Real World Quantum Network Deployments

Aliro

www.alirotech.com

Real World Quantum Networking Deployments

Contents

Abstract

Interest and investment in entanglement-based quantum networking has been steadily increasing. Unlike Quantum Key Distribution (QKD), which can only be used to exchange an encryption key, entanglement-based quantum networks are multi-purpose networks, capable of simultaneously enabling Quantum Secure Communication alongside other use cases and applications. Exploring quantum network use cases could pay dividends, as both organizations and their clients can benefit extensively from access to entanglement-based quantum networks. Quantum networks are not a brand-new futuristic idea pulled from science fiction. Quantum networks are being built today, and core components of the technology have existed for decades.

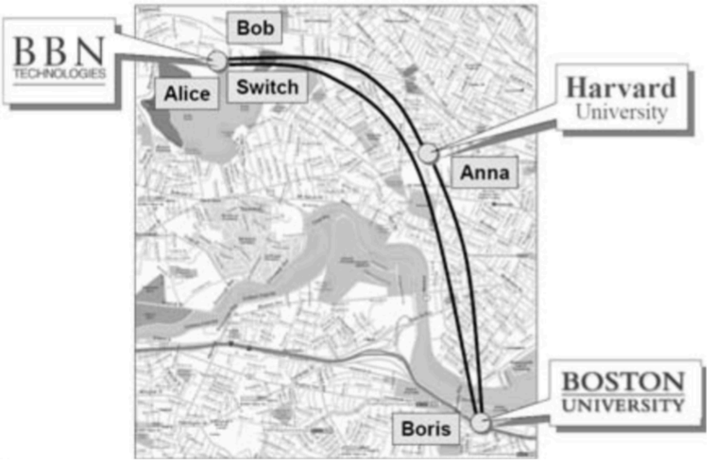
This white paper explores the renewed interest in quantum networks, the use cases that are supported by entanglement-based quantum networks, and four case study briefs based on Aliro Quantum customers. For each of these customer examples,we'll present the customer's goals and challenges, the recommended quantum networking solutions, high level project plans, and a few lessons that can be gleaned from each project.

Introduction

Quantum networks are not a brand-new futuristic idea pulled from science fiction. Quantum networks exist today, and core components of the technology have existed for decades.

For example: BB84[BB84], one of the first quantum communication protocols to be created, was developed by Charles Bennett and Gilles Brassard in 1984 as a method of securely sending a private key from one entity to another. More protocols followed, and many of the protocols that enable the use cases unique to quantum networking have been known for years. E91[E91] and BBM92[BBM92], developed in 1991 and 1992 respectively, are the two earliest examples of QSC protocols. A quantum teleportation protocol[TELEPORTATION] with a key role in many entanglement-based applications was first proposed in 1993. Protocols that enable practical quantum networks have been known for decades, and so have many of the promising use-cases and applications that represent the staggering potential of entanglement-based quantum networks.

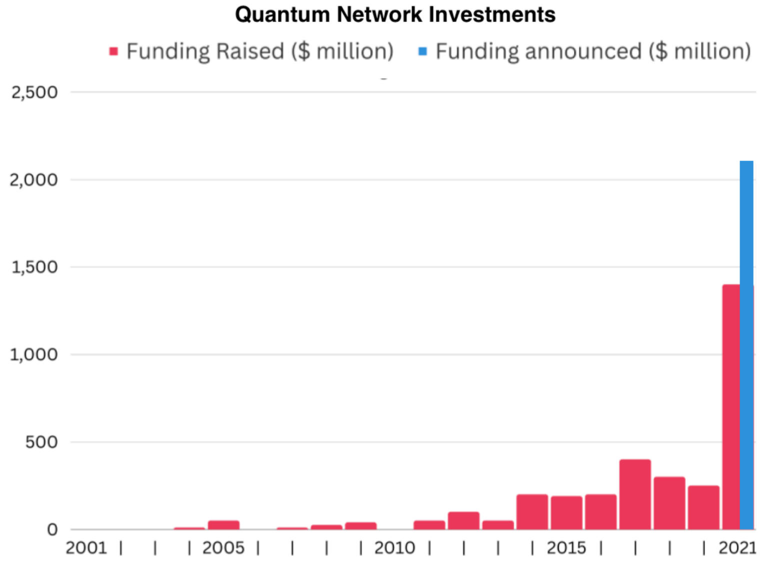
The first quantum network in the US went live in 2003. The DARPA Quantum Networkas seen above was a 10-node quantum key distribution (QKD) network built in Massachusetts that was active from 2003 to 2007.[DARPA] By the end of the project, the DARPA Quantum Network extended between Harvard University and Boston University, using fiber running under the streets of Cambridge. The network went beyond previous demonstrations of single-link QKD to create a network of interconnected nodes—giving it claim to the title of "first quantum network." While this network didn't include the technology



DARPA Quantum Network, 2003 - 2007

needed for large-scale quantum networks (such as quantum repeaters), it was a major step towards the development of future quantum networks. The program demonstrated the feasibility of QKD protocols on a network and contributed several other achievements.

In 2021, the first multi-node entanglement-based quantum network was deployed.[MULTINODE] This fact comes down to a bit of semantics around what constitutes an entanglement-based quantum network, but by many definitions/accounts this is considered to be the first entanglement-based quantum network. Soon after this deployment in 2021, many other entanglement-based quantum networks were deployed or announced. A contributing factor for the delay between entanglement-based quantum network protocols and the launching of entanglement-based quantum networks is due to a lag in development of technology to implement the protocols. Two important developments have allowed for this influx in deployments of entanglement-based quantum networks: the improved performance and commercial availability of high-rate entangled photon pair sources, and high-fidelity single-photon detectors compatible with telecom wavelengths.

