European Commission

JRC SCIENCE FOR POLICY REPORT

THE IMPACT OF QUANTUM TECHNOLOGIES ON THE EU'S FUTURE POLICIES

PART 2
Quantum communications: from science to policies

Adam M. Lewis, AML
Martino Travagnin, MT

2018

EUR 29017 EN

Joint Research Centre

Contact information
Name: Adam Lewis
Address: TP 186 Centro Comune di Ricerca, Via E. Fermi 2749, 21027 Ispra (VA), ITALY
Email: Adam.Lewis@ec.europa.eu

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

JRC107386

EUR 29017 EN

PDF ISBN 978-92-79-77314-3 ISSN 1831-9424 doi:10.2760/881896

Ispra, Italy: European Commission, 2018

How to cite: Author(s); title; EUR; doi

Quantum communications: from science to policies

Abstract
Quantum physics yields cryptographic applications which are expected to contribute to communications security, in particular by providing protection against attacks by future quantum computers. Technology development programmes in quantum communications, including the deployment of quantum networks, are therefore being funded worldwide. Europe should accelerate the industrial uptake of its scientific knowledge in the field.

Contents

Acknowledgements 1
Executive summary 2
1. Introduction 4
2. Scientific background 6
2.1. Quantum key distribution 6
2.2. Other quantum cryptography primitives 9
2.3. Physical implementations 11
3. Technology development 16
3.1. Patent landscape 16
3.2. Industry players 20
3.3. Public programmes 26
4. Policy issues 36
4.1. The threat of quantum computing 36
4.2. Technology push and market pull 40
4.3. Application areas 43
4.4. International commerce 46
4.5. Privacy and security 49
5. Conclusion 53
References 56
List of abbreviations and definitions 79
List of figures 80

Acknowledgements

We would like to thank the delegates who attended the workshop on quantum key distribution organised by the JRC on June 15, 2016, at the Politecnico di Torino (Italy). We are indebted to our JRC colleagues Naouma Kourti, Carlo Ferigato, Igor Nai Fovino, Laurent Beslay, Jean-Pierre Nordvik, and Pierpaolo Malinverni for helpful discussions. We are also grateful to the referees who contributed to improving the quality of the manuscript, by pointing out some inaccuracies and providing additional information.

This work was funded by the JRC as part of its institutional work programme, work package 3792 of project 244.

Executive summary

Quantum communications technologies encode information in quantum states of light to transmit it at macroscopic distances, and enable particularly transformative applications in cryptography. Among them the most technologically mature is quantum key distribution (QKD), which allows securely sharing a private encryption key. QKD exploits quantum physics to make apparent any eavesdropping attempt taking place during the key exchange and to measure the leaked information, thus enabling two legitimate partners to know whether the private key they intend to use for encryption was compromised during its transmission, and to which degree. Commercial QKD systems are already available on the market, and other quantum cryptography primitives based on the same principles and similar technologies are expected to soon emerge from research labs, to ensure e.g. message authenticity, integrity, and non-repudiation. Given the importance that cryptography has for privacy and security, the rise of completely novel tools has to be analysed also with regard to its policy implications.

Quantum cryptography is based on fundamental physics, and is therefore robust against crypto-analytical progress. An important technology driver could therefore be the development of a general-purpose quantum computer, which would allow running already available quantum algorithms able to break significant segments of classical cryptography. Opinions about the actual usefulness of quantum cryptography are however starkly divided. Its critics highlight its limitations in terms of compatibility with existing telecom infrastructure, performances, and cost; they underline its vulnerability to implementation loopholes, and add that algorithmic quantum-safe cryptography can be developed to address in a more practical way the threats posed by quantum computing. Conversely, its backers stress that ongoing research has removed all serious vulnerabilities and increased performance to a level high enough for various practical applications, that compatibility issues are being addressed, and that cost will decrease as technology spreads. They add that many unknowns shroud the development of secure quantum-safe algorithms, which in any case will remain vulnerable to progress in crypto-analysis, both from the theoretical and the computational side.

Ensuring communications privacy is such a high-stake challenge in the era of mass communications, that the potential economic value of quantum cryptography is huge even if it turns out to be suitable to play only a circumscribed role. Several industries are therefore investigating this technology: manufacturers of telecom equipment and optoelectronic devices, communications providers, information technology enterprises, suppliers of internet services, firms in the security and defence sectors, and some start-ups which have emerged from the academic world. The interest of governments is also keen, and not limited to fostering economic growth. Cryptography is indeed important for applications such as preventing interception of classified information, providing governmental services, protecting critical infrastructure, and in the military field. Banks and financial institutions, data centres providers, and players in the health sector can also be potential users. A home-grown industry mastering a technique that potentially guarantees future-proof communications security can hence be seen as an issue of national security. Quantum cryptography constitutes, therefore, a sensitive issue, and public programmes aimed at technological development and transitioning from laboratory science to industrial applications in real-world settings are being pursued all over the world.

In Europe, the fundamental and applied research that has been done especially by universities constitutes a promising basis for technology transfer and market uptake. However, big manufacturers from the USA and Japan have shown much more commitment in industrial take-up than European ones. Additionally, China has demonstrated, in pushing this technology, an extremely effective top-to-bottom approach, and can now be considered at the forefront both for applied research and for deployments. The European Commission recently started a quantum technologies (QT) flagship initiative to address the risk that other countries will take advantage of the know-how developed in Europe, and several national programmes in QT are being

funded by EU Member States. QuantERA, an ERA-NET co-fund in quantum technologies spanning 26 (mostly European) countries, issued its first calls in 2017. Meanwhile, the European Space Agency has begun working on satellite quantum communications, and the EU Cooperation in Science and Technology (COST) programme has started a project dedicated to QT space applications.

It is a shared conviction among both academic and industrial researchers that, in order to open up a market for quantum cryptography technologies, standardisation and certification procedures must be agreed at supranational level and use-cases of interest to private businesses must be elaborated. Measures should also be taken to break disciplinary boundaries, e.g. by establishing working groups including, alongside quantum specialists, also experts on conventional security and telecom engineers, and by deploying pilot quantum networks to be used both as testing grounds by researchers and as demonstrators for possible users. To enhance market pull, the EU should also consider acting as an early adopter, in fields such as e-government, infrastructure protection, or in the common defence policy area. Existing EU networks could be upgraded to accommodate photonic services and quantum cryptography, and new backbones should start to be planned in coordination with national initiatives already underway. It must also be taken into account that at the moment Europe is critically dependent on foreign vendors for some high-tech components that hold a large share of the economic value of a quantum communications system: the EU, and in particular DG GROW, should therefore consider funding manufacturing pilot lines for quantum devices, flanking the ones already set up in the framework of its actions concerning photonics as a key enabling technology.

Legislative measures must also be taken to eliminate the fragmentation of the internal market, which still severely affects security and defence industries. To this aim, it is essential to embed quantum cryptography in policy agendas already being pursued, e.g. the DG Migration and Home Affairs programme 'Industry for Security'. Barriers to commerce such as country-specific regulations should be eliminated. Limitations to export should also be reduced, e.g. by including quantum cryptography in the negotiation of free trade agreements or in the ongoing revision of the regulation of dual-use technologies exports, carried on by DG for Trade. Measures should also be taken to protect European know-how as industries try to enter difficult markets, and notably the Chinese one.

It is also necessary to keep a watchful eye on longer-term policy implications that could become of primary concern if a widespread diffusion of quantum cryptography takes place. For example, a properly engineered QKD system makes it impossible to intercept the private encryption key without being detected. It therefore contributes to the EU policy commitment for strong cryptography, which is seen as both a significant economic driver and an essential pillar for cybersecurity. On the other side, it has been recognised that the increasing availability of robust cryptographic schemes is already depriving law enforcement agencies (LEAs) of valuable instruments for crime prevention and investigation, since it prevents gathering of information by intercepting the communication line. In the EU, purposely weakening cryptographic techniques by implanting backdoors or by indiscriminately exploiting security loopholes has never been considered as a policy option to give back LEAs their interception capabilities. Conversely, new investigative techniques are being developed, such as targeted device hacking under proper legislative safeguards. The EC is indeed encouraging Member States to develop a toolbox of alternative investigation techniques and to share them, simultaneously stating that measures that could weaken encryption or have an impact on a larger or indiscriminate number of people would not be considered. The development of quantum cryptography constitutes therefore a new technology driver for this approach, as well as an additional instrument to engineer EU long-term policy aims.

1. Introduction

The European Commission Joint Research Centre (JRC) has started studying the policy implications of developments in quantum technologies in an 'Issue paper' published in 2016 [JRC QuantumTech 2016], to which the reader is referred for background information on motivations, methods, and purposes. A first report dedicated to quantum time has already been published [JRC QuantumTime 2017]. The JRC is now continuing its work by analysing the emergence of information processing and communication technologies based on quantum physics: this second report deals with quantum communications, while a last one on quantum computing is in preparation.

Quantum communications allows transformative applications for communications security. The most technologically mature is quantum key distribution (QKD), which allows the secure distribution of a private encryption key to be employed by two partners to exchange confidential information along a public channel. Several other cryptographic applications exploiting quantum principles are starting to emerge, and many researchers expect that they will play an important role for communication security. By exploiting fundamental physical laws instead of computational algorithms, quantum cryptography constitutes a significant shift with respect to current practices.

In Chapter 2 we provide the reader with a basic scientific background, to allow him or her to appreciate the role quantum cryptography can play for communication security. In Chapter 3 we shift from science to technology: we briefly overview the main players who are developing intellectual property and physical systems for quantum key distribution, and describe the public programmes that governments worldwide are funding to foster cryptographic applications of quantum communications. Chapter 4 then is devoted to an analysis of the related policy issues. It is organised in five different sections, which deal respectively with each one of the themes we found to be of interest for policymakers:

1. In section 4.1 we explain how the most important technological driver behind the interest for quantum cryptography is the practical progress towards a quantum computer and its crypto-analytical capabilities. Indeed, being based on physical principles and not on computational hardness, quantum cryptographic protocols cannot be attacked by the crypto-analytical capabilities of a quantum computer. However, solutions based on new cryptographic algorithms resistant to quantum-enabled crypto-analysis are also being developed. Security agencies are starting to acknowledge the risks posed by quantum computation, and standardisation bodies are working on quantum-safe cryptography, based both on new algorithms and on quantum physics. The approach taken by regulators against the likeliness that some cryptographic practices now widely in use become unsafe following the development of quantum computers will strongly influence the diffusion and the market uptake of quantum cryptography.
2. In section 4.2 we show that there are two main policy drivers for state-sponsored technology push programmes in quantum communications: develop a domestic capability in a novel industry, which has critical security implications alongside significant economic potential, and build communication backbones which will remain resistant to malevolent actors and foreign intelligence even in the post-quantum era. China is currently the country where state intervention is having by far the largest impact, and its policies seem to be determined by techno-nationalistic considerations not less than economic ones. However, all developed countries are to varying degrees funding national policies of technology development. Several industries are also positioning themselves in this field, but in the present situation it seems far from assured that market forces by themselves will provide the conditions for a wide use of this technology, because of the several factors which still constitute severe hindrances for market uptake. The overall perception is that the diffusion of quantum cryptography will depend on policy decisions and regulatory frameworks not less than on technical issues and economic factors, and that a careful mix of technology push and market pull is necessary to help quantum cryptography find its right place in the communications security landscape.

3. In section 4.3 we review the main application areas where quantum cryptography is being tested, and the businesses which are acting as early users. In the public sector, quantum networks are being built essentially to shield from interception sensitive governmental and military communications. However, also the possibility to use QKD for the protection of critical infrastructure against cyber-attacks is being analysed. Work is more advanced for smart grids and power distribution systems, but also transport, telecom infrastructure and satellite constellations used for navigation are being considered. In the private sector, early adopters have been firms that needed to connect headquarters with other corporate sites, enterprises in the health sector dealing with sensitive information, and owners of data centres willing to secure the back-up process. The banking industry is also testing QKD systems, sometimes via government-funded quantum backbones. Short-range quantum communication chips integrated in mobile phones are also being developed, and their use to download encryption key from a network of 'quantum-enabled' cash dispensers can constitute a route to consumer QKD.
4. In section 4.4 we will see that policy action is also necessary to ensure a free market which is as wide as possible, where fair competition among industry players can take place. In particular, country-specific certification for governmental uses among EU Member States represents a significant burden for compliance, especially for small players: even at the EU level trade barriers, often raised quoting homeland security concerns, still exist. In the international landscape, the determined top-to-bottom approach chosen by China is actually contributing some market pull. However, local firms are granted privileged access and foreign competitors are forced to forge joint ventures with domestic players, so that measures to protect intellectual property of industries trying to enter the Chinese market must be taken. Legislation on export restriction due to the dual-use nature of cryptographic technology must be carefully balanced, in such a way that it does not hurt European industries more than their international competitors.
5. In section 4.5 we assess how the balance of privacy versus security will be affected by quantum cryptography. It is already acknowledged that the increasing availability of strong end-to-end encryption in internet-based communications is making it extremely difficult for law enforcing agencies to gain potentially important information by employing lawful interception along the communication line, and quantum cryptography is likely to compound this problem. As a consequence, LEAs recur more and more frequently to hacking the suspect's personal devices in order to intercept a communication before it is encrypted or after it has been decrypted. The use of these so called 'offensive technologies' is considerably more intrusive for privacy than intercepting communication on the flight along the telecom infrastructure, and therefore requires careful balancing the right of the individual against the possible investigative advantages. In addition, being based on exploiting security flaws or purposely inserting them, it entails some degree of cybersecurity risk, lest some of the relevant know-how becomes available to malevolent actors. The policy responses triggered by the progressive availability of unassailable cryptographic techniques must therefore carefully weight risks against advantages, and proper regulatory frameworks must be developed whenever necessary.

In Chapter 5 we draw the main conclusions of our analysis, providing a set of policy recommendations and suggestions for further actions to be undertaken at the EU level.

We hope that this report will shed some light on the challenges that EU policymakers and regulators are to face in order to nurture and manage the cryptographic applications of quantum communications. Despite difficulties and uncertainties always associated with the development of novel technologies, we think that a clear case can be made for the EU to support quantum cryptography, since it holds the promise of becoming a significant driver for European economic growth and for global security.

2. Scientific background

Quantum cryptography introduces communication security in the physical layer, and therefore differs profoundly from currently employed conventional cryptographic techniques, which operate via algorithms running in the data layers. Although several quantum cryptography primitives are currently being investigated, quantum key distribution is the first one to have been experimentally demonstrated and the most technologically mature, as well the only one for which commercial systems are available on the market — systems that may constitute the basis for the practical implementation of other primitives. We will therefore take QKD as the starting point for a basic introduction to quantum cryptography ([1]).

QKD exploits quantum physics to allow two legitimate parties to share a private key that is subsequently used to encrypt a confidential message to be transmitted along a public classical channel. The key is ensured to be private since it is transmitted along a quantum channel in a way that makes any eavesdropping attempt apparent to the legitimate parties. This is accomplished by taking advantage of fundamental laws such as the uncertainty principle (that limits the amount of total information that can be extracted from measurements on pairs of conjugate variables), the no-cloning theorem (that prevents the creation of an identical copy of an unknown arbitrary quantum state), and the existence of entanglement (by which two physically separated particles are intertwined in such a way that interacting with one of them unavoidably affects the state of the other). Because of these fundamental principles any information leakage from a quantum channel always results in a degradation of the information that is actually transmitted, and this degradation can be quantitatively related to a measurable increase in the quantum bit error rate by employing appropriate techniques. Quantum key distribution is indeed based on the possibility to establish an upper limit on the amount of information leaked from a quantum communication channel: by using suitable mathematical procedures, this amount can then be reduced to a level deemed acceptable for the relevant security purposes. It is important to note that an existing optical link cannot automatically be assumed to be compatible with a QKD protocol, since in general it includes devices such as optical amplifiers, routers, and transceivers, which destroy the information encoded in quantum states.

In section 2.1 we give a general introduction on encryption and explain the role of QKD, while in section 2.2 we briefly present other quantum-enabled cryptographic primitives; finally, section 2.3 overviews the possible implementations of these scientific principles.

2.1. Quantum key distribution

Encryption is at the core of information security in the digital age, and consists in the transformation of a 'cleartext' readable by everyone into a 'cyphertext' that can be understood only by the intended recipient. All the cryptographic methods used in modern telecommunications involve the use of disclosed mathematical algorithms and secret keys, in accordance with Kerckhoffs's principle. They are divided into two broad categories: symmetric key systems and asymmetric key systems.

([1]) Since this report is intended for a public without a background in quantum physics, we will eschew all the technical details regarding the issues under discussion, which constitute the object of the hundreds of scientific papers that are published annually. Indeed, a quick Scopus search on 'quantum key distribution' (which is by far the most explored sub-field of quantum communications) reveals that a total of ~ 5 300 papers have been published on this subject up to April 2017. The trend has been rising for at least 20 years, and culminated with the ~ 500 papers published in 2016.
A recent primer on quantum technologies for the non-specialist is [The Economist 2017]. For Quantum Communications, the reader is referred to [Gisin 2002] for a first overview, and to [Diamanti 2016] for a recent update. In [Dusek 2006] and [Alléaume 2014] topics specific to quantum cryptography are dealt with. The scientific event of reference in this field is the 'International Conference on Quantum Cryptography': the last in the series is the 2017 edition (see http://2017.qcrypt.net).

In symmetric key systems the same secret key is used by the sender Alice to encrypt the message, and then by the recipient Bob to decrypt it. This obviously opens the problem: how can the two parties share a secret key if they need it to establish a secure communication? Asymmetric key systems solved this issue in the 1970s by introducing a pair of mathematically related different keys: a public key used for the encryption, and a uniquely related private key that is necessary for the decryption. The intended recipient of a message generates a public/private key pair, and broadcasts the public key. The sender uses this public key to encrypt his message, and then sends the cyphertext to the recipient that can decrypt it with the private key corresponding to the broadcasted public one.

Asymmetric key systems therefore allow for secure transmission over an unsecure channel, since the private key is never transmitted to anybody and the algorithm is chosen so that deducing it from the public key is 'computationally hard', i.e. unfeasible in practice. However, given that using asymmetric cryptography is computationally much more demanding than symmetric, the broadcasted public key is typically not employed to encrypt the actual message: rather, it provides the solution for the problem stated above, by providing a way to securely exchange along an unsecure channel the private symmetric key that will be used both to encrypt and to decrypt the message.

A preliminary problem must also be addressed to provide secure communications along a public channel, namely the verification of the identities of the two parties. Let us take the example of e-commerce: how can I be sure that a swindler is not impersonating the vendor I think I am communicating with, and therefore that I am not sending him, encrypted with the public key he broadcasted, my credit card data, that he will then decrypt with his private key? In other terms, the public channel along which the communication takes place has to be 'authenticated', to prevent man-in-the-middle attacks where a third party impersonates Alice to Bob, and impersonates Bob to Alice.

The authentication issue is addressed by resorting to a public key infrastructure (PKI): a limited number of trusted certificate authorities (CAs), which can be either private companies or governmental agencies) verify the identities of organisations or individuals requesting an asymmetric key pair, and then issue them the pair, or certify their one. Commercial web browsers are then manufactured in such a way that they automatically recognise when a broadcasted public encryption key has been issued or certified by the CAs, and only in this case assume its validity.

The classical algorithms ordinarily used for asymmetric and symmetric cryptography are founded on the mathematical principle of computational hardness, i.e. on an extremely demanding computational task. They would not provide security against a hypothetical adversary with unbounded computational power: they are not 'information theoretically secure' (ITS). What they do provide is 'practical computation security', meaning that the best attack among those we know would require computational resources much larger than the ones we estimate our adversary will be able to deploy against us.

Practical computational security is typically achieved by using long enough encryption keys: a trade-off however exists, because longer keys imply that the legitimate user will also have to spend more resources for encryption and decryption. In addition, practical computational security allows a patient adversary to steal the encrypted data now, and decrypt them later on, when he could have developed more powerful computational resources (crypto-analytic algorithms, processing speed, memory, time, etc.). In particular, as will be discussed later on, the development of a quantum computer can represent a major threat for some of the algorithms employed in classical cryptography.

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 Alice to a receiver Bob 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 to ensure the secrecy of the key. Several different

QKD implementations exist, all of them requiring as initial resources a public quantum channel and an authenticated public classic channel.

Channel authentication is a key issue also for conventional cryptography. It has been demonstrated that to authenticate a classical public channel in an ITS way the two legitimate players need only to share a short initial secret key [Wegman 1981]. Conversely, a crucial result of information theory states that to achieve ITS encryption one needs a random key with an entropy as great as the message itself: loosely speaking, we can say that the random encryption key must be as long as the message. In addition, it is required that the key must be used only once, e.g. in a so-called one time pad (also known as Vernam's cipher), which is its bit-by-bit XOR composition with the message.

In a classical scenario, these essential requirements for ITS communications imply the continuous transmission of extremely long secret keys: the entropy of the short secret key used for channel authentication is indeed too small, and cannot be increased by classical means. From this point of view, QKD can be seen as a key expansion technique that has no classical counterparts, since it exploits quantum physics to expand the entropy of the short authentication key to any required level. In principle, QKD can be employed to obtain a key as long as the message, and then encrypt it by using one time pad. In practice smaller entropy than that needed for true ITS communications is often considered enough, and all the available commercial systems make use of a block cypher like the Advanced Encryption Standard (AES) [NIST FIPS 197].

Another important property of QKD is universal composability, meaning that when used in combination with other cryptographic protocols which are information theoretically secure (ITS) and universally composable (UC), the resulting composed cryptographic protocol will also be ITS and UC. One-time pad is universally composable, and therefore when used with a QKD-expanded key the resulting protocol will be both UC and ITS: as a consequence, even an adversary with unbounded (classical or quantum) computational power will never be able to crack it.

Any QKD system requires a quantum channel and an authenticated classical channel to connect Alice and Bob. It is assumed that an eavesdropper Eve can intercept all the traffic flowing through these two channels, but that well-defined 'safe boundaries' around Alice and Bob equipment cannot be penetrated. This last assumption can somewhat be relaxed with so-called device-independent protocols, whose implementations however are characterised by much lower performances and technology-readiness with respect to more conventional 'prepare and measure' ones.

Generally speaking, any QKD process 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, Alice and Bob 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 Eve might have been intercepting to an arbitrarily small level, allowing therefore the distillation of a private key. Any QKD system therefore requires as initialisation step the authentication of a classical public channel. We have already seen that this can be done in an ITS way via a short secret initialisation key shared by the legitimate users, and a practical solution would be to use public key cryptography to establish this initialisation secret key. Of course, in this case the whole scheme would no longer be information theoretically secure. However, to take advantage of this weakness the eavesdropper is obliged to mount a man-in-the-middle attack during the very first channel authentication round. If this attack is not successful, then the key expanded via QKD would be perfectly secure, and a part of it could later be used for successive channel authentications.

QKD therefore denies an adversary the possibility of a 'store now, decrypt later' approach. Consequently, in order to decide on the asymmetric cryptography algorithm to be used and its key length, the legitimate parties only have to make reasonable

assumptions about the computational resources an adversary can deploy during the first authentication of the channel. Indeed, if the authentication is not broken during the first round of QKD, even if it is only computationally secure, then all subsequent rounds of QKD will be ITS. In this sense, it is usually said that QKD allows building long-term unconditional security out of short-term assumptions, and that under these conditions it provides everlasting secrecy. QKD can therefore be used in combination with a public key infrastructure that offers the necessary simplicity and flexibility: even if the asymmetric scheme is deemed secure only for a limited time span, long-term security is then ensured by QKD.

Everlasting secrecy is different from the forward secrecy that can be obtained with conventional public key cryptography, which relies on the use of different ephemeral keys to authenticate the channel in each traffic session. In this way the symmetric encrypting keys that are being established in each session are independent from one another, and if one of them is at any time compromised only the traffic exchanged during that particular session can be decrypted.

Everlasting secrecy is a much stronger property and includes forward secrecy, since it depends only on the security of the first channel authentication round. Since the term 'unconditional security' is employed as a synonym for 'information-theoretic security', it is necessary to clarify that the demonstrated QKD unconditional security is actually based on a series of conditions: indeed, in addition to the secrecy of the initial channel authentication key, the following assumptions have to be made:

1. The laws of quantum mechanics hold true. The non-cloning theorem in particular is exploited for the more technologically ready implementations based on discrete states prepare and measure, while the Bell inequality is at the basis of more advanced device-independent implementations.
2. As with classical cryptography, the adversary has no access to Alice's and Bob's QKD equipment, but only to the communication channels. Note that the presence in QKD of a public quantum channel alongside the classical one allows exploiting possible additional quantum-specific loopholes alongside classical ones, therefore allowing for 'quantum hacking'.
3. The implementation should not have non-idealities which are not properly addressed. This means that every possible side-channel that could allow for information leakage must be known and properly characterised: only so called device-independent QKD allows relaxing this issue, at least to a certain extent. In particular, the algorithms used for the generation of pseudorandom numbers must pass specific randomness tests, as e.g. those included in the NIST Statistical Test Suite, Special Publication 800-22.

We remark that randomness is an extremely important issue also in classical cryptography. Physical-based randomness can be achieved e.g. by employing quantum random numbers generators, and some devices that generate true random number by exploiting quantum physics are already in the market, having passed the relevant certification processes [IDQ QRNG], [Quintessence QRNG].

2.2. Other quantum cryptography primitives

Here we will give a brief overview of other quantum-based cryptographic primitives. Our overview will be limited to cryptographic primitives that have been experimentally demonstrated, and will not cover all the protocols that have been subject to theoretical investigation and rely on quantum memories or quantum computation. Although limited in scope, this short summary will show how, building on QKD know-how, protocols and physical systems allow the addressing of a rich variety of different (and sometimes much subtler) cryptographic tasks: in this regard, QKD can be seen as both an entry point and an enabler for many other cryptographic techniques.

To give some historical perspective, we point out that the very first suggestion on the use of quantum physics to accomplish cryptographic tasks impossible in a classical

framework predates the publication of the BB84 QKD protocol in 1984. In the 70s, a paper was written that outlined how quantum communication can provide a way to merge two classical messages in such a way that the recipient can extract either of them, but not both. Additionally, it showed also how quantum techniques could be employed to produce banknotes impossible to counterfeit. The paper was rejected by the journal to which it was submitted and went unpublished until 1983 [Wiesner 1983].

It is now clear that quantum physics has a fundamental role to play in the field of discreet decision-making, where two parties have to make a joint decision based on their private information, compromising its confidentiality as little as possible. We have already seen that quantum physics allows for unconditionally secure communication between parties that trust each other. Conversely, when the parties do not trust each other but must somehow collaborate, quantum physics will in general not suffice to guarantee security, and extra assumptions are to be made. In particular, most of the cryptographic primitives we will describe below are not secure if a quantum channel is available to an adversary that is not subject to further restrictions and can exploit non-local quantum correlations such as those provided by entanglement. Nevertheless, two-party protocols are so pivotal to modern cryptography that it is essential to explore scenarios that allow provable security in important real-world settings where realistic restrictions bound the adversary's actions.

