubit stability for the time required for complex operations and long-distance transmissions.

Long-distance transmission
Due to its instability, difficulty to transmit qubits ensuring their integrity and reliability.

Interconnection of quantum and classical networks
Difficulty in interconnecting quantem networks with each other and those of the classical internet.

Quantum repeaters
Classic repeaters cannot be used to transmit qubets.

Figure 5: Specific challenges of the quantum internet infrastructure [Source: Axon]

- **Scalability:** Extending quantum networks to support long distances and a larger number of qubits will mean overcoming current physical and technological limitations.

- **Qubit fabrication and control:** Manufacturing qubits with high precision and controlling them – especially in large quantities – is likely to be an exceptionally demanding process.

- **Qubit stability:** Qubits are highly sensitive to environmental conditions. Adverse conditions could lead to rapid loss of quantum coherence, which is necessary for performing computations and reliably transmitting information. At the moment it is hard to guarantee qubit stability over the times required for complex operations and long-distance transmissions (see below).

- **Long-distance transmission:** The ability of current quantum communication systems to transmit qubits without losing their quantum information is limited. Photons, which carry quantum information, can be absorbed, or scattered in the transmission medium (such as optical fibers or free space), limiting the effective distance that quantum information can travel.

- **Interconnection of quantum and classical networks:** Integrating quantum networks with existing classical networks – and ensuring they work together seamlessly – requires sophisticated devices capable of converting quantum information into classical forms and vice versa, all while maintaining quantum speed and security.

- **Quantum repeaters:** Unlike classical repeaters that amplify signals, quantum repeaters must preserve the quantum properties of entanglement and superposition. Developing effective quantum repeaters that can maintain these properties over long distances is crucial. It's also difficult – but it is already a strong focus of research.

Adverse conditions could lead to rapid loss of quantum coherence, which is necessary for performing computations and reliably transmitting information

Additional, less specific challenges include:

Quantum security
It is a new and developing technology, so its potential vulnerabilities are not yet fully understood.

Standards and regulations
There is currently no regulation governing the quantem internet.

Figure 6: Less specific challenges of quantum internet [Source: Axon]

- **Quantum security:** Although the quantum internet offers enhanced security through mechanisms like QKD, it is a nascent technology. The full spectrum of potential vulnerabilities has not yet been completely identified or understood.

- **Standards and regulations:** As an emerging technology, the quantum internet lacks established regulations. It is crucial to define and establish international standards and regulations for its integration and global operation, covering all relevant aspects such as interoperability, device compatibility, and ensuring the security and privacy of quantum communications. It is also essential that these networks are globally accessible, secure, and efficient.

Overcoming these challenges is essential. It will help to enhance this cutting-edge technology and achieve the ideal goals of the quantum internet: global accessibility, safety, efficiency, and utility for all.

5. The quantum internet: hero or villain?

The quantum internet could bring a wealth of benefits, revolutionising how we communicate, compute, and more. It could also introduce significant risks.[8] For example:

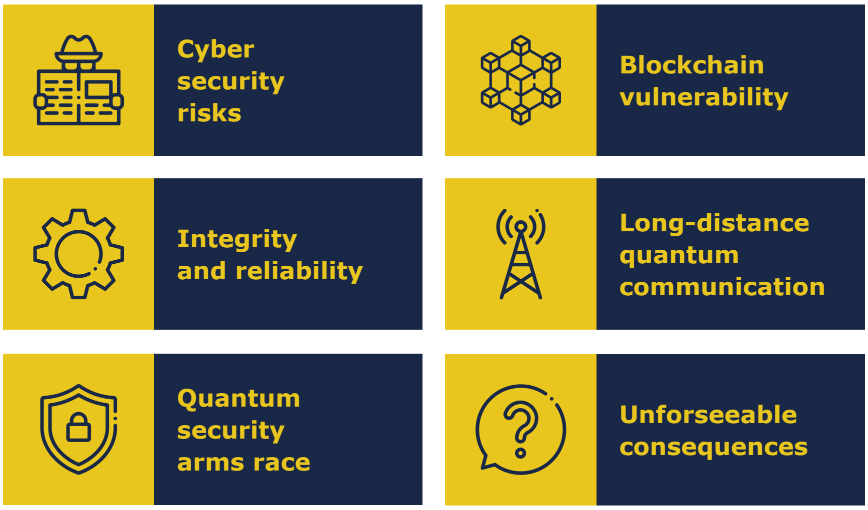

Figure 7: Risks associated with quantum internet [Source: Axon]

- **Cybersecurity risks:** Threats to the cyber systems that our critical infrastructure and democratic institutions rely on are becoming more sophisticated. Quantum computing could be one of them. It could potentially break current encryption methods, jeopardising the security of communications, financial transactions and the confidentiality and integrity of all online information. This includes the ability to decrypt widely used protocols like SSL/TLS and crack encryption standards such as RSA. To mitigate these threats, it is crucial to accelerate the development and adoption of post-quantum cryptography (PQC), designed to withstand quantum attacks.

