European Commission

JRC TECHNICAL REPORTS

A Secure Quantum Communications Infrastructure for Europe: Technical background for a policy vision

Lewis, Adam M.
Travagnin, Martino

2022

EUR 31133 EN

This publication is a Technical report by the Joint Research Centre (JRC), the European Commission's science and knowledge service. It aims to provide evidence-based scientific support to the European policymaking process. The scientific output expressed does not imply a policy position of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use that might be made of this publication.

Contact information
Name: Adam M. Lewis
Address: Centro Comune di Ricerca, Via E. Fermi 2749, I-21027 Ispra (VA) ITALY
Email: adam.lewis@ec.europa.eu
Tel.: +39 0332 785786

EU Science Hub
https://ec.europa.eu/jrc

JRC129425

EUR 31133 EN

PDF ISBN 978-92-76-53705-2 ISSN 1831-9424 doi:10.2760/180945

Luxembourg: Publications Office of the European Union, 2022

How to cite this report: Lewis, Adam M., and Travagnin, Martino, *A secure quantum communications infrastructure for Europe: technical background for a policy vision*, EUR 31133 EN, Publications Office of the European Union, Luxembourg, 2022, ISBN 978-92-76-53705-2, doi:10.2760/180945, JRC129425.

Contents

Abstract

This document describes a vision for a European terrestrial fibre and satellite infrastructure for quantum communications. It will initially provide quantum-secured distribution of encryption keys to ensure communications confidentiality; other security-linked applications will be progressively added as they reach the necessary technological maturity level. In addition, it will seed the ground for a quantum network connecting quantum computers and quantum sensors, to enhance their performance for societal benefit. Use cases for this secure Quantum Communications Infrastructure are briefly described in telecommunications, data centres, critical infrastructure protection, secured synchronisation, defence, government communications, space-based systems, and distributed quantum computing. A roadmap for its deployment is presented and the challenges to be faced, including at the policy level, are reviewed.

Acknowledgements

We gratefully acknowledge the experts who participated in workshops in the spring of 2019 and provided material and advice. Considerations of confidentiality prevent us from thanking them by name. We also wish to thank our European Commission colleagues who contributed to this work, and especially Thomas Skordas, Ali BenMoussa, Rafael Tesoro Carretero, Pravir Chawdhry, Gilles Lequeux, Pascal Maillot, and Giuditta Montesanti.

This work is part of JRC Work Package 6315 and was funded by the European Commission's Directorate-General for Communications Networks, Content and Technology, under Administrative Arrangement No. 35420-2019 with the JRC.

Authors

Adam M. Lewis

Martino Travagnin

Explanatory note – added in June 2022

This Report was written in 2019 with the aim to provide a scientific background for an EU policy initiative on quantum-secured communications. It was commissioned by DG CNECT to DG JRC, and used to foster the interest of the Member States on what was to become known as the EU Quantum Communication Infrastructure.

Indeed, on 28 July 2021 the EC released a press note declaring that "all 27 EU Member States have committed to working together alongside the European Commission and the European Space Agency (ESA) to build the EuroQCI — a secure quantum communication infrastructure that will span the whole EU. The EuroQCI will be part of the space-based secure connectivity system currently being planned by the Commission" ([1]).

The Report was initially marked as "sensitive" with report number JRC116937, and its distribution limited to EC, ESA, and representatives of the Member States, since the concept of EU QCI had not then been publicly announced. The Commission has now decided to release the report publicly.

To preserve its historical significance and to avoid any misunderstandings that could arise by having two different versions of the same work, the Report is now published in its original form, with only minor editing. Since 2019 further work on architectural options, alternative and complementary technologies, and deployment priorities has been made both by the Commission and by consortia of industrial and academic partners, and part of it may become publicly available in the next future. In November 2021, the Digital Europe Programme published a first call for proposals for action grants on an EU secure Quantum Communication Infrastructure ([2]).

[1] https://digital-strategy.ec.europa.eu/en/news/all-member-states-now-committed-building-eu-quantum-communication-infrastructure

[2] https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/digital/wp-call/2021/call-fiche_digital-2021-qci-01_en.pdf

Executive summary

This document concerns a conceptual study for developing a communications infrastructure, which would allow highly secure communications using methods based on quantum physics. The study considers known future threats to cryptography, including from quantum computers, and the background of an already worrying situation in cybersecurity.

A quantum communications infrastructure (QCI) spanning the whole of Europe, consisting of terrestrial fibre links and space elements is envisaged. The first service offered would be distribution of quantum-secured encryption keys, followed by other services such as digital signatures, authentication and synchronisation of ultraprecise time signals. In the long term, the infrastructure might evolve into a quantum internet, linking quantum processors and sensors.

Key requirements which have been identified are that the QCI should be compatible and interoperable with existing telecommunications technologies, it should be built to address known use cases but be flexible and upgradable, and it should contain the right mixture of algorithmic and hardware defensive measures (including quantum key distribution) that will dramatically reduce the cybersecurity risk and ensure security for the long run.

Various relevant initiatives are already underway in several EU agencies, Member States, and ESA. Only a commitment at the EU level could match the resources that international competitors such as China, Korea, US, Japan, and others are devoting to similar projects. Skills and assets from across the entire EU will be needed for construction of a QCI, and the project would help to foster a new industry in quantum communications components and systems, ensuring that the EU develops the industrial capability and the supply-chain non-dependence and sustainability that will guarantee its strategic autonomy.

Compelling reasons to act now include the possibility that large-scale quantum computers may be available to attackers before reliable quantum resistant encryption algorithms are available and deployed. In particular, some encrypted data being stored today may well still be sensitive when quantum computers might render vulnerable their current cryptographic protections. Apart from the steady progress being made in quantum computation, other risks of advances in algorithmic attacks on cryptography are always present and their potential consequences are becoming more severe all the time, as we become more and more dependent on information technology.

The study presents several use cases for the QCI in telecommunications networks, datacentres, critical infrastructure, secured synchronisation, defence, government data and communications, space systems and quantum computing. Such use cases span across national borders, further demonstrating the necessity to act at EU level.

Quantum communications are now mostly confined to short distance (in the range of 50-100 kilometres) and point-to-point connections. Some of these limitations could be overcome by using satellites, which would additionally ensure global coverage, enabling secure communications with EU assets worldwide. Quantum repeaters are being developed which, in time, would provide end-to-end quantum security also by using fibre-based links. The QCI implementation roadmap needs to be synchronised with the ongoing technology evolution. Nuclei of the network in several countries already exist or could be created soon to demonstrate its practical utility in different use cases, including in more distant member states, reached by satellite links.

This is an intermediate report explaining the vision and motivation and providing a first statement of use cases and high level system requirements for QCI. A second report with more detailed statements of these is planned for later in the year.

1 Introduction

Communications privacy is a citizen's right, a security and defence tool, a driver for economic growth, and a vital factor for the smooth functioning of markets - even more so in the era of mass communications enabled by the Internet. Cryptography is an essential instrument of privacy and secrecy, used to authenticate two parties who have never interacted before, then to ensure confidentiality by protecting their communications from eavesdropping, and also to safeguard data at rest.

Modern cryptographic techniques now in use are based on "intractable" computational problems, so-called because their solution, with the best algorithms known, requires an exceedingly long time even with the most powerful computers available. Such techniques are vulnerable to advances in mathematics, computational power and algorithms, and to "side-channel" attacks exploiting non-ideal features of the hardware. A new threat is coming from progress in quantum computing, which exploits quantum effects to solve problems intractable to classical computers. Quantum algorithms have been devised that can effectively break current cryptography systems which are in widespread use in current Internet communications. In particular asymmetric cryptography, where different keys are used to encrypt and decrypt the message, will be compromised with the advent of large-scale quantum computers. Proof-of-principle experiments have shown that the small quantum processors which are already available can successfully run these algorithms[3,4,5].

It is presently impossible to forecast precisely if and when a quantum computer large enough to constitute a concrete security threat to state-of-the art cryptography will be realised[6]. Were it to happen, the disruption would be momentous. Early action must be taken well in advance to address the risk, since significant time will be required to upgrade the existing telecom infrastructure, and data with long-term confidentiality periods must be protected from "intercept now, decrypt later" attacks as soon as possible. In the worst scenario, we may already be too late to protect some important data which are being stored or exchanged now.

Quantum physics itself offers a unique basis for a solution to this threat by enabling completely novel cryptographic techniques based on fundamental physical laws rather than on assumptions about computational difficulty. This basis is thus distinctively secure against crypto-analytical progress, even of the kind made possible by quantum computers.

[3] Martin-Lopez, E. , Laing, A., Lawson, T., Alvarez, R., Zhou,X. –Q and O'Brien J. L., Experimental realisation of Shor's quantum factoring algorithm using qubit recycling, Nature Photonics 6, 773-776 (2012), DOI: 10.1038/nphoton.2012.259

[4] Dash, A. , Sarmah, D., Behera, B. K. and Panigrahi, P. K., Exact search algorithm to factorize large biprimes and a triprime on IBM quantum computer, arXiv:1805.10478v2 [quant-ph] 12 Jul 2018

[5] Lucero, E., Barends, R., Chen, Y., Kelly, J., Mariantoni, M., Megrant, A., O'Malley, P., Sank, D., Vainsencher, A., Wenner, J., White, T., Yin, Y., Cleland A. N. and Martinis J. M., Computing prime factors with a Josephson phase qubit quantum processor, Nature Physics volume 8, pages 719–723 (2012), DOI: 10.1038/nphys2385

[6] For example, experts surveyed by the JRC in 2017 gave a wide range of opinions. The median estimate was 2032, so the community did not see it as a distant threat. See Lewis. A. M., Ferigato C., Travagnin. M. and Florescu., E., The impact of quantum technology on the EU's future policies: Part 3 Perspectives for quantum computing, EUR 29402 EN (2018) DOI: 10.2760/737170

2 Vision

The vision is to provide ultra-secure quantum communication tailored to user needs, permitting the secure exchange of information and data, the long-term protection of stored data, and the protection of critical infrastructure.

The first stage, analysed and discussed here, is to develop and deploy a secure quantum communications infrastructure (QCI) for distribution of encryption keys, to link critical data and communications assets all over the EU.

The QCI will then be used to deploy other applications and services, such as digital signatures, authentication[7], and ultraprecise clock synchronisation[8], as each becomes technologically mature.

QCI is also the first part of a much more ambitious vision. It is intended to become the backbone of a "Quantum Internet" which will connect quantum computers, simulators and sensors throughout Europe to radically enhance their performance and enable a new technological revolution.

3 Background and Motivation

3.1 What is the problem?

Europe already has an extremely serious cybercrime problem; increasingly sophisticated cyberattacks are undermining the functioning of our communications networks, critical infrastructure and services and, ultimately, of our society. Some evolutionary trends in information technology threaten to make the situation worse, because new opportunities will be created for criminals. If our cryptographic defences were no longer reliable, the door would be open to a cybercrime catastrophe. In 2016, 80% of EU companies reported a cybercrime incident and, in some member states, half of all crime is cybercrime. Ransomware attacks have increased threefold between 2015 and 2017 and the economic impact of cybercrime rose fivefold since 2013[9]. Europol stated in its 2018 internet organised crime threat assessment that each year they report cyberattacks of an unprecedented scope and scale. One third of Member States reported cases involving attacks on critical infrastructures. Cyberattacks on infrastructure may be politically motivated or of a terroristic nature[10]. McAfee recently estimated a global yearly impact of USD 600 billion for cybercrime[11]:

As everything is more and more connected, the scale of the damage produced by cyberattacks increases. A typical cybercrime attack on a company might cost of the order of USD 10 million[12] . The 2017 NotPetya ransomware attack on the Maersk shipping line, estimated to have cost USD 200–300 million[13], was possible because of heavy reliance on a tightly connected network of computers. The more automated processes are, the more vulnerable they are to systematic errors produced by an attack. We can expect to see the

[7] Zawadzki, P. Quantum Inf Process (2019) 18: 7. https://doi.org/10.1007/s11128-018-2124-2 gives some examples of schemes for quantum identity authentication and proposes an improved protocol

[8] QCI is intended to interface closely with ongoing work to link fundamental time standards at national metrology sensors by fibre optic lines, to include also security of the distribution. This concerns applications such as high speed financial trading where assurance of the authenticity of the time signal is crucial.

[9] https://www.consilium.europa.eu/media/21480/cybersecurityfactsheet.pdf

[10] https://www.europol.europa.eu/sites/default/files/documents/iocta2018.pdf

[11] https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf?utm_source=Press&utm_campaign=bb9303ae70EMAIL_CAMPAIGN_2018_02_21&utm_medium=email

[12] https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

[13] https://www.maersk.com/news/2018/06/29/20170816-a-p-moller-maersk-improves-underlying-profit-and-grows-revenue-in-first-half-of-the-year

advantages and disadvantages of artificial intelligence deployments in relationship to protection and cyberattacks.

Also, the telecommunications evolution towards 5G will create new potential vulnerabilities. 5G networks are estimated to have hundreds more attack vectors compared to previous 4G networks. This is inherent in the 5G concept of massive Machine Type Communications whereby vastly more devices will be digitally connected to the network and, therefore, potentially be the object of cyberattacks[14].