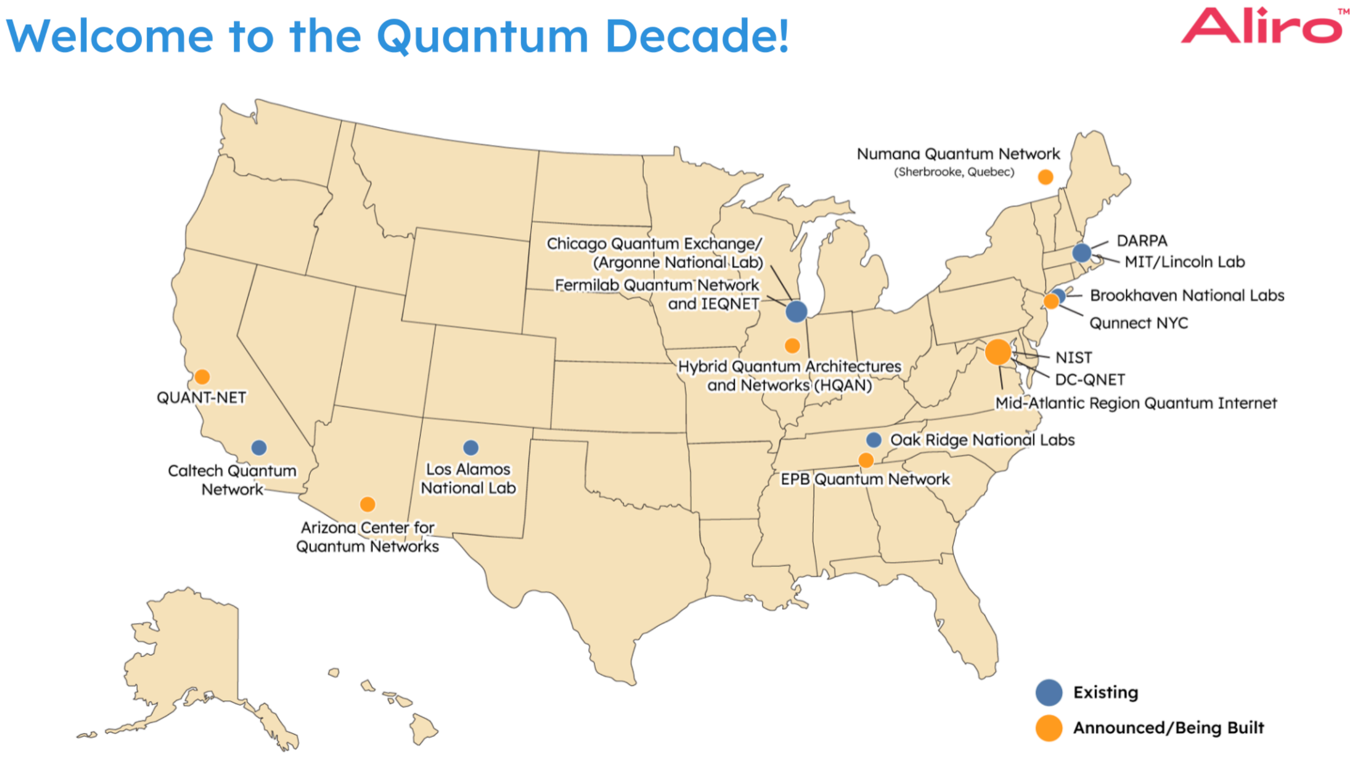


As can be seen in the chart above, over the last few years there has been a revival of interest and attention on quantum networking.[INVESTMENTS] Why is that? The science has been documented for decades. Some of the theories used to create quantum networks date back decades prior to the classical internet. However, the technology to implement those theories and the protocols that followed weren't yet capable of being put into real world applicable use. The ongoing progress made in research labs has enabled the advancements in hardware needed to implement quantum networks. Many companies and organizations have made strides in creating, developing and deploying the technology that enables these quantum networks.

There are other contributing factors that have helped drive the recent boom around quantum computing and quantum networking. Within the US in the early 2000s, there was active investment in developing quantum networks. Then there was a period in the 2010s that interest activity and investments slowed. Toward the end of the 2010s there was renewed interest in quantum networks as the catastrophic security threats associated with quantum computing was understood more clearly.

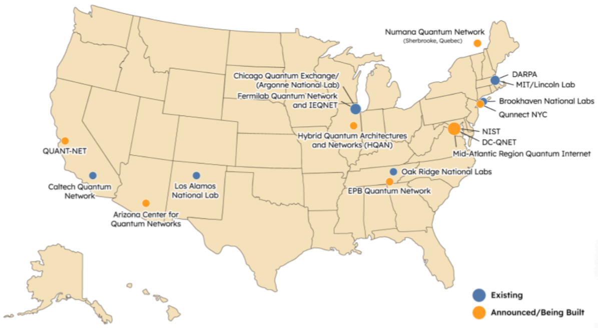
Another contributing factor to the increased investment in quantum networking is federal governments have begun to drastically increase funding for quantum initiatives. In the United States, the federal government has stepped up in the last five years with increased funding toward the research agencies to continue to develop and deploy the technology necessary to not only mitigate classical and quantum cybersecurity threats, but to also enable key use cases such as quantum computing, quantum sensing, and quantum secure communications.[US FUNDING] One way Aliro is securing customer networks against classical and quantum cybersecurity threats, and simultaneously enabling these quantum use cases, is through the design and deployment of entanglement-based quantum networks.

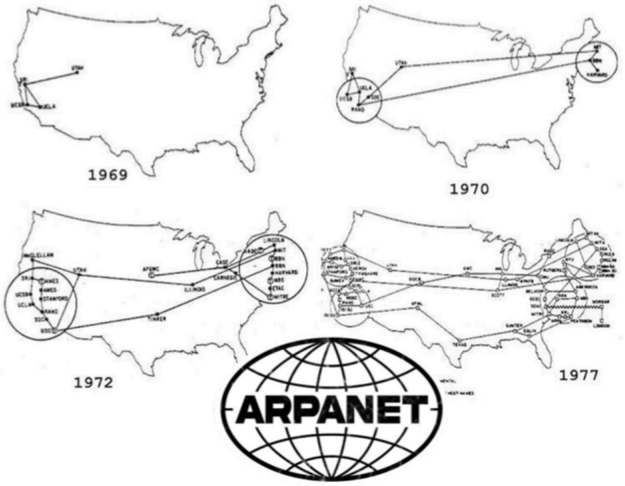
This renewed interest drove an increase in funding and investments to companies and organizations to further develop and deploy these quantum networks at scale. That renewed interest in quantum networking has led us into the quantum decade.


Welcome to the Quantum Decade!

In the graphic above, we see existing quantum networks as well as those quantum networks that were announced through 2022. Ten noteworthy quantum network deployments were announced in North America. These networks represent a variety of use cases, from public test beds and networks such as the Department of Energy's Brookhaven National Lab, to commercially available networks, like the network in Chattanooga, Tennessee. These networks and testbeds all started small - some just two or three nodes - but were then scaled up, some to the Metropolitan size. They will continue to scale and connect to other networks across the country.

This approach - deploying small LANs then growing them and connecting them together - has been used before. The graphic below shows the progression of ARPANET, the foundations for what would become the Internet, in the late 60s and 70s: building and deploying smaller scale networks, and then scaling those across the country and eventually, globally.[ARPANET] As the Quantum Decade unfolds, we'll see the foundations for the future Quantum Internet come into sharper focus.



