CCSIRS | POLICY PAPER

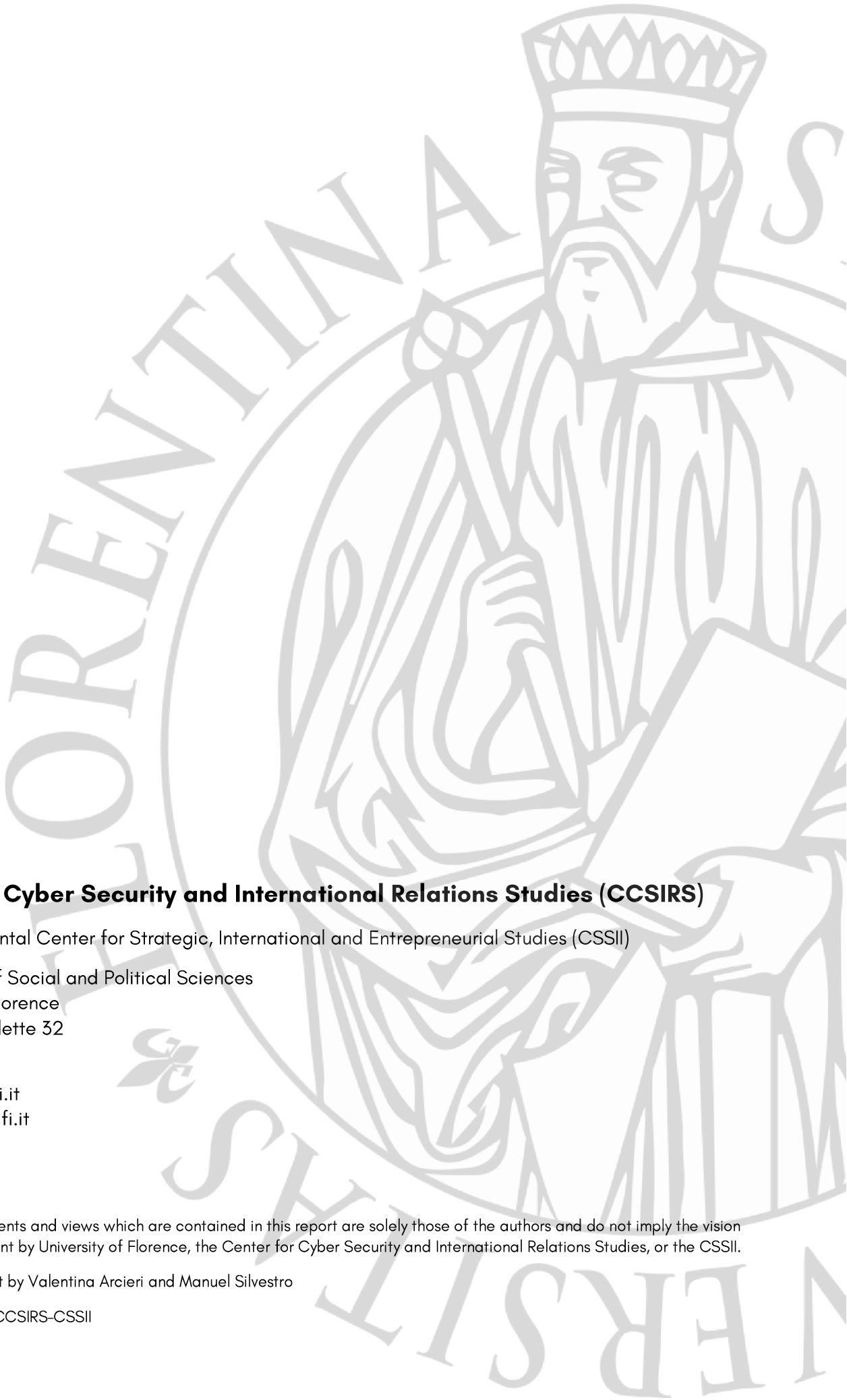
EMERGING AND DISRUPTIVE TECHNOLOGIES

SECURITY IMPLICATIONS AND APPLICATIONS OF QUANTUM TECHNOLOGIES (SERIES 1)

Lisa Borlotti
Marzio Di Feo
Daniela Giordano
Susi Reitan

Center for Cyber Security and International Relations Studies

ISSUE
June 2021



Center for Cyber Security and International Relations Studies (CCSIRS)

Interdepartmental Center for Strategic, International and Entrepreneurial Studies (CSSII)

Department of Social and Political Sciences
University of Florence
Via delle Pandette 32
50127 Firenze

www.cssii.unifi.it
cyber@cssii.unifi.it

Design and layout by Valentina Arcieri and Manuel Silvestro

CCSIRS | POLICY PAPER

EMERGING AND DISRUPTIVE TECHNOLOGIES

SECURITY IMPLICATIONS AND APPLICATIONS OF QUANTUM TECHNOLOGIES (Series 1)