Quantum signatures. Digital signatures are stronger than channel authentication, because they guarantee transferability and non-repudiation of a message which is ensured not to have been forged or tampered with, i.e. whose integrity is guaranteed. The algorithms on which digital signatures are based rely on computational hardness, whose validity will cease with the advent of a quantum computer. Quantum signature protocols that do not need trusted authorities, are ITS, and can be implemented with QKD components have been demonstrated [Amiri 2016], although their limited performances make them presently unsuitable for practical use.

In **position-based quantum cryptography** the geographical position of a person is the only credential for accessing secured data and services, and enables secure communication over an insecure channel without having any pre-shared key. It also allows users to verify that a received message originates from a particular geographical position and was not modified during the transmission. While with classical communication such tasks are impossible, it has been demonstrated within well-specified limits they can be achieved if players resort to quantum communication, and experimental results based on QKD hardware have been demonstrated [Broadbent 2016], [Schaffner homepage], [ERCIM news].

Bit commitment is a two-phase protocol between two mistrusting parties, Alice and Bob. In the first step Alice decides a bit value and sends Bob a confirmation that she has committed to a value, giving a 'hint' to it that however does not allow Bob to actually learn the committed value. In the second step Alice reveals the value to Bob, and the hint received in the previous step allows him to detect whether Alice has cheated, i.e. has changed the bit value she previously committed. Information-theoretically secure bit commitment schemes cannot exist classically, and it has been demonstrated that the same holds true even with protocols resorting to quantum mechanics: actually, quantum effects such as entanglement can be exploited by either of the two parties to cheat. In other terms, quantum physics is not enough to guarantee security unless extra assumptions are made. We point out that such assumptions need not be of a technological nature, and could be based on fundamental laws coming from other realms of physics: for example, unconditionally secure bit commitment has been experimentally demonstrated using QKD systems by taking advantage of relativistic causality constraints [Lunghi 2013], [Liu 2014].

Quantum coin flipping. As we have seen, QKD allows distributing a secret key with information-theoretic security between two trusted and collaborating communicating parties. However, in many advanced cryptographic schemes the two parties do not trust

each other and hence cannot collaborate. Coin flipping, where two spatially separated distrustful parties share a randomly generated bit whose value must be unbiased, is especially important for example in distributed computing. Although unconditionally secure coin flipping is known to be impossible both in the classical and in the quantum domain, some advantages of quantum over classical communication have been demonstrated in a scheme that makes use of QKD hardware [Pappa 2014].

In an **oblivious transfer** protocol a sender transfers one of potentially many pieces of information to a receiver, but remains oblivious as to what piece (if any) has been transferred. In a one-out-of-two (1 out of *n*) oblivious transfer, Alice has two (*n*) messages that she sends to Bob in such a way that he can decide to receive either of them at his choosing, but not both (all). Alice never finds out which message Bob receives. Such a protocol is essential for secure multi-party computation, since it allows a user to get exactly one database element without the server getting to know which element was queried, and without the user knowing anything about the other elements that were not retrieved. An experimental implementation of oblivious transfer in the noisy storage model, based on a modified entangled quantum key distribution system, has been demonstrated under the physical assumption that an adversary does not possess a large reliable quantum memory [Erven 2014].

2.3. Physical implementations

In this paragraph we will briefly describe how a QKD system works. Since there are several different ways to implement the various QKD protocols developed to date, our explanation has mainly the aim of providing some background to anchor general concepts. Because of its simplicity and didactic value, we focus on the BB84 protocol, which was the first one to be proposed (in 1984). It is still used today, and is also the starting point from which more sophisticated protocols have been developed. As will become clear from the description, BB84 is an example of the 'prepare and measure' protocol applied to discrete variables and based on the no-cloning theorem. For the sake of clarity, we will consider the case when the quantum state being transported is the polarisation of single photons [Qui 2010].

Let us assume that the sender Alice generates a random bit (i.e. a '0' or a '1'), and then encodes it in one of two different polarisation bases (respectively called rectilinear and diagonal), randomly chosen. In the first basis a '0' is encoded by a photon with horizontal polarisation (0 °) and a '1' by a photon with vertical polarisation (90 °), while in the second basis a '0' is encoded by a photon with diagonal polarisation (45 °) and a '1' by a photon with antidiagonal polarisation (135 °). Since the receiver Bob does not know Alice's basis selection, he measures the polarisation of the incoming photons by randomly choosing the rectilinear or the diagonal basis. If he happens to use the same basis employed for the encoding, he will measure the right polarisation; conversely, if he chooses the wrong basis, the result of his measurement will be a random projection on it of the encoded polarisation, which gives the correct result only with a 50% probability. After a long sequence of photons has been exchanged, Alice and Bob compare the basis they have respectively employed for encoding and measuring, communicating via the authenticated channel. They keep only the random bits generated and detected with matched basis, which are said to constitute the sifted keys. In an ideal system without noise, imperfections, and disturbances, the sifted keys are identical, and can be used as a private key.

Let us now imagine that an eavesdropper Eve intercepts Alice's photons, measures their polarisation, and then sends forward to Bob photons with polarisations identical to the ones she has measured. Since she doesn't know the basis used by Alice for polarisation encoding, she will use the right one only in 50 % of the interceptions: in these cases she measures the right polarisation and sends forward to Bob photons with a polarisation identical to the one transmitted by Alice. But since the other 50% of the intercepted photons will be measured in the wrong basis, they will be projected on the wrong

polarisation with a 50 % probability. To summarise, three quarters of the photons intercepted by Eve give her the right bit value and are forwarded unchanged to Bob; the last quarter, on the contrary, will give her the wrong bit, and will be forwarded to Bob in a state different from the one encoded by Alice. As a consequence, when Alice and Bob compare their sifted keys, they will be able to detect the interception, because of this 25 % quantum bit error rate. It is therefore impossible for Eve to gain information from the quantum channel without introducing errors: this feature, which has been here illustrated for a particular communication protocol, constitutes a general property of quantum communications.

What we have here described is a 4-state BB84 protocol, but qubits can be encoded also using only two (non-orthogonal) polarisations, or conversely using six different polarisation states, with different advantages and disadvantages. Polarisation encoding is typical of free air QKD, since, to first approximation, free-space propagation does not affect polarisation. However, information can also be encoded in the relative phase of photons, and this is actually the preferred option when the quantum channel is an optical fibre, which does not preserve the polarisation state of a propagating photon.

Whatever the actual protocol chosen, in any real world implementation some errors will unavoidably be present (e.g. generated by imperfections in the polarisation controllers, disturbances in the transmission channel, noise in the detectors, and so on). Although the legitimate partners may have some knowledge about the quantum bit error rate (QBER) level associated with the intrinsic limitations and imperfections of their system and of the quantum channel, the most conservative behaviour would be to attribute all the errors to Eve's eavesdropping activity. It can be demonstrated that if the QBER is above a certain threshold, a secure key cannot be generated and the qubit transmission process must be repeated [Gottesman 2008]. Conversely, below a certain QBER threshold, information reconciliation (i.e. error correction) and privacy amplification algorithms can be applied that will lead to establish an identical key, shorter with respect to the initial one but with the guarantee that any possible information Eve may have acquired about it has been reduced to an arbitrary small level.

Just to fix the ideas, here is the description of a basic error correction code: Alice chooses a random pair among the bits she has transmitted, and communicates to Bob which pair she has chosen (i.e. which bits, not their actual values) and the result of her XOR operations. Bob performs the same operation between the corresponding bits he has received, and compares his result with the one communicated by Alice. If the two results coincide, Alice and Bob keep the first bit of the pair, otherwise they reject both of them. It can be demonstrated that by repeatedly applying this procedure, the differences among the sifted keys can be reduced to an arbitrary low level, i.e. information reconciliation can be achieved. In practical systems, this means reducing the QBER from $\sim 10^{-2}$ to $\sim 10^{-9}$. Once the QBER has been suppressed, a privacy amplification protocol is used to reduce the information that Eve may have gained about the sifted key. A basic scheme works as follows: as before, Alice chooses a random pair of bits and performs an exclusive or (XOR) on them, but now she communicates to Bob only the pair she has chosen — not the result of her XOR operation. Bob calculates the value of the XOR of his corresponding pair, and both of them substitute in their sifted keys the pair with a single bit, to which they give the value of the pair XOR that each one of them has calculated. This scheme exploits the fact that Eve's information about the XOR of a pair of bits is smaller than whatever (incomplete) information she might have about the two bits of the pair. As a consequence, by repeatedly applying the procedure, Alice and Bob can reduce the information possibly leaked to Eve to an arbitrary small level.

The information reconciliation and privacy amplification algorithms that are actually employed are much more sophisticated than those here described; they however work on the same principle of combining the information distributed among several qubits: this unavoidably implies that the higher the initial QBER and the smaller the acceptable level of leaked information, the shorter will be the final secure key. We have therefore

here at play some fundamental factors that limit the bit rate at which a secure ('distilled') key can be obtained.

Another unavoidable limitation in the performance of the system is determined by the optical losses inevitably introduced by the transmission channel: the longer the channel, the higher the fraction of photons that get lost during their flight. In addition, some of those which actually make it to their destination are not measured, because of the finite efficiency of the single photon detectors. These factors will introduce a trade-off between the distance and the bit rate at which Alice and Bob can transmit a secure key. Note that the reduced bit rate can ultimately represent a security weakness, since it will prevent refreshing the private key as often as it would be desirable, resulting in a so-called 'stale key'. For a fibre-based commercial system the current state of the art is a key rate of ~ Mbit/s (which is deemed acceptable for AES encryption and for video transmission) 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. Although this solution allows for easy integration of lawful interception systems, it runs against the 'end-to-end' encryption approach that is presently preferred by most services providers. 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.

Having thus described in some detail the BB84 protocol, let us now briefly mention other ways to implement a QKD system which make use of different peculiarities of quantum physics. Continuous-variable QKD is based on the Heisenberg uncertainty principle, applied to the quadrature components of the electromagnetic field associated with a propagating light beam [Grosshans 2003], [Diamanti 2015]. In a typical CV-QKD embodiment, Alice superimposes random Gaussian modulations on the amplitude and phase of the coherent states that are transmitted to Bob as successive optical pulses, alongside a phase reference signal. For each received pulse, Bob randomly chooses one of the two components, and using the reference signal in a homodyne detection scheme measures its modulation with a low-noise detector. He then informs Alice about which quadrature he has chosen, so that from each one of the transmitted pulses the two partners extract a pair of values, corresponding respectively to the applied and the measured modulation in the randomly chosen quadratures. By collecting these values over several pulses two pairs of Gaussian distributions will emerge, one at Alice's side and one at Bob's, which constitute a set of correlated Gaussian variables, to which suitable information reconciliation and privacy amplification protocols can be applied. The evidence of a possible eavesdropping follows from the fact that the two field quadratures correspond to non-commuting observables, and that Eve cannot do better than randomly choosing one of them for each of her eavesdropping measurements. When she happens to measure the wrong one, because of the Heisenberg principle she will introduce a disturbance in the orthogonal one, which was actually chosen by Bob. As a consequence, the legitimate partners can detect her activity by comparing their correlated Gaussian distributions: these are said to constitute a Gaussian key, from which a common binary key can be obtained via a specifically designed reconciliation algorithm. With respect to discrete variable protocols like BB84, the main advantage of CV-QKD is the fact that it makes use of the standard devices used for coherent telecommunications: in particular it dispenses with single photon detectors, since information is encoded in light pulses containing several photons. On the other hand, it requires heavier computational post processing, and suffers from an increased sensitivity to channel noise that reduce somewhat the maximum distance with respect to discrete variable protocols: typical key rates of ~ Mbit/s for distances of ~ 10 km can be achieved. Longer distances have however been demonstrated [Jouguet 2013], as well as

compatibility with standard data traffic [Kumar 2015]. Small start-ups sell commercial systems, while big telecom corporations are involved in pre-competitive research.

Entanglement is another peculiarly quantum phenomenon that can also be exploited for QKD. We recall that two entangled photons are correlated non-classically in such a way that any action (typically a measurement) that projects one of them into a quantum state instantaneously projects the other member of the pair into the orthogonal state, independent of their distance. Let us imagine that a source of polarisation-entangled photons, generating pairs in either the rectilinear or diagonal basis, is placed between Alice and Bob, in such a way that each one of them receives one of the photons of the pair. They then randomly choose one of the two bases to measure the polarisation, and by comparing their results they can see whether someone is staging an intercept and resend attack. Indeed, for an ideal system and in the absence of eavesdropping a perfect anti-correlation of the measured polarisation is the expected result whenever the same measurement basis is used by the two legitimate partners.

Entanglement can be used for quantum cryptographic purposes also by testing the quantum non-local correlations that can be revealed by a Bell inequality violation, since any eavesdropping would destroy such correlations. The recent loophole-free experimental demonstration of a Bell inequality violation [Hensen 2015] represented a major advance in this field, and raised interest in so-called device-independent QKD approaches, which reduce the room an eavesdropper may have in the exploitation of implementation loopholes. Attacks to detectors, which are usually the most vulnerable part of a QKD apparatus, can be tackled effectively with measurement-device-independent QKD, which is often implemented employing entangled photons. MDI-QKD can also be used to enrich the topology of a QKD network beyond the simple point-to-point, by putting at the centre of a star of users a single untrusted node at which all measurements are made.

In general, all known systems based on entanglement have far lower performance in terms of key rate for a given distance than the 'prepare and measure' implementations we described above, and are less technologically mature. Nevertheless, in the longer run, entanglement is expected to play a major role for quantum cryptography, since it is at the core of the quantum repeaters that must be developed to increase the reach of QKD systems without resorting to 'trusted node' architectures.

Quantum repeaters, for which various schemes have been proposed, work by establishing entanglement stepwise between parties at progressively greater distances until the required span is attained. Unlike classical repeaters, each step requires a data exchange overhead. Over long distances, multiple repeaters will be required. Nevertheless, the reduction in the data rate due to the total overhead can be much less than the one associated with optical losses in a single-link scheme, in principle allowing end-to-end quantum encryption over continental distances. The demonstration that quantum memories are not necessarily needed for quantum repeaters certainly represented an advance in this matter: however, a quantum repeater without quantum memory suffers from larger overheads, and its final advantages are still a matter under investigation. In general, the development of quantum repeaters to a technology readiness level that allows for field deployment is still seen as a long-term (i.e. more than 10 years) challenge.

Long-range QKD can be achieved also by deploying a space-based entanglement source, which will provide the coverage of a large area, possibly up to intercontinental scale. It has been pointed out that entanglement can also be used to ensure that a key has not been compromised after it has been transmitted, thus providing key storage security in addition to key transmission security. For this aim, the two legitimate partners have to measure the entangled variables and compare their results also before the key is used, and not only as they receive the photons. Of course, this requires efficient ways to transfer the entanglement from photons to systems (e.g. atomic or nuclear spin) more

suitable to long-term storage of quantum states: indeed, entanglement transferral and quantum memories are important long-term research topics for quantum cryptography.

Let us also briefly mention the main directions into which applied research on QKD systems is unfolding. First of all, work is progressing to enhance system performance, by developing more efficient quantum devices such as single photon emitters, single photon detectors, low-noise detectors, modulators, sources of entangled photons, quantum random number generators, and (for the longer term) quantum repeaters. It has been pointed out that also control electronics and data processing can play a major role in certain embodiments. Then we have efforts aimed at increasing system reliability and decreasing cost, in particular by resorting to chip-scale integration of components such as sources and modulators, polarisation controllers, interferometers, and detectors. Another important topic is system security, which is enhanced by identifying and addressing non-idealities in devices and loopholes in engineering implementations, working out theoretical security proofs for the existing protocols, looking at new and possibly device-independent protocols, and compiling catalogues of possible attacks. We have also the issue of the integration with existing infrastructure (e.g. multiplexing quantum and classical signals on the same fibre), and the enlargement of addressable use cases (e.g. by enriching QKD network topology, developing mobile hand-held QKD). The activities related to standardisation and certifications must also be mentioned, in particular the ETSI efforts for security implementation [ETSI 2017].

To complete this scientific overview, we briefly summarise some critical voices. On a fundamental level, some researchers challenge the claim that QKD is information-theoretically-secure and affirm that there are some flaws in the related demonstrations [Hirota 2012], [Yuen 2016], [Bernstein paper 2016]. On the implementation level, a flourishing line of so-called 'quantum hacking' investigations [Makarov website], [Scarani 2012] have shown how engineering loopholes have repeatedly affected the application of the theory to practical systems, so that new defence mechanisms have had to be developed for each type of attack. It does appear that until now, QKD system builders have been able to counter all of the known hacks. But this has required ad hoc defence measures such as detectors to monitor for invasive light pulses or filters to exclude them. Researchers in QKD see these investigations as a necessary feedback mechanism that will contribute to the development of increasingly secure systems. They add that also conventional cryptography can be attacked in the physical layer by exploiting side channels, e.g. the characteristic noise patterns emitted by a computer while performing certain cryptographic operations.

3. Technology development

In this chapter we provide some elements that allow identifying the main players in the technology development of quantum communication, and in particular of its most technologically mature application, i.e. quantum key distribution. In section 3.1 we present a patent analysis to evidence the business sectors which are positioning themselves in this area, by developing intellectual property and know-how. Section 3.2 presents a list of the industries which are actually developing QKD systems, working at a precompetitive level or actually selling products. In section 3.3 we finally overview the technology development programmes on quantum communications which are being funded by several governments, with the aim of supporting a technology that is seen simultaneously as a driver of economic growth and a factor of national security.

3.1. Patent landscape

Patent analysis can be used to gain some insight on the main players which are developing a technology, and a certain foresight at the unfolding trends. An investigation of the patenting landscape on QKD has been done in September 2016 by using the European Patent Office Global Patent Index database, using the query {('quantum' AND 'key' AND 'distribution') OR ('quantum' AND 'cryptography') OR ('QKD')} for text in the title and abstract of all patent applications. We point out that such automated searches may fail to capture the entire intellectual property portfolio of a single firm, and are intended to give just a first rough indication of who the main players are, and how their patenting activity evolved over the years.

Having eliminated false positives, duplicates, dropped applications, and some patents lapsed because of missing annual fee payment, we were left with 600 patent families. From the data plotted in Figure 1, we can see that 1. patenting in QKD starts in 1992; 2. after a relative maximum in 2004-2005 a new peak has been reached in 2014, which is the last year for which complete data are available; 3. the majority of applications are by industrial players. The last year for which complete data are available is 2014, and only applications filed in China contribute to the 2015 tally.

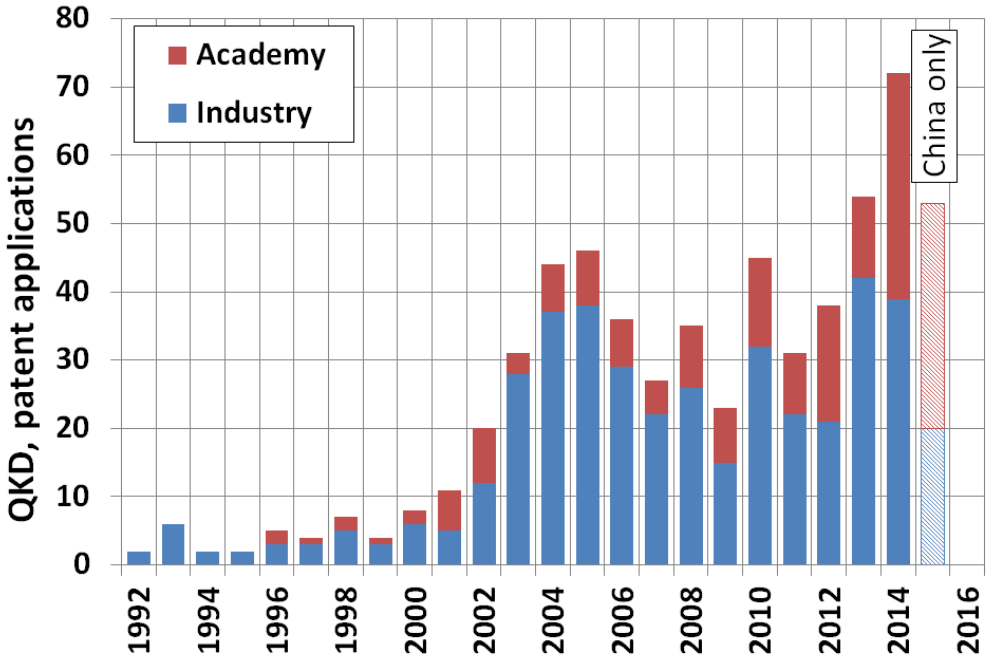

Figure 1: Yearly distribution of patent applications in QKD, by academy and industry. The bar relative to 2015 is dashed, to highlight that only applications filed in China contribute to it. Indeed, an 18 months confidentiality period is normally observed between the filing of the application and its disclosure; the applicant may however waive the non-disclosure right, and this appears to be the standard procedure for patents filed in China.

We now proceed to examine the nationalities of the institutions that file the applications. In the case in which there is more than one applicant for a given application, we have attributed the entry to a 'most significant applicant' according to the following criteria: 1. If the applicants are a private citizen and an institution, we have attributed the patent to the institution: this is by far the most common case; 2. if the applicants are a university and an industry, we have attributed the patent to the industry; 3. if the applicants are two or more institutions of the same nature, we have attributed the patent to the institution with the biggest number of applications in the field.

A distribution of the applicant nationality is plotted in Figure 2: we see a prevalence of China and USA, followed by Japan and Great Britain. We point out that some players file the applications in a country different from the one in which they are headquartered. Toshiba (JP) has a research centre in Great Britain, and some of its applications are first filed there. The same holds true for Hewlett Packard, a US company that has a research centre in Great Britain. Fujitsu (JP) filed a total of three patents on QKD: one in Japan, one in Germany, and one in Great Britain. ID Quantique, a Swiss start-up, routinely makes the first deposit and claims priority in the US. Overall, the country in which more applications by foreign firms take place turns out to be Great Britain, a possible sign of the capacity to attract foreign investment in R & D in this area.

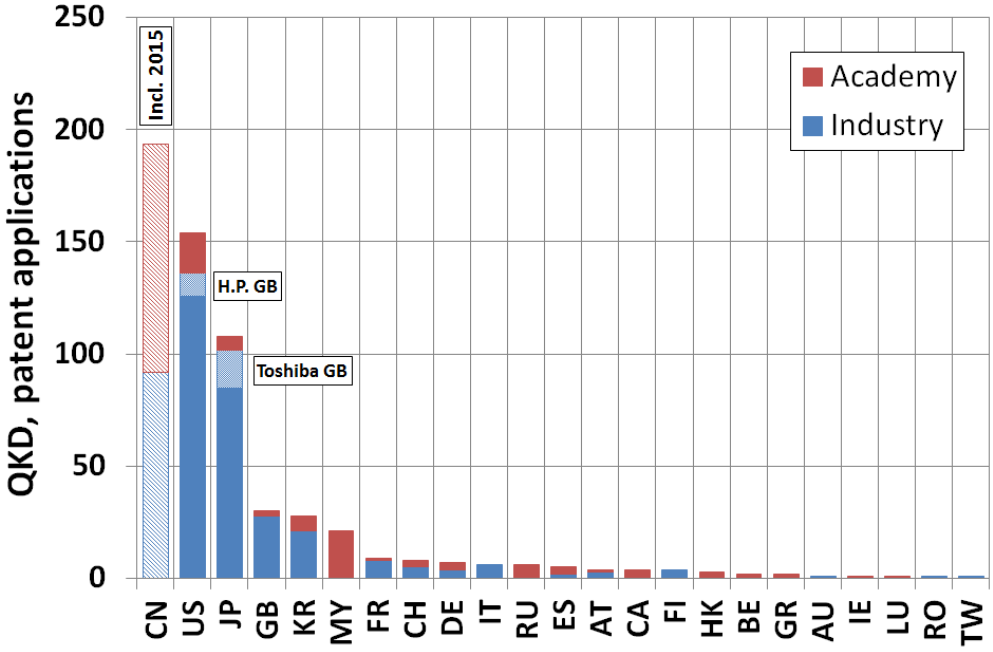

Figure 2: Distribution of the applicants' nationalities, determined on the basis of the country in which the patent assignee is headquartered.

Inspecting Figure 2, we can see a prevalence of industrial players over the academic ones, with the notable exception of China, in which almost half of the applications are filed by universities, and Malaysia, where all the patents are filed by a single national research centre. Note the patterned bars referring to Chinese applications, to highlight once again that since they apparently use to waiver the 18 months confidentiality period they could be over-represented with respect to applications filed in other countries. More specifically, all the ~ 50 disclosed applications submitted in year 2015 have been filed in China.

In the following Figure 3 we grouped together all the European players, that is applicants headquartered in AT, BE, CH, DE, ES, FI, FR, GB, GR, IE, IT, LU and RO. We see that European applications have been more or less steady over the years: the peak in 2008 is due to a single GB company, Qinetiq, which filed 13 applications. Early players were British Telecom in Europe and IBM in US: they were the only applicants until 1996. US patenting activity peaked in the 2003-2005 period, and is now more or less stable. Japan

started patenting a bit later that Europe and US, but then maintained a very constant output over the years. Later adopters have been Korea and Malaysia, but the most notable feature made apparent by Figure 3 is the growth of China in the last 5 years.

The first 30 institutions, ranked per number of applications, have been plotted in Figure 4: each one of them has filed at least four patents, for a total of 422 out of 600. This means that approximately a third of patents are filed by entities that seem not to be interested in building large portfolios of IP. Such institutions turn out to be typically universities, especially from Europe and USA; conversely, some Chinese universities filed a lot of applications and therefore appear at the top of the list. Among the industries we have microelectronics manufacturers, telecom providers, and firms active in the defence, security, and aerospace sectors. There are also several start-ups specialised in the development of QKD systems: in particular a great number of Chinese patents belong to medium-sized firms of very recent foundation, which are known to be providing the QKD equipment for the deployment of the Beijing–Shanghai quantum backbone. Conversely, we are aware of at least three small European university spin-offs that have gone out of business (SmartQuantum (FR), SeQureNet (FR), CryptoCam (I)).