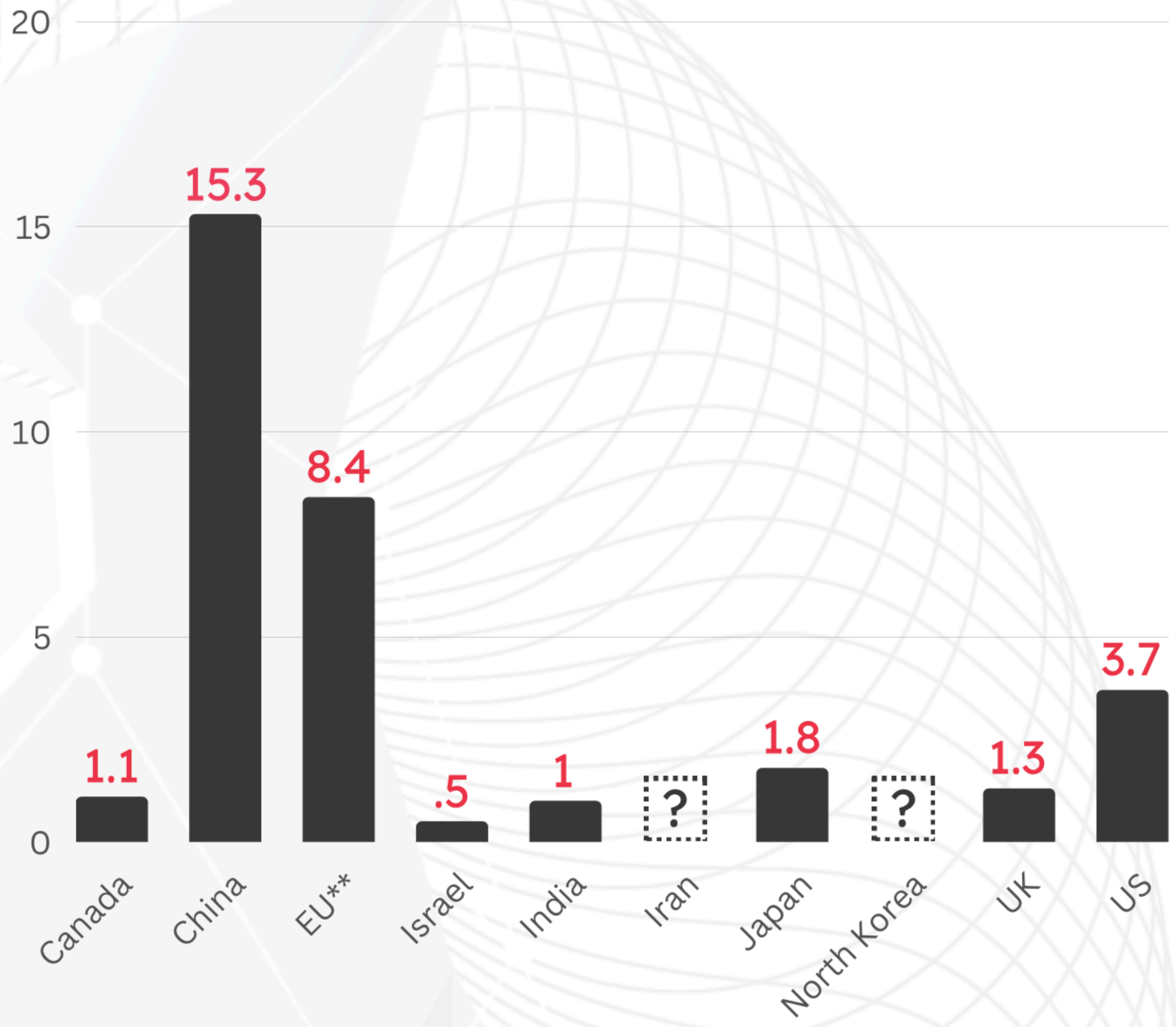


Investments in Quantum Technology Globally

The United States has been in the middle of the pack in terms of funding invested in Quantum Information Sciences. This is partly due to the dormancy of investment by the US in the 2010s, where other countries not only continued to invest in quantum networks during that same time period, but also began steadily increasing investments / funding in the 2020s as well. This has resulted in these countries deploying quantum networks at a larger scale. For example, China has built a quantum network that is over 4600 kilometers long. There are also sizable quantum networks in Russia, South Korea, in the UK, and throughout Europe. With the uptick in investment and renewed interest in funding quantum networks, there are quite a few joint quantum network initiatives in development. For example, China and Russia have discussed networking their quantum networks, and there are multiple EU wide quantum networking projects being executed, with the investment and focus continuing throughout Europe. Several European countries have made groundbreaking strides that have enabled the development and deployment of quantum networks. Future funding will only increase the speed from development to deployment.

Investments in Quantum Technology Development by Country

This chart represents planned, publicly announced governmental investments as of 2022, as reported by McKinsey in The Quantum Technology Monitor, April 2023. Amounts are in billions USD. This is not an exhaustive listing.



***Included in the EU estimate are funds contributed by the EU and member countries including Germany, France, Netherlands, and Sweden.*

The countries that have deployed first generation quantum networks and who have continued to develop these networks have contributed to accelerating progress for more mature entanglement-based quantum networks. By continuing to increase government funding and private investments, countries and organizations that are behind in developing entanglement-based quantum networks can catch up to those who are more advanced in developing quantum networks, and even leap beyond the progress of those countries that are only investing in Quantum Key Distribution (QKD) networks.

While QKD networks and entanglement-based quantum networks have limited overlapping hardware, entanglement-based quantum networks require hardware not used in previous quantum networks, such as entanglement sources which can be used for other applications beyond quantum secure communications.

This advanced hardware technology contributes to a more robust performance and broader application uses. While QKD networks are single-purpose and can be used only for key exchange, entanglement-based quantum networks are multi-purpose and can be used for myriad other use cases and applications.

Previous generations of quantum networks require the use of trusted relay nodes to enable long-distance communication. The term “trusted relay node” is somewhat misleading: it is not a relay node that is certifiably trustworthy, but in fact a relay node that is presumed trustworthy. If a trusted relay node is compromised, so too will be the quantum information that is transmitted by it. It is not a relay node you can trust, but one you are forced to trust. If the quantum information being transmitted must remain confidential, then this is a significant and unavoidable vulnerability. Entanglement-based quantum networks do not have this vulnerability.

Entanglement-Based Quantum Networks

Entanglement-based quantum networks connect quantum devices together by distributing quantum entanglement between them. Quantum entanglement is a property of physics where two particles become correlated in such a way that the state of one particle impacts the state of the other almost instantaneously, regardless of the distance between them. These correlations can be used to transmit information securely across vast distances very quickly, without ever exposing confidential information to the network itself. In addition, entanglement also enables the construction of much larger quantum computers through distributed quantum computing, improved sensing capabilities through distributed quantum sensing, and many other applications that haven’t been discovered yet.

Entanglement-based quantum networks use quantum repeaters for long-distance communication. Even if the quantum repeater becomes compromised, the quantum information that is transmitted by it will remain confidential. This is in part true due to leveraging quantum teleportation to communicate quantum information to endpoints on the network – without that information ever being exposed on the network itself. In this way, the security of the quantum information in an entanglement-based quantum network is “device-independent.”

The progression of previous distance limited quantum key distribution (QKD) networks, like the DARPA Quantum Network, to today’s modern entanglement-based quantum networks can be compared to the transitioning from telephone networks which could only be used to make telephone calls, to the Internet which can carry data, voice, video, and hundreds of thousands of applications. Similarly, we’re now at a point of transition, moving from single-purpose quantum key distribution networks to multi-purpose high-potential entanglement-based quantum networks.