Apart from human factors and implementation errors, computational assumptions typical of today's crypto systems bring in potential encryption vulnerabilities. In addition, there are practical limitations depending on environment: critical infrastructures often depend on legacy SCADA (Supervisory Control and Data Acquisition) systems, Internet of Things environments have limited computing resources, telecommunication networks progress towards software defined networks and network function virtualization, which are inherently more susceptible to cyberattacks. Whatever other cybersecurity vulnerabilities affect these systems, they all share one weakness: the computational security assumptions for key distribution.

The security of current computational encryption technologies relies on some computational hardness assumptions, which means that an unforeseen breakthrough in cryptanalysis could render current systems vulnerable. Both our infrastructure and encryption systems are always at risk of being compromised by such advances in cryptanalysis, perhaps combined with ever more powerful computing brute force, and by sophisticated hardware-layer attacks (differential power analysis, fault injection, timing attacks, etc.). These could leave Europe's communications networks and services and sensitive data (energy, health, financial, security or defence-related and more) extremely vulnerable. Quantum computation has now become an additional threat, since quantum algorithms have been discovered with a crypto-analytical potential which could make obsolete some of the cryptographic techniques currently in use. For now, quantum processors big enough to run them are lacking, but intense research efforts in this direction are being pursued both by private players and governments.

3.2 What are the possible solutions?

What are termed "post-quantum" or "quantum-resistant" algorithms (QRAs), intended to be resistant to attacks from quantum computers, are currently being developed and standardization activities are underway[15]. However, there is no formal guarantee that QRA are resilient to all possible cryptanalysis attacks with a quantum computer, or indeed even that they would be secure against some new improved crypto-analytical algorithm running on a classical computer.

Quantum physics can be exploited to protect against eavesdropping by creating private symmetric encryption keys, using a technique known as Quantum Key Distribution (QKD) which, if correctly implemented, allows establishing a secure encryption key at the two ends of a communications line. By exploiting quantum physics, the legitimate partners can indeed detect any eavesdropping attempt and discard a compromised key. This is a distinct feature of QKD, which sets it apart from key distribution by human courier or algorithmic encryption. Once a provably secure key has been established, it will then be used to ensure the confidentiality of communications taking place along public channels.

The security of the key, for the first time, can be directly determined. It is guaranteed by the laws of physics to be safe against any progress in mathematical crypto-analysis and

[14] https://business.financialpost.com/telecom/attack-surface-has-multiplied-5g-networks-more-vulnerable-to-hackers-conference-told

[15] https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

in computational power, including the one provided by quantum computation. Its security depends on correct hardware implementation to guard against physical-layer attacks[16].

QKD provides a solution to the problem of sharing an encryption key fundamentally resilient to computational attacks, quantum or classical. Typically it is used together with one-time-pad (which is information-theoretically secure) or a classical symmetric cryptography algorithm such as AES (for which no credible crypto-analytical attack is known, quantum or classical). The rationale for thinking that this will remain the case is that it is widely believed that cracking symmetric cryptography is intrinsically harder because cipher designers are less restricted in the choice of mathematical functions than in asymmetric cryptography.

Keys distributed using QKD can also be used to continue to authenticate data transmissions without relying on computational assumptions i.e. guarantee that the transmitting party is genuine and not an interloper. This allows increased security in preventing unauthorized access, for example to critical infrastructures.

A combination of QKD (in the physical / hardware layer) and QRA (in the virtual / software layer) will therefore dramatically reduce the risk and ensure security for the long run. QKD will not replace traditional cybersecurity mechanisms but rather complement them in a new security mix to make highly critical infrastructures more robust to cyberattacks. In fact, it is likely that, to tackle different issues and use-cases, several quantum-safe methods will emerge. Some of them will rely on new algorithms designed to be impervious to quantum attacks, and some on quantum physics: both areas are the object of intense development and standardisation efforts. Practical information security depends on closing all loopholes and side channels, and the use of quantum techniques does not in itself guarantee that this has been done. The best mix of physical layer, quantum, and computational cryptographic techniques will depend on the use case. The role of QKD will depend on its performance, cost, infrastructure compatibility, and potential vulnerabilities to implementation loopholes.

Quantum key distribution is based on a fundamental principle of quantum physics, namely that under certain conditions it is impossible to gain information about quantum states being transmitted from a sender to a receiver without perturbing the states. This principle can clearly be exploited for communications security purposes and, in particular, to establish a symmetric encryption/decryption key, since it allows one to detect the activity of an eavesdropper, assess the amount of leaked information, and take the necessary countermeasures. Several different QKD protocols and implementations exist, all of them requiring as initial resources a public quantum channel and an authenticated public classic channel.

A typical prepare-and-measure QKD protocol begins with the encoding of random bits in quantum states, which are then transmitted along the quantum channel. By exchanging classical information about random subsets of the quantum bit flux, the communicating parties compare the states that have been prepared by the sender with those that have been actually measured by the receiver. They then apply error correction and privacy amplification codes that reduce the amount of quantum information that an eavesdropper might have been intercepting to an arbitrarily small level, thus allowing the distillation of a private key. There exist prepare-and-measure protocols based on multi-photon light pulses instead of single photons, which have the advantage that they are more compatible with the technologies currently deployed in optical networks and do not require expensive single-photon detectors. There are also entanglement-based protocols, which exploit the quantum correlations existing between two entangled photons to test for the presence of an eavesdropper between the legitimate players.The quantum state being transmitted can be the polarisation, the phase difference, a quadrature modulation, and so on. Each implementation has its own strengths and weaknesses in terms of

[16] https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp27_qkd_imp_sec_FINAL.pdf

performance, sensitivity to implementation loopholes, and suitability to the transmission medium (e.g. optical fibres, free-air).

For a fibre-based commercial system the current state of the art is a key rate of a few Mbit/s (which is deemed acceptable for AES encryption) for a distance of ~ 50 km, the most critical factors being the channel loss and the detector's efficiency. It has been calculated that even by using low-loss fibres and high-efficiency detectors it will not be possible to deploy a QKD span longer than ~ 300 km. The easiest way to extend the QKD range, which is used in all the fibre-based backbones deployed up to now, is based on the use of 'trusted nodes', i.e. classical relay systems that connect subsequent quantum cryptographic spans. The security of trusted nodes is ensured by classical means such as hardware security modules, protected enclosures, and physical surveillance. True end-to-end quantum security is not therefore achieved. Another option which is being currently explored is to resort to space communications, using satellites as trusted nodes to provide long-distance connectivity. High altitude balloons and drones have been tested. Quantum repeaters are also being investigated, which exploit entanglement to extend the range along which quantum information can be transmitted. Proof-of-principle experiments have been done, but the development of field-deployable quantum repeaters which would enable end-to-end quantum security is still seen as a rather long term challenge (2025+).

QKD could be the first cybersecurity-service of a future certified secure end-to-end Quantum Communications Infrastructure (QCI). This QCI could be deployed in the next decade all over Europe, first for encryption key generation and distribution, later for more applications that require a quantum channel, and be further expanded and developed as a number of technologies would become more mature. The QCI would link EU's critical data, communication, storage, and processing assets.

4 Current initiatives

4.1 In Europe

European Union

EU programmes which fund quantum communications projects comprise the European Quantum Technologies Flagship (QT-Flagship, with a ten-year funding of 1 B€), the QuantERA programme[17], COST Actions[18] (QTSpace and NQO), the EURAMET metrology programme[19], FET Open[20] , EITdigital[21] and the space programme. The EU QT flagship has now entered the ramp-up phase. From the first call for Research and Innovation Actions, 19 projects have started on 1 October 2018 with a budget of 130 M€, of which four are on quantum communications, aiming at: the development of ground-breaking devices and systems for a future quantum internet (QIA), photonics technologies enabling quantum communications (UNIQORN), quantum random number generators (QRANGE) and continuous variable quantum key distribution links (CiViQ). Projects will also aim to achieve entanglement and teleportation across quantum multi-node networks. The QCI will provide a means to exploit successes achieved in these Flagship projects.

In 2018 as part of H2020, DG CNECT launched a 15 M€ call SU-ICT-04-2019 pilot project for developing a testbed aiming to validate the feasibility of the QCI concept based on QKD and to demonstrate the interoperability of quantum components from different

[17] https://www.quantera.eu/
[18] https://www.cost.eu/
[19] https://www.euramet.org/
[20] https://ec.europa.eu/programmes/horizon2020/en/h2020-section/fet-open
[21] https://www.eitdigital.eu/

vendors; another objective is the standardization and security certification of QKD-based secure communications solutions. This pilot project is expected to start in September 2019.

Standardisation efforts for QKD have been undertaken by the European Telecommunications Standards Institute (ETSI), starting as far back as 2008. A portfolio of specifications has been produced, and work is now extending towards certification.

It is of crucial importance that the EU space systems meet the security needs of users in the future. For Galileo, a QKD Experimental Payload has been proposed by DG GROW to ESA. Also Copernicus and GovSatCom could take advantage of the quantum security solutions enabled by the QCI.

European Space Agency

The European Space Agency is currently studying three different QKD missions.

The QUARTZ and the QKDSat projects are both studying a low earth orbit based QKD service aiming at providing commercial services in the 2020s. QUARTZ was proposed by an industrial consortium led by the satellite operator SES (Luxembourg) and is co-financed by the ARTES ScyLight programme. QKDSat was proposed by an industrial consortium led by the company Arqit (United Kingdom) and is co-financed under the ARTES 33 Partner programme. Both studies are financed for first phases with their continuation depending on the successful completion of the ongoing work and subsequent financing for the future implementation phases.

Complementary to the commercially oriented LEO based QKD systems, ESA has started internal studies for a GEO based QKD system named SAGA (Secure And cryptoGrAphic Mission). SAGA provides a complimentary service compared to other QKD concepts using LEO satellites and single downlinks. The entangled photon protocol with double downlinks and the GEO locations provides unique advantages for security and continental coverage, but is demanding in terms of optical apertures requiring large telescopes in space and on ground to close the link budget and to reach a useful key rate. The cost per kbit of key will be higher compared to LEO based systems and it is expected that only governmental entities will be able to afford the service and are willing to host the larger-size optical ground station telescopes. SAGA is proposed as a new project for the SPACE19+ council meeting of ESA.

In addition, ESA is executing several smaller studies and technology developments for QKD user cases (for critical infrastructures), laser communications technologies (terminals, components, ground segments, atmospheric modelling, QKD protocol simulations).

Member States

Several initiatives are already preparing the development of the technology components needed for the deployment of quantum communications in Europe. In Europe, several countries have started to develop their own (limited) quantum communications infrastructures. For example, a quantum network is under deployment in the Netherlands between Amsterdam, Delft, Leiden and The Hague as the first step towards a future "Quantum Internet". Also Austria and Switzerland have deployed quantum networks and performed QKD in-field experiments, and Germany has recently funded a 15 M€ euro project for the development of quantum repeaters.

The Madrid Quantum Network (MQN) was started in summer 2018; the core is owned by Telefónica de España, has 3 Points of Presence installed in the operational facilities, and it is intended to verify high Technical Readiness level components. The core network will be extended to include part of the academic network (RedIMadrid Network) which is also in operational use, but with less restricted access for technical intervention. In the new

connections several wavelengths are used in each fibre, and some of the links will be made available for experiments during relatively large periods of time. Both networks are expected to be fully connected in the near future, to demonstrate inter-provider and inter-network quantum interoperability. The MQN has been used to demonstrate data connections, network virtualization and the security of the software defined network control plane.

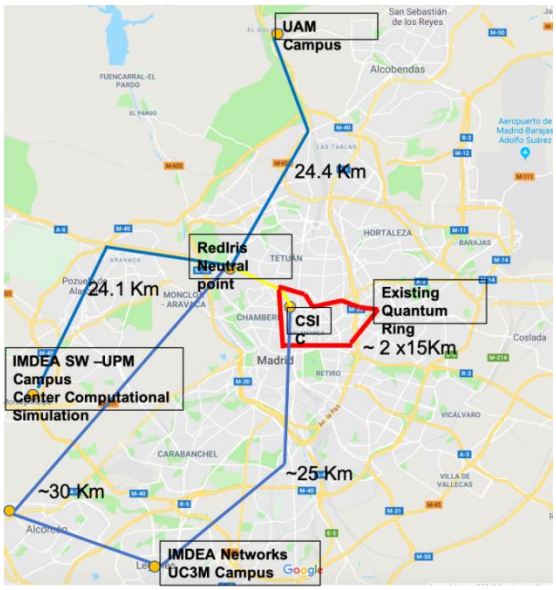

Figure 1. Madrid Quantum Network showing in red the core installed in Telefónica Production Facilities and in blue the extension in the RedIMadrid academic network (courtesy Universidad Politécnica de Madrid).

The Italian national quantum backbone, coordinated by INRiM, includes a QKD backbone from Turin to Florence, with a QKD metropolitan network being built in Florence (by LENS and CNR). Entanglement distribution from Sicily to Malta (~100 km submarine cable) has been demonstrated. The project also includes precise-time and frequency distribution for scientific and financial applications.