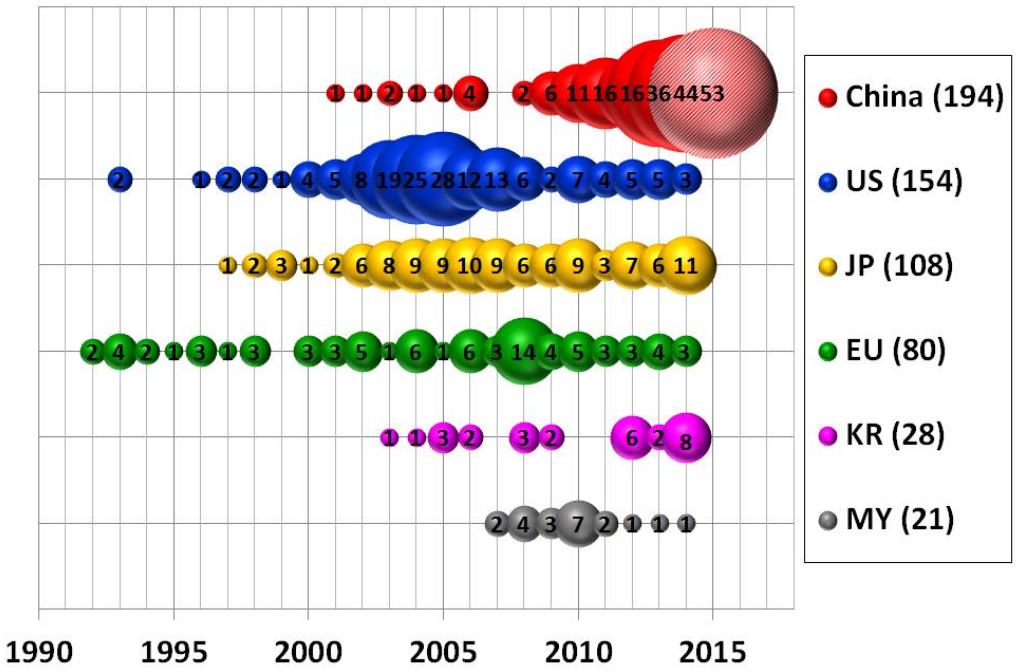

Figure 3: Applications by firms headquartered in different countries over the years. Note that 585 out of the total 600 patents are covered by these selected nationalities.

To contrast the rising Chinese activity, it is worth noting that several western firms have stopped applying for patents. Large US players (MagiQ, BBN, and HP), as well as GB Qinetiq, have not filed any new application after 2010. BT has not filed a single patent in quantum communications in the last 20 years, and Thales in the last 10 years. Most of the patents filed in recent years are therefore coming from China, Japan, Korea and Malaysia, and from smallish European and American players.

In the defence and security sector, the main players are western companies such as MagiQ (US), BBN Raytheon (US), Qinetiq (UK), Thales (FR), and Selex (IT). Applications from this sector seem to have peaked, first in the USA, then also in Europe.

With regards to electronics and telecoms, the main players are from Japan (NEC, Toshiba, Mitsubishi, NTT), and Korea (SK Telecom, Korea Electronics). Also European firms from Europe are present (BT, Nokia, Telefónica, Siemens), but their interest seems to be diminishing, particularly after the conclusion of the FP6 SECOQC project which ran from 2004 to 2008. Conversely, only few patents have been requested by the big firms

of the USA telecom sector, like Cisco, Nortel, Lucent, and Verizon. HP has a somewhat more consistent patent portfolio: however, the HP Quantum Information Processing Group in Bristol has now been closed, and although its operations have allegedly been moved to Palo Alto (USA), most of its leading scientists work in other research institutions, notably in Europe and Japan. The Chinese telecom giant Huawei has very recently established in Munich (Germany) a research centre named Quantum Communication and Computation Laboratory, under the management of Huawei Technologies Düsseldorf GmbH.

From the analysis of patents, it is evident that there is also a substantial activity by firms which play in fields not immediately associated with QKD, but that are obviously interested in data security. In this regard, the issue of infrastructure protection figures prominently, especially with Chinese players like China Electric Power and China State Grid Corporation, but also with US players like e.g. General Electrics and the governmental Los Alamos Laboratories, as well as start-ups like GridCom Technologies (now named Qubitekk), which in August 2014 received USD 3 million from the US Department of Energy to 'Help Protect Nation's Power Grid From Cyber Attack' by using QKD. A chapter entirely devoted to QKD has been included also in the IEEE document 'IEEE vision for smart grid communications: 2030 and beyond' (2013).

1	US	57	MAGIQ TECHNOLOGIES	Defence
2	JP	43	NEC	Electronics
3	CN	29	ANHUI ASKY QUANT.	Startup
4	CN	29	ANHUI QUANT. COM.	Startup
5	JP	29	TOSHIBA	Electronics
6	MY	22	MIMOS BERHAD	R&D Center
7	CN	22	UNIV SOUTH CHINA	University
8	GB	18	QINETIQ	Defence
9	US	16	RAYTHEON BBN TECH.	Defence
10	US	13	HEWLETT PACKARD	Electronics
11	JP	12	MITSUBISHI	Electronics
12	KR	12	SK TELECOM	Telecom
13	CN	12	STATE GRID CORP	Infrastructure
14	GB	11	BRITISH TELECOMM	Telecom
15	CN	11	USTC UNIV SCIENCE	University
16	CN	9	UNIV SHANGHAI	University
17	CN	9	UNIV TSINGHUA	University
18	JP	8	NTT	Telecom
19	CN	8	UNIV BEIJING	University
20	KR	6	KOREA ELECTRONICS	Electronics
21	FR	6	THALES	Defence
22	CN	5	ANHUI LIANGZI COM.	Startup
23	US	5	LOS ALAMOS NAT SEC.	Infrastructure
24	CN	5	UNIV PLA	Defence
25	US	5	VERIZON	Telecom
26	US	4	AT&T	Telecom
27	CH	4	ID QUANTIQUE	Startup
28	US	4	LUCENT TECHNOLOGIES	Electronics
29	FI	4	NOKIA	Telecom
30	IT	4	SELEX	Defence

Figure 4: Main players, listed by number of patent applications.

3.2. Industry players

We provide in this section a list of industrial actors which are actively working on quantum communications. We focus on private corporations that have acquired a specific know-how in the field, e.g. by developing systems or deploying them in the field. University and public-funded research is not included, unless in the case of applied research clearly focused towards real-world applications. Firms that work in the development of quantum devices are also left out, except in some specific cases where quantum cryptography seems to have been a major driver for their activity, and the devices have tested in QKD field deployments. To our knowledge, a complete mapping of the industrial players, including suppliers, potential users, and a value-chain analysis, is currently missing. Some additional information on industrial drivers and inhibitors can be found in the Ph.D. thesis of Thomas Langer [Langer 2013].

- **NTT** (JP), Telecom
  Field tests of quantum communications, development of QKD devices and systems
  https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201109fa6.html
  http://www.ntt.co.jp/news2015/1509e/150914a.html
  https://is.ntt-it.co.jp/search/client.cgi?nc=1&pnum=10&in=E&out=E&tp=tp&num=10&by=D0&cd=A&syn=1&cw=1&uid=ddd27e654f9f957dbc9d68e3f0b81087&key=qkd&from=11

- **NEC** (JP), Electronics/Telecom/Healthcare/Automotive/etc.
  Devices for quantum communications, field tests of systems
  http://www.nec.com/en/press/201509/global_20150928_02.html

- **Mitsubishi** (JP), Electric/Electronics/etc.
  QKD test fields, in particular for mobile phones
  http://everything-quantum.postach.io/post/mitsubishi-electric
  http://www.mitsubishielectric.com/news/2010/1014-b.html

- **Fujitsu** (JP), IT/Electric/Electronics/Telecom/etc.
  Single-photon emitters for quantum communications, field tests
  http://www.fujitsu.com/global/about/resources/news/press-releases/2015/0928-02.html

- **NICT** (JP) — National Institute of Information and Communications Technology
  Development of system and devices, field deployments, space-based QKD
  http://www.nict.go.jp/en/quantum
  https://directory.eoportal.org/web/eoportal/satellite-missions/content/-/article/socrates

- **OKI** (JP), Telecom/Mechatronics
  Entangled Photon Source for Cryptography (ATM)
  https://www.oki.com/en/press/2012/02/z11104e.html

- **Toshiba** (JP), Electric/electronic/life science
  Development of systems and devices; Field deployments, both in Japan and in UK
  http://www.toshiba.eu/eu/Cambridge-Research-Laboratory/Quantum-Information-Group/Quantum-Key-Distribution/Toshiba-QKD-system
  http://www.toshiba.eu/eu/Cambridge-Research-Laboratory/Quantum-Information-Group/Quantum-Key-Distribution

- **Qasky** (China), Quantum Communications
  Commercial QKD systems
  http://www.qasky.com/EN

- **QuantumCTek** (China), Quantum Communications
  Commercial QKD systems
  Main provider of the hardware for the Chinese quantum backbone
  http://www.quantum-info.com/English/

- **ROI Optoelectronics Technology** (China), Vendor of optoelectronic instruments
  Was invited to a tender for quantum communication hardware for the national backbone
  http://www.roiop.com (only in Chinese)

- **IDQ-Jiuzhou Quantum Technologies** (China), Quantum Communications
  Joint Venture Company formed in China between ID Quantique and Jiuzhou Quantum Technologies to serve the Chinese market in the field of QKD and QRNG.
  http://idq-qtec.com

- **Huawei** (China), Telecom/electronic/IT/etc.
  Newly established Quantum Communications research centre Germany; some staff were formerly at AIT (Austrian Institute of Technology)
  https://docbox.etsi.org/Workshop/2016/201609_QUANTUMSAFECRYPTO/TECHNICAL_TRACK/Huawei_PEEV.pdf

- **Alibaba** (China), Internet services
  It collaborates with the Chinese Academy of Sciences on research and development of practical applications of quantum cryptography for secure data transmission, to improve the reliability of the Alibaba Group's cloud services.
  http://asia.nikkei.com/Business/Companies/Alibaba-Chinese-academy-team-on-quantum-cryptography

- **ZTE** (China), Telecom
  Quantum encryption for Optical Transport Network (OTN), not yet commercially available
  http://www.zte.com.cn/global/about/press-center/news/201609ma/0928ma
  https://www.fibre-systems.com/product/zte-develops-otn-based-quantum-encryption-system

- **South Korea Telecom** (SK), Telecom
  Deployment of SK QKD backbone;
  https://www.facebook.com/skquantum
  https://docbox.etsi.org/Workshop/2016/201609_QUANTUMSAFECRYPTO/TECHNICAL_TRACK/SK_telecom_cho.pdf
  SK Telecom has also invested in ID Quantique:
  http://startupticker.ch/en/news/december-2016/south-korean-telecom-giant-makes-strategic-investment-in-idq
  SK telecom works on QKD and quantum safe systems with Nokia and Deutsche Telekom:
  http://www.prnewswire.com/news-releases/sk-telecom-and-nokia-sign-cooperation-agreement-for-quantum-cryptography-300413873.html
  http://www.prnewswire.com/news-releases/sk-telecom-and-deutsche-telekom-establish-quantum-alliance-for-worldwide-quantum-safe-network-ecosystem-300413853.html

- **Samsung** (SK), Telcom/Electronics/Electric/etc.
  http://www.ipnomics.net/?p=17209

- **KIST** — Korea Institute of Science and Technology, (SK)
  Quantum cryptography systems and devices
  https://eng.kist.re.kr/kist_eng/?sub_num=1616; https://eng.kist.re.kr/kist_eng/?sub_num=580

- **Korea Telecom** (SK), Telecom
  In 2014, the KT Institute of Convergence Technology, the Korea Telecom branch that conducts research on future technologies, started probing quantum key distribution technology, spurring speculation that KT would compete with SK Telecom in this area.
  http://www.netmanias.com/en/post/korea_ict_news/6889/kt-sk-telecom/kt-is-after-quantum-key-distribution-too-engaged-in-quantum-competition-with-sk-telecom

- **Senetas** (Australia), Communication security
  Commercial encryptors supporting QKD, field-tested
  http://www.prweb.com/releases/2010/10/prweb4670214.htm

- **QuintessenceLab** (Australia), Quantum communication start-up
  Encryption solutions and QKD systems
  https://www.quintessencelabs.com

- **QinetiQ** (UK), Defence/Security
  Patents peak in 2008. In 2009 stated interest for QKD set-up in London. Now seems inactive.
  https://www.qinetiq.com

- **British Telecom** (UK), Telecom
  Field test of QKD, with Toshiba and **ADVA** (provider of optical networking solutions)
  http://www.toshiba.eu/eu/Cambridge-Research-Laboratory/Quantum-Information-Group/Quantum-Key-Distribution/QKD-with-10Gb-Traffic
  BT is stepping up its efforts in the quantum domain
  http://www.gazettabyte.com/home/2017/5/5/bt-bolsters-research-in-quantum-technologies.html
  Also research on QKD in software-defined networks (with Telefónica and Huawei)
  https://obj.umiacs.umd.edu/extended_abstracts/QCrypt_2016_paper_188.pdf
  ... and a proposal for space-based QKD for infrastructure protection
  https://artes.esa.int/sites/default/files/32%20-%20Wakeling%20BT%20Group.pdf

- **KPN** (NL), Telecom
  Field deployment of QKD systems. Member of the High Level Steering Committee of the Quantum Technologies Flagship.
  https://corporate.kpn.com/press/press-releases/kpn-to-implement-quantum-encrypted-connection-qkd.htm

- **Cryptographiq** Limited (UK), Spinoff of Leeds University
  Is working with Airbus Defence and Space and L3-TRL on quantum-based cryptography
  http://www.physics.leeds.ac.uk/index.php?id=263&uid=1207

- **Thales** (FR), Defence
  Participated in the SECOQC project, but seems to be no longer active in QKD. Presently working on quantum devices, and quantum-safe cryptography. Participated in the High Level Steering Committee of the European Commission Flagship in Quantum Technologies.

- **SmartQuantum** (FR), Start-up
  QKD systems. Not any more operational
  https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=34723601
  http://emits.sso.esa.int/emits/owa/!ViewData.baseData?pentityid=31133&parea=O&cname=&coun=&groupName=GeneralInformation&ul=Guest&pSME=Y

- **SeQureNet** (FR), Start-up
  CV-QKD system Cygnus. Not anymore operational
  https://www.photoniques.com/vitrine-de-l-innovation-2013/1768

- **Safran** (FR), Defence
  Funding a chair on 'ultimate photonics', for quantum cryptography in integrated photonics
  https://www.safran-group.com/media/20150318_chair-ultimate-photonics-safran

- **Swisscomm** (CH), telecom
  QKD field trials, fibre link Geneva-Neuchâtel (2008)
  https://arxiv.org/abs/0809.5264

- **ID Quantique** (CH), SME
  They sell commercial QKD systems and quantum-safe cryptography; Member of the High Level Steering Committee of the Quantum Technologies Flagship.
  http://www.idquantique.com

- **GÉANT** (EU), e-infrastructure for research and education
  At the TNC17 Networking Conference GÉANT presented a paper that describes 'the results of an investigation into the feasibility of using the existing network infrastructure to distribute quantum keys'. The work was done in collaboration with Toshiba, and sets out 'an experimental roadmap towards a field trial', discussing 'how the next generation of technology will help solve the challenge of implementing quantum key distribution (QKD) on long-haul GÉANT fiber routes'.
  https://tnc17.geant.org/core/presentation/24
  In an earlier publication, GÉANT discussed the applications that could be spurred by the opening up of the optical transport infrastructure, considering also QKD.
  https://geant3.archive.geant.org/Media_Centre/Media_Library/Media%20Library/GN3-13-140_Photonic_Services-making_the_case.pdf

- **Siemens** (DE), Electronic/Electric/IT/etc.
  Participated in the SECOQC project (Wien QKD network, 2004-2008). In 2010 tested a link between data centres in The Hague and Zoetermeer (NL), with Senetas and ID Quantique.
  http://www.prweb.com/releases/2010/10/prweb4670214.htm

- **AIT** Austrian Institute of Technology (Austria)
  Quantum key distribution system made available as prototype for research and teaching; development of software for QKD data processing
  https://www.ait.ac.at/en/research-fields/physical-layer-security/optical-quantum-technologies/
  https://sqt.ait.ac.at/software/projects/qkd

- **Telefónica** (ES), Telecom
  Participated in the SECOQC project, and deployed a QKD network in Madrid. Presently active on the use of QKD in software-defined networks.
  https://link.springer.com/content/pdf/10.1007/978-3-642-11731-2_18.pdf

- **Nokia** (FI), Telecom/Electronics
  Participated in the SECOQC project, now working on QKD for mobile phones. Collaborating with SK Telecom and with the UK Quantum Communications hub.
  https://www.osapublishing.org/DirectPDFAccess/3E0BF3B1-C6F2-3619-10F9CE84B7C3D480_361628/oe-25-6-6784.pdf?da=1&id=361628&seq=0&mobile=no

- **Selex Galileo,** now Leonardo Finmeccanica (IT), Defence
  Development of QKD prototypes, and funding research contracts.
  http://www.nanoitaly.it/nanoitaly/it/home-ita/11-curriculum-ita/310-fabio-antonio-bovino
  http://informaticapertutti.net/la-crittografia-quantistica-corre-sulla-fibra-ottica

- **MagiQ** (USA), Defence/Security
  Developed QKD systems (Navajo, Q-Box, and QPN-8505) in 2003-2006, now not any more active.
  http://www.magiqtech.com
  http://seqre.net/seqre2014/qkd.php (tested the system)

- **BBN Raytheon** (USA), Defence
  Research on QKD distance/speed limits and on quantum repeaters. Now collaborating with Quintessence Lab on QKD networks.
  http://www.raytheon.com/capabilities/products/quantum

- **Applied Communication Sciences** (USA), Defence/Security
  Now at Vencore Labs, formerly Telcordia and Bell Labs
  QKD over reconfigurable fiber networks, scalable quantum networks
  http://www.appcomsci.com/research/quantum-communications-and-computing

- **Batelle** (USA), Research services in Defence/Security/Energy/Environment/Health/etc.
  With ID Quantique, installed in 2013 a QKD link between Columbus and Dublin (Ohio); plans to extend it to connect Washington, DC, for a total span of 700 km.
  https://www.battelle.org/case-studies/case-study-detail/quantum-key-distribution

- **Alcatel-Lucent,** formerly Bell Labs (USA), now part of Nokia, Telecom/Electronic/IT/etc.
  Used to work on MEMS subsystem for high-capacity QKD networks and to develop systems compatible with metro-scale all optical data networks, but seems to be not any more active.

- **Oak Ridge National Laboratory** (USA) Security
  DI-QKD systems & protocols for ship-to-ship communications. For the Department of Energy project Cybersecurity for Energy Delivery Systems (CEDS), it developed 'Practical Quantum Security for Grid Automation', working with ID Quantique and General Electrics
  https://www.ornl.gov/division/projects/reconfigurable-loss-tolerant-measurement-device-independent-quantum-networks

- **NIST** — National Institute for Standard and Technology (USA)
  Development of QKD systems
  https://www.nist.gov/publications/high-speed-quantum-key-distribution-over-optical-fiber-network-system
  https://www.nist.gov/people/alan-mink
  Quantum physics for metrology, but also quantum information
  https://www.nist.gov/topics/quantum-information-science
  Running project on post-quantum cryptography
  http://csrc.nist.gov/groups/ST/post-quantum-crypto

- **Darpa,** Defense Advanced Research Project Agency (USA)
  Throughout the 5-year Quantum Information Science and Technology (QuIST) programme, Darpa funded the first quantum key distribution network. It provided encryption to a fibre-optic loop connecting Harvard University, Boston University, and the office of BBN Technologies in Cambridge (Mass.), and was completed in 2007. Seems currently to be no longer active in QKD.
  https://www.govcon.com/doc/darpa-announces-quist-program-baa-0001
  http://www.darpa.mil/about-us/timeline/quantum-key-distribution-network
  http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA471450

- **Los Alamos National Laboratory** (USA), Security
  Development of fibre-based and free-air QKD systems
  http://www.lanl.gov/science/centers/quantum/cryptography.shtml
  QKD for infrastructure protection
  https://energy.gov/sites/prod/files/2017/02/f34/Day%201%20-%20Quantum%20-%20ORNL-LANL.pdf
  https://www.energy.gov/oe/articles/look-how-innovation-los-alamos-national-laboratory-helping-keep-our-nation-secure
  https://energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity/national-scada-test-bed
  Some of the LANL technology was licensed by the provider of security solutions Whitewood Encryption Systems
  http://whitewoodsecurity.com/whitewood-encryption-systems-announces-the-awarding-of-a-u-s-patent-for-its-secure-multi-party-communication-with-quantum-key-distribution-managed-by-trusted-authority

- **Sandia National Laboratories**
  Sandia enabled communications and authentication network using quantum key distribution (SECANT QKD) aims to construct chip-scale, handheld quantum transceivers to be used in networks of mobile trusted nodes, and that can implement discrete variable, continuous variable, free-space, and fibre-based QKD. It also aims to demonstrate a hybrid QKD network with chip-scale transceiver nodes.
  http://www.sandia.gov/research/laboratory_directed_research/secant

- **Hewlett-Packard** (USA), Electronic/Electric/IT/etc.
  Had in Bristol a Quantum Information Processing Research centre, now closed. Quantum activities in Palo Alto (California), but apparently not working any more on QKD. Participated in the SECOQC project, patented quantum repeaters. Tim Spiller is now with York University (UK) and leads the communications hub of the UK national programme, Bill Munro is with NTT (JP), Radu Ioniciou with Horia Hulubei National Institute (Romania)
  http://www.hpl.hp.com/research/qip

- **Nucrypt** (USA), Quantum Optics instruments
  Received SBIR/STTR money for development of QKD devices, protocols, and systems
  http://www.nucrypt.net
  https://www.sbir.gov/sbc/nucrypt-llc

- **Qubittek** (USA), Quantum technology start-up
  Quantum cryptography based on entanglement, especially for infrastructure protection. Funded also via the SBIR/STTR programme for the development of entanglement sources.
  http://qubitekk.com; https://www.sbir.gov/sbc/gridcom-technologies-inc

- **Boeing** (USA), Defence
  Awarded a 4-year contract (2016-2021, ~ USD 3.5 million) from the USAF, in the framework of the RASTER Project (R & D for Advanced Space Superiority Technology and Engineering Requirements) for QKD research and development
  https://govtribe.com/contract/idv/fa945116d0001

- **AT&T** (USA), Telecom
  In May 2017 AT&T announced that its Foundry Innovation Center in Palo Alto was joining the California Institute of Technology and form the Alliance for Quantum Technologies, to address the 'need for capacity and security in communications through future quantum networking technologies'
  http://about.att.com/story/beyond_quantum_computing.html

3.3. Public programmes

In the last 20-30 years, as the era of worldwide electronic mass communications made inescapable the economic implications of cryptography, it became clear to governments worldwide that communications security is simultaneously (i) a driver of economic growth, (ii) a key factor for national security, (iii) an essential component of defence, and (iv) a crucial issue for geo-strategic prominence. The importance attached to each one of these factors depends of course on the governments' priorities, and policy decisions impact heavily on the choices of technology developers and potential users.

Despite its shortcomings, the potential security advantages provided by QKD are such that numerous public initiatives aimed at real field deployments and infrastructural build-ups are taking place in several countries. In the last years a number of countries have taken important decision with regards to QKD, often reacting to programmes undertaken by strategic competitors. Considerations of national security are explicitly quoted in many governmental programmes, alongside the economic opportunity of spurring the development of a completely new industry, which can offset the incumbency advantages of the established providers of information and communication technologies — which are typically from the USA.

In the international playground, the most evident trend is the rise of China in the last decade: QKD deployments have been made both in local area networks and in long-haul backbones, and entanglement-based QKD on continental and intercontinental scale by means of a dedicated satellite has been demonstrated. The increasing perception of the threat to communications security constituted by developments in quantum computing has probably also played a role in the Chinese technology push in quantum communications: indeed, in the race towards a fully-fledged quantum computer the USA undoubtedly enjoy a great advantage, not only for its academic research and public-funded research but also thanks to the engagement of powerful industry players.

China

Quantum communications and computation is one of the top 10 scientific priorities in the 5-year research plan 2016-2021, presented by the Chinese premier Li Keqiangin in a speech to open the National People's Congress on 5 March 2016 [McLaughlin 2016]. A comprehensive public programme for the deployment of a QKD infrastructure is being pursued, and now comprises a ~ 2 000 km Beijing–Shanghai quantum backbone, several metropolitan networks, a ~ 50 km free air link, and a quantum satellite for intercontinental communications [Qiu 2014], [Chen Nov 2014], [Xiang 2015], [Lixin 2016], [Qiang Zhang 2016].

The first field deployment was a four-user system built in the commercial fibre network of China Netcom Company in Beijing (March 2007). The quantum communications network in Hefei [Wang 2014] was completed in 2012, linking 40 telephones and 16 video cameras installed at city government agencies, military units, financial institutions and health care offices, at the cost of 60 million yuan (USD 9 million) for the Hefei government. A similar civilian network which connects some 90 users in Jinan was completed in 2014. Some spans of the Beijing–Shanghai backbone are now operational [Courtland 2016]: though the government has not revealed its budget, some Chinese scientists told state media that the construction cost would be 100 million yuan (USD 15 million) for every 10 000 users, while other sources estimate a total cost of USD 100 million In the ETSI/IQC quantum-safe workshop recently held in London (13-15 September 2017) a presentation outlining the latest Chinese developments and policy decisions regarding quantum communications was delivered by a representative of the IDQ-QTEC joint venture, and is available in [IDQ QCTEC 2017].

In parallel with these deployments, an indigenous QKD industry has risen, as evidenced also by our patent analysis. A quantum satellite (named 'Micius') was launched in August 2016 [Gibney 2016], and operational tests are now underway: it is estimated to be 'a USD 100 million mission', but no official figures have been disclosed and rumours say the actual cost can be much higher. In June 2017, entangled photons generated in the satellite orbiting at 500 km at 8 km/s were distributed to pairs of ground stations ~ 1 200 km apart [Yin 2017], [China satellite 2017]. This result was reported by *The Economist* in the 2 September (2017) issue, in an article subtitled 'The world's first quantum-cryptographic satellite network will be Chinese' [The Economist China 2017].

The Chinese Academy of Science announced on 30 September 2017, that 'a 2 000-km quantum communication line opened on Friday between Beijing and Shanghai', that 'the line is connected with the world's first quantum satellite, which was launched by China in August last year, through a station in Beijing', and that 'Bai Chunli, president of the Chinese Academy of Sciences, talked with staff in Hefei, Jinan, Shanghai and Xinjiang Uygur Autonomous Region, through the line. He also had a video call with Austrian quantum physicist Anton Zeilinger (in Vienna), through the satellite' [CAS Sept. 2017].

Having established its position in quantum communications, China is now investing in a 10 billion dollar research facility for quantum technologies, apparently geared mainly towards military applications of quantum computation and sensing. The press reported that the 'key mission of the laboratory is to build the nation's first quantum computer that could break an encrypted message in seconds' [South China MP 2017].

Japan

In Japan several industrial and public partners have jointly developed an extensive quantum network in Tokyo, which was inaugurated in October 2010 [Sasaki 2011]. The network operations include video transmission, eavesdropping detection, and rerouting to secondary secure links; the Japanese teams participating in the project belong to NICT (National Institute of Information and Communications Technology) and private companies such as NEC, Mitsubishi Electric, and NTT.