The recent influx in both activity and investment in quantum networks should be seen as no surprise. Entanglement-based quantum networks are often considered the next generation, and really the future, of quantum networks. This is because they offer much greater capabilities and return on investment than did their predecessors.

Use Cases

Three of the most exciting use-cases for entanglement-based quantum networks are networked quantum computing, distributed quantum sensing, and Quantum Secure Communication.

Networked quantum computing is the interconnecting of quantum computers. These computers can have a range of distance from each other - from being located right next to one another, such as in a computer cluster in a single room, to being on opposite sides of the world. Distributed quantum sensing is the interconnection of dispersed quantum sensors. Again, these connections could be near or very apart. Networked quantum computing and distributed quantum sensing can be used to scale the performance of quantum computers and quantum sensors.

Quantum Secure Communications (QSC) refers to the entanglement-based quantum security protocols, communications, and control that are enabled and employed by entanglement-based quantum networks. Entanglement inherently enables detection of the presence of an eavesdropper on the network. This makes it possible to establish a key that is guaranteed to reach its intended destination and know if it has been intercepted. The entanglement-based principle known as quantum teleportation can be used to communicate quantum information to endpoints on the network without that information ever being exposed on the network itself. These two distinguishing characteristics enable QSC to provide **provably** secure communication. QSC works in both theory and in practice.

For more detailed information on each of these use-cases, and the applications that come with them, you can check out the on-demand webinar "Why Quantum Networks, Why Now," which is available here https://www.brighttalk.com/webcast/19861/568067 on the Quantum Network BrightTalk channel.

The race is on to not only address the threat from quantum computers, but also to capitalize on the advantages that will come with quantum computers, entanglement-based quantum networks, and other quantum technologies. These technologies will enable faster computing and bolster the cybersecurity of IT infrastructure.

Real World Deployments: Examples

Aliro Quantum serves organizations and companies in a variety of different industries, including Enterprises, federal entities, and academic organizations in the US as well as internationally. Each of these is unique, with differing requirements, goals, and plans for their quantum network deployments. Each also has unique challenges, accompanied by new lessons learned. Here we'll take a high level exploration using real-world examples of customer use cases and deployments. With the exception of the first use case, EPB, we have changed some details about the organizations to protect their privacy.

EPB

EPB is a power distribution and telecommunications organization located in Chattanooga, Tennessee. This organization is building the first commercially available quantum-as-a-service offering. EPB has deployed a quantum network and made it available to private and public organizations, allowing these organizations to accelerate the commercialization of quantum technologies. This quantum network will be used to test and validate quantum products and performance, test components and software, confirm equipment interoperability, and run quantum security applications.

EPB has the telecommunications fiber required for a quantum network readily available, but still required additional quantum hardware and quantum software to build and manage the quantum network. In addition, deploying the first quantum-as-a-service offering comes with some unique demands:

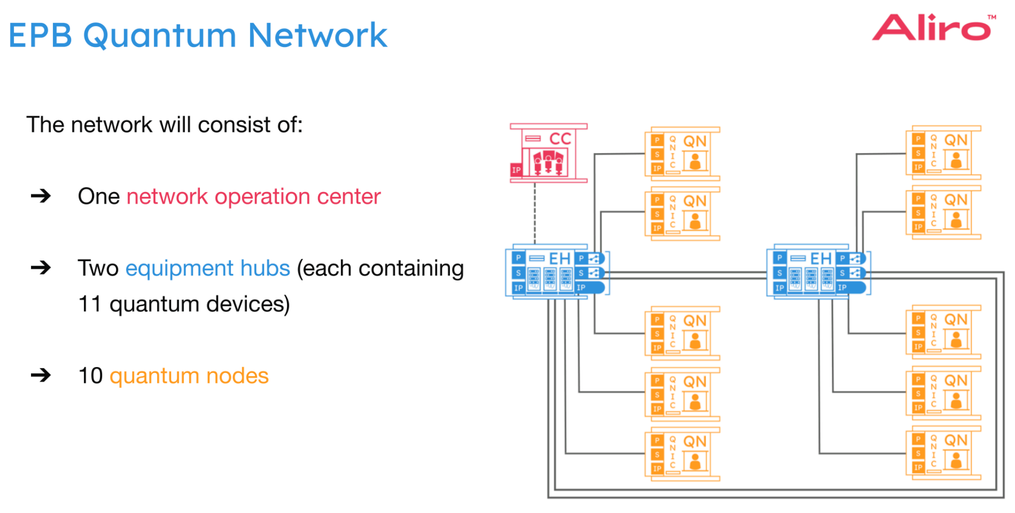
- The network needs to allow for hardware components to easily be swapped in and out for testing. This is a very challenging requirement to meet, as standards have not been established for quantum hardware.
- Managing a network with these hardware components is no easy task either. EPB needs the right software to manage the network and allow its customers to use the network or conduct experiments.
- Identifying and marketing to customers who will utilize this emerging technology as a service could be challenging.

To meet these unique challenges, EPB partnered with industry leaders that could assist in building the EPB Quantum Network. It is important to note that although the EPB Quantum Network will be used in part to test quantum technologies, it will also carry out end-user applications beyond testing and is thus considered a quantum network, not a testbed.

EPB partnered with Qubitekk for the necessary quantum hardware along with the design and build of the network. Qubitekk offers a complete set of hardware components, and can deliver all the hardware needed to build EPB’s quantum network. Entanglement-based quantum networks do not yet have established standards for interoperability - making compatibility between hardware vendors particularly challenging. Qubitekk hardware is best-in-class and comes equipped with important capabilities, such as protocols for timing and synchronization.

EPB partnered with Aliro to provide AliroNet which implements control and orchestration of the quantum network. The EPB Quantum Network consists of over 30 quantum devices. Without AliroNet, each device would need to be configured separately and manually, which is nearly impossible to maintain and manage, particularly as the network scales. AliroNet centralizes, automates, and simplifies control of the network providing great value to network operators and users alike.

AliroNet also provides the network with multi tenant role-based access control, which determines which users have access to what configuration, management, and data on the network. There will be multiple (and potentially competing) organizations using EPB’s quantum network, and ensuring each user organization’s confidential information remains internal is imperative for security reasons. Multi tenant role-based access control provides necessary network security and separation even within the same organization.



EPB Quantum Network

The network will consist of:

➔ One network operation center

➔ Two equipment hubs (each containing 11 quantum devices)

➔ 10 quantum nodes

The EPB quantum network topology consists of:

- A network operation center, as shown in red,
- 2 equipment hubs, as shown in blue, each containing specialized quantum equipment that can be reconfigured by network users
- 10 quantum nodes, as shown in yellow, where the users can bring their equipment and physically connect to the network.

The EPB Quantum Network has been a huge success. The project had an almost ideal set-up: a motivated organization (EPB) with a progressive strategic vision, access and ability to deploy dark fiber, access to funding, Qubitekk with a complete set of devices that is also best-in-class, and a quantum network software company (Aliro) with a software solution to simplify, secure, and enable usage of the network for both operators and users. Collaboration of this magnitude has contributed significantly to the success of the EPB Quantum Network.