Figure 2. The Italian national quantum backbone (courtesy INRiM).

The UK Quantum Communications Hub is building a trusted node QKD network as shown in Fig. 3, of which the sections between Cambridge University, Toshiba Research Europe Ltd. (TREL) and the BT research campus at Martlesham are already operational[22,23].

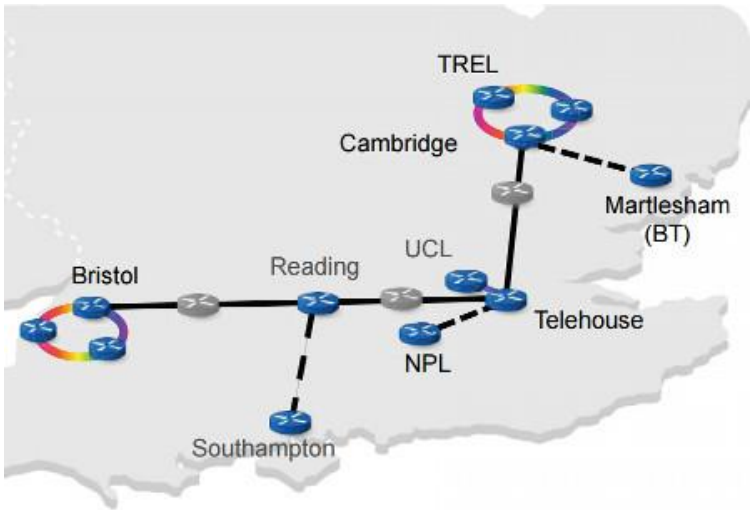

Figure 3. The UK Quantum Network (courtesy University of York).

[22] https://www.cam.ac.uk/research/news/cambridge-launches-uks-first-quantum-network
[23] https://www.quantumcommshub.net/news/hub-partners-collaborate-to-extend-the-uks-quantum-network-into-the-telecommunications-industry/

4.2 Worldwide

Several groups around the world have demonstrated QKD use in the field, deploying several fibre networks with different architectures (e.g. point to point, point-to-multipoint with access network available to several final users) and even demonstrating key distribution from LEO satellites. Alongside Europe, the main players are China, the USA, Japan, and South Korea. International organisations (ITU-T, IEEE-SA and ISO/IEC) are also now following ETSI into the field of quantum communications standards.

A broad-brush overview is given in the following paragraphs.

China

A low-orbit satellite named Micius was launched in 2016, and has since been used to perform several quantum communications experiments. In particular, an encryption key has been exchange with Graz (Austria) and used to protect a video-conference. It has recently been announced that Micius would work at least two more years beyond its two-year working lifetime, and it is expected to be used for inter-continental quantum key distribution experiments with Italy, Russia and South Korea[24]. Jian-Wei Pan, a professor at the University of Science and Technology of China (USTC) known as China's "father of Quantum" says that over the next five years China will launch four more low-orbit quantum satellites, and a high-orbit geostationary one will follow shortly thereafter[25].

On the ground, a 2,000km operational QKD fibre link based on 32 trusted nodes connects Beijing and Shanghai via Hefei and Jinan, and is being complemented by ever-expanding metropolitan networks. For example, in Jinan quantum links will connect Party and government offices, government agencies, the military, finance players and electricity providers, deploying 200 terminals at an estimated cost of 120 million yuan ($19.5 million)[26]. The backbone link is planned to be further extended, both to the north of Beijing and to the south, to reach Hong-Kong[27].

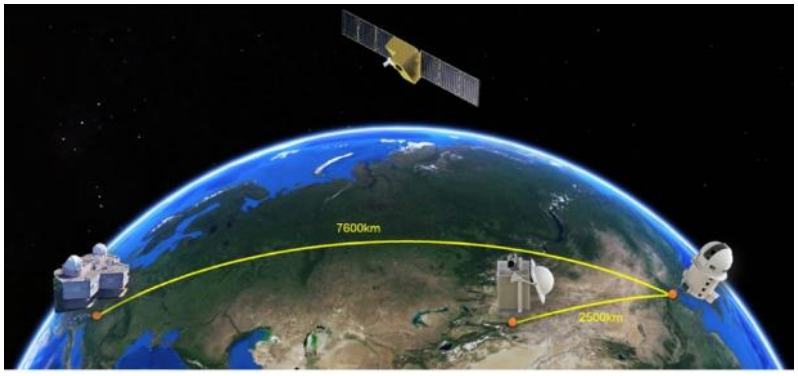

Figure 4. Intercontinental satellite-based QKD between China and Europe[28].

China is actively fostering technology and component production capabilities in the quantum space, producing alongside scientific and technological results also significant intellectual property and pushing for standardization. Several international committees have started standardising quantum communications protocols, and in this framework it is likely that the solutions of the first comers will be promoted. This could potentially give Chinese players an advantage over counterparts from elsewhere, including Europe.

[24] http://english.cas.cn/newsroom/news/201902/t20190218_205416.shtml
[25] https://www.technologyreview.com/s/612596/the-man-turning-china-into-a-quantum-superpower/
[26] http://www.chinadaily.com.cn/china/2017-07/11/content_30065215.htm
[27] http://2018.qcrypt.net/wp-content/uploads/2018/slides/Wednesday/06.Yu-Ao%20Chen.pdf
[28] https://arxiv.org/ftp/arxiv/papers/1801/1801.04418.pdf

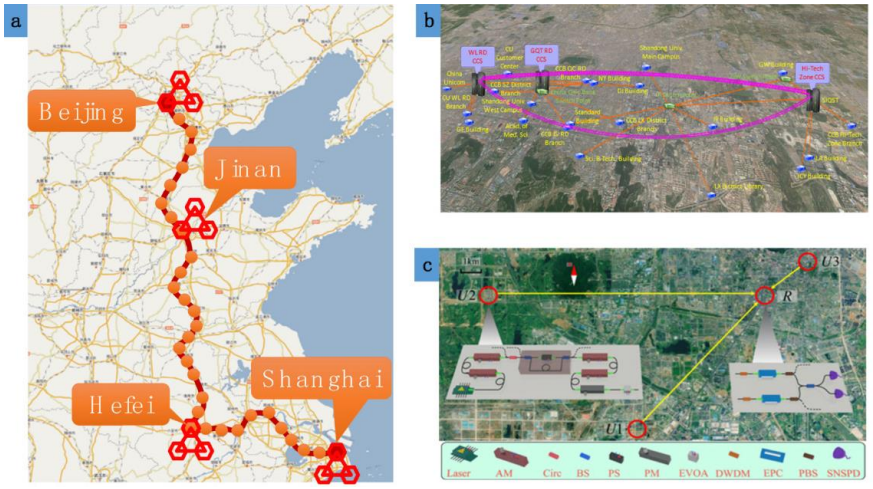

Figure 5. (a) Outline of the Beijing-Shanghai 2000 km QKD backbone (b) Topology of the Jinan metropolitan QKD network (c) Example of a MDI-QKD network with three user nodes and one untrusted relay node[29].

USA

The first fibre-based QKD network worldwide was funded by DARPA: it started operating in June 2004, securing a fibre-optic loop connecting facilities at Harvard University, Boston University, and the office of BBN Technologies in Cambridge (Massachusetts) for a total of six nodes[30]. The DARPA network apparently stopped operating in 2006 and no other field deployments by USA government agencies are known. However, Los Alamos National Laboratories are working with Oak Ridge National Laboratories and a utility company to advance the use of QKD to secure the energy grid[31]. Batelle, a private non-profit company, was the first one to deploy a QKD network for internal use, starting from 2013[32] and using hardware provided by the Swiss manufacturer IdQuantique.

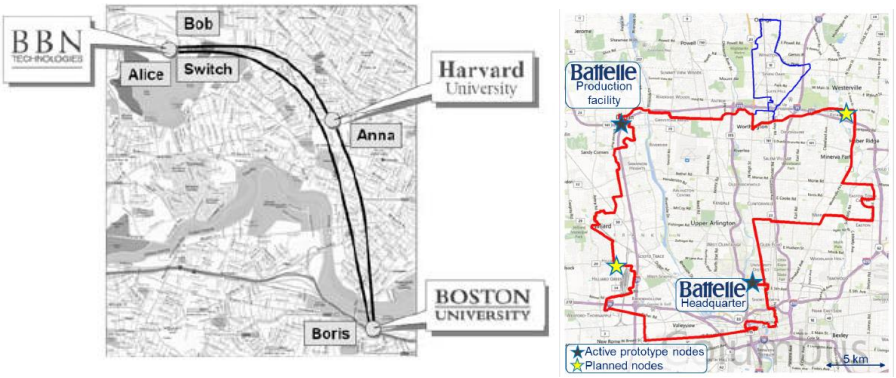

Figure 6. Darpa QKD network in Cambridge[33] and Batelle QKD network in central Ohio[34].

A company named "Quantum exchange" recently unveiled plans to link Boston with Washington via an 800-km trusted-nodes link based on dark fibres: technical collaboration with Toshiba is ongoing, and a $10 million funding round has already been completed. Quantum Xchange said it will start by connecting Wall Street's financial

[29] https://www.osapublishing.org/oe/abstract.cfm?URI=oe-26-18-24260
[30] https://arxiv.org/ftp/quant-ph/papers/0503/0503058.pdf
[31] https://www.lanl.gov/discover/news-release-archive/2019/February/0212-grid-security-tech.php
[32] http://2014.qcrypt.net/wp-content/uploads/Hayford.pdf
[33] https://arxiv.org/ftp/quant-ph/papers/0503/0503058.pdf
[34] "Towards a North American QKD Backbone with Certifiable Security", Nino Walenta et al, QCrypt 2015

markets with back-office operations based in New Jersey, offering on a subscription basis a QKD service designed for banks and other financial institutions that need to ensure their data is safe and secure[35].

The Office of Advanced Scientific Computing Research of the Department of Energy has published in 2018 a document advocating the deployment in the USA of "Quantum Networks for Open Science", which will comprehend QKD alongside sensing and computation. Its deployment could leverage the DOE High-Performance Optical Backbone Network. Chicago (with Argonne national laboratories, FermiLab, University of Chicago, and University of Chicago at Urbana Champaign) is likely to become a DOE hub in quantum networking, with an authorized funding level up to $60 million for 5 years. There is an ongoing debate on forming a National Science Foundation quantum networking hub between MIT/Harvard, Stanford and Caltech, with a possible funding of $25 million for 5 years.

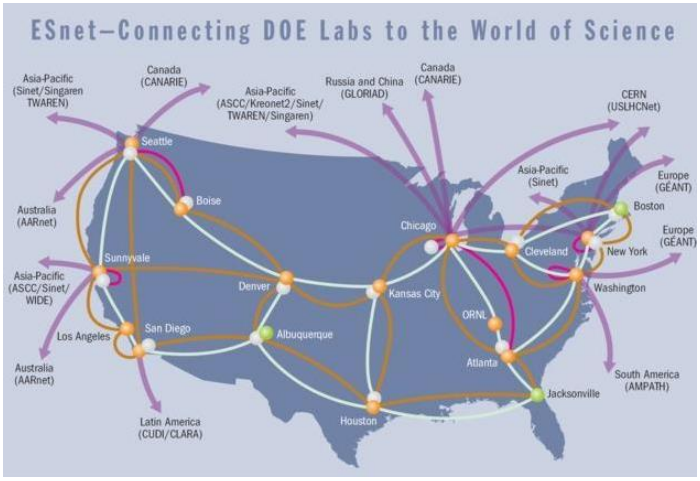

Figure 7. The ESnet network operated by the DoE to interconnect critical scientific resources[36].

Japan

An extensive quantum network in Tokyo was inaugurated in October 2010, which includes video transmission, eavesdropping detection, and rerouting to secondary secure links; applications that have been implemented include one-time-pad on smartphones and transmission of genetic data, as well as signature and authentication schemes to ensure long-term integrity also of data at rest. Alongside several industrial players (Japanese and non-Japanese), the main contributor has been the National Institute of Information and Communications Technology (NICT). NICT is also working on space-based QKD by developing an optical transponder for satellites and equipping receiving ground stations. In August 2016 single photons transmitted by the SOTA transponder on board the LEO satellite SOCRATES were received by a ground station located in an urban area of Tokyo[37].