Several European teams participate in the project, notably from Toshiba Research Europe, ID Quantique, the Austrian Institute of Technology, the Austrian Institute of Quantum Optics and Quantum Information, and the University of Vienna [UQCC Project website]. Applications that have by now been implemented include one-time-pad smartphones and the transmission of genetic data, as can be seen from the presentations given by A. Shields and M. Sasaki at the UQCC 2015 conference [UQCC 2015]. The NICT is working also on space-based QKD, developing an optical transponder for satellites and equipping telescope ground stations [Toyoshima 2015].

South Korea

On 12 December 2016, a so-called 'special law on Quantum Industry' was proposed at a seminar on Quantum Technologies held at National Assembly. The bill aims at the development of quantum information communication technology and the promotion of their industrialisation. In particular, it states that 'The South Korean Government realised the importance of quantum industries such as quantum information communication and put out a variety of policies such as the designation of quantum industry among one of the 10 promising technologies in the future, the establishment of a K-ICT strategy, and the development of medium and long-term strategies for quantum information communication' [South Korea Law 2016].

Several metropolitan quantum networks already exist in South Korea, and the government is funding the development of a ~ 250 km quantum backbone to connect them [Kim 2016], [Walenta 2016]. The main players are the Korea Institute of Science and Technology Information (KISTI) and SK Telecom, which has a longstanding collaboration with Nokia. To promote interoperability, SK Telecom and Deutsche Telekom launched a group called the 'Quantum Alliance' at the Mobile World Congress 2017 in Barcelona [Williams 2017].

Malaysia

Mimos Berhad, the National Research Centre in ICT, has an information security division aimed at 'developing Malaysia's home-grown technology in cyber security to bolster self-reliance in order to maintain its e-sovereignty' [Mimos Berhad website]. Commercialisation of developed technologies is seen as an integral part of Mimos mission, and several QKD patents have been awarded to its researchers. In 2011 they engineered the construction of a five nodes quantum cryptography network, which remained operational for 3 years, and was terminated in 2014 after the project accomplished its objectives [Mohamed Ridza Wahiddin 2017]. A Malaysian Quantum Information Era Strategic Hub started operating in 2017 [myquantum website], co-funded by a governmental cybersecurity agency.

Singapore

Quantum cryptography figures prominently in the scientific activities of the Centre for Quantum Technology (CQT), which was established in 2007 by the National Research Foundation (NRF) and the Ministry of National Education, and is hosted by the National University of Singapore (NUS). CQT has been particularly effective in recruiting researchers from around the world, including Europe.

In October 2016 a funding initiative of USD 42.8 million (over 5 years) was announced by the Singapore Deputy Prime Minister and Coordinating Minister for National Security, aimed at establishing a Cyber Security Research and Development Laboratory with the mission to detect and respond to security attacks and to come up with new approaches to IT systems that are 'secure by design'. In particular, staff from Asia's leading communications group Singtel will be working with researchers from the CQT to develop QKD for Singtel's fibre network [CQT 2016]. In the framework of the SPEQS (Small Photon-Entangling Quantum System) project, a nanosatellite hosting an entanglement source has been launched and tested, and a system of ground stations to track it is being developed [The SpooQy Lab website], [CQY 2014].

Australia

The government is implementing a Government Quantum Network for intra-governmental communications in Canberra. Leading the technical effort is the 'Centre for Quantum Computation and Communication Technologies' (CQC2T), which is a centre of

excellence of the Australian Research Council [Aust. Nat. Univ. website], [cqc2t website]. The CQC2T states that 'the main goal of this programme is to demonstrate Quantum Cryptography in the Australian Parliamentary Triangle. In close partnership with QuintessenceLabs, University of Queensland and Lockheed Martin Australia, we will implement the Government Quantum Network (GQN). This is an initiative of multiple governmental agencies to provide the highest level of information security for intra-governmental communications in Canberra.'

A 'Space-based quantum communications funding' has been announced by the Minister for Higher Education, Training and Research in November 2016, to demonstrate the technology for an Australian quantum ground station to support secure space communication links [ANU space]. In a recent interview (3 February 2017) the vice-president of the Australian QKD firm Quintessence Lab declared that its products are deployed at the 'Australian bank Westpac, and the global data centres of a leading cloud storage provider', adding that 'pilot projects are also underway with a number of defence prime contractors and government agencies' [Extance 2017].

South Africa

A quantum communication security solution has been deployed starting from 2008 in Durban's municipal fibre-optic network [University KwaZulu-Natal website]. From the project website we learn that 'Physicists at the University of KwaZulu-Natal's Centre for Quantum Technology are all set to install a quantum communication security solution over the eThekwini Municipality fibre-optic network infrastructure propelling the City of Durban to become the world's first Quantum City. Based on the eThekwini SmartCity initiative, the QuantumCity project aims to provide the City with the capabilities to offer quantum security solutions to users of their recently installed fibre-optic network.' According to a conversation we had in 2016 with Professor Francesco Petruccione (University of KwaZulu-Natal) who oversaw the project, the network has now been dismantled.

Russia

A national research centre in quantum technologies was established in 2010, and safe data transmission networks are quoted among the potential results of its activity [RQC website]. Real field demonstrations of quantum communications have been made, in particular for the banking sector. The developers point out that 'to become certificated in Russia, the device should be produced in Russia', and their stated aim is to build a quantum key distribution industrial product in 2017 [kurochkin 2016]. A cooperation agreement with the telecom provider T8 has been signed, as well as an agreement with PricewaterhouseCoopers to develop and commercialise quantum information security systems [t8 press 2016], [pwc press 2017]. Export markets are also being investigated [The Hindu 2016]. Additionally, we point out that researchers from the Russian Quantum Center published in 2017 a paper describing the experimental realisation of a quantum-safe blockchain platform that utilises quantum key distribution across an urban fibre network [Quantum blockchain].

USA

An overview of the US policies on Quantum Technologies can be found in a report issued by the Executive Office of the President in July 2016, and entitled 'Advancing quantum information sciences: national challenges and opportunities' [White House 2016]. In it we read that 'Federal agencies have supported research in QIS (Quantum Information Sciences) and related areas since the field emerged over 20 years ago. This support has played a significant part in enabling US scientists to establish their present leading roles in the field. Federally funded basic and applied research in QIS is currently of the order

of USD 200 million a year'. The main funding agencies quoted by the report are the Department of Defence, the Department of Energy, IARPA, DARPA, NIST, and the National Science Foundation.

On June 22, 2017, a 'Call for a National Quantum Initiative' has been published by the National Photonics Initiative, a body formed by experts from industry, academia and government which assembles 'recommendations that will help guide US funding and investment'. It calls for an investment of USD 500 million over 5 years to set up a limited number of Quantum Innovations Labs, which 'will accelerate the development of commercially available quantum-based technologies to facilitate growth in the US economy and keep pace with accelerating international competition'. Quantum Communication is one of the three activity areas which have been identified, together with computation and sensing [NQI USA 2017].

On 24 October 2017, the US Congress Committee on Science, Space, and Technology hosted a hearing on 'American Leadership in Quantum Technology', with high-level testimonies by NIST, NSF, DOE, academy and industry [US Congress 2017]. Widely recognised was the transformative potential of this technology, and the necessity for a public action to maintain the US edge. In particular, from the DOE testimony we read that 'DOE and other US Government (USG) agencies believe that QIS will continue to grow in importance in the coming decade and are planning appropriate investments accordingly'. The call for a National Quantum Initiative assembled by the National Photonic Initiative was also presented at the hearing.

With regards to quantum communications, we mention that the perceived threat represented by Chinese activism has been evidenced by the testimony presented on 16 March 2017 to the US–China Economic and Security Review Commission and entitled 'Chinese Efforts in Quantum Information Science: Drivers, Milestones, and Strategic Implications' [Costello 2017], [Costello 2017 testimony]. In it we read 'The US remains at the forefront of quantum information science, but its lead has slipped considerably as other nations, China in particular, have allocated extensive funding to basic and applied research. Consequently, Chinese advances in quantum information science have the potential to surpass the United States.' The situation is considered to be particularly worrying in the field of quantum communications: we read indeed that 'The United States was once the leader in quantum information science, but the lack of funding, structural and institutional issues, and lack of government coordination have reduced both the levels and consistency of support that are necessary to maintain capacity in this critical research area. The resulting void has caused the locus of research in certain quantum information science areas — most notably quantum cryptography — to shift to other countries where funding and support for basic research are more reliable.'

We recall that the first fibre-based QKD network worldwide was funded by DARPA, as part of the Quantum Information Science and Technology (QuIST) programme: 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, Mass, for a total of six nodes [Elliott 2005]. An extensive (~ 400 km) quantum network has been deployed by a private company, Batelle, in central Ohio [Hayford 2014]. DARPA is presently funding programme 'Quiness', aimed at investigating novel technologies capable of high-rate and long-distance quantum communications.

The Department of Commerce NIST has developed QKD systems and devices, implementing a secure QKD video surveillance application [NIST ITL website]; in 2013 NIST and NTIA (National Telecommunications and Information Administration) announced a plan to establish a new centre for advanced communications, whose programmes include quantum-based applications [NTIA press 2013].

The Department of Energy with Los Alamos Labs focused on the use of QKD for infrastructure protection, emphasising cost reduction to enrich the network topology and including authentication alongside encryption [Hughes 2013]. The Oak Ridge National Laboratory has a quantum information science group, which is working on device-

independent CV-QKD applied to energy grid security. Sandia National Laboratories are conducting projects on chip-scale quantum communication devices.

In 2012 NASA hosted a conference on quantum technologies [NASA Quantum 2012] in which it proposed a mixed terrestrial–satellite network to be deployed in California [Williams 2012], and closely follows Chinese activities in this field [Nasa 2016]. QKD technologies, both for space-based communications and for infrastructure protection, have been funded also via the SBIR-STTR programme, specifically aimed at SME.

Canada

A survey overview of Canada's quantum ecosystem has been published in March 2017, and a set of recommendations for a national quantum strategy will be released in autumn 2017 [NRC quantum 2017]. In particular the Ontario regional government has a well-established programme aiming at the commercialisation of quantum technologies, in collaboration with private investors such as the Lazaridis and Fregin's Quantum Valley Investments fund [The Guardian 2016], [PI press 2016].

The Institute for Quantum Computing at the University of Waterloo is a world leader in applied QKD, and it has a particular expertise in quantum hacking and satellite-based QKD. A government funding for the deployment of a quantum satellite has been announced in April 2017 [Gov Canada 2017].

Europe

Following the presentation of a Quantum Manifesto in May 2016 [Quantum Manifesto] calling for an European-wide initiative to develop European capabilities in quantum technologies, a flagship programme is now being prepared by the European Commission's DG for Communications Networks, Content and Technology[Quantum Europe]. A workshop has been held in Malta in February 2017, where recommendations for a strategic research agenda were presented and some national initiatives outlined, as evidenced by the presentations that can be downloaded using the following list of links:

- Prof. Serge Haroche: Why Quantum Technologies?
- Prof. Jürgen Mlynek: Quantum Technology: preparing the new European Flagship
- Prof. Massimo Inguscio: Quantum Technologies in Italy
- Prof. Paul Indelicato: French national initiatives and their complementarity with the FET-Flagship
- Dr Herbert Zeisel: German national Initiative and the EU Flagship
- Barbara Weitgruber: National Quantum Technology Initiatives: Austria
- Sir Peter Knight: UK National Quantum Technology Programme
- Prof. Peter Domokos: National quantum technology programme of Hungary

The latest developments at the EU level, as per October 2017, are here summarised:

- The final Report by the Quantum Flagship High Level Steering Committee has been completed, and will be handed over to the European Commission on 6 November 2017 in Brussels, see https://tinyurl.com/qt-hlsc-report
- The first QT Flagship calls are pre-published in the Draft Horizon 2020 FET WP 2018-2020,

  https://ec.europa.eu/programmes/horizon2020/sites/horizon2020/files/02._h2020-fet-2018-2020_09_21_2017_prepublication.pdf

- A Call for Proposals for an Innovation Action under the satellite communication technologies topic SPACE-15-TEC-2018 which mention 'adapting to quantum technologies' for secure and robust satellite communications was published on October 27, 2017

  http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/space-15-tec-2018.html

- A more specific Call for Proposals for an Innovation Action for the deployment of a QKD testbed will be published under the cybersecurity section of the ICT Leadership in Industrial Technology (LEIT) part of the H2020 programme, see:

  https://ec.europa.eu/programmes/horizon2020/sites/horizon2020/files/h2020-leit-ict-2018-2020_pre_publication.pdf

- The QuantERA Cofund Initiative in quantum technologies has also published its 2017 calls, see https://www.quantera.eu

We now briefly summarise the main national programmes which are being carried on in Europe in the specific field of quantum communications, restricting ourselves to those aimed at fostering real-world applications and market uptake.

UK

In 2015 the UK government announced a GBP 270 million investment on quantum technologies over 5 years [UK quantum 2015]. A quantum communications hub [UK QuantumComm Hub] has been set up, comprising universities, industries, and public sector bodies, with the aim to 'deliver quantum encryption systems that will in turn enable secure transactions and transmissions of data across a range of users in real-world applications: from government agencies and industrial set-ups to commercial establishments and the wider public.' A detailed work plan has been presented, articulated in four work packages (respectively devoted to short-range consumer QKD, chip-scale QKD, quantum networks, and next-generation quantum communications), including the construction of a quantum backbone connecting Bristol with Cambridge [Thompson 2015].

Netherlands

The national programme on quantum technologies seems to be focused on computing, and the main engineering effort is being carried on by QuTech [QuTech website], with partners such as Microsoft and Intel. Quantum communications are however also contemplated, and a quantum network will be established between Amsterdam, Delft, Leiden and The Hague, as a first step towards a future 'Quantum Internet' [QuTech comm], [CWI news 2017].

Belgium

The Brussels Institute for Research and Innovation funded in 2007-2013 a project which aimed at 'the design of an integrated practical toolbox of cryptographic and security primitives based on the promising results obtained over the last decade in the area of quantum information, in particular in quantum cryptography' [VUB cryptasc website]. In a final white paper entitled 'Cryptographie Quantique' a section on the 'Potentiel des techniques QKD dans la Region Bruxelles Capitale' is included, suggesting in particular applications in e-Health, e-Government, and e-Banking.

Denmark

A national Quantum Innovation Centre was set up in May 2016, with the mission to 'exploit the very strong Danish research positions within quantum technology for value creation by commercialisation of strongholds in Danish quantum technology' [QUbiz website]. Within this framework, it is planned to 'implement a field test prototype of quantum key distribution for secure communication in the Copenhagen area, integrated into existing security infrastructure.'

Poland

The 'Quantum Information Centre in Gdańsk' (KCIK) was established in 2007, to create an 'integrated basis for interdisciplinary research in fields of quantum information processing and foundations of physics'. Supported by the University of Gdańsk, research grants of Foundation for Polish Science, National Centre of Science, Ministry of Science and Higher Education and framework programme of European Union [KCIK website], it is in particular active in the field of device independent QKD. The 'National Laboratory of Quantum Technologies' was created in 2008, and it is funded by the National Centre for Research and Development upon the Innovative Economy Operational Programme co-financed by the European Union: it helped establishing a QKD network in Wrocław [NLQT website], [Seqre website]. Also the Military university of Technology in Warsaw is active in the field of quantum cryptography.

Switzerland

Switzerland was the first country to use QKD to secure the transmission of ballot results in 2007, and a quantum network has been extensively tested around Geneva [Swissquantum paper]. The Swiss National Science Foundation is funding a National Centre of Competence in Research devoted to Quantum Science and Technology, and one of its aim is to promote applications of quantum cryptography [NCCR qsit]. A feasibility study financed by the Swiss space office to explore satellite-based long range QKD is currently under way [Huttner 2017].

Finland

In June 217 the Academy of Finland announced it will be opening the Finnish Centre of Excellence in Quantum Technology, expecting its research 'to have impact beyond academia as well'. Partners will be Aalto University, University of Turku and VTT Technical Research Centre [Academy Finland 2017]. Aalto University, which already hosts a Centre for Quantum Engineering with expertise in quantum communications, will be tasked with the construction of a quantum computer, and has received an additional ~ EUR 1 million from two private foundations [Aalto QC 2017]. In 2016 the Finnish Scientific Advisory Board for Defence commissioned a study on the use of commercial QKD equipment for 'extra high security requirements' [Finnish defence].

Sweden

In November 2017 Chalmers University of Technology announced a SEK 1 billion (EUR 100 million) initiative on Quantum Technologies, backed by SEK 600 million from the Wallenberg Foundation. It will start from January 2018 and have a 10-year time span [Chalmers 2017]. The research programme, published by the Wallenberg Centre for Quantum Technologies, puts the development of a quantum computer based on superconducting circuits at the core of the initiative. The quantum communications part will concentrate on the development of quantum repeaters, single-photon sources, and quantum memories; the main players will be the Royal Institute of Technology KTH and Stockholm University [Wallenberg CQT 2017].

Germany

The Leopoldina National Academy of Science published in 2015 a national recommendation entitled 'Quantum Technology: from research to application' [Leopoldina 2015] highlighting the potential for communication security. A national programme named QUTEGA and estimated to involve EUR 300 million in 10 years is now in preparation [QUtega website], and in its framework a call for tenders on quantum communication will take place. The final goal is 'the development of highly secure communications links in which every attack can be recognised, and the encryption systems of which cannot be broken even with high-power quantum computers.' The Alliance for Quantum Innovation Programme, funded by the Ministry of Baden-Württemberg and started in fall 2016, has a programme line directed at integrated quantum devices engineering [IQST website].

France

Traditionally, the national research funding agency ANR funds quantum communications research projects within a generic yearly call concerning all fields, and according to scientists in the field the success rates are pretty low. However in October 2017 the ANR has started a specific call on Quantum Technologies, with a budget of EUR 10 million per year, for 3 years [Eleni Diamanti, private communications].

There are also specific initiatives at the regional level. The Ile-de-France region is financing a network on quantum technologies (SIRTEQ, funded with EUR 2.5 million per year, for 4 years), that includes a quantum communications axis [Sirteq website]. The Grenoble region has also started a Quantum Engineering programme [Grenoble quantum website]. Contacts are underway for collaborations in specific quantum communications projects with industrial partners (such as Nokia Bell Labs and Thales Alenia Space) and with the national defence agency DGA.

Italy

A national quantum backbone is currently being developed by the national metrological institute (INRIM) that will provide QKD, alongside time stamping for financial applications and frequency/time distribution to scientific institutions which have already been implemented [Calonico 2016].

The Ministry of Defence started funding research on practical uses of QKD more than 10 years ago [Bovino 2005], and is still active on the issue (QUCRYPNET project), having both universities and defence contractors working on it [Ministero Difesa 2016], [Bovino 2016]. Researchers at University of Padova and the Italian Space Agency have pioneered demonstrations of QKD using satellites with corner-cube reflectors [Vallone 2015].

Spain

In 2002, the Institute of Photonic Sciences (ICFO) was founded [ICFO website], financed by the Spanish and Catalonian governments. It comprises a technology transfer unit in charge of maximising business opportunities arising from research. Research on quantum cryptography at ICFO is financed also by NATO and by the AXA Research Fund.

The Comunidad Autónoma de Madrid is financing project Quitemad (Quantum Information Technologies in Madrid), which 'includes experimental proposals and collaborations with leading international laboratories, multinational companies and even SMEs that are associated to the project for its experimental and industrial realisation' [Quitemad website].

The communication provider Telefónica established a QKD pilot in Madrid, in collaboration with a team from the Universidad Politécnica [QKD Madrid website]. A poll on the community of quantum technologies in Spain has been published in 2017 by RICE, a network of researchers: it evidences a low average funding per researcher, dependence on international funding, and lack of experimental groups in key areas, such as quantum communications [RICE 2017].

Austria

The first real-world application of a QKD link took place in Vienna in 2004 [Knight 2004], and a working quantum key distribution network was demonstrated in the framework of the SECOQC international conference, prompting the creation of the ETSI Industry Specification Group on QKD [Secoqc website]. The Austrian Institute of Technology developed an entanglement-based system and in 2012-2015 worked to deploy QKD on real communication networks in the framework of a project funded by the Austrian FFG-Programme FIT-IT [AIT website], [QKD telco]. Vienna's researchers led the experiment that yielded the world record for free-space entanglement-based quantum communications, and are now working with the Chinese academy of science on satellite source of entangled photons [Iqoqi website]: according to a press release issued in coincidence with a visit by the Austrian Minister for Science and Research and the Vice-President of the Chinese Academy of Sciences, 'the Vienna Quantum Space Test Link, contractually agreed upon in 2011, is an outstanding example of the successful and long-term cooperation between the Chinese Academy of Sciences and the Austrian Academy of Sciences' [Wien university press 2013].

4. Policy issues

In this chapter we analyse the policy issues linked to the emergence of the cryptographic tools enabled by quantum communications.

We start in section 4.1 by reviewing what is considered its main technological driver. As the development of a quantum computer large enough to run the already available crypto-analytical algorithms is increasingly seen as likely on a medium-term time scale, several governments are acknowledging the threat and starting to take counter-measures. Quantum cryptography is based on physical principles, and therefore it is immune from attacks made possible by advances and even paradigmatic shifts in computation: it can therefore contribute to 'quantum-safe' communications. However, due to its novelty, drawbacks, and unknowns, it is encountering a certain resistance by the established community of communication security practitioners. Nevertheless, as we have seen in the previous chapter, several industries are positioning themselves to take advantage of the economic potentials that ensuring communications security in the so called 'post-quantum' era will entail. In this situation, the regulatory framework can represent an important factor influencing the choices of potential users. Also ensuring the right mix of technology push and market pull will be a major policy issue, as we will explain in section 4.2. In the private sector several business sectors can act as early adopters and therefore contribute momentum to the market — among them we have finance, health, and defence, see section 4.3; the public sector can also provide a powerful market pull for quantum cryptography, not only because of governmental applications (e.g. by security agencies and administrative services) but also for the protection of critical infrastructures. In section 4.4 we address another major issue, i.e. ensuring the conditions for a truly fair and free international market, in which industries compete and thrive only on the basis of technical excellence. Import restrictions are often applied to cryptographic products, both out of security concern for certain sensitive applications and because at least to a certain degree every government will be trying to breed a national industry, driven by a mix of economic, security, and geostrategic reasons. In addition, cryptography is classified as a double-use technology, and therefore subjected to export limitations. A last point, addressed in section 4.5, is the privacy vs security balance. Along with already available strong encryption technologies, quantum cryptography will reinforce the trend by investigative agencies of shifting from interception along the telecom line to hacking the personal communication device of a suspect. This practice is much more intrusive for privacy, and not immune from cybersecurity risks: it must be therefore strictly regulated. The core of the policy question here shifts from economic issues to the fundamental question of maintaining the correct balance between privacy and security in the presence of new technologies that represent an especially strong disruption.

4.1. The threat of quantum computing

In this section we analyse the impact that quantum computing is having as a technology driver for quantum cryptography. A necessary premise is that, according to publicly available information, quantum computers are not being developed specifically for crypto-analytical purposes. A technological roadmap for this particular application is therefore missing, and the only available scientific publications on this issue have a theoretical approach, which translates in a big uncertainty about the timescale over which an operational quantum computer will represent a concrete communication security threat. However, there has recently been some press cover about China funding the development of a quantum computer to 'boost military's code-breaking ability' [South China MP 2017], and indeed it is well known that a sufficiently large general-purpose quantum computer would allow the running of already available crypto-analytical algorithms (e.g. the Shor algorithm) that can break the asymmetric cryptography implementations currently in use, irrespective of the key length. It is widely accepted that, although also symmetric cryptography will became more

vulnerable, for AES the use of longer keys would suffice to re-establish adequate protection against quantum attacks [Buchanan 2016].
The quest for new cryptographic mathematical algorithms that can resist quantum crypto-analysis is the object of post-quantum cryptography, and standardisation bodies like ETSI and NIST are working on the issue [ETSI 2015], [NIST 2016]. NIST has launched a call of proposal for quantum safe algorithms [NIST PQC call], and in the EU a 3-year post-quantum cryptography project has been founded by Horizon 2020 in 2015, including 11 partners from academia and industry [EU pqcrypto]; a recent review on the status of the research on post-quantum cryptography can be found in [BernsteinLange 2017]. The main aim of such efforts is to devise computational problems that can be used to design a cryptographic scheme that is secure against any polynomial-time quantum adversary, therefore constructing a quantum-safe public-key cryptosystem. A further extension would be finding computational problems that a quantum computer also finds hard to solve in one direction but easy to do in reverse: such an asymmetry would be the basis of a quantum public key encryption system, to be employed in a scenario where quantum computers were widely available, both to legitimate partners and eavesdroppers. The quest for such problems has been extended also to the quantum realm, and several different possibilities have been proposed [Nikolopoulos 2008], [Kawachi 2012], [Vlachu 2016].
As we already anticipated, it is extremely difficult to evaluate the timescale over which the threat represented by quantum computation will actually materialise. On the one hand, the efforts and resources devoted to producing a working large-scale universal quantum computer are increasing year by year, and some credible and respected scientists envisage that a machine capable of executing tasks inaccessible to conventional high performance computers might be brought into existence on a time scale of 10-20 years. On the other hand, making a quantum machine large enough to represent a real threat to modern cryptographic methods may be further off. Implementation of Shor's algorithm to break public key crypto currently in use (like e.g. 1024 bit RSA) would require a computer with ~ 2 000 logical qubits ([Proos 2004] and [Kirsch 2015]), which is two order of magnitude larger than the prototypes that have been actually developed up to now [IBM Q experience]. Extrapolating from the current rate of progress, this could take several decades [Weimer 2011], and the engineering path required to advance from the current state of the art to this level is scarcely known. On the other hand, it must be pointed out that new ways are being discovered to make better use of the available qubits. In addition, it is a shared view among researchers that quantum simulators and dedicated machines specialised in certain computational tasks will become available much earlier than a large general purpose machine. A commercial 'quantum annealer' employed to address specific optimisation problems is indeed already commercially available, and is finding its first applications in physics and engineering [DWave website]; several experts think that other special-purpose machines will become available in a 5-year time span. The possibility that a quantum machine large enough to perform some crypto-analytical tasks emerges well before a general-purpose quantum computer large enough for that task becomes available can't therefore be ruled out.
A key consideration is also the lead time necessary to upgrade the global cybersecurity infrastructure against the quantum threat, as well as the time span over which transmitted data need to be kept confidential. Advocates of 'quantum preparedness', and of course among them commercial firms that sell quantum-safe cryptography, argue we need to start now: sensitive data that can be the object of 'intercept now, decrypt later' attacks and must remain secret for x years could already be compromised if y years are needed to implement quantum safe communications practices, and a concrete threat will materialise before $z = x + y$ years [Stebila 2009]. In some areas, e.g. intelligence, defence, or health, confidentiality periods of decades are the norm. If we take a confidentiality period $x = 30$ years and imagine that $y = 10$ years are necessary to upgrade the existing infrastructure to quantum-safe grade, then sensitive information being transmitted now is already compromised if a powerful enough quantum computer will be available for eavesdropping in less than 40 years. It is evidently not possible to provide policymakers with a reliable technological foresight for such a distant future, and

on the other side scientific developments will be influenced to some extent by policy decisions.
A clear-cut approach against the threat of quantum computing has been taken by the Information Assurance Directorate of the USA National Security Agency, which in August 2015 wrote that 'IAD will initiate a transition to quantum resistant algorithms in the not too distant future. Based on experience in deploying Suite B, we have determined to start planning and communicating early about the upcoming transition to quantum resistant algorithms. Our ultimate goal is to provide cost effective security against a potential quantum computer' [NSA 2015].
Several EU bodies deal with sensitive information, and awareness of the threats brought forward by quantum computation is starting to emerge, as can be seen e.g. in a briefing issued in 2016 by EU-LISA, the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, which is responsible for the operational management of the second generation Schengen Information System (SIS II), the Visa Information System (VIS) and the Eurodac fingerprints database for asylum seekers [EU-LISA 2016].
The role of QKD in the communication security scenario brought forward by developments in quantum computing is a matter of debate among scientists. Quantum-safe cryptographic methods based on algorithmic solutions and on physical-layer implementations like QKD typically do not address the same issues, and present completely different ranges of weaknesses and advantages. Advocates of QKD concede that presently the technique can address only a limited range of problems, but are nonetheless convinced that physical-layer quantum cryptography and algorithmic-based post-quantum cryptography will both have a role to play in providing security solutions for the future communications landscape. They add that the security of algorithmic schemes may turn out not to be as reliable as thought, since these are presently mostly checked out only against Shor's and Grover's algorithms, while there is no specific reason why attacks with other quantum algorithms, or even non-quantum attacks, might not be possible. They also point out that existing trends towards cloud computing will be reinforced by the availability of large-scale quantum computation facilities, and envisage a 'quantum internet' where high-level encryption will be ensured by QKD [CloudSecurityAlliance 2017].