National Research Laboratory

Government-funded research labs across the US are building, or have already built, quantum network testbeds. Each of these labs has distinct requirements for their quantum networks and testbeds, such as different quantum hardware and software needs. However, they each share a common goal: at a high level, they all want to accelerate the progress of quantum networks and technologies.

The scientists and engineers at this research lab did incredible work developing the quantum hardware used to build the network, but required control and orchestration software to shift the network from experimental to scaleable operation and enable more users to leverage the testbed.

Deploying orchestration and control software was necessary to give the national research lab’s quantum network the ability to carry out desired tests of hardware and protocols, as well as the ability to run applications.

This lab needed orchestration and control software to centralize, automate, and simplify control of the network to provide value to network operators and users alike.

This lab also needed a quantum network simulator – with the requisite capabilities and performance – to simplify and expedite the ongoing design process, as well as make it more cost-effective. Design begins when initially planning a network, but throughout a network's lifespan design and simulation is needed for changes, upgrades, and scale. A simulator can be utilized to choose the best components, configurations, modifications, and protocols in accordance to its owner's needs before actually purchasing or implementing any of these things. For more in-depth information about using a quantum network simulator, including what capabilities to look for in a simulator, see our on-demand webinar, Quantum Network Simulator Demo.
https://www.brighttalk.com/webcast/19861/576132

Collaboration with industry partners could alleviate understaffing issues that many research labs face. The right industry partners can assist with everything from policy to publications. This collaboration is mutually beneficial, as the national research labs have developed or acquired cutting-edge hardware and facilities that will accelerate their partners' own quantum technologies. Simplifying how users interface with these networks would make collaboration between research labs and industry partners much easier.

While plans among different research labs might vary in some ways, this example gives us insight into the plans other research labs have for implementing quantum networks.
In this case, the research lab has already built its quantum network testbed, with the goal of growing the testbed into an experimental facility open to a user community. To achieve this goal, the testbed is upgrading (particularly in terms of software) and scaling (in terms of capabilities, size, and scope).

Aliro Orchestrator and Aliro Controller simplify and enable usage of this quantum network for internal and external users. It also provides secure access control, which is vital for any network and especially those used by multiple organizations.

The lab intends to scale its network from a local-area network consisting of two nearby nodes to a metro-area network spanning multiple major cities. In order to enable these longer-distance links, the lab will eventually use quantum repeaters. While not yet commercially available, the components that comprise quantum repeaters are available today. While there are other near-term scaling options available now - before quantum repeaters are readily accessible - this research lab is specifically interested in developing quantum repeater technology which can be managed and controlled with Aliro Controller and Aliro Orchestrator..

The lab is currently working to connect their quantum testbed with other quantum networks located in the same general region of the country. This strategy was used to scale classical networks (precursors to the Internet) and is a strategy being used to scale quantum networks today. This approach has been used with other existing quantum networks and it will be vital to building the Quantum Internet. Until quantum repeaters are ready for deployment, the lab is considering using free-space optical components (which could be terrestrial, such as with fixed laser telescopes or non-terrestrial, such as with satellites) to connect its network with the other networks.

Many national research labs have taken a waterfall approach to building quantum networks. The majority of their resources and focus have gone to building, acquiring, and developing the hardware necessary for the networks, only looking to meet the software requirements of the quantum network once the hardware is in place.

However, the most advanced quantum networks globally have addressed quantum hardware and software simultaneously in their deployments. This has proven to be the most efficient and effective approach. Simultaneous deployment of hardware and software is often the best approach for other quantum and classical technologies.

Engagement with quantum network software vendors will accelerate progress in the field without adding much work or responsibility to the national research lab.

Intelligence organization

The specific agency in this example has employees all over the world and their quantum network needs to be able to support Quantum Secure Communication (QSC) for that staff and their mission, regardless of their location.

One of the challenges for these agencies is the limiting funding for quantum initiatives. In the United States, a majority of quantum technology funding goes to the national labs and research agencies versus federal defense and intelligence organizations. This is primarily because many of these organizations weren’t aware of this technology, and as a result they didn't request essential funding during the previous budget cycle. Thus, the lack of funding for larger scale quantum network projects in the following year.

While this intelligence organization is eager to deploy a global quantum network now, realistic timelines for a network of that magnitude relies on the maturity of quantum repeaters, which aren’t yet commercially available. However, it’s still possible to begin building out their quantum network today by deploying local area quantum networks to secure communication at individual locations or between nearby locations. Doing so provides great value to the organization and is a vital step toward developing its global QSC solution.

For longer distance communication, the intelligence organization can utilize Post-Quantum Cryptography (PQC), a purely classical solution that offers additional, but not provable, security. PQC is relatively cheap and easy to implement, as it is a purely classical solution that can be run over existing classical networks.

It is important to note that when quantum networks do scale, PQC and QSC can actually be used together to provide security that has been proven to be at least as strong as each solution individually. Using PQC will create defense in depth, providing an additional layer of security over existing in-use classical security solutions, which is something our clients, and specifically this intelligence organization, certainly want as the quantum networks are scaling to secure the clients information. This combined solution is proven to be at least as strong as PQC and QSC individually. This is because an adversary would need to be able to crack both the PQC and QSC portions of the security in order to crack the combined solution.

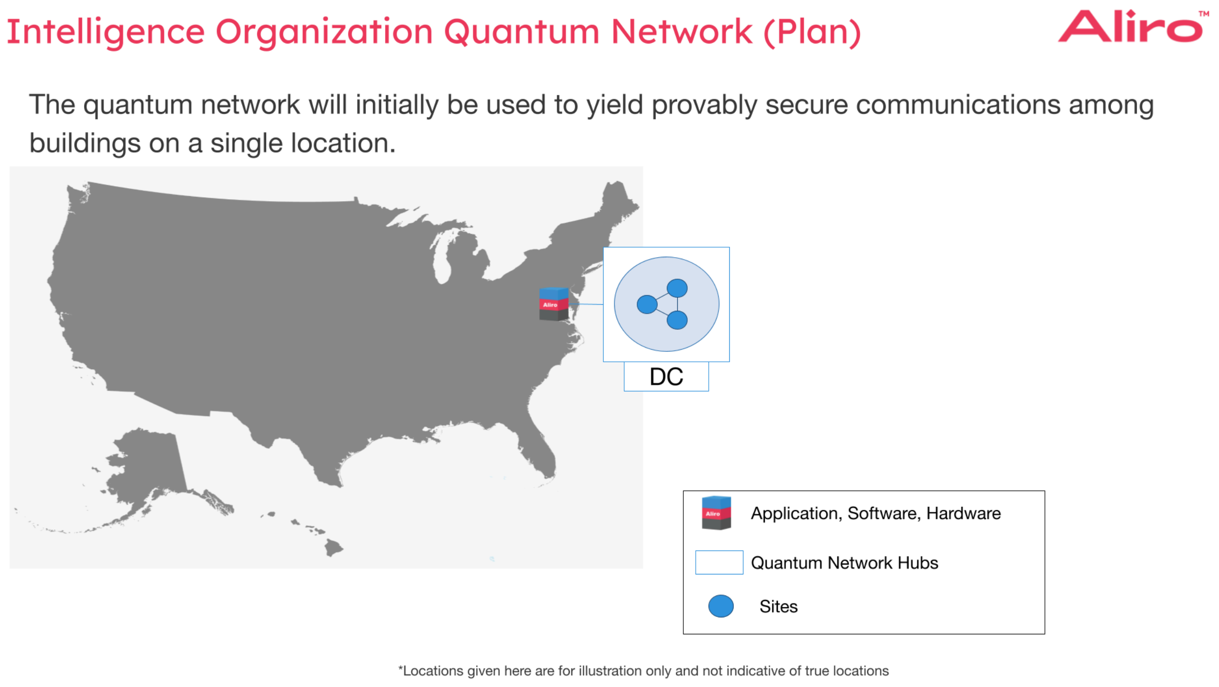
The intelligence organization will be mandated to use PQC as part of its security solution going forward, which is part of the National Security Mandate, NSM 10.[NSM10]