[35] https://siliconangle.com/2018/06/26/quantum-xchange-build-first-quantum-network-u-s-offering-unbreakable-encryption/

[36] "Quantum Networks for Open Science Workshop", U.S. Department of Energy, Office of Advanced Scientific Computing Research, Rockville, Maryland, September 25 - 26, 2018; QNOS Workshop Final Report, March 2019, DOI: 10.2172/1499146, https://www.researchgate.net/publication/332041110_QNOS_Workshop_Final_Report

[37] Alberto Carrasco-Casado, Hideki Takenaka, Mikio Fujiwara, Mitsuo Kitamura, Masahide Sasaki, Morio Toyoshima "QKD from a microsatellite: The SOTA experience", Proceedings Volume 10660, Quantum Information Science, Sensing, and Computation X; 106600B (2018) https://doi.org/10.1117/12.2309624 https://doi.org/10.1117/12.2309624

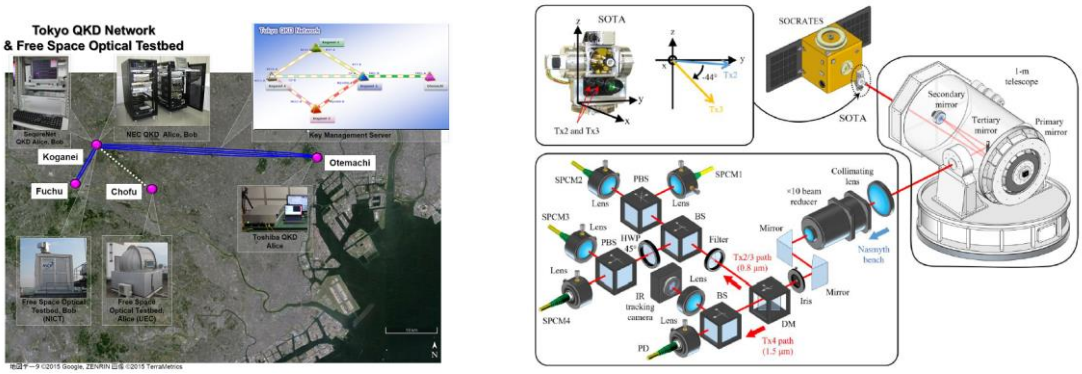

Figure 8. The Tokyo QKD network and a layout of the Socrates satellite QKD experiment[38].

South Korea

The government is funding the development of a ~ 250 km quantum backbone, of which ~200km have already been completed. Main use cases are commercial metro network and 4G LTE commercial network, and in the longer term also 5G networks. The main players are the Korea Institute of Science and Technology Information (KISTI) and SK Telecom: in the last two years SK Telecom announced a collaboration with Nokia on QKD[39], revealed that it is applying its quantum security system to the trial network of Deutsche Telekom[40], signed a ~$8.9 million deal supply contract with the U.S. quantum crypto communications company QuantumXchange[41], and bought for ~$65 million a controlling quota of the Switzerland-based firm IDQuantique, which provides quantum-safe cryptography solutions[42]. IdQuantique in turn had announced in December 2016 the creation of a joint venture with China Quantum Technologies (QTEC) to bring the company's Quantum Random Number Generators (QRNGs) and Quantum Key Distribution (QKD) solutions to the Chinese market[43]. SK Telecom is also active on standardization, proposing new International Telecommunication Union (ITU) standards regarding quantum cryptographic systems and quantum random number generators with IDQ, Quantum Xchange, Florida Atlantic University and the University of Geneva.

Figure 9. Deployment phases of the south-Korean national QKD network[44].

[38] https://arxiv.org/ftp/arxiv/papers/1810/1810.12405.pdf
[39] https://www.prnewswire.com/news-releases/sk-telecom-and-nokia-sign-cooperation-agreement-for-quantum-cryptography-300413873.html
[40] https://pulsenews.co.kr/view.php?year=2018&no=473861
[41] http://www.businesskorea.co.kr/news/articleView.html?idxno=23945
[42] https://www.zdnet.com/article/sk-telecom-buys-half-of-swiss-quantum-safe-crypto-firm-for-65m/
[43] https://www.idquantique.com/idq-qtec/
[44] https://www.photonics.com/Articles/Quantum_Networks_Photons_Hold_Key_to_Data/a60541

5 Rationale for an EU QCI

5.1 Why should we act at EU level?

In several European states, initiatives to build quantum communications infrastructures are being taken. However, there is a strong case for EU-level co-ordination of the deployment of a pan-European secure quantum communications infrastructure. First, more and more critical infrastructures are already today at a European scale. Examples are electric power networks, banking networks, navigation systems, air traffic control systems, coordinated intelligence networks, etc. Second, the challenge will require the leverage of joint efforts by several countries to reach the level deployed in the P.R. of China, Korea and not lag behind. Not all EU member states have strong practical know-how and industrial capability in quantum communication technology; a European solution will enable the best capabilities to be applied and shared where they are needed. Experience will be gained as the QCI is built and operated and, crucially, many more people will acquire expertise as they participate in the work.

In short, the need for data security is of transnational nature and touches government and public sector communications. All security and defence aspects call for public support at national and EU levels. Such a support will foster the development of an EU quantum technology industry, which will ensure EU strategic autonomy in a critical technology. With time, the technology will extend from niche high security applications to a wider market, thus contributing to economic growth.

QCI will contribute to long-term EU cybersecurity and to communications security by deploying an infrastructure in Europe to strengthen the security of data communicated, stored and processed. All sectors of our economy and society would greatly benefit, as the QCI will help secure financial transactions, safeguard medical records, shield highly sensitive national and cross-border critical infrastructures, and ensure confidentiality of sensitive governmental information. An additional protection layer for the EU's key digital assets will be created for the transmission and the long-term storage of sensitive data, to the advantage of citizens, businesses, and governments.

5.2 What advantages would it offer for industrial development?

Developing the QCI would permit the EU to maintain its mastery of quantum security technologies critical for its strategic autonomy. Currently we see advanced technology for quantum communications being developed and deployed especially in China, with significant efforts taking place also in several other countries and notably in the USA, Japan, Canada, and Korea. A large-scale and Union-wide project like the QCI will stimulate diversity of provision of quantum security technology and know-how and foster the development of a new high-tech industry dedicated to the development of quantum-based security solutions.

The QCI should address concrete use cases in a useful and practical way, by integrating quantum cryptography and innovative quantum products into conventional communications infrastructures, and by complementing the entire system with conventional security protections. In this way could it create a large market pull, which would promote the development of new, innovative technologies and systems, stimulate a market and provide EU industrial players with the opportunity to become leaders in quantum technologies likely to be of major economic importance. This would drive the development of a non-dependent European quantum communications manufacturing capability which, as well as being an economic asset, would provide strategic autonomy in the future.

5.3 Why now?

The time scale for an operational quantum computer large enough to constitute a cybersecurity threat is very uncertain, but quantum-safe encryption has to be ensured as soon as reasonably practical since (i) there are data whose confidentiality must be maintained for longer time spans, since they can be targeted by intercept now/decrypt later attacks, and (ii) there are critical infrastructures requiring high-security communications for which development and deployment times or the lifetime can be very long.

There is a definite present-day reason to provide higher security for EU digital assets. Considering the threat from software and hardware progress, and the ever-present possibility of unexpected mathematical progress in cryptoanalysis making current cryptosystems insecure, quantum-safe encryption is a must and should include both quantum cryptography and algorithmic methods.

5.4 Why an integrated system of terrestrial and space segments?

Many important sites for secure data exchange are located close together in or near major cities and economic corridors, and may be best served by terrestrial links. In such places, fibre infrastructure which could be used may already exist. On the other hand, the vision of linking critical data and communications assets all over the EU implies continental-scale reach and provision of services to island territories, for which satellite technologies may well offer the most effective solution. In this respect, QCI resembles other long-distance networks in which both terrestrial and space segments are used, although it does have specific characteristics concerning existing technology on the ground and in space, and what is expected according to the technology roadmap. The optimum space-segment to ground-segment balance moving forward will depend on the relative rates of progress in quantum repeater technology and satellite-based quantum communications technologies.

5.4 What is the list of requirements?

- Be compatible and interoperable with existing secure communications systems.
- Address identified use cases but be flexible enough to meet the requirements of new ones as they appear.
- Be certified/accredited to be secure.
- Be upgradable to include new applications and improved technology as it becomes available.

6 Use cases

There are several credible public and quasi-public sector application scenarios, and it is essential to design the QCI to support these use cases. Typical use cases are in infrastructure protection and in transmission of very sensitive information. It is expected that other use cases will emerge over time, and it is also essential to retain flexibility to accommodate them. QCI should therefore be modular and upgradable. It will also evolve as new enabling devices become available, on different time scales.

6.1 Telecommunication networks

Rationale

This is an infrastructure use case with the following specific features:

1) The infrastructure is itself a communications network and an enabler for QCI
2) The trend to software-defined networking (SDN) and network functional virtualization (NFV) increase opportunities for an attacker
3) The use case is one of the best researched, including in practical experiments.
In SDNs, the point-of-presence is considered a secure location, and so it is suitable for the location of a QKD trusted node. Beyond the use case of securing the network itself (i.e. the network control and management plane) it is possible to use the QKD keys to secure the data plane, thus potentially extending the security end-to-end to any two points connected through the network, as is required in other use cases. NFV is a new paradigm that is proving to be crucial in new networks: its general idea is to substitute typical network elements like routers, firewalls, etc. by software instances running in general purpose servers. These network elements can be instantiated or eliminated as required, and also chained to provide new network services. Both SDN and NFV conform to the current trend of network *softwarization*, being adopted by all major telecommunication companies, to add flexibility and agility to communications networks. However, these benefits come also with a higher risk that can be mitigated with technologies like QKD. QKD can be used as an additional security layer on top of existing mechanisms, thus facilitating the integration in the current security ecosystem[45].

Architecture

Architecture concepts related to this use case are already being researched for standardisation at the ETSI (European Telecommunications Standards Institute). The flexibility typical of the SDN paradigm affords a fully integrated classical-quantum network, which facilitates a broad deployment of quantum technologies, starting from QKD and progressively extending to other quantum communications techniques, such as entanglement distribution between quantum computers. The central idea is that the QKD link is well integrated with the software defined network control. The controller has a global view and thus can optimize the full network, taking into account the classical as well as the quantum communications.
Indicative parameters for a small scale metropolitan network are available from the Madrid experiments. The network is a metropolitan area (~10 km) the secret bit rate achieved was in the range of the tens of kbits per second, which allowed for a much faster key refresh than the one for which the AES ciphers were designed (one 256 bits key in a few seconds). A very high compatibility with classical channels was also shown, with up to 17 classical channels co-propagating in the same optical fibre together with the quantum channel for a theoretical 1.7 Terabits per second of classical data in the same band when using 100 Gbps transceivers.

[45] A. Aguado, V. Lopez, J. Martinez-Mateo, T. Szyrkowiec, A. Autenrieth, M. Peev, D. Lopez and V. Martin. "Hybrid Conventional and Quantum Security for Software Defined and Virtualized Networks", JOCN 2018

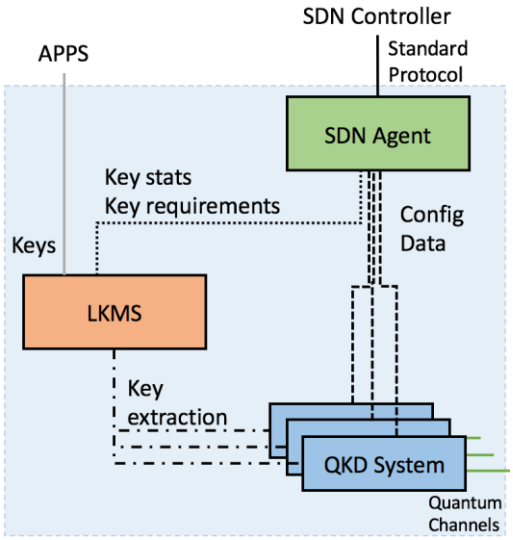

Figure 10. SDN node architecture for end-to-end encryption using QKD as is considered in the European Telecommunications Standards Institute[46].

Roadmap

3 years: deployment of metropolitan-scale testbeds with integration of SDN and QKD in the core and in the access networks
6 years: demonstration of full network stack integrated classical/quantum SDN network in metropolitan area networks
10 years: wide area deployment of integrated QKD networks; demonstration of other quantum communications protocols and applications

6.2 Data centres

Rationale

Data centres are key components of the telecommunications and data network infrastructures (~7,500 worldwide, ~2500 in Europe[47]), which store huge quantities of data. A successful cyber-attack would therefore have very high impact, and protecting data centres will be a high-priority task for the QCI. As a physical protection measure, data centres are typically located away from the place where the data are generated and used, and, to achieve redundancy and guarantee business continuity, they are usually interconnected in pairs at a distance within the range of QKD fibre links e.g. 10's of km. QKD can be used also to protect data storage, although for this particular application the key generation rate should be improved with respect to what is currently achieved [48].

Architecture

Within QCI, a secured Data Centres (DC) Interconnection is composed of pairs of DC that exchange data using quantum secured communications (e.g. with QKD). More data centres can be interconnected, realising a so-called secured data lake. Deploying a secured DC interconnection at intra-metropolitan scale creates a secured ecosystem where independent operators can share their contents stored in different data centres, empowering the business case while preserving the highest security level. Secured

[46] ETSI GS QKD-015 "Quantum Key Distribution Control Interface for Software Defined Networks" A. Aguado, V. Martin, D. Lopez, V. Lopez, J.P. Brito, M. Peev (draft Jan. 2019)
[47] https://cloudscene.com/datacenters-in-europe
[48] Mashide Sasaki "Quantum networks: where should we be heading?" Quantum Sci. Technol. 2,02501, (2017)

interconnection of DCs at longer distances (inter-metropolitan scale) ensures secured disaster recovery. Each DC would implement their storage using quantum keys.