Other communities, e.g. the Internet Engineering Task Force, are much more sceptical about the practical prospects of quantum computing [IETF 2015], and although accepting the need to start preparing for its purported crypto-analytical capabilities, tend to view QKD as 'pointless'. Also big telecom corporations stress the various limitations of QKD, and point out that it will be extremely difficult to accommodate it with the ongoing Internet of Things trend [McGrew 2015]. Commercial providers of cryptographic solutions are starkly divided: some of them tend to be dismissive of the threats represented by quantum computers and assert that by the time a real risk materialises new solutions rooted in current practices will have been found [Entrust 2009], while others are actively engaged in QKD deployments [Senetas 2010], [Keymile 2016].

We remark that the debate among researchers recently experienced a flare-up because of the developments in the decisional process on public RTD funding on quantum technologies. We mention in particular the comments on the flagship research programme proposed by the European Commission [EC Futurium 2016] posted by the coordinator of the Horizon Post-Quantum Cryptography project we already mentioned, and the vision of QKD as something in between 'snake oil' and a 'security fraud' purported by a well-known and opinionated cryptography expert [Bernstein blog 2016] in commenting on the same programme.

At the level of policy decisions, the uncertainties and limitations of quantum cryptography are heavily impacting on the view of some governmental agencies in charge of information security. For example, in a report [BSI 2016] entitled 'The State of IT Security in Germany 2016', in addressing the threat of quantum computing the German Federal Office for Information Security BSI writes: 'Besides quantum-computer-

resistant cryptographic mechanisms, reference is also made to methods from the area of quantum cryptography as potential solutions for establishing secure data connections in a world with quantum computers. This concerns technical systems which use physical effects to solve a similar security problem to public key cryptographic mechanisms by mathematical means. Quantum cryptographic mechanisms require, in particular, specialist hardware for the data connection and a traditional cryptographically authenticated channel for key negotiation. The security guarantees of such mechanisms are also heavily dependent on implementation aspects. Both practically and in terms of security, quantum cryptography is therefore not currently regarded as a strong alternative to post-quantum methods'. In a recent white paper [NCSC 2016] that spells out the position on QKD of the UK National Cyber Security Centre, part of GCHQ, an assessment of its strengths and weaknesses is presented. Based on this analysis, the NCSC decides at the end to 'not endorse QKD for any government or military applications' and to 'advise against replacing any existing public key solutions with QKD for commercial applications'. Also the military sector seems wary: in 2015 the USAF Scientific Advisory Board published a study on the 'Utility of Quantum Systems for the Air Force', in which it states that 'quantum key distribution significantly increases system complexity but is unlikely to provide an overall improvement in communication security as it provides little advantage over the best classical alternatives' [USAF 2015 abstract], [USAF 2015 comment].

We have however seen how, despite the critical views sometimes expressed by agencies in charge of cybersecurity policies, all of the advanced countries' governments are funding research programmes in quantum communications, testing pilot schemes, and in some cases also deploying large-scale infrastructures. The German Federal Ministry of Economics and Technology (BMWi) participates in the ETSI Industry Specification Group on QKD, and the German Federal Minister of Research Johanna Wanka announced in early 2017 a call for tenders on quantum communication, with the final goal of developing 'encryption systems which cannot be broken even with high-power quantum computers' [Qutega 2017]. In the UK, the Government Office for Science included in a paper entitled 'The Quantum Age: technological opportunities' two recommendations specifically related to the role that the National Cyber Security Centre is expected to play on QKD, stating respectively that 'The National Cyber Security Centre should support a pilot trial of QKD using realistic data in a realistic environment' and that 'The National Physical Laboratory, the National Cyber Security Centre, and academia should form a partnership to perform conformance tests and issue accreditation certificates' [UK Gov Office for science 2016].

An explicit acknowledgement by regulators of the threat represented by quantum computing to communications security would undoubtedly be a strong policy driver for the development of quantum-safe communications and therefore also for quantum cryptography. However, to make sure that policy choices will not compromise technical excellence, European policymakers must continue to avoid technology mandates, and regulators must remain technology-neutral. Even when dealing with potentially transformative technologies like quantum computing and quantum communications, funding of research and of technology transfer must be carefully balanced against all possible alternatives, so that it will be the task of free markets to pick up the best solutions. In this regard, we point out that quantum cryptography is still a quite esoteric academic discipline, and its practitioners are just starting to confront themselves with the wider world of conventional communications security. If quantum cryptography is to become part of the established telecom landscape, it is paramount to fund projects and deployments where the quantum communications research community is forced to collaborate with 'classical' partners. An idea endorsed by both academy and industry is to deploy a fibre-based quantum key distribution pilot, fully integrated with the communication network and freely accessible to all researchers, that will be used as a technology test-bed and possibly as a pilot for the certification processes.

4.2. Technology push and market pull

As we have already seen in Chapter 3, presently the main players in the international panorama are the USA, China, Japan, and Europe. Two contrasting attitudes constitute perennial poles of attraction as governments develop their industrial strategies, pitting techno-nationalistic mercantilism characterised by state-sponsored innovation, promotion of national champions and shielding of internal markets from foreign players against the acceptance of open worldwide competition and private-led innovation, which leads to market-picked winners.

- The USA was the first country to establish a technical know-how, driven essentially by potential applications in defence and security. The peak of this research effort was ~ 10 years ago, but afterwards a commercial pull failed to materialise; activity in quantum communications seems now to be low-key in the private sector, but a renewed interest is starting to materialise at the policy level. Intelligence experts have recently signalled to the US Congress the narrowing of the nation's technological edge in quantum communications with respect to other countries (notably China), and the associated geopolitical risks.
- China has made quantum communications a national priority, establishing in the last ~ 15 years cutting-edge scientific and technological capabilities, and spurring the rise of an indigenous industry which includes several commercial vendors. A large-scale infrastructural deployment is also taking place, comprising a national quantum backbone and a quantum satellite for long-range communications. It is however not clear how much the private sector is actually using this infrastructure.
- Japan seems to be the country where the largest effort from private enterprises is taking place: producers of communications equipment, telecom providers, information technology and electronic corporations are working on QKD devices and systems, even in the absence of major public funding, and extensive deployments are being done.
- Europe has first-class academic research in quantum communications, which attracts many foreign students and researchers. Several foreign companies are allured by the human capital formed in European universities, and inward investment seems to be on the rise. The Japanese multinational firm Toshiba has been doing pre-competitive research on quantum communications in the UK for several years, and the Chinese telecom giant Huawei recently opened a research centre to work on the topic in Germany ([2]). However, the European industry basis is weak overall. Some telecom providers (e.g. British Telecom, Swisscomm, Telefónica, etc.) acquired a specific know-how by working in (small) public-funded temporary pilots, but among the several university spin-offs that have been founded in the last decade or so only the Swiss start-up ID Quantique still operates as a commercial vendor of QKD systems. In addition, the supply chain for the quantum devices necessary for system integration relies heavily on vendors based in Japan or in the USA; some items are dual-use and can be subject to ITAR restrictions.

Given the facts on the ground, it is reasonable to foresee that in the near term the applications for which QKD could become a viable option will involve only the most sensitive communications: a typical example could be secret communications for which couriers are now used to transmit cryptographic keys, where it would allow to eliminate the risks associated with the human element. Although at the beginning QKD will likely

([2]) We refer to a large multinational company operating in the global market with the indication of the nation in which it is headquartered, which usually coincides with the country where it was originally founded and where the majority of the members of its directors' board have their citizenship. The indication of such 'home country' is a widely used practice, even though multinational companies have customers all over the word, their manufacturing plants and research centres can be found in several countries, and their supply chains know no borders; in addition, when they are publicly owned their shares are usually traded in the stock markets of several nations.

be used only by large organisations (private and governmental) in a limited range of applications, in the longer term it would allow expanding high security communications to all parties who enjoy an optical link. The banking sector has started testing this technology, with banks branches being connected among them and to data centres, and even linked to metropolitan rings and quantum backbones (notably in China, but also in Switzerland and the UK). In the longer term, the use of 'quantum ATM' could also provide a path to mass consumer quantum cryptography, enabled by short-range communication chips integrated in mobile phones. The case can also be made for governments to act as early users for applications in the public administration (e-government) or when economic considerations can be deemed of secondary importance and security is the paramount priority (infrastructure protection, defence and space).

It is however clear that a sizeable market will not materialise in the absence of sound business cases. Presently, the overall perception is that private enterprises are not exerting a significant 'market pull', and it is debatable whether the 'technology push' funded by public money will be enough to ensure the transitioning from laboratories to real-world settings. QKD is affected by well-known drawbacks in terms of distance, rate, compatibility with existing infrastructure, and cost, which severely hinder market uptake. According to some experts such limitations are so serious that they will deny to this technology any commercial sense, except in very limited niches [Cisco 2013], [HP Colloquium 2012], [McGrew 2012]. A risk analysis approach has also underlined that the key exchange is presently one of the strongest links in the communication security chain, so that QKD essentially solves a non-existing problem [Schneier 2008]. In addition, practitioners of conventional cryptography point out that the potential for yet unexplored loopholes that may lead to new kinds of attacks is huge, and that the transition from mathematics to physics unavoidably entails trading computational security for implementation security [Paterson 2009], [IETF QKD pointless].

On the other side, an ETSI Industry Specification Group has been formed which sees several industries which are involved in technology development working together with some perspective users. The ETSI QKD ISG has compiled a catalogue of possible attacks on QKD physical implementations [ETSI ISG QKD], and has published a white paper to propose credible business cases [ETSI 2010]. The practical aspects of security certification for commercial systems have also been addressed [Alléaume Standards 2014], and some researchers are trying to quantify the cost per bit of exchanged secure key in their systems [Mo 2011], [Elser 2012]. The challenges facing successful commercialisation of quantum communication technology are being studied [Lo 1999], [Natsheh 2015], and market analysis is included in many research programmes on quantum communications [UniWaterloo Market Study], along with industry and user engagement [UK Hub Ind. Engag.]. In 2017 two market reports on QKD were published by CIR, a consultancy for the optical networking business: the overall conclusions are that 'its addressable market is expanding from specialised projects sponsored by governments and giant financial institutions to large data centres, of which there are a large and growing number', and that 'as we are entering a period in which permanent quantum networks are being built', 'opportunities at the service level, but more immediately at the components and modules levels will be created' [CIR 2017 Quantum Encryption], [CIR 2017 Quantum Networking].

Most of the economic worth of a QKD system resides indeed in some of its components, and ensuring its supply chain can be a significant market opportunity for enterprises mastering advanced manufacturing techniques, and for producers of key enabling technologies in the photonics, microelectronics, and optoelectronic industries. At present, European manufacturers of QKD systems heavily depend on foreign providers of components. On the other hand, Europe has first-class research results in quantum devices. In this scenario, EU may consider encouraging industry uptake by funding pilot production lines (e.g. in chip-scale integrated components) with the double aim of generating economic growth and assuaging the dependency on foreign component

providers. We add that for space applications devices such as sources, modulators, and detectors must be space-grade certified, entailing industrial processes which represent an additional source of value. In the USA the small business research initiative (SBIR/STTR) has been widely employed by larger firms and public actors (in particular the military sector and NASA) to outsource to SME the development of high-tech quantum communications components.

In the QKD supply chain, single photon detectors based on avalanche photo diodes are among the most sensitive (and expensive) items: European system integrators depend on American producers and to a lesser extent on Japanese ones. Conversely, Europe is relatively well positioned in superconducting detectors which, although not yet used in commercial QKD systems, are expected to be key components for future quantum communications solutions and notably quantum repeaters. With regard to imaging-capable SPADs (single-photon avalanche diodes) arrays, which might be used in next-generation QKD systems which encode quantum information also in the transverse propagating modes, we note that the export from the USA is subject to ITAR restrictions.

Indeed, some quantum communications components have a dual-use nature, and a QKD system can be of great interest for military applications. In cooperation with The Netherlands EU Presidency, the European Defence Agency held a Research and Technology (R & T) Conference in April 2016 in which two presentations were devoted to Quantum Technologies [EDA press 2016], [EDA report 2016]. The European Commission has acknowledged that to enhance the competitiveness of the EU security industry in times of financial constraints 'an emphasis should be given to a better exploitation of synergies between civilian and defence orientated research' [DG HOME industrial policy]. In the UK, the Department of Defence Science & Tech Lab DSTL is active within the national-funded Quantum Communications Hub, and participates in projects funded by the Engineering and Physical Sciences Research Council [EPSRC 2014]. In the USA, a ~ USD 3.5 million contract spanning from 2016 to 2021 has been awarded to Boeing by the USAF for the development of QKD systems [USAF Boeing 2016].

Balancing considerations of economic growth with those of national security, governments usually try to enforce policies aimed at fostering a national cybersecurity industry which can thrive in domestic and foreign markets, while simultaneously ensuring that advanced encryption technologies which have been developed internally do not become available to potentially hostile countries. The existence of home-grown cryptographic capabilities is often seen as a matter of national security, a view reinforced by the fact that in the international landscape some nations have tried to limit the public's and foreign nations' access to cryptography strong enough to resist decryption by their intelligence agencies (the so-called 'crypto wars', [Wiki CryptoWars]). In addition, massive communication surveillance programmes have repeatedly been put in place, to gain business advantages alongside political and military information [Wiki GlobalSurveillance]. We mention in this regard a 1999 study by the European Parliament Science and Technology Options Assessment panel (STOA) [STOA 1999] and a report presented to the European Parliament 'on the existence of a global system for the interception of private and commercial communications' prepared by the Temporary Committee on the ECHELON Interception System in 2001 [EP Echelon 2001]. The report makes reference to QKD as a way to ensure that the interception of a key exchange could not pass unnoticed, and the EU SECOQC research project was indeed presented by some of its researchers and by the specialised press as 'an effort to cope with Echelon' [Willan 2004], [Sans 2004]. More recently, following the so-called 'Snowden's revelations' about the existence of a US surveillance programme, a 6-month EU Parliament inquiry into electronic mass surveillance of EU citizens took place, leading to EP resolutions in March 2014 [EP NSA 2014] and again in 2015 [EP Pressroom 2015]. The European Parliament's Committee on Foreign Affairs, in dealing with transatlantic digital economy and data protection, insists on the necessity of 'creating a transatlantic dialogue to rebuild trust' [EP Foreign Affairs 2016]. It is a matter of debate to what extent the 'Snowden revelations' contributed to the Chinese quantum communication

infrastructural build-up [Moore 2014], [Chen Jun 2014]. In any case, existing regulations governing encryption require that systems sold within China use certain indigenous technologies if they have a high risk of impacting national security or domestic stability should they be compromised [Segal 2016].

In this regard, the presence in Europe of research centres of multinational companies working on quantum communications requires careful attention from the policymakers. It is widely recognised that foreign investment, a typical head mark of large multinational corporations, can be an important driver of technological innovation, and in some cases it can be highly beneficial for the economic growth of the recipient country. However, proper policies must be implemented to ensure that public money spent to foster technology development will bear fruit in Europe itself. In addition, actual events have repeatedly brought to the fore the potential for conflicts between factors rooted in national policies and the activity of multinational firms, which although operating in the global market typically maintain for the most diverse reasons a privileged relationship with their home country. Communication and information technologies, with their security implications, are certainly a case where such confrontations can become extremely high-pitched. This is a fact that cannot be ignored for quantum cryptography, since among its early users we are likely to find governments, in particular for applications by agencies requiring high security communications. Here is not the place for an attempt to analyse the degree to which a given multinational company is intertwined with the interests of a particular national government. Just to give an example of the ongoing confrontations, we recall an 'Investigative Report on the US National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE' prepared by the US Congress Permanent Select Committee on Intelligence and published on 8 October 2012, from which it followed that 'Chinese multinationals Huawei and ZTE are banned to sell network equipment to USA governmental agencies', see respectively [US House 2012] and [Techonomy 2013]. An article entitled 'China's ghost in Europe's telecom machine' which states that 'growing security worries could derail Huawei's 5G ambitions' was published in Politico in December 2017 [Politico 2017]. More recently, 'American government agencies have been ordered to stop using antivirus software made by Kaspersky Lab, whose headquarters are in Moscow', see [NYtimes 2017].

4.3. Application areas

In this section we review the business sectors that demonstrated interest for the actual use of QKD systems. In the sector of corporate applications, the largest private user of QKD is the American firm Batelle, which installed in 2013 a QKD link to connect its sites in Columbus and Dublin (Ohio), and is now planning to extend it to connect Washington, DC, for a total span of 700 km [Batelle deployment]. In Europe, Siemens deployed in 2010 a QKD secured link between its data centres in The Hague and Zoetermeer [Siemens deployment] and the telecom provider KPN is also planning a field deployment of QKD systems [KPN deployment]. The connection of data centres is seen as a QKD early market by some the CIR analysts we already mentioned.

In the health sector, a QKD link to protect the transmission of genome analysis data is being tested by Toshiba in Tokyo since August 2015. Actual genome data produced at the Toshiba Life Science Analysis Centre are transmitted to Tohoku Medical Megabank Organization, over a distance of 7 km. For 2 years the free-air QKD system will be verified for communication stability and speed, and the impact of environmental conditions will be verified. Toshiba aims to use the results of the testing to support commercialisation within 5 years of a quantum cryptographic communication system able to guarantee secure transfers of confidential information, with potential users including public agencies and medical institutions [Toshiba Genome 2015].

The interest of companies in the defence sector has been evidenced also by our patent analysis: indeed, we found that both in the USA and in Europe the main applicants are

firms active in these areas. The latest developments of quantum technologies for advanced security and defence systems have been the object of a SPIE conference held in Warsaw in September 2017, with two sessions devoted respectively to QKD and quantum communications [SPIE Defence 2017]. Big European security and defence companies such as Thales, Airbus, Selex, and Qinetiq have a quantum agenda and are actively involved in the quantum flagship coordinated by the EC. In a recent presentation, Selex in particular declared that 'within the UK Defence Community, Quantum Technologies are viewed as a key area for providing new and innovative capabilities for our forces' [Selex 2014]. The UK Defence Science and Technology Laboratory is involved in the national quantum technology programme, and in a recent presentation of its activities in the field mentioned its main issues: 'control IP and knowhow, build resilient sovereign capabilities, circumvent ITAR issues and create on shore industries' [DSTL 2015].

Other examples of QKD application can be found in the protection of infrastructure deemed to have critical importance. The EU agency for Network and Information Security ENISA published a short briefing on QKD in 2009, explaining the basic physical principles and the main limitations, but without elaborating on possible applications in the field of infrastructure protection [ENISA QKD 2009]. The directive on security of networks and information systems (NIS Directive 2016/1148, adopted by the European Parliament on 6 July 2016) constitutes the first piece of EU-wide legislation on cybersecurity. It makes explicit reference to the protection of critical infrastructure in sectors like energy, transport, banking and finance, health, water, and communications. Several events in the last couple of years highlighted the necessity for such protection: large-scale cyber-attacks to power distribution networks happened for example in Ukraine in December 2015 and again in December 2016. In May 2017, the ransomware WannaCry targeted among others the United Kingdom's National Health Service, Spain's Telefónica, and Deutsche Bahn. In June 2017, a malware called NotPetya compromised IT systems at Ukraine's central bank, state telecom, municipal metro, and Kiev's airport.

The use of QKD to protect the energy grid is being studied both in China (State Grid Corp) and in the USA (Los Alamos National Labs and Department of Energy), on the rationale that the increasing presence of diffuse and unpredictable power generation from green sources needs more sophisticated control communications that must be safeguarded. An IEEE white paper on smart grid research entitled 'IEEE Vision for Smart Grid Communications: 2030 and Beyond' includes QKD among the emerging technologies that may have a disruptive impact in ensuring infrastructure security. To our knowledge, no European power distribution operator is presently working on the possible use of QKD to protect grid service communications. Conversely, the telecom sector (Telefónica, British Telecom [Whitley 2015]) is investigating the feasibility of adopting QKD systems to secure the control plane in software-defined communications networks, a possibility explored also by the Chinese Huawei. British Telecom has proposed to this aim the development of a global satellite QKD overlay platform integrated with terrestrial telco operations [Wakeling 2017].

In transport, EuroControl funded a project to evaluate the enhancement of air-ground telecommunication security by using quantum cryptography technology. As a conclusion, a paper was published that shows how the Aeronautical Telecommunication Network (used by air traffic authorities, controllers, aircrafts and ground stations to communicate voice and data) can be secured by using quantum cryptography (QC) instead of classical PKI [Bellot], [Eurocontrol 2008]. In the same field, our patent survey detected a couple of patents on QKD assigned to Boeing.

The sector which has demonstrated most interest in quantum cryptography is the financial one: as we have seen, the first field application of QKD in Europe involved a bank transaction in Vienna, in 2004. Banks and national financial regulation authorities seem to be among the users of the Chinese quantum backbone, and some Swiss banks have tested and experimented ID Quantique QKD equipment, in some cases using it for several years. In Moscow, Gazprombank has tested equipment developed by the Russian

Quantum Center. The provider of digital security solutions Gemalto declares in its white paper 'Securing financial services data in transit' that it 'provides a QKD integrated solution that has been successfully deployed in a number of major European financial institutions' [Gemalto website]. KTN, the Knowledge Transfer Network which is Innovate UK's network partner and provides innovation networking to drive UK growth, has included a chapter on Quantum Communications Applications into the Finance Industry in a paper entitled 'Quantum Technologies in Finance' [KTN Quantum Finance]. The Australian Westpac Banking Corp has invested in the QKD startup QuintessenceLab [Financial Review 2015], and the insurance company AXA is funding a chair on quantum cryptography at the Barcelona Institute of Photonic Sciences (ICFO) [Axa 2015]. The interest from the financial sector has been demonstrated also by the workshop 'Quantum Technologies in Finance', held in London in February 2016.

Several regulations are in force, which outline best practice to mitigate operational and financial risk in the banking, finance, and insurance sector, and that mandate the encryption of sensitive data (e.g. payment card data, private data, data related to financial reporting). For example, both the international Basel II accord and the EU eighth company law directive (euro-Sox) mandate the use of encryption to protect sensitive data related to financial reporting, and demand high conditions for information security systems and internal IT control systems.

We recall that 'Cryptographic equipment specially designed and limited for banking use' does not fall into the trade restrictions in place for dual-use technology, as will be detailed in the next section. We point out here that the banking sector can constitute also an avenue for the so called 'consumer QKD', which envisages the download of encryption keys to the user's mobile phone from a network of cash dispensers connected to a quantum backbone. Short-range quantum communication chips are being developed for this purpose, both by public programmes and industries.

Another sector that could benefit from the security ensured by quantum cryptography is space. Satellites can indeed be seen as a critical infrastructure, whose protection can be reinforced by using QKD to prevent interference with control communications. In this framework, Germany's space and technology company OHB is funding a professorship at the Institute of Information Technology at the University of the German Federal Armed Forces (Munich) to improve cyber security in satellite communications [OHB 2017]; in February 2017 OHB announced a joint collaboration agreement on space-based quantum communications with TNO and QuTech [Dirks 2017]. Encryption is also fundamental for the public regulated GNSS services provided to governmental authorised users and sensitive applications that require high continuity, as explained by the European Global Navigation Satellite Systems Agency [GSA Galileo PRS], and QKD might be used to secure critical links in the ground segment of the infrastructure.

A trend that can facilitate the use of QKD to ensure data confidentiality and integrity in space communication is the push to use optical communications instead of radio, because of the allowed substantial (10^5) increase in bit rate. The Swiss company Ruag (now part of Thales Alenia Space) is working on high-speed inter-satellite laser communication, alongside Tesat-Spacecom from Germany. Tesat in particular is analysing the possibility of adapting the Laser Communication Terminal of their Alphasat geostationary satellites to perform quantum communications [Elser 2015]. Developments in this field could be of interest for the secure transmission of data by the European Data Relay System, and therefore for the Copernicus constellation [OSA 2017]. The military sector is also interested: in a document released by the Office of the US air force chief QKD is mentioned in connection with laser communications, since it 'can provide verifiably secure encrypted transmissions', which can link 'critical Air Force satellite, air, and ground network nodes and can help shift the rapidly growing demand for bandwidth to frequencies where spectrum management is far simpler' [USAF 2011].

We have therefore seen how QKD can be used to secure satellites and satellites' signals. On the other hand, satellites can also be used to implement long-distance quantum

communications, since they can be used as 'trusted nodes' while waiting for the development of field-deployable quantum repeaters. Several European research groups are working on this issue (see e.g. [Oi 2017]), and space-based quantum communications are included in the 4-year action 'Quantum Technologies in Space' started by the European Cooperation in Science and Technology in October 2016 [COST space QT 1], [COST space QT 2]. The COST action comprehends a working group dedicated to 'identify potential applications besides fundamental tests of physics', which will 'aim at establishing links to industrial partners for future implementations'. In particular, it states that 'space-based sources of entangled photons promise the formation of global quantum communication networks'.