To be as effective and efficient as possible, the intelligence organization must appropriately choose where and when to use different scaling technologies (quantum repeaters, terrestrial or non-terrestrial optical free-space components, etc.). This decision-making will be greatly aided by use of a quantum network simulator.

By engaging with and educating different members - especially the mission owners - throughout the intelligence organization, they will begin to understand the value and applicable use-cases quantum networks will provide to support their mission. Mission owners will utilize this information to request additional funding to support the deployment of the quantum network.

We give the intelligence organization’s plan for implementation as a series of evolving topologies. The locations given in the topologies are intentionally not accurate, but do give a sense of how the organization’s quantum network could evolve.

The organization could first deploy a local area quantum network in the D.C. area at a single location. This network would provide provably secure communications via QSC between buildings at the location.



Intelligence Organization Quantum Network (Plan)

The quantum network will initially be used to yield provably secure communications among buildings on a single location.

Application, Software, Hardware

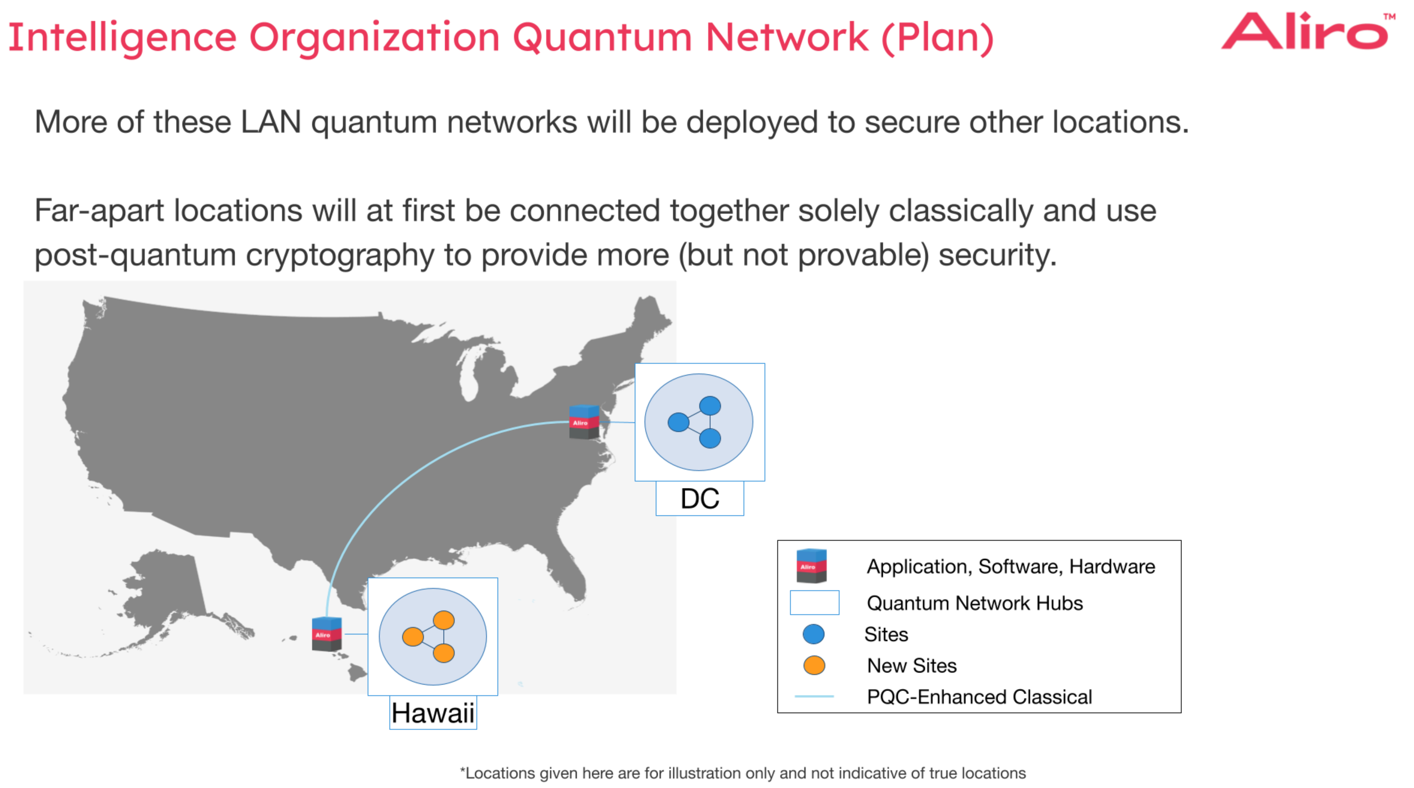
□ Quantum Network Hubs

● Sites

*Locations given here are for illustration only and not indicative of true locations

The organization would deploy a second local area quantum network to secure its location in a location such as Hawaii. These two far-apart locations will be connected classically and use PQC to offer additional security.

The organization will go from solely having individual local area quantum networks, to having metro/wide area quantum networks. This will be done through use of terrestrial and non-terrestrial free-space components. Here, we see that the Hawaii and DC quantum networks are connected by a satellite and can now use QSC to secure communication between these two locations.



Intelligence Organization Quantum Network (Plan)

More of these LAN quantum networks will be deployed to secure other locations.

Far-apart locations will at first be connected together solely classically and use post-quantum cryptography to provide more (but not provable) security.