This architecture will provide high resilience, disaster recovery, wide sharing of contents among different operators with the lowest latency time but minimising the possibility of massive eavesdropping from the interconnection. If the security of one DC is compromised, the transfer to another DC using the quantum secured channel allows a faster restoration. One-time pad seems not a practical strategy. Needed key rate for an effective interconnection is expected to exceed the present possibilities and to be achieved in the QCI in the medium term.

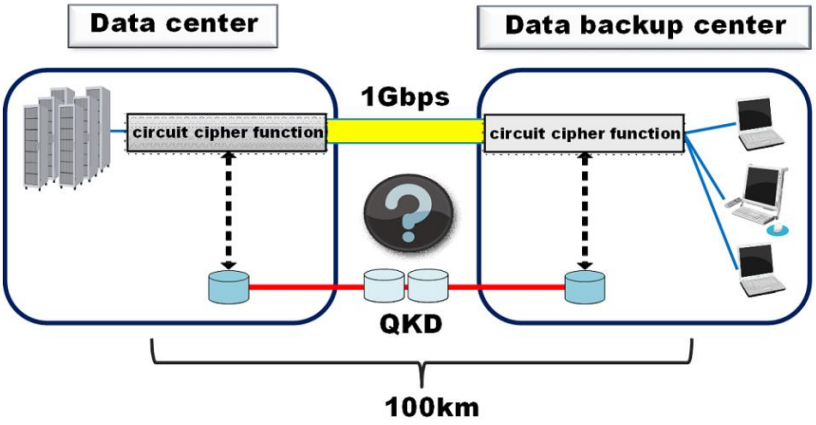

Figure 11. QKD for data centre backup network[49].

Roadmap

3 years: commercial installations expected[50]
6 years: deployment within the QCI for data centres of critical public importance
10 years: data lake secure interconnection within QCI

6.3 Critical infrastructure

Rationale

Cyber-attacks on critical infrastructure are recognized as a European-level threat in the Network and Information Systems (NIS) Directive[51] which identifies some essential services which are very critical for society and are potentially vulnerable to digital attack: energy, digital services, air transport, banks, water supply and healthcare. Priority sectors in the Critical Infrastructure Protection (CIP) Directive[52] are energy and transport, including rail transport, which we also propose be considered for QCI. For all the infrastructure-related use cases, the QCI should guarantee the authentication of the entity requiring access, and the confidentiality and integrity of the data being exchanged and stored.

[49] http://www.uqcc.org/research/technology/subjectD2015_01.html
[50] Some installations have already been done (IDQuantique SA, private communication)
[51] Council/Parliament Directive (EU) 2016/1148 of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems
[52] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. It formally defines critical infrastructure to mean an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.

Architecture

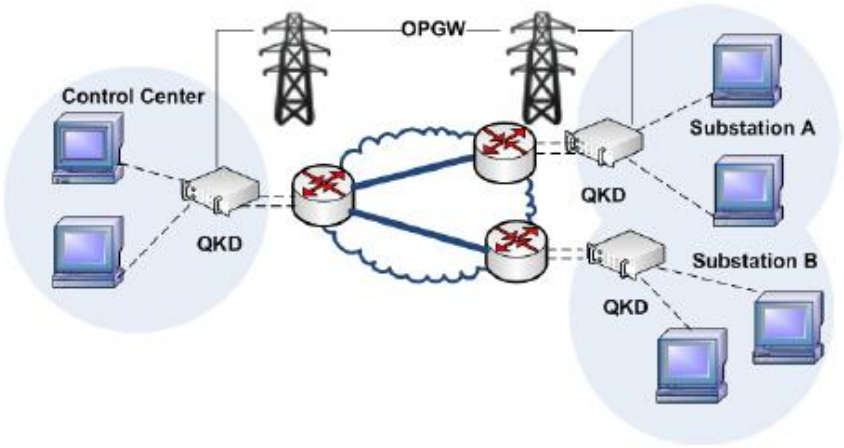

Figure 12. Application of QKD in the power grid. The grid's optical ground wire (OPGW) lines are used to provide the QKD channels[53].

Characteristic of this use case is that many of the infrastructures already have their own dedicated data networks, some of which include fibre links which are sufficiently short for already-available QKD equipment to be used directly.
In aviation, the infrastructure is the air traffic control (ATC) network, especially links between ATC hubs and shorter-distance links to ranging and distance measuring radio beacons and instrument landing system equipment. Eurocontrol has produced a document on the use of QKD to enhance the security of air-to-ground communications[54].
For rail, the goal would be protection of signalling systems and the power network.
Several applications do exist also in the energy sector. For example, the ESA-sponsored project QKD4ECI ("Quantum Key Distribution for European Critical Infrastructure") has identified the remote control of transformer stations as a possible use case for the use of quantum-secured encryption keys distributed by a LEO satellite, and IEEE has considered QKD in its "Vision for smart grid communications"[55].
The QKD architecture and, in particular, the governance of any trusted nodes would be managed by the owners of the critical infrastructure. The high level architecture would be long-haul coverage over terrestrial fibre optic, and an access distribution on Passive Optical Networks, to cover multipoint connections. A possible scenario is an architecture built on two layers: a core layer, defended by quantum communications, which could offer the resilience for essential operations during a cyber-attack, and a peripheral layer, with a less powerful protection, that can be shut-down during a cyber-threat.

[53] http://www.cired.net/publications/cired2013/pdfs/CIRED2013_0154_final.pdf
[54] https://eurocontrol.int/eec/gallery/content/public/documents/projects/CARE/Quantum_Crypt_WP3.pdf
[55] https://ieeexplore.ieee.org/document/6679201

Roadmap

3 years: first examples of infrastructures in the NIS list equipped for QKD
6 years: multipoint QKD distribution on passive optical network infrastructures
10 years: international NIS infrastructures covered by QKD

6.4 Secured synchronization

Rationale

Accurate synchronization of time-related network operations is a core feature of various strategic networks, such as power distribution, telecommunications, and financial trading. New generation wireless telecommunications (i.e. 5G networks) will have a substantial impact on society through the Internet of Things, smart cities, smart transportation and e-commerce. Synchronization better than 20 nanoseconds at all core-locations is required. Smart power distribution grids are a second example of a critical technology that requires real-time control and monitoring systems to ensure stability under increasingly complex conditions. Financial markets require trading venues to synchronize the business clocks to Coordinated Universal Time (UTC).

All these applications are sensitive to perturbation in the network synchronization and a malicious attack to timing could cause serious damage to high speed communications, electrical distribution, and financial trading.

Architecture

QCI will ensure a quantum-secured time distribution. Synchronization uses atomic clocks as primary references, and their reference signal is distributed using one fibre of a pair. Different time transfer techniques are possible, such as coherent methods i.e. keeping the phase of the signal precisely controlled from end to end, or internet protocol-based techniques e.g. Precision Time Protocol (PTP, within the IEEE-1588 standard) where time information is encoded and transmitted digitally. The synchronization signal is encrypted and the key is distributed using QKD. At the beginning, QCI could implement point-to-point secured connection for relevant uses cases such as banks (financial trade synchronization), while in the longer term the architecture will evolve to include multi-point distribution, to serve networks with several synchronized nodes, such as power grids. Quantum-secured synchronization will thus prevent attacks on the smart grid, where managing the synchronization of power flux is crucial and a malicious synchronization could lead to relevant failures. In smart grids, the synchronized network is spread over a large area: hence, long-haul quantum secured channels are required.

QCI will also enable applications where high-density core nodes need to be synchronized, e.g. 5G nodes in metropolitan areas: here a large number of nodes must be synchronized over a relatively small area. In this case the typical distance between nodes is rather small and the QCI architecture will consists of point-to-point segments. A typical topology will be star-like, i.e. with a master core connected to peripheral nodes.

In this use-case, QKD will not be employed since the beginning to reach each single receiver of a 5G networks: at the start, the QCI will not be characterized by a "QKD to the home" architecture, but it will serve only the main nodes. The development of effective multipoint implementations and low-cost chip-scale integrated devices will make possible a further step: we can envisage in particular 5G applications requiring the highest security levels, such as autonomous driving.

Long-haul connections will be based on trusted nodes, which will be managed by the same operator providing the synchronization, or by the owner of the infrastructure to be secured.

Advanced synchronization based on quantum techniques will lead to an intrinsically secure timing facility, embedding the QKD advantages on complex networks such as the one depicted in Figure 13.

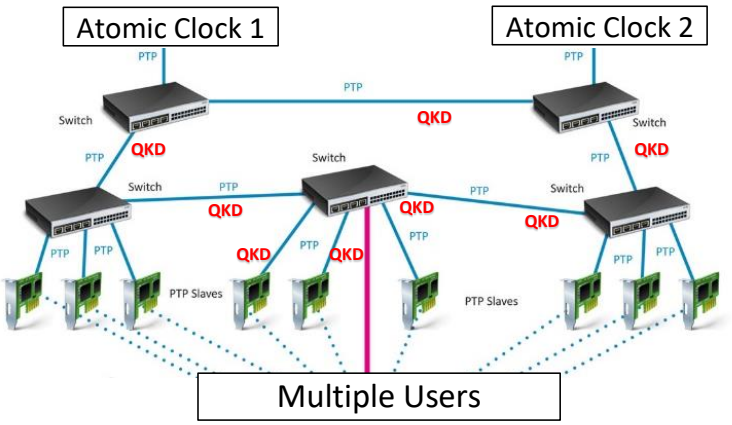

Figure 13. Example of network of secured synchronization, showing a Precision Time Protocol (PTP) time transfer. Two master atomic clocks are used as reference for a network of timing nodes. Time transfer is realized encrypting a protocol-based time signal over fibre. All the fibre connections are secured using a QKD among the nodes. QCI will deploy also multi-point architectures (courtesy INRiM).

Roadmap

3 years: implementation of QKD security for point-to-point time distribution
6 years: star architecture in high-density node networks (e.g. 5G networks)
10 years: certified time stamping with QKD on multi-point architectures

6.5 Governmental data storage and communications

Rationale

Government data requires the highest level of security. With a secrecy lifetime of up to 50 years, it would have devastating consequences if the secrecy of data stored in or exchanged between government centres is compromised. Both long-term secure storage and protection against intercept-now-decrypt-later attacks must be provided, so the increased protection level provided by QKD is definitely valuable. Potential adversaries include hostile governments with very high crypto-analytic resources. At the EU level, both intragovernmental and intergovernmental communications can take place, as well as communications between EU institutions and Member States, among Member States themselves, or among EU institutions themselves. Each of these use-cases has its own peculiarities, but all of them can be addressed at the technical level by the QCI, provided a shared governance model for the infrastructure is developed.

Architecture

An architecture based on fibre links within metropolitan areas would provide useful connectivity for e.g. offices handling classified information and communications between high level political leadership. In the longer term, key distribution to Member State capitals, including from satellite, would become possible. This would be the preferred option for communications among more remote Member States. One-time pad quantum communications could be used for e.g. brief messages between leaders and would be available as a last resort in the case that *all* known cryptographic algorithms were

compromised. QKD and one-time pad will indeed provide an avenue for information-theoretically secure communications: however, with one-time pad the limitation of quantum key transmission rate would represent a significant bottleneck for data transmission, making such application suitable only in case of catastrophic failures of other more efficient approaches.
Given the current distance limitations of QKD, in a first period, an architecture based on trusted nodes needs to be employed for links longer than 50-100km. Such a solution would not guarantee end-to-end quantum security, and both classical physical-layer approaches and algorithmic solutions should be used to ensure the security of the trusted nodes. In addition, a highly redundant architecture which would enable key distribution via different routes is to be adopted, so that the keys remain safe even if some of the nodes are compromised[56]. QKD links can contribute since the beginning to the security of the stored data and of the trusted nodes, by taking advantage of the approach demonstrated for example in the Tokyo deployment[57].
In the EU, the use of trusted nodes will require additional political agreement to ensure trust between the Member States. A typical scenario could start with local networks which do not require trusted nodes, e.g., between EU institutions in Brussels or between governmental authorities located in different ministries in the capital of a Member State. Later, trusted-node enabled links between Brussels and Strasbourg or between Brussels and different capitals of Member States could follow, provided shared procedures to handle the nodes are put in place. A model could be the TESTA network which is currently in use.
Technical solutions such as secret sharing would guarantee that no players hold more control than any other on the infrastructure. In the longer term, the trusted nodes approach will be superseded by the adoption of quantum repeaters and satellite-based QKD links, in such a way that an information-theoretically secure infrastructure will be built. The use of satellites used in the framework of GovSatCom, equipped with an additional QKD payload, can be envisaged for this particular use case.