8 "13 Risks That Come With The Growing Power Of Quantum Computing", https://www.forbes.com/sites/forbestechcouncil/2022/11/08/13-risks-that-come-with-the-growing-power-of-quantum-computing/?sh=72f2afa254b8

Using applications like quantum key distribution (QKD) theoretically offers a secure method of encryption. But the adoption of PQC seems to be lagging behind advances in quantum technology. This means hackers could collect encrypted data today with plans to decrypt it later as quantum capabilities advance. In other words data that is secure now could be vulnerable in the future.

- **Blockchain vulnerability:** Quantum computing poses a serious threat to blockchain technology, which relies heavily on cryptographic security methods. The quantum capability to break these methods could enable unauthorised access to blockchain wallets and transactions, potentially destabilising the crypto economy.

- **Integrity and reliability:** Ensuring the integrity and reliability of data transmitted over the network is crucial. Qubit instability must not compromise data accuracy. For example, quantum-secured voting systems may seem like a good idea – but can we ensure voting data remains unchanged during transmission?

- **Long-distance quantum communication:** The quantum internet poses the challenge of transmitting information over long distances without altering the quantum state of qubits. Developing technology that can transfer this information reliably without state alteration is critical. This challenge is evident in current quantum key distribution (QKD) systems, which need to maintain the integrity of quantum states over long distances to ensure secure communications.

- **Quantum security arms race:** Antivirus software evolves to address new and more sophisticated malware. In the same way, investment in research and development of quantum security technologies is required to protect critical infrastructures from emerging threats. The expected advent of the quantum internet has already triggered a new security arms race, necessitating advanced defenses to counteract quantum-driven attacks.

- **Unforeseeable consequences:** AI technologies brought new types of adversarial attacks that exploit subtle changes in data inputs (as we explained in an Axon whitepaper in April 2024[9]). Similar unforeseen vulnerabilities might arise with quantum technologies – and could be exploited by malicious actors.

Quantum computing poses a serious threat to blockchain technology, which replies heavily on cryptographic security methods

The expected advent of the quantum internet has already triggered a new security arms race, necessitating advanced defenses to counteract quantum-driven attacks

9 https://axonpartnersgroup.com/ai-vs-ai-how-artificial-intelligence-can-enhance-and-threaten-cybersecurity/

AXON CONSULTING

6.
Conclusion

The quantum internet could change communication for the better, massively enhancing our capability to securely process and transmit information by leveraging the unique properties of quantum mechanics. The benefits of the quantum internet, such as unparalleled security through quantum key distribution (QKD), as well as its potential in areas like quantum cloud computing and enhanced sensor networks, promise to revolutionise our digital landscape.

The benefits of the quantum internet, such as unparalleled security through quantum key distribution (QKD) as well as its potential in areas like quantum cloud computing and enhanced sensor networks, promise to revolutionise our digital landscape

Yet these advantages bring substantial technological challenges. How do we stabilise qubits over long distances? Can we create a global network through quantum repeaters and satellites? How do we integrate the quantum internet with existing technologies? It's clear that, along with its benefits, the quantum internet also poses complex problems. These must be navigated carefully.

We must also consider cybersecurity. The quantum internet could pose a threat to existing encryption standards. How do we safeguard sensitive information from misuse of the anticipated capabilities of quantum technologies? We should be considering the development and adoption of post-quantum cryptography sooner rather than later. The risks also extend to blockchain technologies and the integrity of data transmission. All these concerns underline the need for new security protocols that are resilient to quantum threats.

Remember: the quantum internet is not going to be just a technological upgrade. It will be a paradigm shift in how we understand and utilise communication networks. Continuous research, strong international collaboration, and proactive policymaking are essential to harness its potential – and minimize risks.

The quantum internet, then, is a double-edged sword. It could bring substantial improvements to how we connect and interact with the digital world. It could also bring substantial new threats to cybersecurity and network integrity. But the new era of quantum communication is coming whatever happens, and policymakers, technologists, industry leaders and every other stakeholder need to work together to ensure it can be a force for good – while being alert to its potential for harm.

AXON CONSULTING

About
Axon Consulting

Axon is an international firm founded in 2006 that provides investment and advisory services to a broad client base in the ICT and digital space in more than 70 countries across the world.

Axon's cybersecurity practice is central to its business and an increasingly important service area for clients. Its work in this field includes strategy, policy and regulation, governance and research at business and governmental level. Axon works closely with government representatives and other clients to help them understand their cybersecurity needs and challenges in their territories, and to define actionable recommendations aimed at improving their cybersecurity ecosystems.

Tel: +34 913 102 894
Email: marketing@axonpartnersgroup.com