Application, Software, Hardware

□ Quantum Network Hubs

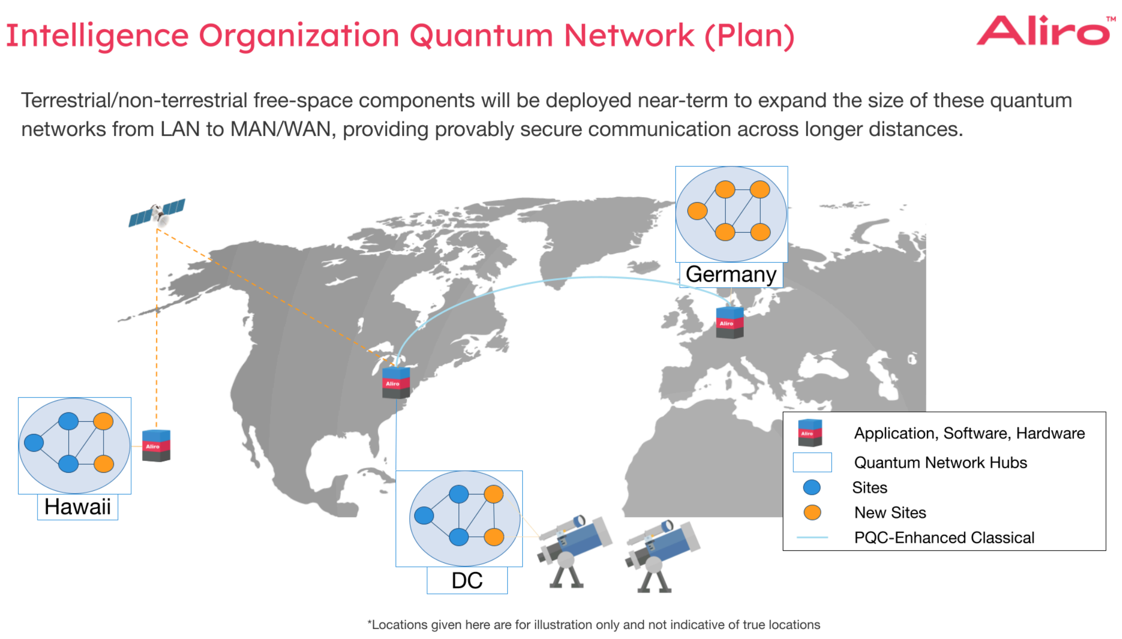
● Sites

● New Sites

— PQC-Enhanced Classical

*Locations given here are for illustration only and not indicative of true locations

The DC quantum network will scale from a local area network to a metro area network through use of laser telescopes.



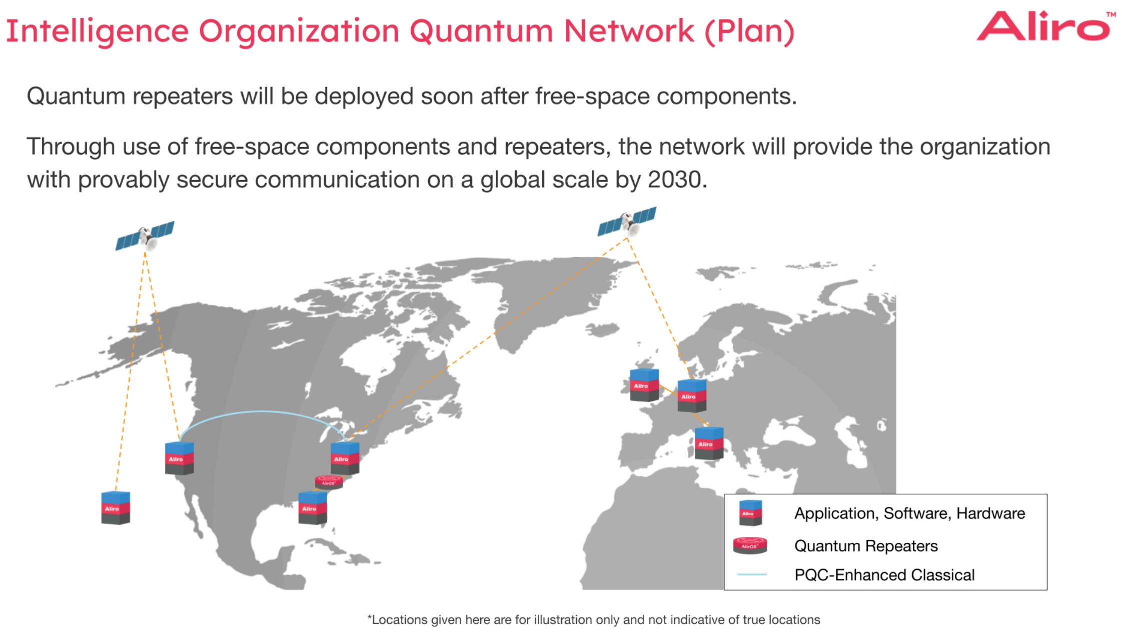
Intelligence Organization Quantum Network (Plan)

Terrestrial/non-terrestrial free-space components will be deployed near-term to expand the size of these quantum networks from LAN to MAN/WAN, providing provably secure communication across longer distances.

*Locations given here are for illustration only and not indicative of true locations

An additional local area quantum network could be implemented in Germany and would be connected to the DC quantum network classically. This classical connection utilizes PQC.

The organization will implement quantum repeaters, as they start to become commercially available, to assist in the scaling of its quantum network. Through use of both repeaters and free-space components, the network will become global offering provably secure communication between locations around the world.



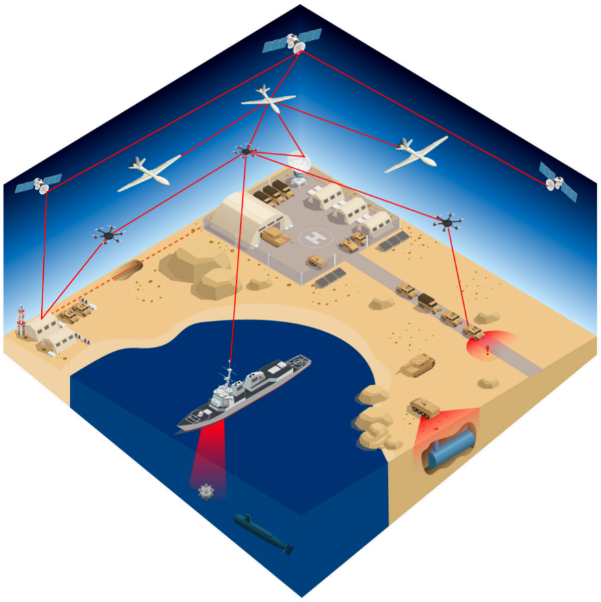
Intelligence Organization Quantum Network (Plan)

Quantum repeaters will be deployed soon after free-space components.

Through use of free-space components and repeaters, the network will provide the organization with provably secure communication on a global scale by 2030.

*Locations given here are for illustration only and not indicative of true locations

While the intelligence organization is most focused on quantum secure communications, it is well aware of and interested in exploring and utilizing the other quantum network use-cases. As its quantum network scales, the organization will explore, test, and use applications of distributed quantum computing and sensing for additional offensive and defensive capabilities.



Pictured above is an example of what a quantum-enhanced battlefield might look like.