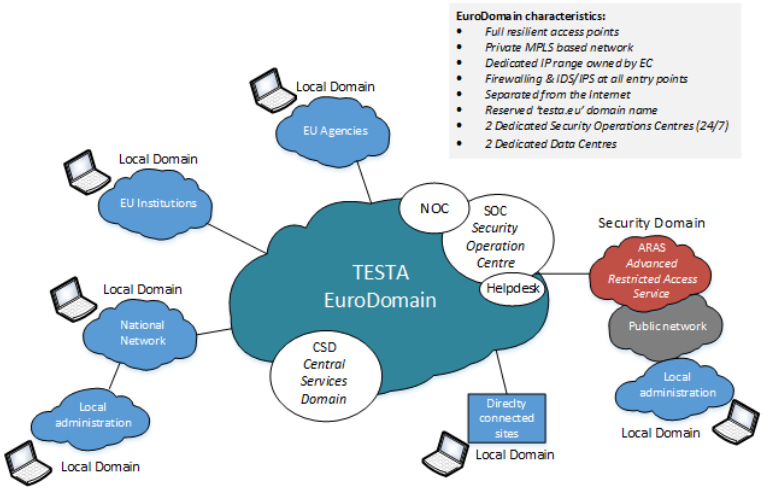

Figure 14. Example of an EU government communications network: the Trans-European Services for Telematics between Administrations (TESTA)[58].

Roadmap

3 years: Terrestrial connections in metropolitan areas
6 years: Fibre-based connections between adjacent metropolitan areas
10 years: Long-range terrestrial and space connections

[56] L. Salvail, M. Peev, E. Diamanti, R. Alléaume, N. Lütkenhaus, and T. Länger "Security of trusted repeater quantum key distribution network", Journal of Computer Security, vol. 18, no. 1, pp. 61-87, 2010
[57] M. Fujiwara, A. Waseda, R. Nojima, S. Moriai, W. Ogata, and M. Sasaki "Unbreakable distributed storage with quantum key distribution network and password-authenticated secret sharing", Scientific Reports 6:28988, 2016
[58] https://ec.europa.eu/isa2/sites/isa/files/testa_-_20_years_-_isa2_june_2018.pdf

6.6 Space systems

Rationale

Space systems are very large investments for which it is reasonable to devote significant resources to protect. Although satellites can be loaded with cryptographic keys at launch, if they are compromised it is not ordinarily possible to access them directly to re-key. QKD can be then used to secure (i) ground (space) to space (ground) communications, (ii) satellite-to-satellite communications and ii) ground-to-ground communications, via the use of a satellite link.

We are now witnessing a new era of space utilisation with ambitious goals: seamlessly connecting users across the globe at high bandwidths, serving as the backbone for the future Internet of Things and ultimately providing space-based cloud services such as data storage and computation. This technical revolution is fuelled by a paradigm shift away from large, individual, costly (~100+ million-Euro) satellites towards scalable, low cost and self-organizing Low Earth Orbit (LEO) satellite constellations. Those offer the unique advantage of providing link speeds previously only known from fibre networks, but now bridging connections across devices, cities, countries and continents.

Already, several commercial constellations aimed at communications and internet distribution have been announced by OneWeb[59] (backed by Airbus), SpaceX[60], and Amazon[61], each with a number of satellites spanning in the thousands. Also Hispasat[62] and Telesat[63] have announced initiatives to enter the small satellite constellation market. New space-based business segments are also quickly emerging, envisaging e.g. a swarm of small satellites equipped with low-cost cameras for earth imagery at a massive scale[64], an array of LEO satellites to generate high-resolution radar images of Earth[65], or even data centres and parallel processors in space[66].

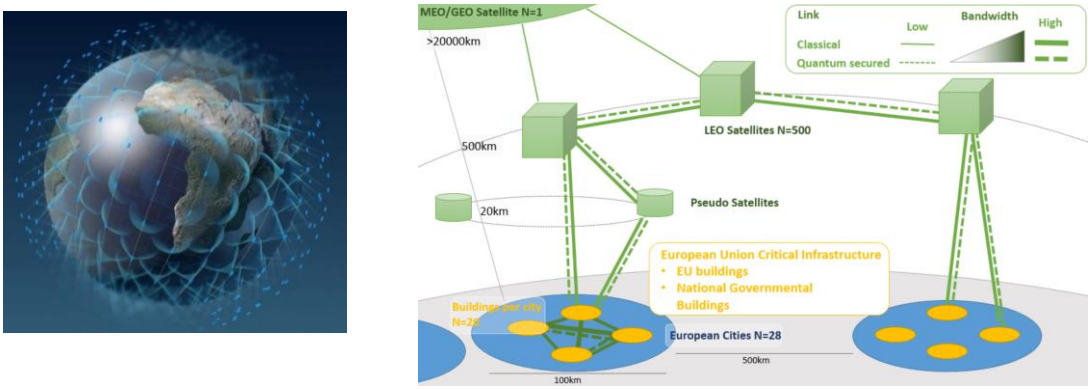

Figure 15. Artist representation of the OneWeb constellation, and possible architecture of a quantum-secured European network via LEO satellites (courtesy Airbus).

A European-designed and operated communications network based on LEO satellites will have substantial benefits for Europe's Member States. Securing those networks with quantum technologies as proposed via the QCI initiative in turn will place Europe in the pole position for continent-wide secure communications among all global players. The

[59] https://www.oneweb.world/the-mission
[60] https://www.spacex.com/webcast
[61] https://www.reuters.com/article/us-amazon-com-broadband/amazon-plans-to-launch-over-3000-satellites-to-offer-broadband-internet-idUSKCN1RG1YW
[62] https://www.hispasat.com/en/press-room/press-releases/archivo-2018/339/hispasat-and-leosat-sign-strategic-investment-agreement
[63] https://www.telesat.com/services/leo/why-leo
[64] https://www.planet.com/
[65] https://www.capellaspace.com/
[66] https://www.datacenterknowledge.com/edge-computing/idea-data-centers-space-just-got-little-less-crazy

QCI initiative could serve as a catalyser for the European Union and its business players to capture a large share of this new space market. For instance, QCI applied to space systems would push the development of LEO-to-ground and LEO-to-LEO optical links adapted to low-cost, mass-produced satellites, a holy-grail in this new space market[67]. As a follow-on step, information could be relayed between data-carrying LEO satellites by leveraging QKD.

Architecture

A recent investigation into a LEO constellation to address the G20 nations indicated that as few as 16 satellites could help distribute 100 Mbits of secure key per year among the 20 capitals[68]. This offers high bandwidth quantum secure communications with a quantum key renewal every minute. A network of similar size is proposed as a minimum 'quantum umbrella' in the sky. In line with the rationale, this QKD capability could be developed as an add-on to a European network in the sky, dedicated to communications, distributed computing, earth observation and/or data processing.

Roadmap

First satellite demonstrations sponsored by EU Member States[69] as well as the European Space Agency[70] are already underway. Importantly, the design requirements of a LEO constellation in terms of availability and performance are in line with those of a free-space quantum secured network: efficient optical satellite-to-satellite and satellite-to-ground connections will provide both high classical and quantum-secured communications channels. Therefore, adding a quantum secured channel already at the design phase would enhance the security of the network while minimizing additional costs. The deployment of additional satellites to gradually form the space segment of the QCI would build on the experience and results of these first activities.

6.7 Defence

Rationale

We include defence use cases here with the understanding that it is still not known whether the defence community will use the EU QCI or will develop its own separate infrastructure. Military use cases will likely include the transmission of classified information related to command and control systems, as well as the distribution of keys toward defence institutions, military bases, military platforms (e.g. aircraft), sensors (e.g. radar systems), or other apparatus. Long range secure communications networks are desired (ideally on a global scale) to reach even Forward Operating Bases in very distant theatres of operations: satellite quantum infrastructure would strongly help to efficiently cover this gap.

Architecture

The defence domain poses strong needs in terms of communications functionalities, which are integrated in the broader suite of technologies for Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance systems (so called C4ISR systems). Communications is said to have applicability for the three levels of warfare—strategic, operational, and tactical—and across the full range of military operations from major combat operations to stability and peacekeeping operations.

[67] Regulation around inter-satellite links is today not well established. Levels of concern around this legal vacuum vary. See for example: https://spacenews.com/oneweb-says-regulatory-concerns-main-reason-its-forgoing-inter-satellite-links/

[68] Vergossen et al., "Satellite Constellations for Trusted Note QKD Networks," arXiv:1903.07845v1, 19 Mar 2019

[69] https://www.bmbf.de/upload_filestore/pub/Quantum_technologies_from_basic_research_to_market.pdf

[70] https://www.ses.com/press-release/esa-and-ses-led-consortium-develop-satellite-based-cybersecurity

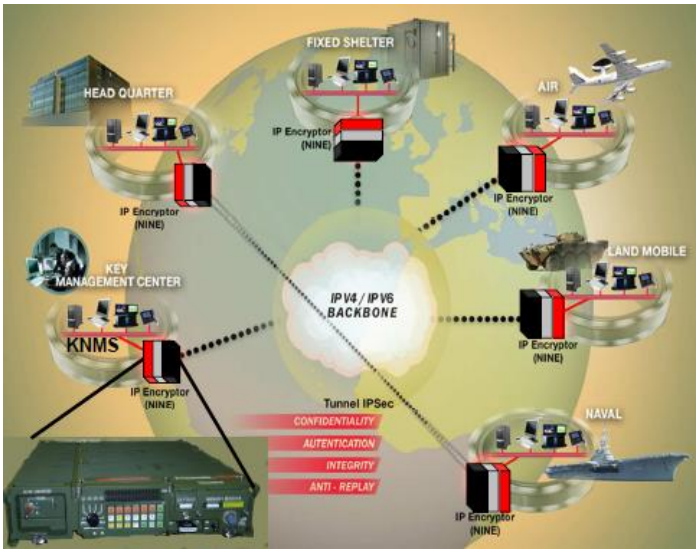

Figure 16. QKD use case for defence (courtesy Leonardo S.p.A).

As in defence use-cases a very high level of classified information may be exchanged, with a strong impact on national security, such a domain poses very stringent requirements. Among such requirements the distribution of sufficiently long keys, possessing a high and certified level of entropy with refresh rates ranging from few key-refresh cycles per hour up to much higher levels, are very general demands.
A potential QKD use case in the military domain may concern strategic infrastructures for national defence. In this case there is a need to interconnect crypto devices to form a "virtual private network" (VPN) able to protect the classified traffic, generated by "trusted" (or red) networks and conveyed over an "untrusted" (or black) IP network. Within the military domain itself, very often segregated networks are used which are intentionally kept separated from each other by a so called "air gap", in order to minimise impact of any security breach. This approach might pose limits to full interaction with an external public communications infrastructure.
In any case, the EU-QCI will foster the development of industrial capabilities of relevant importance for defence. Conversely, the defence sector will be crucial for the development of an EU supply chain of the critical components (e.g. devices such as sources, detectors, but also encoding schemes, protocols, processing and distillation algorithms) to be used in quantum communications, for their extensive testing, and their integration in field-deployable systems. In addition, the military sector is likely to carry out all the security assurance processes up to the highest level. Given the level of reliability and trust that systems developed for defence uses necessitates, this will unavoidably be a rather long process.

Timescale

For this use-case it is more difficult to sketch a roadmap since the timescale will depend on military planning processes. We are currently witnessing a strong interest from EDA and NATO, in terms of dedicated boards and task groups on secure communications based on quantum technologies. Initiatives may be included in the European Defence Fund, which will address defence research and development needs in the next multiannual financial framework[71].

[71] NATO has already funded projects on QKD, including "Secure Quantum Communication Undersea Link SEQUEL" which set up the Sicily-Malta link mentioned in section 4.1. EDA has included quantum communications in its recently issued Call PADR-FDDT-EMERGING-03-2019.

6.8 Distributed quantum computing

Rationale

This decade has seen the emergence of the first quantum processors, and the EU Flagship on Quantum Technologies aims to realize the first European quantum computer. The biggest processors currently count ~ 50 quantum bits, these are still noisy but roughly 100-200 noisy quantum bits could enable quantum simulations to explore new materials and designs for medicines. However, it is expected that for the next 40-50 years, quantum computers will remain very expensive, prompting the use of remote quantum computing services in quantum computing centres.
Using a quantum communications infrastructure makes it possible to use remote quantum computing. What is at stake is to enable feeding remote computers with quantum inputs, and retrieve quantum outputs when processing is done. It is possible to work in a mode such that the entity offering such quantum computing services does not know what the quantum computer is being used for. Specifically, this means a user can use remote quantum computing services without disclosing the design for proprietary new materials and medicines.

Roadmap

This use case being longer term, estimates of the timescales are difficult to make. In the EU Flagship on quantum technologies, activities aim to demonstrate an elementary version of secure delegated quantum computation on remote processors by 2021 and the extension of this through satellite links.
In the later stages QCI can enable networks that connect such quantum processors. Such quantum networks also form the first step towards a pan-European quantum internet enabling many more applications in the future with many use cases beyond the domain of security.