The European Space Agency is also an active quantum communications player [ESA Willie]. More than 10 years ago ESA commissioned a pioneer feasibility study for the placement of an entangled photon source on the International Space Station [Ursin 2008], [ESA Bulletin 2009]. Despite the positive conclusions put forward by this study, no further steps were taken. The Chinese successes in the field recently acted as a catalyst, and in January 2017 a new ARTES (Advanced Research in Telecommunications Systems) programme element named ScyLight (SeCure and Laser communication Technology) was initiated [ESA Scylight 1]. It will 'support the development and deployment of innovative optical technologies for satellite communication and assist industry develop new market opportunities for optical communication technologies', comprising a programme line dedicated to quantum cryptography technologies, which will 'cover the related developments as well as in-orbit and service demonstration, including quantum key generation and distribution systems, and the demonstration of related end-to-end systems' [ESA Scylight 2], [ESA Scylight 3].

4.4. International commerce

The export of dual-use technology is regulated by several international agreements. We mention in particular the 1996 multilateral Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, which was established 'to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilising accumulations', and also 'to prevent the acquisition of these items by terrorists' [Wassenaar website].

At the EU level, the regulatory framework is established by Regulation 428/2009, which sets up 'a Community regime for the control of exports, transfer, brokering and transit of dual-use items'. Cryptography is in the list of dual-use items (Annex I), under Category 5 'Telecommunications and Information security', which mentions also quantum cryptography and QKD. Quantum key distribution is explicitly referred to also in the context of the sanctions put in place towards embargoed countries, towards which some high-technologies export from the EU can be restricted. We note in addition that 'equipment designed or modified to perform cryptanalytic functions' is in the Annex IV list of items for which the responsibility for deciding on transfer within the Community lies with national authorities, so that for such technologies commerce can be restricted even within the EU borders. Indeed, while cryptographic technology export is regulated at the EU level, interpretation and enforcement of regulations is left to Member States: historically, this introduced differences, costs, and uncertainties that may represent major hurdles, especially for small start-ups. To level the playing field, EU should work with the Member States to remove any inconsistencies in export controls and cut out all unnecessary red tape.

The regulation has been revised by the Commission Delegated Regulation 1382/2014, and a major review of dual-use export control is now under way following the ordinary legislative procedure which sees Parliament and Council on an equal footing. On the issue, the European Commission's DG for Trade published in September 2016 a Staff Working Document [SWD 315 2016]. According to the EC SWD, the main aim of the

review is to strike the right balance between security and competitiveness by adapting the EU export controls to rapidly changing technological, economic and political circumstances. Among the problems to be addressed, the existence of excessive administrative burden and the uneven implementation and enforcement within the EU are mentioned.

The European Parliament Research Service published a briefing in January 2017 [EPRS dual use 2017], which explains how the revision proposal introduces a controversial new 'human security' dimension to export controls, to prevent the abuse of certain cyber-surveillance technologies by regimes with a questionable human rights record [CIHR 2015]. A 'catch-all' provision has also been proposed by the Commission, which would make it obligatory to obtain an authorisation for the export of dual-use items not included in the control list but destined 'for use by persons complicit in or responsible for directing or committing serious violations of human rights or international humanitarian law in situations of armed conflict or internal repression in the country of final destination'.

DigitalEurope, advocating on behalf the industry, highlights that 'a well-balanced export control policy is crucial to survive today's tough global competition' and that it is 'imperative that the balance between security and trade remain intact in order to avoid self-inflicted trade barriers that would impose a high cost for the EU industry without providing anything in return' [DigitalEurope export 2016]. In general, the industry seems to be concerned that the 'human security approach' can hurt business without contributing to its purposes, and that the catch-all provision proposed by the Commission 'would seriously undermine the competitiveness of European business, as there are no multilateral clauses on this mechanism'. Referring in particular to encryption, DigitalEurope remarks that, 'unlike in the US, where an extensive simplification through the license exemption for encryption exists, an export license is required for most exports of encryption items from the EU'; in addition Member States may also impose their own additional licensing requirements, so that 'the misalignment across the European Union of encryption controls and licensing processes creates a challenging landscape for European companies'.

This view is shared also by the Commission: DG Migration and Home Affairs declares in its 'Industry for Security' agenda that 'the first priority will be to overcome the fragmentation of the EU security markets through the harmonisation of standards and certification procedures for security technologies' [DG HOME website]. Notably, certifications for government applications of encryption differ from country to country, thus hampering the development of a pan-European market, and a Member State can restrict the export of crypto-analytical equipment to other Member States. Also independent academic research acknowledges that commercial companies selling cryptographic technologies face 'a bewildering array of regulations, sometimes unclear and haphazardly applied', and that the regulatory patchwork they have to navigate creates substantial challenges and risks to firms which operate internationally, including the necessity to produce locally in countries that restrict imports, the possibility to incur penalties if cryptography systems are exported to prohibited countries or entities, and the risk to operate where prohibitions on the use of encryption jeopardise their intellectual property [Saper 2013].

In a first step to simplification and harmonisation, and in order to create a level playing field within the EU, DigitalEurope proposes to start converting national general export authorisations (NGEAs) to EUGEAs, beginning with standard commercial encryption technologies. In this way, EU export-control resources could be more effectively 'dedicated to non-standard cryptography that indeed requires stricter controls'. Quantum cryptography would naturally fall into this category. In this regard, it must be pointed out that in Europe some of the quantum cryptography commercial players are start-ups and small university spin-off. None of them figure in the list of DigitalEurope affiliates, which comprises mainly big corporations and multinational firms. For smallish players it could be very demanding to gather the resources, experience, and competences

necessary to address the complex bureaucracy required by some countries to navigate export controls. The firms which seem better positioned for this hurdle are probably the big champions of the defence sector.

In a recent meeting on the 'Technical barriers to trade', WTO members 'extensively debated the impact of cyber security laws on trade in high-technology products, as more than one third of new trade concerns touched upon this issue. Some members were concerned that these newly introduced regulations would negatively impact trade in ICT products, potentially discriminating against non-domestic companies and technologies, and possibly leading to unnecessary disclosure of commercially confidential and technical information' [WTO June 2017]. In particular 'the European Union, Japan, the United States and Canada said that China's draft encryption requirements are highly trade restrictive on ICT products, and could discriminate against a range of companies that use or supply encrypted products and encryption-related services in China'; consequently 'members asked China to ensure that its requirements are developed in accordance with international practices and standards, are non-discriminatory and do not require manufacturers to reveal sensitive and protected information, such as encryption keys or source code.'

Policy analysts assess that China has taken the decision to embark on its large-scale quantum communications programme for a mix of reasons spanning from techno-nationalism to state-sponsored mercantilism. They highlight that one of the main motivations for deploying a country-wide quantum communications infrastructure is to develop communications links not penetrable by foreign potentially hostile actors. In this picture, the development of a particular technology is in the first instance a long-term strategic policy decision, with commercial potential as a welcome side-effect. Market analysts add that state security considerations contributed to the shaping of Chinese policies aimed at promoting national champions, and at protecting them from foreign competition in the internal market. For these reasons, the national infrastructural deployment programme has made China a very difficult market for non-Chinese providers of quantum communications systems, although one the most tempting for its size. Chinese authorities have spurred the rise of a national quantum communication industry by severely restricting the import of cryptographic technology, and foreign firms can access the internal market only via joint-ventures with Chinese players, possibly jeopardising their intellectual property. In addition, there is the risk that they have to develop country-specific technologies, thus contributing to the fragmentation of the global market. There could be also a reputational risk: a draft of China's counterterrorism law included provisions requiring the installation of backdoors and the reporting of encryption keys [Segal 2016].

These issues reverberate in the field of quantum cryptography, as can be seen from the following account. We have already outlined the Chinese national strategy on quantum communications, and highlighted the infrastructural deployments being carried out, in particular the ~ 2 000 km quantum backbone. The University of Science and Technology of China (USTC), general contractor in charge of deploying the Beijing-Hangzhou trunk line, invited the Swiss firm ID Quantique to participate in the tender. The advance notice was however not sufficient (1 week, with all documents to be written in Chinese), and ID Quantique was not able to participate. QuantumCTek, an indigenous firm co-founded by USTC researchers with a much more recently developed know-how and intellectual property portfolio, was instead chosen. In December 2016, ID Quantique announced a partnership with China Quantum Technologies, another Chinese company specialised in quantum communications, 'to bring the company's quantum encryption technology to the Chinese market. The companies will create a joint venture, which will open the Chinese market to IDQ's quantum random number generators (QRNGs) and quantum key distribution (QKD) solutions. IDQ's technology will be adapted for the specific needs

of the Chinese market, and notably will be focused on supplying QKD systems for the development of the extensive quantum communications backbone being built in the country' ([3]). On the one hand, this partnership is an acknowledgement of the technical excellence of a European firm. On the other hand, it allows one to appreciate the challenges that entering the Chinese market of quantum technologies present to external firms, since the lack of transparency leaves them with no other options than finding a local partner.

4.5. Privacy and security

At first-principles level, the right to communication privacy is enshrined in Article 12 of the United Nations Universal Declaration of Human Rights, and in Article 8 of the European Convention on Human Rights ([4]). In line with the two clauses of Article 8, two competing concerns shape the regulatory environment concerning cryptographic technologies in most western democracies: enforcing the law-abiding citizens' right to communications privacy, while simultaneously preventing criminals from taking advantage of it. This has been done among other things also by putting in place regulations restricting the import or/and the export of cryptographic technology, limiting or prohibiting the use of encryption, and even restraining the import of encrypted data [Saper 2013]; also lawful interception is considered a powerful investigative tool. The only legally binding international treaty on crimes committed via the internet and other computer networks is the Budapest Convention on Cybercrime, drawn up by the Council of Europe in 2001 and entered in force in 2004 [Budapest Convention website]. It is intended to serve 'as a guideline for any country developing comprehensive national legislation against cybercrimes', and includes lawful interception among the powers necessary for the investigation and prosecution of cybercrimes. The Convention is in force in all the EU Member States, with the exception of Ireland and Sweden, which have signed but not yet ratified it. Lawful interception is regulated at national level in the EU, although in accordance with the framework established by the European Council Resolution 96/C 329/01 (January 1996), and is technically implemented according to established industrial standards [ETSI Lawful Interception].

From the 1990s, the rise of worldwide communications over the internet brought great attention to the problems and opportunities associated with cryptography: however, the attempts specifically made at international harmonisation of cryptography regulations have been largely unsuccessful. In 1997 the OECD adopted a 'Recommendation Concerning Guidelines for Cryptography Policy', intended to 'promote the use of cryptography without unduly jeopardising public safety, law enforcement, and national

---

([3]) http://www.idquantique.com/idq-qtec

([4]) UN 'Universal Declaration of Human Rights', Article 12:

'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.'

Note that the use of the word 'arbitrary' implicitly suggests the possibility of an exception for lawful interception carried out within a regulatory framework.

European Convention on Human Rights, Article 8:

'1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'

security' [OECD crypto guidelines]. According to the Recommendation, eight principles should be followed by member nations in establishing their own cryptography policies: users should have a right to choose any cryptographic method, subject to applicable law; the development of cryptographic methods should be market driven; the fundamental rights of individuals to privacy should be respected by national policies; and national policies may allow lawful access to plaintext, or cryptographic keys, of encrypted data, but these policies must respect the other principles contained in the guidelines to the greatest extent possible. Reviews on the Recommendation are conducted every 5 years, and according to the OECD the guidelines 'continue to be adequate to address the issues and purpose for which they were developed'.

Despite the OECD guidelines, the worldwide regulatory landscape on cryptography is largely fractured along national boundaries. Also among EU Member States marked differences do exist, in part because historical reasons gave rise to different national sensitivities. National and supranational actors, which pursue different and sometimes conflicting agendas, and hold powers in different areas, contribute to shape the policy debate. Historically, the EU played a crucial role in affirming and enforcing the right to privacy by driving the development and introduction of national data protection laws. The European Union Agency for Fundamental Rights, which has the mission of 'helping to make fundamental rights a reality for everyone in the European Union', has 'Information society, privacy and data protection' among one of its 10 fundamental themes [FRA website]. The European Data Protection Supervisor, which is the EU independent data protection authority, has the responsibility of advising the legislator on proposals for legislation that may affect privacy, and monitoring new technology that may affect the protection of personal information [EDPS website].

The Lisbon treaty, which entered into force in 2009, represented a major step in the development of a more effective methodology for EU legislation on data protection. Prior to this, data protection for private and commercial reasons was a 'first pillar' policy, handled by the European Community, while data protection for law enforcement was a 'third pillar' policy, handled by intergovernmental cooperation. After 2009, the European Parliament became a co-legislator in all data protection matters, on an equal footing with the Council (Article 16 of the Treaty on the Functioning of the European Union, TFEU), and it has not hesitated to make use of its enlarged powers [Europarl website].

The most recent piece of EU legislation is the Data Protection Reform initiated by the Commission in 2012 and culminating in May 2016 with the publication of Regulation 2016/679 [Reg 679, 2016] and Directive 2016/680 [Dir 680, 2016]. The main aims of the reform are safeguarding personal data across the EU, increasing users' control of their data and cutting costs for businesses. In advancing this legislation, the EC stressed its economic impact, affirming that the new rules will 'incentivise businesses to innovate and develop new ideas, methods, and technologies' and 'provide businesses with opportunities to remove the lack of trust that can affect people's engagement with innovative uses of personal data' [EC press 2015]. As a privacy-preserving technology, encryption will play a key role for the compliance with the legal framework established by the European data protection law, and is explicitly mentioned in the Regulation.

The General Data Protection Regulation (GDPR) does not cover communications which do not include personal data. The EC is therefore proposing to modernise the e-Privacy Directive 2002/58/EC with a Regulation on Privacy and Electronic Communications, which will complement the GDPR with the aim of reinforcing trust and security in the Digital Single Market by ensuring that all electronic communications will remain confidential [EC DSM 2017], [EC fact sheet 2017]. In particular, listening to, tapping, intercepting, scanning and storing text messages, emails or voice calls would not be allowed without the consent of the user. The proposed regulation also specifies when processing of communications data is exceptionally permitted and when it needs the consent of the user. Confidentiality of users' online behaviour and devices has also to be guaranteed, and consent will be required to access information on a user's device. The

e-Privacy Directive will therefore encourage the use of encryption technologies to protect users' communications.

The European digital technology industry has disclosed its 'Views on Encryption' in a position paper published in 2016 by DigitalEurope, a trade association [DigitalEurope encryption]. It highlights the importance of promoting data security and privacy both for economic growth and social enhancement, and underlines the role of encryption in ensuring the free flow of data in the digital single market. DigitalEurope also states that national governments should avoid technology mandates and backdoors, which will 'impede innovation, hurt the economy, and weaken data security and privacy'. This point of view is shared by ENISA, the European Union Agency for Network and Information. In its Opinion Paper on Encryption (2016) [Enisa encryption], one of the key messages is that 'law enforcement solutions need to be identified without the use of backdoors and key escrow', since 'limiting the use of cryptographic tools will create vulnerabilities that can in turn be used by terrorists and criminals, and lower trust in electronic services, which will eventually damage industry and civil society in the EU'. On the issue also the European Data Protection Supervisor gave his Opinion on the review of the e-Privacy Directive [EC e-privacy 2017], stating that 'the new rules should also clearly allow users to use end-to-end encryption (without 'back-doors') to protect their electronic communications. Decryption, reverse engineering or monitoring of communications protected by encryption should be prohibited' [EDPS 2016], a position which seems to clash with the desires of some Member States' governments [The Guardian Jun 2017].

One more point highlighted by the DigitalEurope position paper is the necessity of more cooperation between Member States, which 'must overcome conflicts in national legislation'. Indeed, Member States retain the authority to restrict domestic use of cryptographic technologies on the grounds of security concerns. According to a 2010 survey [Cryptolaw website], the policies of EU countries with regards to domestic use of cryptography range from 'no domestic controls' (e.g. Germany) to 'law demanding decryption' (U.K.) to 'small and special controls' (Italy) to 'decryption and special controls' (France) to 'not clear' (Spain). After a period in which restrictions on the use of cryptography were somewhat eased, recent terrorist events seem to be reversing the trend, and several EU governments are contemplating the introduction of measures that prevent strong end-to-end encryption (see e.g. the UK Investigatory Powers Act 2016, and a joint statement from the French and German interior ministers, Paris, 23 August 2016). According to information published by Euractiv in November 2016, Croatia, Italy, Latvia, Hungary and Poland want the European Commission to propose legislation that would make it easier for police to crack encryption technology [Euractiv 2016].

It is therefore apparent that while the wide use of strong encryption technologies is primarily seen by the EC and by the business community as an instrument to ensure the free flow of data in the digital single market and therefore an enabler of economic growth, law enforcement agencies tend to see encryption as a potential threat to their investigative capabilities, which are being outpaced by the speed of change and fundamental shifts in communications services and technologies. The position of national governments is ambivalent, and has been influenced by recent events such as terrorist attacks. As they progressively lose the technical ability to intercept and access communications, LEAs are said to be 'going dark' [FBI goingdark]. An example of the current debate on the role of encryption to the 'going dark' problem has been prepared by the USA Congressional Research Service [Finklea 2016]. As can be deduced also by the joint ENISA-Europol statement on lawful criminal investigation [Europol Enisa 2016], law enforcement agencies are progressively making use of device-hacking techniques to bypass strong encryption.

Among the latest initiatives by the European Council to address the challenges posed by strong encryption to LEAs, we recall a questionnaire that has been distributed among the Member States 'to map the situation and identify the obstacles faced by law enforcement authorities when gathering or securing encrypted e-evidence for the purposes of criminal proceedings' [Council of EU 12368/16], [Rejo Zenger 2016]. A summary of the

responses from some of the LEAs [Council of EU 13434/16], [Monroy 2016] served as a basis for discussion at the kick-off meeting for the European Judicial Cybercrime Network, held in November 2016 [Eurojust 2016]: the top three challenges reportedly are the lack of sufficient technical capacity (in terms of efficient technical solutions and equipment), followed by the lack of sufficient financial resources and personnel capacity. In the draft Conclusions of the European Council of June 2017, a call on industry to address 'the challenges posed by systems that allow terrorists to communicate in ways that competent authorities cannot access, including end-to-end encryption' has been included [Council of EU 8799/17]. In this respect, the EC expressed its position in a 'Communication to the European Parliament, the European Council and the Council' (published on October 18, 2017) where it reports the progress towards an 'effective and genuine Security Union' [EC Security 2017]. In setting out a package of anti-terrorism measures, the Commission recommends some steps 'to support law enforcement and judicial authorities when they encounter the use of encryption in criminal investigation'. The six measures are intended to 'support Member States authorities without prohibiting, limiting, or weakening encryption'. In particular, the Commission states that 'Member States should have a toolbox of alternative investigation techniques at their disposal to facilitate the development and use of measures to obtain needed information encrypted by criminals'. A network of point of expertise should be established, which 'should contribute to developing the toolbox', and 'the European Cybercrime Centre at Europol is best placed to set up and keep a repository of those techniques and tools'. It is clearly stated that 'measures that could weaken encryption or could have an impact on a larger or indiscriminate number of people would not be considered'. The initiative of the Commission is advertised and briefly explained also in a DG Migration and Home Affairs webpage [DG HOME encryption].

The increase in encryption strength guaranteed by quantum technologies will likely reinforce the already unfolding trend by LEAs in the direction of device hacking: in other terms, LEAs will focus on compromising suspects' devices instead of communication lines, developing so called 'state Trojans' [Paganini Feb 2016], [Paganini Aug 2016], [Monroy website]. The approach of recurring to 'alternative technology' or 'offensive technology' carries however some risks, as evidenced e.g. by the study for the European Parliament LIBE (civil liberties, justice and home affairs) Committee 'Legal frameworks for hacking by Law Enforcement: identification, evaluation, and comparison of practices' [EP LIBE 2017]. The EP study points out that 'the existing legal provisions do not provide for the invasive nature of hacking techniques and do not guarantee the required levels of legislative precision and clarity', so that LEAs move in a kind of legal 'grey area'; sometimes, for want of technical capabilities, they may even outsource the task of developing malware to external contractors. A market has developed for so-called 'zero-day exploits', which are undisclosed computer-software vulnerabilities that hackers can exploit to adversely affect computer programmes. Since they are not publicly reported before being exploited, these vulnerabilities leave the software's authors no time (hence 'zero-day') to create patches. The use of malware by LEAs implies that authorities do not share within the IT community their knowledge of weaknesses in widely diffused commercial software, an attitude that increases risks of criminal cyber-attacks to private citizens, commercial firms, and public infrastructures. Indeed, rumours have that some of the malware used in recent cyber-attacks has been built by using exploits stolen from the USA NSA [NY Times, May 2017].

5. Conclusion

In this final section, we summarise a set of policy recommendations that result from the analysis carried out in this report. In it, we synthesised results published in research papers and ideas put forward by academy and industry in scientific conferences, policy publications, and other discussion fora. The following recommendations represent therefore the outcome of a broad interaction with a wide community of experts, including some from outside the quantum communications domain.

It is a shared view that, at this stage of technological development, the main policy issue regarding quantum communications is how to foster the transition to the market of applications enabled by research advances in the field of communication privacy and data security. However, experts in the field point out that a large-scale commercial uptake will not happen until standards for secure communications protocols involving quantum effects, such as quantum key distribution, are endorsed by governments. On the other hand, public authorities will hesitate until the threat of quantum computers is perceived to be real enough to force a global rethink of their policies regarding communication security, data privacy, and infrastructure protection. Lacking this driver, real-world cryptographic applications of quantum communications are bound to remain in a kind of 'wait state', and no significant market will develop.

The timeframe necessary for the crypto-analytical potential of a quantum computer to materialise is extremely uncertain: in addition to the intrinsic difficulties of developing the technology, there is the fact that for this particular application the available scientific publications are of a rather theoretical character, due to the understandable dearth of disclosed players. It is however doubtless that, once built, a quantum computer will be used also against privacy and communications security: and since it will allow 'intercept now, decrypt later' attacks on data whose secrecy must be ensured for long timespans, policymakers are being forced to act well in advance. Cryptographic primitives based on quantum communications are quantum-resistant, but the weight of the role they are likely to play in the future communication security landscape is still uncertain. Regulators should therefore acknowledge that quantum computing will disrupt some fundamental cryptographic techniques now widely in use, but they should remain technology-neutral.

The EC should consider including quantum-safe requirements in policies regarding communication privacy, long-term data security and infrastructure protection.

Industry and application-oriented researchers have repeatedly called for the EU to take direct measures aimed at stimulating markets and generating market pull, both for quantum communications technologies and for the services that these can support. Available commercial devices already allow assembling QKD systems that fit into existing telecom exchanges and data centres: however, compatibility issues, performance limitations, cost, low adoption of standards and security models, and lack of a scheme for certifying compliance remain major obstacles. In all these areas progress is being made at a steady pace, and will undoubtedly accelerate if a significant market interest does materialise. Policy decisions can help to address shortcomings, increase technological readiness, and enlarge the market by funding pilot schemes, encouraging cross-disciplinary collaborations, and identifying early-use public sector applications. In particular, sound business cases must be elaborated: lacking that, any publicly funded deployment of quantum communications, even if very successful from the technical point of view, will not translate into commercial services.

The European Commission (EC) should promote further work on quantum cryptography standards, encourage user-engagement and early adoption, and stimulate the study of business-cases.

It is a widely recognised issue that cryptographic applications of quantum communications are still the domain of a relatively small group of researchers, and that their market uptake will require extensive testing in real-world settings to secure the acceptance of a much broader community of communications security experts. To contribute to breaking the silo mentality and encourage collaboration between researchers with different backgrounds, academic groups should therefore be funded to have access to existing networks and test their solutions together with other industry players.

The EC should consider fostering the development of a shared and accessible fibre infrastructure to test quantum-based security solutions jointly with conventional and post-quantum cryptography in a realistic environment.

The European quantum technology research community agrees in pointing out how the Chinese success story in space-based quantum communications constitutes a missed opportunity for Europe, which has an outstanding scientific competence and a strong industrial basis. It must be recognised that the inertia demonstrated until recently in this field seems to be receding, and encouragingly ESA has included space-based QKD in its programmes. Industry commitment will strongly depend on public support policies in this area, which should be seen as a strategic long-term challenge for the EU.

The European Commission should reinforce its collaborations with ESA to verify the possibility of integrating quantum communications in the existing programmes, such as Galileo.

Given the size and significance of the efforts made by China in quantum communications, and its scientific and technological successes, it is beyond any doubt that China is going to be a very important market player. However, while Chinese firms are welcome in Europe, entering the Chinese market is challenging for foreign firms, since ubiquitous (non-trade) barriers to free trade are in place. European businesses therefore highlight the necessity of redressing the commercial imbalances in the relationship between the EU and China.

Policies aimed at achieving more symmetry and reciprocity with China should be designed and enforced to ensure proper applications of trade agreements. Specific instruments to support SMEs in the Chinese market should be developed.

Lastly, we remark that quantum communications can be an important instrument for the implementation of the EU policies aimed at strong encryption. Cryptography is indeed seen as a significant driver of economic growth as well as a fundamental security pillar; however, it may also represent a challenge for law enforcement agencies. The technological developments in quantum cryptography further motivate the already ongoing initiatives aimed at developing novel interception techniques based e.g. on device hacking. Information gathering by law enforcement agencies making use of such intrusive instruments must however be motivated by compelling investigative necessities and remain under strict legislative safeguards.

The EC should remain aware that the deployment of new lawful interception techniques, effective against strong cryptography, must be constantly balanced against privacy rights and potential cybersecurity risks.

In agreement with the above recommendations, we suggest a set of actions to be undertaken by EU policymaking bodies. In the short-to-medium term the focus will be on policies aimed at technological development and market uptake. With time, technology push programmes will be accompanied by an effort to eliminate commercial and legal hindrances, and to establish a suitable regulatory framework.