The intelligence organization, and many other organizations, recognize that quantum secure communications is the best long-term security solution. However, PQC can have an important role in the near-term for helping to secure communications. There are many important decisions to be made when it comes to how to scale your quantum network. Again, knowledge of the field and use of a quantum network simulator will be incredibly important for such decision-making.

Systems Integrator

The goal of this systems integrator's project is to build a quantum network testbed within their existing innovation lab to enable them to test and evaluate quantum technologies and use cases.

This system integrator has subject matter experts and market leading solutions for classical networking and cybersecurity. What they lack is a robust quantum practice. This challenge is not unique to this system integrator – many of the companies Aliro consults with generally have a very small quantum practice or only a few people who have an understanding of quantum technology. Without clear objectives and go-to-market strategies, it can be difficult to get buy-in from decision makers and business development leads across the organization.

System integrators have two options for overcoming a lack of quantum network knowledge and experience:

1. Hire and/or train a full team to design, build, test, manage, etc. their quantum networks
2. Partner with existing quantum network companies.

Partnering with existing quantum network companies will expedite the quantum networking journey, allowing these organizations to leverage the existing knowledge, skills, and progress of their partner quantum network companies. Quantum industry partners have assembled the necessary subject matter experts and spent years building/developing the quantum products. There is no need for the system integrators to repeat this process. The integrators can focus on their own strengths and utilize the expertise and experience of quantum industry partners to help them to best meet the needs of their customers.

Systems integrators can engage with current and potential customers to assess their needs, providing clear objectives for the integrators' quantum network initiatives. These objectives provide guidance for how to best design and utilize their quantum network testbeds.

There is much more variation among system integrator's quantum network plans than between other types of organizations: they serve different clientele, each with their own unique interests and requirements.

This systems integrator first needed to uncover the interests and requirements of its clients.. By engaging extensively with its clients the systems integrator found out that major federal organizations have substantial interest in using distributed quantum sensing for national defense purposes.

To begin their quantum networking journey, this systems integrator launched three simultaneous projects to develop a quantum network testbed. It has outsourced each of these projects to appropriate industry partners.

- Project 1 is focused on hardware. In this project, the necessary hardware is being bought and/or developed to build a testbed that includes quantum sensors.
- Project 2 is focused on investigating distributed quantum sensing applications and determining which fulfill their clients' needs. Distributed quantum sensing has many applications that can be useful for national defense, and an extensive range of applications beyond defense purposes.
- Project 3 is focused on software. In this project, the necessary software is being bought and/or developed to run the network and desired sensing applications. This will enable applications to be tested and validated on the testbed and eventually used on clients' networks.

The system integrator has internal expertise and experience to leverage in these projects. For example, it is highly aware of its clients needs and requirements. It has a sophisticated process for red-teaming security systems. These strengths will guide the development of each of the three sub-projects.

As with the other quantum network deployments, collaboration will be essential. The systems integrator can focus on leveraging their strengths and outsource the quantum requirements to industry partners that specialize in those competencies.

A full-stack solution for entanglement-based Advanced Secure Networking

Entanglement-based secure networks are being built today by a variety of organizations for a variety of use cases – benefiting organizations internally, as well as providing great value to an organization's customers. Telecommunications companies, national research labs, intelligence organizations, and systems integrators are just a few examples of the organizations Aliro is helping to leverage the capabilities of entanglement-based Advanced Secure Networking.

Building entanglement-based secure networks is no easy task. It requires:

- Emerging hardware components necessary to build the Advanced Secure Network.
- The software necessary to design, simulate, run, and manage the Advanced Secure Network.
- A team with expertise in the science of entanglement-based networking as well as classical networking.
- Years of hard work and development.

This may seem overwhelming, but Aliro is uniquely positioned to help you build your entanglement-based Advanced Secure Network. The steps you can take to ensure your organization is meeting the challenges and leveraging the benefits of the quantum revolution are part of a clear, unified solution already at work in entanglement-based networks like the EPB Quantum Network℠ powered by Qubitekk in Chattanooga, Tennessee.

AliroNet™, the world's first full-stack entanglement-based network solution, consists of the software and services necessary to ensure customers will fully meet their entanglement-based networking goals. Each component within AliroNet™ is built from the ground up to be compatible and optimal with entanglement-based networks of any scale and architecture. AliroNet™ is used to simulate, design, run, and manage entanglement-based Advanced Secure Networks as well as test, verify, and optimize hardware for network performance. AliroNet™ leverages the expertise of Aliro personnel in order to ensure that customers get the most value out of the software and their investment.

Depending on where customers are in their Advanced Secure Networking journeys, AliroNet™ is available in three modes that create a clear path toward building full-scale entanglement-based secure networks: (1) Emulation Mode, for emulating, designing, and validating quantum networks, (2) Pilot Mode for implementing a small-scale quantum network testbed, and (3) Deployment Mode for scaling entanglement-based Advanced Secure Networks and integrating end-to-end applications. AliroNet™ has been developed by a team of world-class experts in quantum physics and classical networking.

To get started (or continue on your advanced secure networking journey), reach out to the Aliro team for additional information on how AliroNet™ can enable your Advanced Secure Network.

www.alirotech.com

References

[ARPANET] Giovanni Navarria. “How the Internet was born: from the ARPANET to the Internet”. The Conversation. Published: 2 November 2016. https://theconversation.com/how-the-internet-was-born-from-the-arpanet-to-the-internet-68072

[BB84] C. H. Bennett and G. Brassard. "Quantum cryptography: Public key distribution and coin tossing". In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, volume 175, page 8. New York, 1984.

[BBM92] Charles H. Bennett, Gilles Brassard, David N. Mermin. "Quantum cryptography without Bell's theorem". Physical Review Letters. 68 (5): 557–559. 3 February 1992. https://doi.org/10.1103/PhysRevLett.68.557

[DARPA] Chip Elliott and Henry Yeh. “DARPA Quantum Network Testbed”. Approved for public release; Distribution unlimited. PA# AFRL-07-0057. July 2007. https://apps.dtic.mil/dtic/tr/fulltext/u2/a471450.pdf

[E91] Artur K. Ekert "Quantum cryptography based on Bell's theorem". Physical Review Letters. 67 (6): 661–663. 5 August 1991. https://doi.org/10.1103/PhysRevLett.67.661

[INVESTMENTS] Mateusz Masiowski, Niko Mohr, Henning Soller, Matija Zesko. “Quantum computing funding remains strong, but talent gap raises concern”. 15 June 2022. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/quantum-computing-funding-remains-strong-but-talent-gap-raises-concern

[MULTINODE] Delft University of Technology. "Entanglement-based quantum network." ScienceDaily. ScienceDaily, 15 April 2021. www.sciencedaily.com/releases/2021/04/210415142619.htm

[NSM10] The White House. “National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems”.
4 May 2022.
https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

[TELEPORTATION] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. “Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels”. Phys. Rev. Lett. 70, 1895 – Published 29 March 1993 https://doi.org/10.1103/PhysRevLett.70.1895

[US FUNDING] https://www.quantum.gov