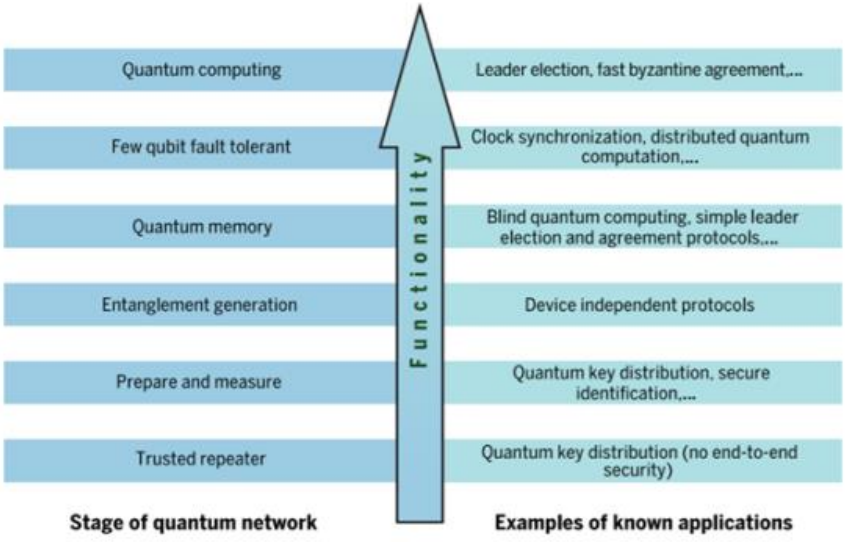

Figure 17. Development roadmap of quantum internet assets[72].

[72]Quantum Internet – A Vision for the road ahead, S. Wehner, D. Elkouss, R. Hanson, Science 2018 https://science.sciencemag.org/content/362/6412/eaam9288

7 Technology status and perspectives

7.1 Ground segment

For fibre-based QKD, early-stage commercial equipment can be purchased. However, no EU supplier is currently present in the market, and the available equipment does not necessarily implement QKD protocols and key processing methods which adhere to formal security standards. Various QKD technologies are available in the EU at lower technology readiness level. For example, measurement-device-independent QKD (MDI-QKD) has been demonstrated both in lab and in the field, offering advantages such as additional guarantees against physical-layer attacks, a star-shaped configuration which allows going beyond point-to-point links, and a better starting point in view of the integration of quantum repeaters. Scaling from point-to-point to more complex topologies is a key element for having the first practical use cases.

Presently, a critical limitation of fibre-based QKD is the distance: at a typical fibre length of ~50km a key rate of 1Mbps can be achieved, which decreases to 10kbps at 100km. To reach longer distances, either trusted nodes, satellite links or quantum repeaters are required, each having different degrees of technology readiness, performance and security. The use of trusted nodes, where acceptable, will definitely enable a series of use cases early on, which then would be upgradable with end-to-end quantum security using quantum repeaters. Although no quantum repeater has been demonstrated yet, Europe is at the forefront in certain areas (e.g. producing long-lived entanglement at distance) which are of key importance for the development of quantum repeaters. Giving the critical importance of these devices for quantum communications, it is crucial to test the technologies they are based on (e.g. photonic quantum memories, quantum light sources, long-lived spin-photon interfaces) in a real world environment, to accelerate their technology evolution and make them available for the later stages of the QCI.

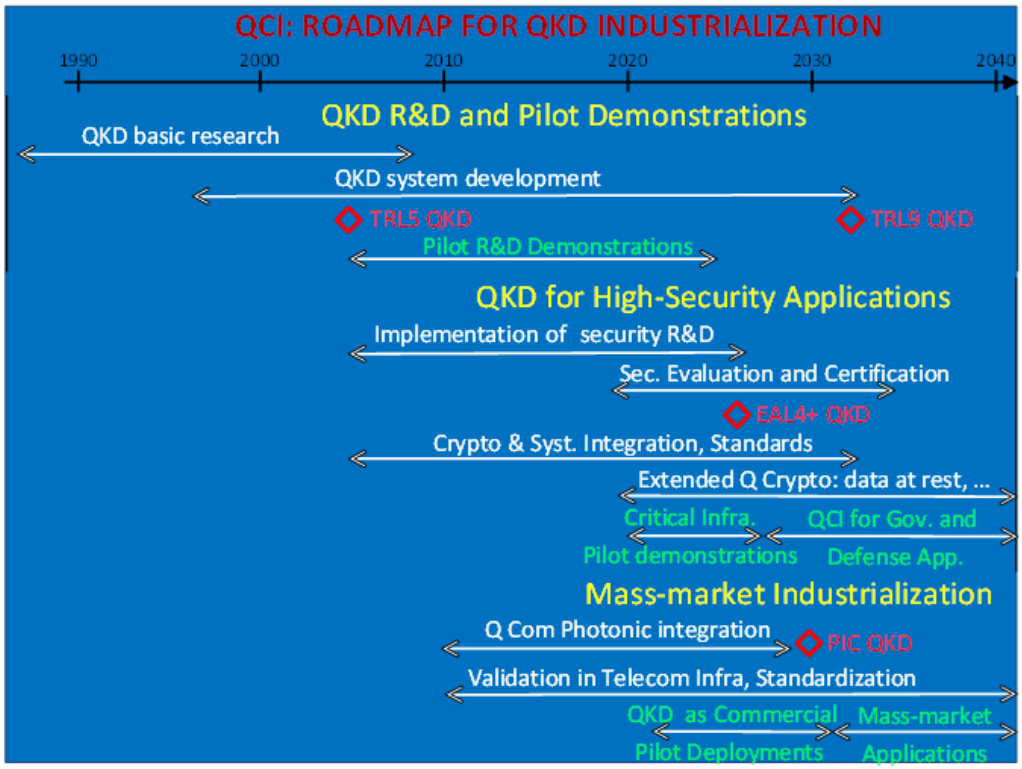

Figure 18. Roadmap for fibre-based QKD development (courtesy Télécom ParisTech).

It must be pointed out that developing QKD equipment will not automatically translate into increased security for European communications and critical infrastructures. An entire ecosystem needs to be built, involving industry all along the value chain and including security professionals capable of integrating quantum security into existing network infrastructures. Testbeds must be deployed, where innovators (e.g. software developers, hardware industry, internet service industry, security professionals) can get access to technology-testing, where new standards, procedures, protocols and security policies can be examined and tested. They will serve as platforms where the quantum and the conventional cybersecurity communities can find a common ground, nurturing trust and acceptance in the technologies which will be used for the QCI. A possible timeframe for the industrial development of commercial-grade QKD solutions is presented in Fig. 18.

As a next step, a more detailed analysis of what are the key technologies and technology components is required for deploying successfully QKD terrestrial networks. The analysis should include an understanding of the critical technology gaps and the steps to be taken to fill them. The above analysis needs to be complemented by a first analysis of the value chain that exists in Europe (from an industrial perspective) that would help us understand better what is the situation today and what would need to be further developed and in which time frames.

Technology perspectives (ground segment)

A provisional timeline is provided below and will be further refined in the next months.

Short term

- Faster and cheaper commercial QKD equipment
- Measurement-device independent approaches
- First multi-node test networks deployed
- Elementary repeater link

Mid-term
First testbeds including quantum repeaters

Long term
Long distance quantum repeater links (e.g. connecting government offices)

7.2 Space segment

Quantum-secured intercontinental connections have been shown by the Chinese LEO satellite Micius, and several tests with planes, unmanned aerial vehicles (UAV), high-altitude platforms (HAP), micro and nanosatellites have been made, also by EU players. Fig. 19 summarizes the main quantum communications programmes being funded.

Constellations of low-Earth-orbit (LEO) satellites are now emerging as a powerful platform to connect remote partners with high-bandwidth free-space optical links. The combination of broadband connectivity and long distance quantum-enforced security make LEO satellites and pseudo-satellites ideal candidates for quantum secured communications. Building a European wide network requires reliable quantum secured interfaces across thousands of kilometres, which could be realized by connecting the quantum secured network of satellites (and potentially pseudo satellites). The optimum combination of LEO, MEO and GEO satellites is the subject of ongoing studies, and is another major design decision for QCI. The space segment will be composed of a space

infrastructure and a ground infrastructure, each of them embedding a telescope and a QKD source and/or QKD receiver.

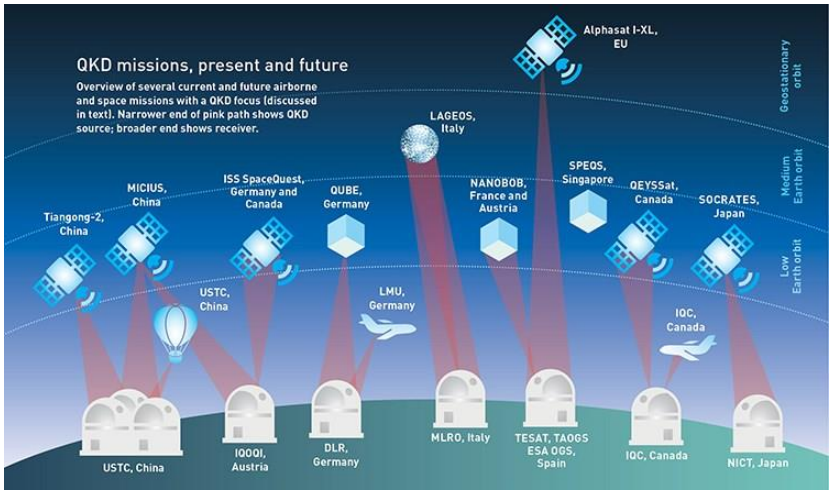

Figure 19. Potential platforms for space-based QCI[73].

Space-based QKD may be used by the QCI to protect long-range communications ensuring end-to-end quantum security. When quantum repeaters become available, they may substitute the satellite links for some applications but we expect that QCI will retain a satellite component long-term for securing space communications, for example in GovSatCom applications. The space segment of the QCI will also be used to protect distributed infrastructure on the ground and space assets by securing communications among remote sites (intercontinental links), potentially benefitting EU programme like Galileo and Copernicus. The ground based telescopes of the QCI could also be used to secure command and control communications with EU satellite assets, if these will be equipped with QKD payloads in the future.

Technology perspective (space segment)
The first priority will be to develop the space segment network architecture, based on the current and future needs. On such basis, the roadmap will be defined. A provisional timeline is provided below and will be further refined in the next months.

Short term
- Space-qualified components
- Field tests with UAV, HAP, nanosatellites

Mid-term
- Dedicated payload on satellites
- Prepare and measure QKD protocols
- Research LEO satellite

Long term
- Dedicated MEO and GEO satellites
- Space-based entanglement distribution

[73] https://www.osa-opn.org/home/articles/volume_29/february_2018/features/satellite-based_qkd/

7.3 A Roadmap of QCI-enabling technologies

Achieving the QCI vision requires several enabling technologies, which are not yet mature. They are expected to become available on different timescales, progressively allowing more and more complex architectures to be deployable. Fig. 20 below shows a 20 year roadmap for the different kinds of quantum network, terrestrial, airborne and satellite-based.

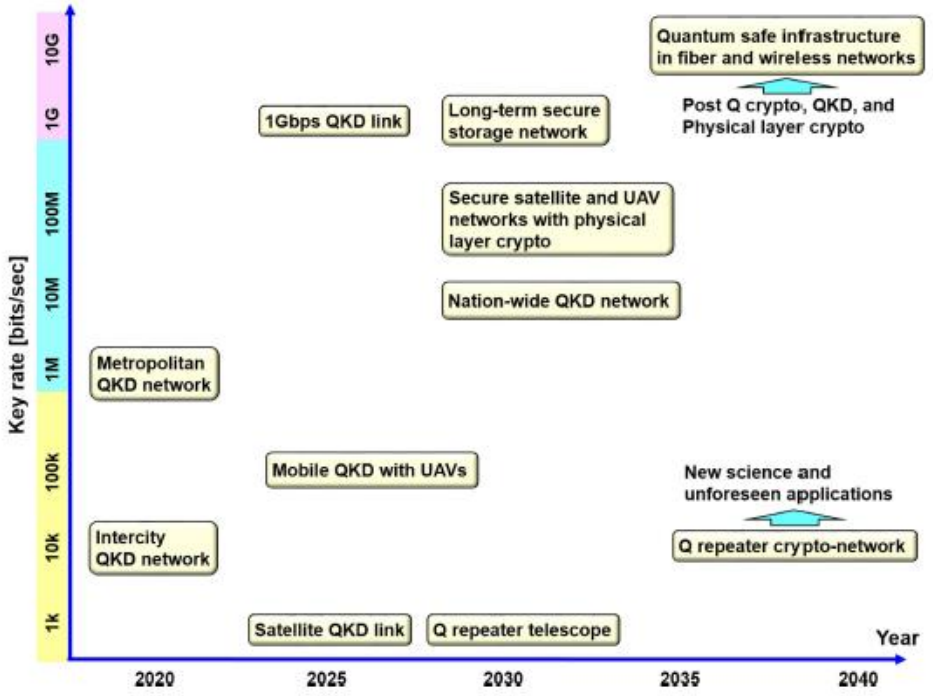

Figure 20. Example of a roadmap for quantum network architectures[74].

7.4 First analysis on challenges to making QCI a reality in the EU

The EU is among the world leaders in fundamental and applied research on quantum technologies. However, more investment and a coordinated effort are needed to translate this body of knowledge into real-world applications. Hindrances to the adoption of novel solutions such as those envisaged by the QCI can in some instances be of a technical nature or due to cost factors, but the real obstacle is probably the acceptance by the wider security community whose advice could and should influence decision makers.