Fundamental and applied research for devices and systems	Research funding (EC DG CNECT)
	Research survey and exploratory projects (EC DG JRC)
	Industrialisation and manufacturability (DG GROW)
	Standardisation (EC DG JRC, DG GROW)
	Incentivise SME (DG RESEARCH COSME, European Institute of Technology)
Technology transfer and market uptake	Demonstrators funding (EC DG CNECT)
	Technology demonstrators for user engagement (EC DG JRC)
	Embed quantum cryptography in the Industry for Security agenda (EC DG HOME)
Definition of a EU-wide project	Space-based quantum communications (e.g. ESA)
	Euro-wide fibre quantum network for academies and research (GEANT)
	Euro-wide fibre quantum network for e-Government (EU-LISA)
Elaboration of use-cases	Data-centres back-up (EC DG DIGIT)
	Communications with databases (EU-LISA)
	Securing public-regulated service signals (European GNSS Agency)
	Civil infrastructure protection (ENISA)
	Military uses (EDA)
Small-scale pilots	Energy grid and telecom infrastructure security (EC DG JRC)
	E-government (EU-LISA)
	Common defence area (EDA)
Address hindrances to free commerce	Remove obstacles within single market (EC DG HOME)
	Export of dual-use technologies (EC DG TRADE, EP INTA Committee)
	Free-trade agreements (EC DG TRADE)
Monitor broader policy implications	Law enforcement (Europol, Council of the EU)
	Fundamental rights (EC DG JUST, Fundamental Right Agency)
	European Parliament (in particular STOA, EPRS, LIBE Committee)
	Legislation for data protection (EDPS, EC DG JUST)

References

[JRC QuantumTech 2016]
Lewis, A. M. et al. (2016), 'Quantum Technologies: Implications for European Policy', *JRC Science for Policy Report*,
https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/quantum-technologies-implications-european-policy-issues-debate

[JRC QuantumTime 2017]
Lewis, A. M. (2017), 'The impact of quantum technologies on the EU's future policies. Part 1: Quantum Time', *JRC Science for Policy Report*,
https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/impact-quantum-technologies-eus-future-policies-part-1-quantum-time

[The Economist 2017]
Technology Quarterly 'Here, there and everywhere: Quantum technology is beginning to come into its own', 11 March 2017,
http://www.economist.com/news/essays/21717782-quantum-technology-beginning-come-its-own

[Gisin 2002]
Gisin, N. et al. (2002), 'Quantum cryptography', *Rev. Mod. Phys.* 74, 145,
https://arxiv.org/abs/quant-ph/0101098

[Diamanti 2016]
Diamanti, E., Lo, H.-K., Qi, B. and Yuan, Z. (2016), 'Practical challenges in quantum key distribution', *NPJ Quantum Information* 2, 16025,
https://www.nature.com/articles/npjqi201625

[Dusek 2006]
Dusek, M., Lutkenhaus, N. and Hendrych, M. (2006), 'Quantum Cryptography', *Progress in Optics*, Vol. 49, pp. 381-454, Edt. E. Wolf, Elsevier,
https://arxiv.org/abs/quant-ph/0601207

[Alléaume 2014]
Alléaume, R. et al. (2014), 'Using quantum key distribution for cryptographic purposes: a survey', *Theoretical Computer Science*, Vol. 560, Part 1, pp. 62-81,
https://arxiv.org/abs/quant-ph/0701168

[Wegman 1981]
Wegman, M. N. and Carter J. L. (1981), 'New hash functions and their use in authentication and set equality', *J. Computer and System Sciences*, Vol. 22, 3, pp. 265-279,
http://www.sciencedirect.com/science/article/pii/0022000081900337

[NIST FIPS 197]
Federal Information Processing Standards Publication 197 (2001), 'Specification for the Advanced Encryption Standard (AES)', 26 November,
http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

[IDQ QRNG]
http://www.idquantique.com/random-number-generation

[Quintessence QRNG]
https://www.quintessencelabs.com/products/qstream-true-random-number-generator

[Wiesner 1983]
Wiesner, S. (1983), 'Conjugate Coding', *SIGACT News*, 15(1), pp. 78-88,
http://dl.acm.org/citation.cfm?id=1008920

[Amiri 2016]
Amiri, R., Wallden, P., Kent, A. and Andersson, E. (2016), 'Secure quantum signatures using insecure quantum channels', *Phys. Rev.* A 93, 032325,
http://journals.aps.org/pra/abstract/10.1103/PhysRevA.93.032325

[Broadbent 2016]
Broadbent, A. and Schaffner, C. (2016), 'Quantum Cryptography Beyond Quantum Key Distribution', Designs, Codes and Cryptography, Vol. 78, Issue 1, pp. 351-382,
http://arxiv.org/abs/1510.06120

[Schaffner homepage]
Personal homepage of Christian Schaffner, Centrum Wiskunde & Informatica, and QuSoft
http://homepages.cwi.nl/~schaffne/positionbasedqcrypto.php

[ERCIM news]
The European Research Consortium for Informatics and Mathematics
https://ercim-news.ercim.eu/en85/special/position-based-quantum-cryptography

[Lunghi 2013]
Lunghi, T. et al. (2013), 'Experimental bit commitment based on quantum communication and special relativity', *Phys. Rev. Lett.*, 111:180504
https://arxiv.org/abs/1306.4801

[Liu 2014]
Liu, Y. et al. (2014), 'Experimental unconditionally secure bit commitment', *Phys. Rev. Lett.*, 112:010504,
https://arxiv.org/abs/1306.4413

[Pappa 2014]
Pappa, A. et al. (2014), 'Experimental plug and play quantum coin flipping', *Nature Communications* 5, 3717,
http://www.nature.com/articles/ncomms4717

[Erven 2014]
Erven, C. et al. (2014), 'An experimental implementation of oblivious transfer in the noisy storage model', *Nature Communications* 5, Article number: 3418,
https://www.nature.com/articles/ncomms4418

[Qui 2010]
Qi, B. et al. (2010), 'A brief introduction of quantum cryptography for engineers',
https://arxiv.org/abs/1002.1237

[Gottesman 2008]
Gottesman, D. and Lo (2008), H.-K., 'Proof of security of quantum key distribution with two-way classical communications',
https://arxiv.org/pdf/quant-ph/0105121.pdf

[Grosshans 2003]
Grosshans, F. et al. (2003), 'Quantum key distribution using gaussian-modulated coherent states', *Nature*, Vol. 421,
https://www.researchgate.net/publication/251808860_Quantum_key_distribution_using_Gaussian-modulated_coherent_states

[Diamanti 2015]
Diamanti, E. and Leverrier, A. (2015), 'Distributing Secret Keys with Quantum Continuous Variables: Principle, Security and Implementations',
https://arxiv.org/abs/1506.02888

[Jouguet 2013]
Jouguet, P. et al. (2013), 'Experimental demonstration of long-distance continuous-variable quantum key distribution', *Nature Photonics* 7, 378
https://arxiv.org/abs/1210.6216

[Kumar 2015]
Kumar, R., Qin, H. and Alléaume, R. (2015), 'Coexistence of continuous variable QKD with intense DWDM classical channels', *New Journal of Physics*, 17(4), 043027
http://iopscience.iop.org/article/10.1088/1367-2630/17/4/043027/pdf

[Hensen 2015]
Hensen, B. et al. (2015), 'Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres', *Nature* 526, pp. 682-686
https://arxiv.org/abs/1508.05949

[ETSI 2017]
ETSI White Paper (2017), 'Implementation Security of Quantum Cryptography: Introduction, solutions, challenges'
Draft in preparation

[Hirota 2012]
Hirota, O. (2012), 'Incompleteness and Limit of Quantum Key Distribution Theory'
https://arxiv.org/abs/1208.2106

[Yuen 2016]
Yuen, H. (2016), 'Security of Quantum Key Distribution',
https://arxiv.org/abs/1602.07602

[Bernstein paper 2016]
Bernstein, D. J. (2016), 'Is the security of quantum cryptography guaranteed by the laws of physics?'
https://sidechannels.cr.yp.to/qkd/holographic-20160326.pdf

[Makarov website]
Quantum Hacking Lab website, University of Waterloo
http://www.vad1.com/lab

[Scarani 2012]
Scarani, V. and Kurtsiefer, C. (2014), 'The black paper of quantum cryptography: real implementation problems', *Theoretical Computer Science* 560, 27-32,
https://arxiv.org/abs/0906.4547

[Langer 2013]
Langer, T. (2013), 'The practical application of QKD', Ph.D. Thesis, Lausanne.

[McLaughlin 2016]
McLaughlin, K., 'Science is a major plank in China's new spending plan', *Science*, 7 March 2016,
http://www.sciencemag.org/news/2016/03/science-major-plank-china-s-new-spending-plan?utm_campaign=email-news-latest&et_rid=17669279&et_cid=324673

[Qiu 2014]
Qiu, J., 'Quantum communications leap out of the lab', *Nature*, 23 April 2014,
https://www.nature.com/news/quantum-communications-leap-out-of-the-lab-1.15093

[Chen Nov 2014]
Chen, S., 'China to launch hack-proof quantum communication network in 2016', *South China Morning Post*, 4 November, 2014,
http://www.scmp.com/news/china/article/1631479/china-launch-hack-proof-quantum-communication-network-2016

[Xiang 2015]
Xiang, H. and Han, Z.-F., 'The Chinese QKD networks', presentation given at the 3rd ETSI Quantum Safe Cryptography Workshop, Seoul, Korea, 5-7 October 2015
https://docbox.etsi.org/Workshop/2015/201510_IQCWORKSHOP/UofChongqing_HongXiang.pdf

[Lixin 2016]
Lixin, Z., 'Scientists lead China's quantum ambitions', *China Daily USA*, 2016-08-26
http://usa.chinadaily.com.cn/epaper/2016-08/26/content_26628045.htm

[Qiang Zhang 2016]
'Recent Progress of Quantum Communication in China', talk given by Qiang Zhang of the University of Science and Technology of China, Brussels SPIE conference, April 2016
http://spie.org/Publications/Proceedings/Paper/10.1117/12.2228229

[Wang 2014]
Wang, S. et al. (2014), 'Field and long-term demonstration of a wide area quantum key distribution network', *Optics Express* Vol. 22, Issue 18, pp. 21739-21756,
https://www.osapublishing.org/oe/abstract.cfm?uri=oe-22-18-21739

[Courtland 2016]
Courtland, R. (2016), 'China's 2 000-km Quantum Link Is Almost Complete', IEEE Spectrum, 26 October 2016,
http://spectrum.ieee.org/telecom/security/chinas-2000km-quantum-link-is-almost-complete

[IDQ QCTEC 2017]
Huang, W. (2017), 'QKD in Fiber-Based Optical Networks in China', ETSI/IQC Quantum Safe Workshop,
https://docbox.etsi.org/Workshop/2017/201709_ETSI_IQC_QUANTUMSAFE/TECHNICAL_TRACK/S01_WORLD_TOUR/IDQQTEC_HUANG.pdf

[Gibney 2016]
Gibney, E. (2016), 'Chinese satellite is one giant step for the quantum internet', *Nature*, 16 August 2016,
https://www.nature.com/news/chinese-satellite-is-one-giant-step-for-the-quantum-internet-1.20329

[Yin 2017]
Yin, J. et al. (2017), 'Satellite-based entanglement distribution over 1 200 kilometers', *Science* 356, 6343, 1140-1144,
http://science.sciencemag.org/content/356/6343/1140

[China satellite 2017]
Popkin, G. (2017), 'China's quantum satellite achieves 'spooky action' at record distance', *Science*, 15 June 2017,
http://www.sciencemag.org/news/2017/06/china-s-quantum-satellite-achieves-spooky-action-record-distance

[The Economist China 2017]
'Quantum Cryptography in space: The early bird', *The Economist*, 2 September 2017,
https://www.economist.com/news/science-and-technology/21727889-quantum-cryptographys-early-birds-first-quantum-cryptographic-satellite

[CAS Sept. 2017]
China Opens 2 000-km Quantum Communication Line, 30 September 2017,
http://english.cas.cn/newsroom/news/201709/t20170930_183642.shtml

[South China MP 2017]
http://www.scmp.com/news/china/society/article/2110563/china-building-worlds-biggest-quantum-research-facility

[Sasaki 2011]
Sasaki, M. et al. (2011), 'Field test of quantum key distribution in the Tokyo QKD Network', *Optics Express* Vol. 19, Issue 11, pp. 10387-10409
https://www.osapublishing.org/oe/abstract.cfm?uri=oe-19-11-10387&origin=search

[UQCC Project website]
'Updating quantum cryptography and communications', project UQCC, Tokyo QKD,
http://www.uqcc.org/QKDnetwork/

[UQCC 2015]
UQCC 2015 Conference presentation materials,
http://2015.uqcc.org/materials/index.html

[Toyoshima 2015]
Toyoshima, M. (2015), 'Satellite-Ground Optical Communications', UQCC2015,
http://2015.uqcc.org/materials/pdf/Part-III_Toyoshima_b.pdf

[South Korea Law 2016]
Yongjoo, K. (2016), 'South Korean Government to Propose Special Law for Quantum Industry', *ETNews*, 13 December 2016,
http://english.etnews.com/20161213200002

[Kim 2016]
Kim, T. and Kwak, S. (2016), 'Development of Quantum Technologies at SK Telecom', *AAPPS Bulletin*, December 2016, Vol. 26, No 6,
http://aappsbulletin.org/myboard/read.php?Board=featurearticles&id=181

[Walenta 2016]
Walenta, N. and Oesterling, L. (2016), 'Quantum Networks: Photons Hold Key to Data Security', *Photonics Spectra*, May 2016,
https://www.photonics.com/Article.aspx?AID=60541

[Williams 2017]
Williams, M., 'SK Telecom pushes for interoperable quantum crypto systems', *PC World*, 27 February 2017,
http://www.pcworld.com/article/3174825/encryption/sk-telecom-pushes-for-interoperable-quantum-crypto-systems.html

[Mimos Berhad website]
http://www.mimos.my

[Mohamed Ridza Wahiddin 2017]
http://myquantum.cybersecurity.my/speakers.html

[myquantum website]
http://myquantum.cybersecurity.my/index.html

[CQT 2016]
'Bringing quantum tech to new NUS-Singtel corporate lab', 24 October 2016
https://www.quantumlah.org/about/highlight.php?id=25

[The SpooQy Lab website]
https://sites.google.com/site/phylej

[CQY 2014]
https://www.quantumlah.org/about/highlight.php?id=148

[Aust. Nat. Univ. website]
http://photonics.anu.edu.au/qoptics/Research/securequantumcom.html

[cqc2t website]
http://www.cqc2t.org/research/secure_quantum_communications

[ANU space]
http://www.anu.edu.au/news/all-news/boost-for-anu-space-and-quantum-technology

[Extance 2017]
Extance, A. (2017), 'A quantum of security', *Fibre-Systems*, 3 February 2017,
http://www.fibre-systems.com/feature/quantum-security

[University KwaZulu-Natal website]
http://quantum.ukzn.ac.za/research/quantumcity

[RQC website]
'About Us', Russian Quantum Center website
http://www.rqc.ru/about

[kurochkin 2016]
http://ctcrypt.ru/files/files/2016/03%20kurochkin.pdf

[t8 press 2016]
http://t8.ru/?p=7762&lang=en

[pwc press 2017]
'PwC and the Russian Quantum Center have joined forces to develop quantum information security systems', PwC Russia press release, 2 June 2017,
https://www.pwc.ru/en/press-releases/2017/pwc-quantum-center.html

[The Hindu 2016]
http://www.thehindu.com/business/Economy/Russia-offers-technology-to-keep-hackers-at-bay/article16942015.ece

[Quantum blockchain]
Kiktenko, E. O. et al., 'Quantum-secured blockchain', May 2017,
https://arxiv.org/abs/1705.09258

[White House 2016]
Joint Report by the Committee on Science and the Committee on Homeland and National Security, National Science and Technology Council,
https://www.whitehouse.gov/sites/whitehouse.gov/files/images/Quantum_Info_Sci_Report_2016_07_22%20final.pdf

[NQI USA 2017]
'Call for a National Quantum Initiative', National Photonics Initiative, 22 June 2017,
http://www.lightourfuture.org/getattachment/7ad9e04f-4d21-4d98-bd28-e1239977e262/NPI-Recommendations-to-HSC-for-National-Quantum-Initiative-062217.pdf?utm_source=public-policy&utm_medium=email&utm_campaign=public-policy

[US Congress 2017]
US Congress Committee on Science, Space, and Technology, 'American Leadership in Quantum Technology', hearing held on 24 October 2017,
https://science.house.gov/legislation/hearings/american-leadership-quantum-technology

[Costello 2017]
US–China Economic and Security Review Commission
Hearing on China's Pursuit of Next Frontier Technologies, 16 March 2017,
https://www.uscc.gov/Hearings/hearing-china%E2%80%99s-pursuit-next-frontier-tech-computing-robotics-and-biotechnology-video

[Costello 2017 testimony]
Testimony by John Costello (2017), 'Chinese Efforts in Quantum Information Science: Drivers, Milestones, and Strategic Implications',
https://www.uscc.gov/sites/default/files/John%20Costello_Written%20Testimony_Final2.pdf

[Elliott 2005]
Elliott. C. et al. (2005), 'Current status of the DARPA Quantum Network'
https://arxiv.org/ftp/quant-ph/papers/0503/0503058.pdf

[Hayford 2014]
Hayford, D. (2014), 'Quantum-based Product Development at Battelle', Qcrypt 2014,
http://2014.qcrypt.net/wp-content/uploads/Hayford.pdf

[NIST ITL website]
https://www.nist.gov/itl/earlyphases

[NTIA press 2013]
NIST and NTIA Announce Plans to Establish New Center for Advanced Communications, NTIA press release, 14 June 2013,
https://www.ntia.doc.gov/press-release/2013/nist-and-ntia-announce-plans-establish-new-center-advanced-communications

[Hughes 2013]
Hughes, R. J. et. Al (2013), 'Network-Centric Quantum Communications with Application to Critical Infrastructure Protection',
https://arxiv.org/abs/1305.0305

[NASA Quantum 2012]
https://quantum.nasa.gov

[Williams 2012]
Williams, C. P. (2012), 'NASA Quantum Network',
https://quantum.nasa.gov/materials/2012-01-21-A4-Williams.pdf

[Nasa 2016]
https://www.nasaspaceflight.com/2016/08/long-march-2d-quantum-communications-satellite

[NRC quantum 2017]
National Research Council Canada (2017), 'Quantum Canada Survey overview',
http://www.nrc-cnrc.gc.ca/eng/solutions/collaborative/quantum/qc_survey.html

[The Guardian 2016]
https://www.theguardian.com/science/life-and-physics/2016/apr/16/justin-trudeau-and-quantum-computers

[PI press 2016]
'Quantum Technologies a National Priority for Canada',
https://www.perimeterinstitute.ca/news/quantum-technologies-national-priority-canada

[Gov Canada 2017]
'Ministers Bains and Garneau celebrate USD 80.9 million for the Canadian Space Agency'
https://www.canada.ca/en/innovation-science-economic-development/news/2017/04/ministers_bains_andgarneaucelebrate809millionforthecanadianspace.html

[Quantum Manifesto]
http://qurope.eu/system/files/u7/93056_Quantum%20Manifesto_WEB.pdf

[Quantum Europe]
https://ec.europa.eu/digital-single-market/en/news/quantum-europe-2017-towards-quantum-technology-flagship

[UK quantum 2015]
White paper by the Quantum Technologies Strategic Advisory Board 'National strategy for quantum technologies' (2015),
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414788/Strategy_QuantumTechnology_T15-080_final.pdf

[UK QuantumComm Hub]
https://www.quantumcommshub.net

[Thompson 2015]
Thompson, M. (2015), 'National Network of Quantum Technologies Hubs: Quantum Communications Hub',
https://www.epsrc.ac.uk/files/newsevents/events1/quantum-technologies-information-day-presentations/national-network-of-quantum-technologies-hubs-quantum-communications-hub

[Qutech website]
https://qutech.nl

[Qutech comm]
https://qutech.nl/roadmap/quantum-internet

[CWI news 2017]
'Quantum software consortium receives EUR 8.8 million in the gravitation programme', CWI press release, 8 May 2017
https://www.cwi.nl/news/2017/quantum-software-consortium-receives-18-8-million-euro-in-the-gravitation-programme

[VUB cryptasc website]
http://cryptasc.vub.ac.be/doku.php?id=start

[QUbiz website]
http://qubiz.dk

[KCIK website]
http://www.kcik.ug.edu.pl/kcik.php

[NLQT website]
http://www.nlqt.wppt.pwr.edu.pl

[Seqre website]
http://seqre.net/seqre2014/wroclaw.php

[Swissquantum paper]
https://arxiv.org/abs/1203.4940

[NCCR qsit]
Quantum science in Switzerland website
http://www.nccr-qsit.ethz.ch

[Huttner 2017]
Huttner, B. (2017), 'The QuSat project: Towards commercial key distribution from space',
https://artes.esa.int/sites/default/files/29%20-%20Huttner%20ID%20Quantique.pdf

[Academy Finland 2017]
http://www.aka.fi/en/about-us/media/press-releases/2017/academy-of-finland-selects-12-new-centres-of-excellence

[Aalto QC 2017]
http://www.opli.net/opli_magazine/eo/2017/construction-of-a-quantum-computer-begins-at-aalto-university-oct-news

[Finnish defence]
Tittonen, I. et al. (2016), 'Applications of the Quantum Key Distribution method', MATINE/Puolustusministeriö Summary Report, 2016/2500M-0054,
https://www.defmin.fi/files/3665/0054_MATINE_Summary_Report_(2).pdf

[Chalmers 2017]
http://www.chalmers.se/en/news/Pages/Engineering-of-a-Swedish-quantum-computer-set-to-start.aspx

[Wallenberg CQT 2017]
http://www.mynewsdesk.com/uk/chalmers/documents/wallenberg-centre-for-quantum-technology-72717

[Leopoldina 2015]
https://www.leopoldina.org/en/publications/detailview/publication/perspektiven-der-quantentechnologien-2015

[QUtega website]
http://www.qutega.de/en/home

[IQST website]
http://www.iqst.org/research/focus-areas/quantum-electrical-and-optical-engineering.html

[Sirteq website]
http://www.sirteq.org

[Grenoble quantum website]
https://quantum.univ-grenoble-alpes.fr

[Calonico 2016]
Calonico, C. (2016), 'A fibre backbone in Italy for Precise Time and Quantum Key Distribution', 4th ETSI/IQC Workshop on Quantum-Safe Cryptography, September 2016, Toronto
https://docbox.etsi.org/Workshop/2016/201609_QUANTUMSAFECRYPTO/TECHNICAL_TRACK/INRIM_Calonico.pdf

[Bovino 2005]
Bovino, F. et al. (2011), 'Practical Quantum Cryptography: The Q-KeyMaker™',
https://arxiv.org/ftp/arxiv/papers/1104/1104.2475.pdf

[Ministero Difesa 2016]
http://www.difesa.it/SMD_/Eventi/Pagine/chiude-festival-scienza-2016.aspx

[Bovino 2016]
Bovino, F. et al. (2016), 'Increasing operational command and control security by the implementation of device independent QKD', SPIE Conference,
http://proceedings.spiedigitallibrary.org/proceeding.aspx?articleid=2575941

[Vallone 2015]
Vallone, G. et al. (2015), 'Experimental Satellite Quantum Communications', *Phys. Rev. Lett.* 115, 040502,
https://physics.aps.org/featured-article-pdf/10.1103/PhysRevLett.115.040502

[ICFO website]
https://www.icfo.eu

[Quitemad website]
https://quitemadorg.wordpress.com

[QKD Madrid website]
http://www.gcc.fi.upm.es

[RICE 2017]
White paper 'The Quantum Technologies community in Spain', by RICE — Quantum Information Network in Spain,
http://rice.hbar.es/research/articles/quantum-technologies-funding-groups-spain

[Knight 2004]
Knight, W. (2004), 'Entangled photons secure money transfer', *New Scientist*, 22 April 2004,
https://www.newscientist.com/article/dn4914-entangled-photons-secure-money-transfer

[Secoqc website]
http://www.secoqc.net

[AIT website]
https://www.ait.ac.at/en/research-fields/physical-layer-security/optical-quantum-technologies/products-and-instrumentation/quantum-key-distribution-systems-and-combination-with-other-systems/

[QKD telco]
http://www.qkd-telco.at

[Iqoqi website]
Satellite-based quantum communications, IQOQI website,
http://www.iqoqi-vienna.at/research/zeilinger-group/satellite-based-quantum-communication

[Wien university press 2013]
http://medienportal.univie.ac.at/presse/aktuelle-pressemeldungen/detailansicht/artikel/vienna-quantum-space-test-link-milestone-in-quantum-communication

[South China MP 2017]
http://www.scmp.com/news/china/society/article/2110563/china-building-worlds-biggest-quantum-research-facility

[Buchanan 2016]
Buchanan, W. and Woodward, A. (2016), 'Will quantum computers be the end of public key encryption?', *Journal of Cyber Security Technology*,
http://www.tandfonline.com/doi/pdf/10.1080/23742917.2016.1226650?needAccess=true

[ETSI 2015]
ETSI White Paper No 8, 'Quantum Safe Cryptography and Security: an introduction, benefits, enablers and challenges', June 2015,
http://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf

[NIST 2016]
NISTIR8105, 'Report on Post-Quantum Cryptography', April 2016,
http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf

[NIST PQC call]
Post-Quantum crypto Project, NIST website,
http://csrc.nist.gov/groups/ST/post-quantum-crypto

[EU pqcrypto]
Website of project PQCRYPTO, 'Post-quantum cryptography for long-term security',
http://pqcrypto.eu.org

[BernsteinLange 2017]
Bernstein, D. J. and Lange, T. (2017), 'Post-quantum cryptography', *Nature* 188, 549,
https://www.nature.com/nature/journal/v549/n7671/pdf/nature23461.pdf

[Nikolopoulos 2008]
Nikolopoulos, G. (2008), 'Applications of single-qubit rotations in quantum public-key cryptography', *Phys. Rev. A*, 77:032348,
https://arxiv.org/pdf/0801.2840.pdf

[Kawachi 2012]
Kawachi, A. et al. (2012), 'Computational Indistinguishability Between Quantum States and Its Cryptographic Application', *Journal of Cryptology*, Vol. 25, Issue 3, 528-555,
https://eprint.iacr.org/2006/148.pdf

[Vlachu 2016]
Vlachou, C., Rodrigues, J., Mateus, P., Paunković, N. and Souto, A. (2015), 'Quantum walks public key cryptographic system', *International Journal of Quantum Information*, Vol. 13, No 6, 1550050,
https://arxiv.org/abs/1602.01404

[Proos 2004]
Proos, J. and Zalka, C. (2003), 'Shor's discrete logarithm quantum algorithm for elliptic curves', QIC 3, No 4, pp. 317-344,
https://arxiv.org/abs/quant-ph/0301141

[Kirsch 2015]
Kirsch, Z., 'Quantum Computing: The Risk to Existing Encryption Methods',
http://www.cs.tufts.edu/comp/116/archive/fall2015/zkirsch.pdf

[IBM Q experience]
'Explore the world of quantum computing! Check out our User Guides and interactive Demos to learn more about quantum principles. Or, dive right in to create and run algorithms on real quantum computing hardware, using the Quantum Composer and QISKit software developer kit',
https://quantumexperience.ng.bluemix.net/qx/experience

[Weimer 2011]
Weimer, H. (2011), Blog post 'Moore's Law for Quantum Computers',
http://www.quantenblog.net/physics/moores-law-quantum-computer