7.4.1 Technical challenges

We present here the most important topics of debate.

1) QKD requires exchange of initial pairwise secrets to support pairwise authentication to secure the actual QKD protocol exchanges, i.e. establishment of pairwise initial secrets is an absolute precondition for QKD security. QKD cannot protect the communications of two parties that have never "met" before. To allow such interactions it should rely on a public key infrastructure, which means on computational assumption typical of asymmetric crypto.

[74] https://iopscience.iop.org/article/10.1088/2058-9565/aa6994/meta

Rebuttal: the interaction needs to be only very brief, to initiate the secure channel. QKD is said to create long term security from short term assumptions.

2) By fundamentally securing a shared symmetric encryption key, QKD addresses the issue of communications confidentiality, whereas in the large majority of real-world applications key agreement is not as important as authentication and integrity. *Rebuttal*: research is ongoing to extend the scope of quantum communications to address these aspects. Also, there are use cases where confidentiality is the most pressing aspect.

3) QKD is informational-theoretically secure only with one time-pad, and this limits considerably the addressable use-cases. All other encryption schemes, although widely considered to be very secure, are based on mathematical assumptions. *Rebuttal*: the assumptions required for secure-symmetric encryption are not as strong as those made for asymmetric encryption. For example, a quantum computer just large enough to represent a threat to contemporary asymmetric cryptography schemes would be nothing like large enough to threaten contemporary symmetric cryptography schemes, using known algorithms in both cases.

4) The seriousness of the threat represented by quantum computing is still very difficult to assess[75], and quantum resistant algorithms will emerge which could cope with it in a much more practical and cheap way than quantum-based cryptography. *Rebuttal*: the majority opinion is that there is a significant risk of the quantum computing threat becoming real within the lifetime of some currently stored data. While quantum resistant algorithms may provide a more practical solution, this also cannot be guaranteed at the present time. There is no reason why both approaches should not be pursued, subject to the optimal partition of resources between each.

5) Quantum cryptography exploits new technologies to build complex systems, so implementation of security will become a major issue. The potential existence of new unexpected types of side channels, some of them linked to the very existence of the quantum channel ("quantum hacking") cannot be ruled out. Conversely, the side channels which could affect traditional electronic crypto equipment which implements mathematical algorithms have been the object of extensive analysis for a long time, and bad surprises are less likely.
Rebuttal: substantial experience has also been built up by the quantum communications community; defensive measures are well-developed, including protocols which are in principle less vulnerable to side-channel attacks.

6) Trusted nodes would re-introduce a huge number of problems that were successfully solved by end-to-end network encryption protocols in the last 25 years using symmetric and/or asymmetric cryptography. Typical examples: which persons get physical access to the trusted node? How to guarantee the absence of side channels and/or Trojan horses leaking keys or unprotected information outside of this trusted node environment? How to prevent service technicians / others with access to the trusted node introducing new side channel or Trojan horse mechanisms? End-to-end security, i.e. the absence of trusted nodes, is the primary tenet in today's secure communications, and there seem to be no compelling reasons to trade-in this property for complex physical implementations relying on trusted nodes, given that a quantum safe end-to-end implementation by means of post-quantum cryptography is likely to become available.
Rebuttal: quantum communications are advocated because of expected future vulnerabilities in asymmetric cryptography which will imperil our ability to enforce

[75] In particular, it has been pointed out that current engineering approaches could not directly scale to develop a fault-tolerant quantum computer with millions of qubits (which is the dimension presently deemed necessary for practical cryptoanalysis), see "Quantum Computer: progress and prospects", a consensus study report from the USA National Academy Press, https://www.nap.edu/catalog/25196/quantum-computing-progress-and-prospects. As pointed out in a study from the German Federal Office for Information Security, even on such a large machine it would take several days to crack RSA-2048bits asymmetric cryptography by using Shor's algorithm, see https://www.bsi.bund.de/DE/Publikationen/Studien/Quantencomputer/quantencomputer.html.

end-to-end security as it is implemented now. Use cases exist where hardware is, in practice, protected by physical security measures, where the introduction of trusted nodes would be relatively straightforward and QKD could be applied in the short term. In the long term, quantum repeaters ensuring end-to-end quantum security could change the picture, provided the overall QKD scheme will be information-theoretically secure.

7) The absence of certified and authorised devices and certification criteria, and the fact that early commercial products were compromised quite quickly, means that we are still in the phase of experimentation rather than application in concrete use-cases. The fact that no QKD solutions have received a security accreditation is an evidence of the low maturity of QKD implementation robustness.
   Rebuttal: this is the subject of ongoing work by ETSI and BSI. The QCI project will be a driver for this.
8) None of the cybersecurity attacks which have recently produced so much damage have exploited cryptographic weaknesses, and introducing QKD in the affected infrastructures will not reduce their vulnerability against such attacks. European resources should therefore be spent on more pressing cybersecurity issues, such as better system design, withdrawal of known vulnerable software and addressing human factors, especially by training. Since it is already extremely hard to provide protection against the currently known threats, the EU has to carefully select where to spend money to reinforce cyber defences.
   Rebuttal: The scale of the present problem justifies pursuing all available solutions, even those which are currently perceived as more long term.
9) It is difficult to justify on the basis of economic and financial viability, an infrastructure which currently offers only key distribution services. Given its rigid nature (i.e. a point-to-point or multi-point network with dedicated quantum devices at each end using either extensive fibre networks with trusted repeaters or earth-to-satellite links), it is also difficult to see how the QCI could guarantee the mobility requirements expected by businesses and citizens alike. Its clientele is likely to remain limited to cases where mobility can be sacrificed (e.g. a financial organization requiring QKD services for its different branches, a Member State communicating with embassies, and maybe some military applications, given that these require high mobility during operations). Point-to-point solutions do not scale well with the mobile paradigm and the Internet of Things, thus greatly limiting their commercial appeal.
   Rebuttal: the advent of the mobile paradigm does not imply that backbones will become obsolete, for example in 5G they are expected to be of major importance, and there is no sign of datacentres dying out. In addition, low-cost chip-scale QKD is also being researched, and the EU is investing in this within the Quantum Technology Flagship.

7.4.2 Policy challenges

Much more can be said in the debate on the pros and cons of the various security technologies being currently investigated, but the discussion would quickly become of a very technical nature. It is nevertheless reasonable to expect that the best solutions will emerge from the exploration of all the possible directions of research. In the current situation, the existence of promising security use cases for QKD and other related quantum technologies is the object of debate among security experts[76], and to ensure that the infrastructure will actually serve the purpose intended it is essential that all the points of view are taken into account. Since the QCI is intended to be a security infrastructure, its development would require very detailed knowledge about the weaknesses of the solutions currently employed, which are of a sensitive nature and not

[76] http://publications.jrc.ec.europa.eu/repository/bitstream/JRC107386/jrc_report_quantumcommunications.pdf

easily shared by the players. It may therefore be necessary to establish a proper framework where sensitive information can be further developed and shared.

The development of the QCI must be able to trigger European-level collaborations, and possibly integration beyond national cybersecurity ecosystem, for the emerging era of quantum security. This process can only be progressive and necessitates a long-term (at least 10 years) vision. Nevertheless, a concrete action plan starting from 2021 should be put in place to foster the engagement in the technology development process of stakeholders such as the national security agencies and the cybersecurity industry. Such an engagement would ensure that development of security-related technologies is accompanied by a security assurance process which will deliver the appropriate certification and authorisation: this is a necessary pre-condition for most applications.

An independent argument in favour of the QCI is that its development process, if properly managed, would permit the EU to maintain its mastery of quantum technologies, and be ready to adopt quantum communications solutions including but not limited to security in the likely case that new unexpected uses emerge. This mastery will be critical for the EU'S strategic autonomy. Presently, the development of QKD systems belongs essentially to the realm of frontier and applied research, and is aimed at segments of the global market such as academic research, telecommunications, photonics, and network security. Asian companies and governments dominate the deployment of QKD in these market segments, following the national strategic investments that China, Japan and Korea have done in the last ~10 years. Against this background, proper measures should be envisaged to help establish an EU-based supply chain for development of critical components and devices, manufacturing capabilities, system assembly, and production scaling (e.g. including photonic integration); properly skilled human resources are indispensable so relevant training will also be required.

8 Conclusions

There is sound case for the EU to build a QCI, providing some critical conditions are met.

It should be seen as both insurance and investment.

On the insurance side, the threats are 1) the slow but expected emergence of quantum computing, especially if no satisfactory quantum resistant algorithm were found and 2) the possible sudden loss of cryptographic protection if a new cryptanalytical attack was found, whether classical or quantum. Resources to be deployed on QCI should be proportionate and weighed carefully against other cybersecurity priorities. The idea is to spend what is necessary to protect against a loss which could not be easily borne were it to occur, even though the risk might not be high. Indeed, more and more of our economy is dependent on exchange and storage of electronic data, which are mostly protected by only a few cryptographic algorithms: as a consequence, if such algorithms were suddenly no longer reliable, the possible loss would be enormous, affecting not only current data exchange but stored, encrypted data as well. One can also gauge the potential impact from the scale of existing cybercrime.

On the investment side, building a QCI would spur the development of indigenous EU quantum information industry which would be a very valuable security and economic asset, helping the EU to achieve long-term strategic autonomy. It would position the EU well to introduce new quantum communications technologies as they became available. The condition here is that building the industrial and technological base must be given high priority in planning the QCI. It would make little sense to rush ahead to build an infrastructure which depended on "dead-end" technologies or whose future the EU could not control. With time, the QCI will transcend its initial purposes of being essentially a security infrastructure. An already envisaged application is that it would enable an exponential increase in computing power by connecting different quantum processors. Another is to fully exploit the potential of networks of quantum sensors.

The objections raised by critics within the cybersecurity community should not be lightly dismissed but rather seen as warning signs of known risks, which should be taken into consideration in planning. The involvement of this community is crucial, especially with regard to scrutinising the QCI for possible security weaknesses. A formal certification/authorisation process is seen as mandatory.

Quantum communications is an emerging technology field and the timescale for when key technology elements become available is uncertain. But waiting it out at the research level until the situation is known better is unwise, because a rapid deployment could become necessary. Therefore a flexible plan is required, with scaling-up in stages, as knowledge is gained and the best way forward becomes clearer. We have endeavoured here to start this planning process by outlining the most promising use cases and their expected time scales.

List of abbreviations

ARTES	Advanced Research in Telecommunications Systems (ESA programme)
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CIP	Critical Infrastructure Protection
CNR	Consiglio Nazionale delle Ricerche
CSD	Central Services Domain
DARPA	Defense Advanced Research Projects Agency (of USA)
DC	Data Centre
EAL	Evaluation Assurance Level
ENISA	European Union Agency for Network and Information Security
ESA	European Space Agency
ETSI	European Telecommunication Standards Institute
FET	Future and Emerging Technology
FOB	Forward Operating Base
GEO	Geosynchronous Earth Orbit
GovSatCom	Government Satellite Communications
HAP	High Altitude Platform
INRiM	Istituto Nazionale di Ricerca Metrologica
ITU	International Telecommunication Union
JRC	Joint Research Centre
LENS	European Laboratory for Non-Linear Spectroscopy
KISTI	Korea Institute of Science and Technology Information
QRNG	Quantum Random Number Generator
LEO	Low Earth Orbit
MDI	Measurement Device Independent
MEO	Medium Earth Orbit
NFD	Network Function Virtualization
NIS	Network and Information Security
NOC	Network Operations Centre
PTP	Precision Time Protocol
QCI	Quantum Communications Infrastructure
QKD	Quantum Key Distribution
QRA	Quantum Resistant Algorithm
QSC	Quantum Safe Cryptography
SAGA	Secure And cryptoGrAphic Mission
SCADA	Supervisory control and data acquisition
ScyLight	Secure and Laser communications Technology
SDN	Software Defined Network
SOG-IS	Senior Officials Group - Information Systems Security
SOC	Security Operations Centre
TESTA	Trans-European Services for Telematics between Administrations
TREL	Toshiba Research Europe Ltd.
TRL	Technology Readiness Level
UAV	Unmanned Aerial Vehicle
USTC	University of Science and Technology of China
UTC	Coordinated Universal Time
VPN	Virtual Private Network

List of figures

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: https://europa.eu/european-union/contact_en

On the phone or by email

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

- by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),

- at the following standard number: +32 22999696, or

- by electronic mail via: https://europa.eu/european-union/contact_en

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: https://europa.eu/european-union/index_en

EU publications
You can download or order free and priced EU publications from EU Bookshop at: https://publications.europa.eu/en/publications. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact_en).

KJ-NA-31133-EN-N

The European Commission's science and knowledge service

Joint Research Centre

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.

EU Science Hub

ec.europa.eu/jrc

@EU_ScienceHub

EU Science Hub - Joint Research Centre

EU Science, Research and Innovation

EU Science Hub

Publications Office of the European Union

doi:10.2760/180945

ISBN 978-92-76-53705-2