[DWave website]
https://www.dwavesys.com/home

[Stebila 2009]
Stebila, D., Mosca, M. and Lutkenhaus, N. (2010), 'The Case for Quantum Key Distribution', Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Vol. 36, 283-296, Springer,
https://arxiv.org/abs/0902.2839

[NSA 2015]
Webpage on the Commercial National Security Algorithm Suite, from the Information Assurance Department of the National Security Administration
https://www.iad.gov/iad/programs/iad-initiatives/cnsa-suite.cfm
[copy and paste the address in your browser]

[EU-LISA 2016]
'Protecting Large-scale IT systems developed and/or managed by EU-LISA from modern threats: a review of recent developments in IT security and associated technologies',
http://www.eulisa.europa.eu/Publications/Reports/Protecting%20Large-scale%20IT%20systems%20developed%20and%20or%20managed%20by%20eu-LISA%20from%20modern%20threats.pdf

[CloudSecurityAlliance 2017]
White paper (2017), 'Applied Quantum-Safe Security: Quantum-Resistant Algorithms and Quantum Key Distribution',
https://downloads.cloudsecurityalliance.org/assets/research/quantum-safe-security/applied-quantum-safe-security.pdf

[IETF 2015]
IETF blog post, 'Internet Security vs Quantum Computing',
https://www.ietf.org/blog/2015/04/internet-security-vs-quantum-computing

[McGrew 2015]
McGrew, D., 'Living with postquantum cryptography', CISCO presentation at NIST,
http://csrc.nist.gov/groups/ST/post-quantum-2015/presentations/session4-mcgrew-david.pdf

[Entrust 2009]
Moses, T. (2009), 'Quantum Computing and Cryptography: their impact on cryptographic practice', Tim Moses, Advanced Security Technology Director, Entrust,
https://www.entrust.com/wp-content/uploads/2013/05/WP_QuantumCrypto_Jan09.pdf

[Senetas 2010]
'Commercial potential of quantum cryptography', by John Dubois (Senetas), in Quantum Cryptography and Computing — theory and Implementation, edited by Ryszard Horodecki et al., (2010); NATO advanced workshop, Gdansk, Poland, September 2009,
http://www.senetas.com/quantum-cryptography

[Keymile 2016]
Keymile press release, 'Cyber Security in Mission-Critical Networks', 18 February 2016,
https://www.keymile.com/en/idq-security-products-partnerschaft

[EC Futurium 2016]
Contributions by Tanja Lange and Daniel J. Bernstein to the FET Flagships consultation on the Quantum Manifesto for Quantum Technologies,
https://ec.europa.eu/futurium/en/content/quantum-manifesto-quantum-technologies-0

[Bernstein blog 2016]
The cr.yp.to blog of D. J. Bernstein (2016),
https://blog.cr.yp.to/20160516-quantum.html

[BSI 2016]
White paper, 'The State of IT Security in Germany 2016', by the German Federal Office for Information Security,
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2016.pdf?__blob=publicationFile&v=3

[NCSC 2016]
UK Government Communications Headquarters (2016), 'Quantum Key Distribution', White Paper by the CESG,
https://www.ncsc.gov.uk/information/quantum-key-distribution

[USAF 2015 abstract]
USAF Scientific Advisory Board (2016), 'Utility of Quantum Systems for the Air Force', 19 August 2016
http://www.scientificadvisoryboard.af.mil/Portals/73/documents/AFD-151214-041.pdf?ver=2016-08-19-101445-230

[USAF 2015 comment]
Mehta, A. (2015), 'Air Force Study Shows Potential, Limits of Quantum Tech', DefenseNews, 9 August 2015,
http://www.defensenews.com/story/defense/air-space/air-force/2015/08/09/air-force-study-shows-potential-limits-quantum-technology-pentagon/31233467

[Qutega 2017]
Website of QUTEGA — The German national initiative for quantum technologies,
http://www.qutega.de/en/home

[UK Gov Office for science 2016]
UK Government Office for Science (2016), 'The Quantum Age: technological opportunities',
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/564946/gs-16-18-quantum-technologies-report.pdf

[EPSRC 2014]
Details of EPSRC Grant 'Engineering Photonic Quantum Technologies', for Communications and Information Technologies,
http://gow.epsrc.ac.uk/NGBOViewGrant.aspx?GrantRef=EP/L024020/1

[USAF Boeing 2016]
USAF R & D for Advanced Space Superiority Technology and Engineering Requirements (RASTER) program, Contract for Quantum Key Distribution Research and Development,
https://govtribe.com/contract/award/fa945116d0001-fa945117f0004

[Cisco 2013]
Cisco's white paper 'Meeting Today's Data Security Requirements with Cisco Next-Generation Encryption' (2013),
http://www.cisco.com/c/dam/assets/docs/white_paper_c11-728371.pdf

[HP Colloquium 2012]
Bristol Cryptography Blog (2012), on the Hewlett-Packard Colloquium,
http://bristolcrypto.blogspot.it/2012/12/hewlett-packard-colloquium.html

[McGrew 2012]
McGrew (2012), 'The Vernam cipher is better than Quantum Key Distribution', talk given at the Royal Halloway Information Security Colloquium,
see also [HP Colloquium 2012]

[Schneier 2008]
Schneier, B. (2008), 'Quantum Cryptography: As Awesome As It Is Pointless', Wired, 16 October 2008
https://www.schneier.com/essays/archives/2008/10/quantum_cryptography.html

[Paterson 2009]
Paterson, K. G., Piper, F. and Schack, R. (2009), 'Quantum cryptography: a practical information security perspective',
https://arxiv.org/abs/quant-ph/0406147

[IETF QKD pointless]
Internet Engineering Task Force website, 'QKD is pointless',
https://www.ietf.org/mail-archive/web/cfrg/current/msg03825.html

[ETSI ISG QKD]
ETSI Industry Specification Group on Quantum Key Distribution website
https://portal.etsi.org/tb.aspx?tbid=723&SubTB=723

[ETSI 2010]
ETSI Group Specification on Quantum Key Distribution: 'ETSI GS QKD Group Specification: Quantum Key Distribution, Use Cases' (2010),
http://www.etsi.org/deliver/etsi_gs/qkd/001_099/002/01.01.01_60/gs_qkd002v010101p.pdf

[Alléaume Standards 2014]
Alléaume, R. et al., 'Worldwide Standardization Activity for Quantum Key Distribution', Globecom 2014 Workshop on Telecommunications Standards,
http://www.gcc.fi.upm.es/publications/GLOCOMW.2014.7063507.pdf

[Mo 2011]
Mo, X. F. et al. (2011), 'Time-cost analysis of a quantum key distribution system clocked at 100 MHz', *Optics Express*, Vol. 19, No 18, 17729,
https://arxiv.org/pdf/1105.3761.pdf

[Elser 2012]
Elser, D. et al. (2012), 'Network architectures for Space-Optical Quantum Cryptography Services' Proceedings of the International Conference on Space Optical Systems and Applications, ICSOS,
http://icsos2012.nict.go.jp/pdf/1569657077.pdf

[Lo 1999]
Lo, H.-K. (1999), 'Will quantum cryptography ever become a successful technology in the marketplace?',
https://arxiv.org/abs/quant-ph/9912011

[Natsheh 2015]
Al Natsheh, A. et al., 'Identifying the Challenges in Commercializing High Technology: A Case Study of Quantum Key Distribution Technology', Technology Innovation Management Review (January 2015),
https://timreview.ca/article/864

[Uniwaterloo Market Study]
University of Waterloo QKD market Study,
https://uwaterloo.ca/institute-for-quantum-computing/resources/download-quantum-cryptography-market-study

[UK Hub Ind. Engag.]
https://www.quantumcommshub.net/industrial-engagement

[CIR 2017 Quantum Encryption]
Report # CIR-QESM-TB-0617, 'Quantum Encryption Systems Markets: A Technology and Business Opportunity Forecast — 2017 to 2026', published 1 June 2017,
https://www.cir-inc.com/reports/quantum-encryption-systems-markets-a-technology-and-business-opportunity-fo

[CIR 2017 Quantum Networking]
Report # CIR-QN-DCO-0517, 'Quantum Networking: Deployments, Components and Opportunities — 2017-2026', published 19 October 2017,
https://www.cir-inc.com/reports/quantum-networking-deployments-components-and-opportunities-2017-2026

[EDA press 2016]
'EDA R & T Conference to discuss future Defence Research and Technology', April 2016, https://www.eda.europa.eu/info-hub/press-centre/latest-news/2016/04/22/eda-r-t-conference-2016-to-discuss-future-defence-research-and-technology

[EDA report 2016]
EDA R & T Seminar Report, 25-26 April 2016, https://www.eda.europa.eu/docs/default-source/brochures/click-here-to-download-the-final-conference-report.pdf

[DG HOME industrial policy]
https://ec.europa.eu/home-affairs/what-we-do/policies/industry-for-security_en

[Wiki CryptoWars]
https://en.wikipedia.org/wiki/Crypto_Wars

[Wiki GlobalSurveillance]
https://en.wikipedia.org/wiki/Global_surveillance

[STOA 1999]
European Parliament (1999), Scientific and Technological Options Assessment, 'Development of Surveillance Technology and Risk of Abuse of Economic Information', December 1999, http://www.europarl.europa.eu/RegData/etudes/etudes/join/1999/168184/DG-4-JOIN_ET%281999%29168184_EN.pdf

[EP Echelon 2001]
'Report on the existence of a global system for the interception of private and commercial communications' (2001), European Parliament Temporary Committee on the ECHELON Interception System, Rapporteur: Gerhard Schmid, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//EN&language=EN

[Willan 2004]
Willan, P. (2004), 'EU seeks quantum cryptography response to Echelon', NetworkWord, http://www.networkworld.com/article/2333159/lan-wan/eu-seeks-quantum-cryptography-response-to-echelon.html

[Sans 2004]
SANS Institute InfoSec Reading Room (2004), 'Securing Key Distribution with Quantum Cryptography', by Bradford C. Bartlett, https://www.sans.org/reading-room/whitepapers/vpns/securing-key-distribution-quantum-cryptography-1448

[EP NSA 2014]
European Parliament resolution of 12 March 2014, 'On the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs', http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P7-TA-2014-0230+0+DOC+PDF+V0//EN

[EP Pressroom 2015]
Mass surveillance: EU citizens' rights still in danger, says Parliament http://www.europarl.europa.eu/news/en/press-room/20151022IPR98818/mass-surveillance-eu-citizens-rights-still-in-danger-says-parliament

[EP Foreign Affairs 2016]
European Parliament's Committee on Foreign Affairs, 'Transatlantic Digital Economy and Data Protection: State-of-Play and Future Implications for the EU's External Policies', http://www.europarl.europa.eu/RegData/etudes/STUD/2016/535006/EXPO_STU%282016%29535006_EN.pdf

[Moore 2014]
Moore, M. (2014), 'China builds computer network impenetrable to hackers', *The Telegraph*, 7 November 2014, http://www.telegraph.co.uk/news/worldnews/asia/china/11216766/China-builds-computer-network-impenetrable-to-hackers.html

[Chen Jun 2014]
Chen, S. (2014), 'Post-Snowden China looks to "hack-proof" quantum communications', *South China Morning Post*, 13 June 2014, http://www.scmp.com/news/china/article/1531161/post-snowden-china-looks-hack-proof-quantum-communications

[Segal 2016]
Segal, A. (2016), 'China, Encryption policy, and International Influence', Hoover Institution Essay on National Security, Technology, and Law, 1610, http://www.hoover.org/sites/default/files/research/docs/segal_webreadypdf_updatedfinal.pdf

[US House 2012]
'Investigative Report on the US National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE', US House of Representatives, 112th Congress, 8 October 2012, https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf

[Techonomy 2013]
Young, D. (2013), 'Huawei, ZTE Banned From Selling to U.S. Government', *Techonomy*, 2 April 2013, http://techonomy.com/2013/04/huawei-zte-banned-from-selling-to-u-s-government

[Politico 2017]
https://www.politico.eu/article/huawei-china-ghost-in-europe-telecom-machine

[NYtimes 2017]
https://www.nytimes.com/2017/09/13/us/politics/kaspersky-lab-antivirus-federal-government.html

[Batelle deployment]
https://www.battelle.org/case-studies/case-study-detail/quantum-key-distribution

[Siemens deployment]
http://www.prweb.com/releases/2010/10/prweb4670214.htm

[KPN deployment]
https://corporate.kpn.com/press/press-releases/kpn-to-implement-quantum-encrypted-connection-qkd.htm

[Toshiba Genome 2015]
'Commencement of Verification Testing of Quantum Cryptographic Communication System that Theoretically Cannot be Tapped', corporate press release, 18 June 2015, http://www.toshiba.co.jp/about/press/2015_06/pr1801.htm

[SPIE Defence 2017]
https://spie.org/ESD17/conferencedetails/quantum-technologies-quantum-information-science

[Selex 2014]
Matich, G. and Kimber, P. (2014), 'Quantum Technology Challenges for Defence', presentation given at Cambridge University, August 2014,
https://www.turing-gateway.cam.ac.uk/sites/default/files/asset/doc/1608/Kimber.pdf

[DSTL 2015]
Pritchard, J. and Till, S. (2015), 'Quantum technologies in MoD's future research programme', presentation given at the KTN 'Meet the Hubs' event, London, 19 January 2015
https://connect.innovateuk.org/documents/11487824/22230824/Dstl.pdf/9b9bc0a5-bcac-47eb-98a9-d5132e9bc9fa

[ENISA QKD 2009]
Briefing: Quantum key distribution, 27 November 2009,
https://www.enisa.europa.eu/publications/archive/briefing-quantum-key-distribution

[Whitley 2015]
Whitley, T. (2015), 'Quantum Telecommunications Networks', presentation given at the Quantum Communications Hub Launch, 10 April 2015,
https://www.quantumcommshub.net/wp-content/src/Tim-WHITLEY_Quantum-Hub-Launch.pdf

[Wakeling 2017]
Presentation by Jonathan Wakeling at the ESA Scylight, 8 February 2017,
https://artes.esa.int/sites/default/files/32%20-%20Wakeling%20BT%20Group.pdf

[Bellot]
Le, Q.-C. and Bellot, P., 'Enhancement of AGT Telecommunication Security using Quantum Cryptography',
https://pdfs.semanticscholar.org/76cb/db210107a840d386b5087d945ea5faec4bd5.pdf

[Eurocontrol 2008]
'Evaluation of Air Ground telecommunication security and its enhancement using Quantum Cryptography technology', project presented by Michel Riguidel (2008),
http://www.eurocontrol.int/eec/public/standard_page/proj_CARE_INO_II_Cryptography.html

[Gemalto website]
https://safenet.gemalto.com/resources/data-protection/secure-financial-services-data-white-paper

[KTN Quantum Finance]
Walker, T., 'Quantum Technology in Finance', white paper by the Knowledge Transfer Network KTN,
https://connect.innovateuk.org/documents/11487824/0/Quantum%20Technology%20in%20Finance?version=1.1

[Financial Review 2015]
Financial Review (2015), 'Encryption key as Westpac buys into Aussie tech security firm QuintessenceLabs,
http://www.afr.com/technology/encryption-key-as-westpac-buys-into-aussie-tech-security-firm-quintessencelabs-20150612-ghmnaz

[Axa 2015]
Quantum cryptography chair for data protection, Axa corporate press release (2015), https://www.axa.com/en/newsroom/news/quantum-cryptography-data-protection

[OHB 2017]
'OHB funding a foundation professorship to improve cyber security in satellite communications', OHB corporate press release, 3 February 2017, https://www.ohb.de/press-releases-details/ohb-stiftungsprofessur-cyber-security.html

[Dirks 2017]
Dirks, B. (2017), 'Qutech/TNO space-based QKD technology development', ScyLight, https://artes.esa.int/sites/default/files/31%20-%20Dirks%20QuTech%20TNO.pdf

[GSA Galileo PRS]
European Global Navigation Satellite System Agency (GSA), https://www.gsa.europa.eu/security/prs

[Elser 2015]
Elser, D. et al. (2015), 'Satellite Quantum Communication via the Alphasat Laser Communication Terminal', https://arxiv.org/abs/1510.04507

[OSA 2017]
'Researchers Discover Short-Cut to Satellite-Based Quantum Encryption Network', OSA Newsroom, 15 June 2017, http://www.osa.org/pt-br/about_osa/newsroom/news_releases/2017/researchers_discover_short-cut_to_satellite-based

[USAF 2011]
United States Air Force Chief Scientist, 'Technology Horizons: a vision for air force science and technology 2010-2030', http://www.defenseinnovationmarketplace.mil/resources/AF_TechnologyHorizons2010-2030.pdf

[Oi 2017]
Oi, D. et al. (2017), 'CubeSat quantum communications mission', *EPJ Q. Tech.*, 4:6, https://epjquantumtechnology.springeropen.com/articles/10.1140/epjqt/s40507-017-0060-1

[COST space QT 1]
http://www.cost.eu/COST_Actions/ca/CA15220

[COST space QT 2]
http://www.qtspace.eu

[ESA Willie]
Wille, E. and Murphy, E., 'Entanglement and Quantum Key Distribution at ESA', https://artes.esa.int/sites/default/files/27%20-%20Murphy%20ESA.pdf

[Ursin 2008]
Ursin, R. et al., 'Space-QUEST Experiments with quantum entanglement in space' 2008 IAC Microgravity Sciences and Processes Symposium, Glasgow, UK, https://arxiv.org/pdf/0806.0945.pdf

[*ESA Bulletin* 2009]
'Leap ahead in space communication: Quantum Technologies for space systems', European Space Agency | Bulletin 137 | February 2009,
http://www.esa.int/esapub/bulletin/bulletin137/bul137e_perdigues_armengol.pdf

[ESA Scylight 1]
https://artes.esa.int/scylight/overview

[ESA Scylight 2]
https://artes.esa.int/news/scylight-workshop

[ESA Scylight 3]
https://artes.esa.int/news/esa-scylight-industry-day

[Wassenaar website]
http://www.wassenaar.org

[SWD 315 2016]
http://ec.europa.eu/transparency/regdoc/rep/10102/2016/EN/SWD-2016-315-F1-EN-MAIN-PART-1.PDF

[EPRS dual use 2017]
European Parliament Research Service Briefing 'Review of dual-use export controls', 30 January 2017,
http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/589832/EPRS_BRI(2016)589832_EN.pdf

[CIHR 2015]
Centre for Internet and Human Rights (2015), 'Export controls of surveillance technologies', Background paper,
https://cihr.eu/publication-export-controls-of-surveillance-technologies

[DigitalEurope export 2016]
'DIGITALEUROPE position paper on the review of export control policy in the EU', February 2016,
http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=1125&language=en-US&PortalId=0&TabId=353

[DG HOME website]
https://ec.europa.eu/home-affairs/what-we-do/policies/industry-for-security_en

[Saper 2013]
Saper, N. (2013), 'International Cryptography Regulation and the Global Information Economy', *11 Nw. J. Tech. & Intell. Prop.* 673,
http://scholarlycommons.law.northwestern.edu/njtip/vol11/iss7/5

[WTO June 2017]
WTO news, 'Members debate cyber security and chemicals at technical barriers to trade committee', 14 and 15 June 2017,
https://www.wto.org/english/news_e/news17_e/tbt_20jun17_e.htm#

[Budapest Convention website]
http://www.coe.int/en/web/cybercrime/the-budapest-convention

[ETSI Lawful Interception]
http://www.etsi.org/technologies-clusters/technologies/lawful-interception

[OECD crypto guidelines]
http://webnet.oecd.org/oecdacts/Instruments/ShowInstrumentView.aspx?InstrumentID=115&InstrumentPID=111&Lang=en&Book=False

[FRA website]
EU Agency for Fundamental Rights: Information society, privacy and data protection
http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection

[EDPS website]
European Data Protection Supervisor website
https://edps.europa.eu/about-edps_en

[Europarl website]
http://www.europarl.europa.eu/atyourservice/en/displayFtu.html?ftuId=FTU_5.12.8.html

[Reg 679, 2016]
Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016, 'on the protection of natural persons with regard to the processing of personal data and on the free movement of such data',
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

[Dir 680, 2016]
Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 'on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data',
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG&toc=OJ:L:2016:119:TOC

[EC press 2015]
http://europa.eu/rapid/press-release_MEMO-15-6385_it.htm

[EC DSM 2017]
https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications

[EC fact sheet 2017]
http://europa.eu/rapid/press-release_MEMO-17-17_en.htm

[DigitalEurope encryption]
DIGITALEUROPE white paper 'Views on Encryption', Brussels, 15 July 2016,
http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=2241&language=en-US&PortalId=0&TabId=353

[Enisa encryption]
ENISA's Opinion Paper: Strong Encryption Safeguards our Digital Identity (2016),
https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisas-opinion-paper-on-encryption

[EC e-privacy 2017]
https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications

[EDPS 2016]
https://edps.europa.eu/sites/edp/files/publication/16-07-22_opinion_eprivacy_en.pdf

[TheGuardian Jun 2017]
https://www.theguardian.com/technology/2017/jun/19/eu-outlaw-backdoors-new-data-privacy-proposals-uk-government-encrypted-communications-whatsapp

[Cryptolaw website]
http://www.cryptolaw.org/cls-sum.htm

[Euractiv 2016]
https://www.euractiv.com/section/social-europe-jobs/news/five-member-states-want-eu-wide-laws-on-encryption

[FBI goingdark]
https://www.fbi.gov/services/operational-technology/going-dark

[Finklea 2016]
Congressional Research Service Report by Kristin Finklea 'Encryption and the "Going Dark" Debate', 20 July 2016,
https://fas.org/sgp/crs/misc/R44481.pdf

[Europol Enisa 2016]
Europol and ENISA Joint Statement 'On lawful criminal investigation that respects 21st Century data protection' (2016),
https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/on-lawful-criminal-investigation-that-respects-21st-century-data-protection

[Council of EU 12368/16]
http://www.statewatch.org/news/2016/sep/eu-usa-encryption-quest-12368-16.pdf

[Rejo Zenger 2016]
'Input provided by MS on questionnaire on encryption in criminal cases',
https://www.asktheeu.org/en/request/input_provided_by_ms_on_question?nocache=incoming-11727#incoming-11727

[Council of EU 13434/16]
http://statewatch.org/news/2016/oct/eu-encryption-orientation-debate-13434-16.pdf

[Monroy 2016]
Monroy, M. (2016), 'New EU network of judicial authorities to combat the challenges stemming from encryption', 2 November 2016,
http://andrej-hunko.de/component/content/article/7-beitrag/3317-new-eu-network-of-judicial-authorities-to-combat-the-challenges-stemming-from-encryption

[Eurojust 2016]
'Kick-off meeting for the European Judicial Cybercrime Network', Eurojust, 25/11/2016,
http://www.eurojust.europa.eu/press/PressReleases/Pages/2016/2016-11-25.aspx

[Council of EU 8799/17]
http://www.statewatch.org/news/2017/jun/eu-council-concl-22-23-june.pdf

[DG HOME encryption]
https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/encryption_en

[EC Security 2017]
'Eleventh progress report towards an effective and genuine Security Union', Communication from the Commission to the European Parliament, the European Council, and the Council, 18 October 2017,
https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20171018_eleventh_progress_report_towards_an_effective_and_genuine_security_union_en.pdf

[Paganini Feb 2016]
Paganini, P. (2016), 'German authorities approve the use of home-made Federal Trojan', *SecurityAffairs*, 28 February 2016,
http://securityaffairs.co/wordpress/44860/hacking/germany-approves-federal-trojan.html

[Paganini Aug 2016]
Paganini, P. (2016), 'ZITiS is the new German Government cyber unit in wake of terror attacks', *Security Affairs*, 15 August 2016,
http://securityaffairs.co/wordpress/50297/terrorism/zitis-german-cyber-unit.html

[Monroy website]
https://digit.site36.net/2016/11/03/new-eu-network-of-judicial-authorities-to-combat-the-challenges-stemming-from-encryption/#more-435

[EP LIBE 2017]
'Legal framework for hacking by law enforcement: identification, evaluation, and comparison of practices', European Parliament, Study for the LIBE Committee (2017),
http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf

[NY Times, May 2017]
'Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool', The New York Times (2017),
https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html

List of abbreviations and definitions

AES Advanced Encryption Standard

ANR Agence Nationale de la Recherche

BB84 Bennett Brassard 84, QKD protocol

BSI Bundesamt für Sicherheit in der Informationstechnik

BMWi Bundesministerium für Wirtschaft und Energie

CAs certificate authorities

COST Cooperation in Science and Technology, EU programme

CQC2T Centre for Quantum Computation and Communication Technologies

CQT Centre for Quantum Technology

CV-QKD continuous variable QKD

DARPA Defense Advanced Research Projects Agency

DI-QKD device-independent QKD

DoD Department of Defence

DoE Department of Energy

DSTL Department of Defence Science & Tech Lab

EDA European Defence Agency

EDPS European Data Protection Supervisor

ENISA European Union Agency for Network and Information Security

EPSRC Engineering and Physical Sciences Research Council

ETSI European Telecommunications Standards Institute

EUGEAs EU general export authorisations

EU-LISA European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice

EURODAC European Dactyloscopie

GCHQ Government Communications HeadQuarters

GDPR General Data Protection Regulation

IAD Information Assurance Directorate

IARPA Intelligence Advanced Research Projects Activity

IETF Internet Engineering Task Force

ITAR International Traffic in Arms Regulation

ITS information theoretically secure

JRC Joint Research Centre (of the European Commission)

KISTI Korea Institute of Science and Technology Information

LEA law enforcement agency

MDI-QKD measurement device independent QKD

NASA National Aeronautics and Space Administration

NSF National Science Foundation
NCSC National Cyber Security Centre
NGEAs national general export authorisations
NICT National Institute of Information and Communications Technology (JP)
NIST National Institute of Standards and Technology
NRF National Research Foundation (Singapore)
NUS National University of Singapore
NSA National Security Agency
NSF National Science Foundation
NTIA National Telecommunications and Information Administration
PKI public key infrastructure
PQC post-quantum cryptography
QBER quantum bit error rate
QKD quantum key distribution
QRNG quantum random numbers generator
QSC quantum safe cryptography
QT quantum technology
RSA Rivest Shamir Adleman, asymmetric cryptography algorithm
SBIR Small Business Innovation Research programme
SIS II Schengen Information System
SPAD single-photon avalanche diode
STTR Small Business Technology Transfer programme
TFEU Treaty on the Functioning of the European Union
UC universally composable
USAF United States Air Force
VIS Visa Information System

List of figures

Figure 1: Yearly distribution of patent applications in QKD.

Figure 2: Distribution of the applicants' nationalities.

Figure 3: Applications by firms headquartered in different countries.

Figure 4: Main players, listed by number of patent applications.

KJ-NA-29017-EN-N

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

Joint Research Centre

EU Science Hub

Publications Office

doi:10.2760/881896

ISBN 978-92-79-77314-3