Lisa Borlotti

Marzio di Feo

Daniela Giordano

Susi Reitan

Center for Cyber Security and International Relations Studies

ISSUE

June 2021

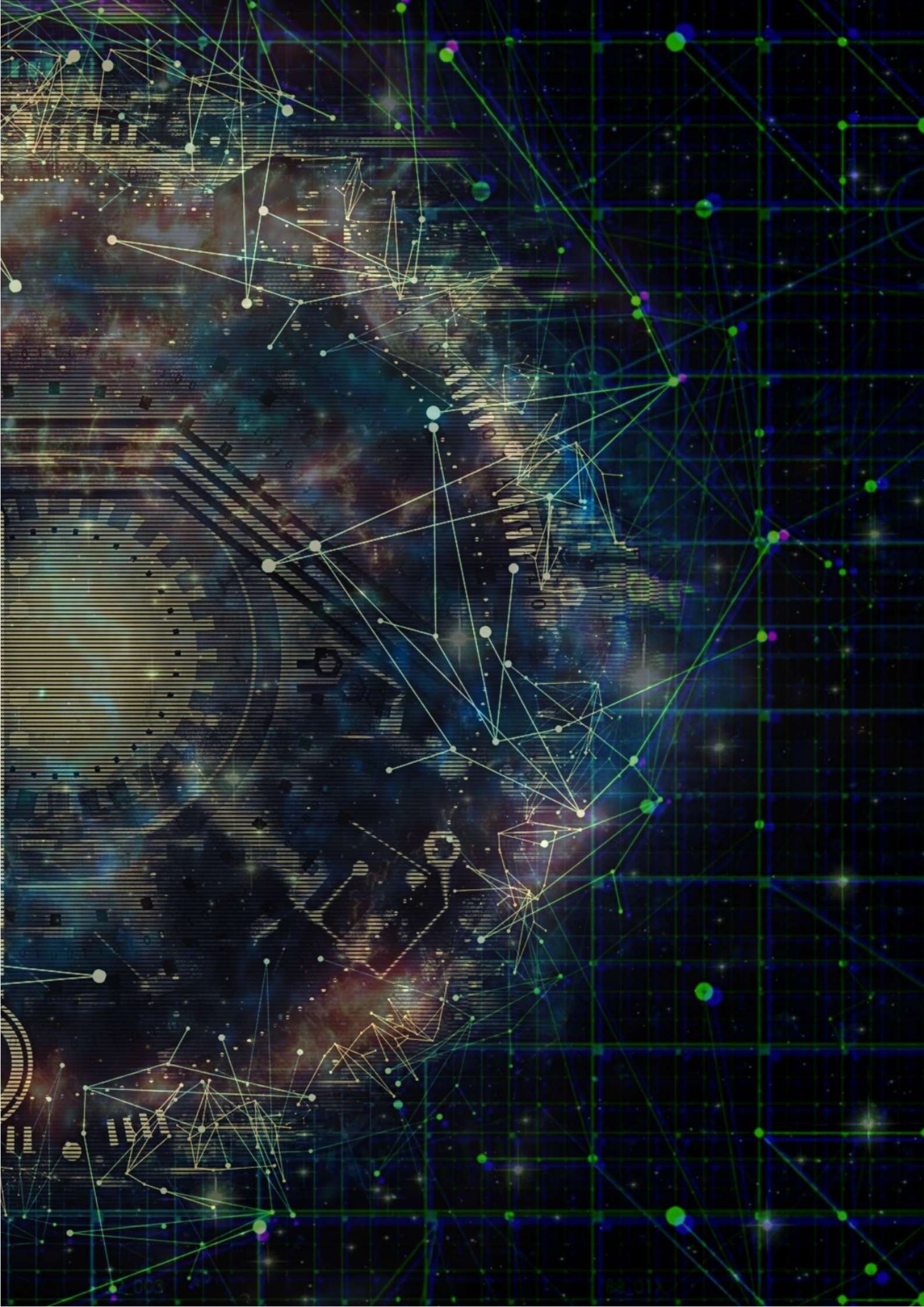
ABOUT THE CENTER

The Center for Cyber Security and International Relations Studies (CCSIRS) is part of the Interdepartmental Center for Strategic, International and Entrepreneurial Studies (CSSII) at the Department of Political Sciences of the University of Florence. Established in 2015, the CCSIRS aims at promoting and deepening the knowledge on cyberspace dynamics through a policy-oriented approach. More specifically, activities are focused on analyzing the influence that cyberspace exercises over both Italian national security and the international system's stability, peace and security.

The Center's multidisciplinary approach succeeds in integrating the traditional fields of Social Sciences (politics, economics, law, strategic and military studies) and Computer Science. The analyses are conducted by Italian and international experts from various sectors and countries. The Center shapes its international activities by creating an ever-increasing solid network of public and private partnerships, aiming at guaranteeing excellent research.

The Center's research focuses on comparative analysis of best cases and best practices in the fields of cyber strategy, governance and policy, critical infrastructures, economic and financial cybercrimes, privacy protection legislations and cyber intelligence structures. Complementarily, it carries out studies on the different approaches adopted internationally by both private and public actors.

Table of contents



1. INTRODUCTION AND RESEARCH QUESTION

According to the Science & Technology Trends 2020-2040 Report, quantum technologies lie among the most relevant emerging threats over the next ten years. The Report also outlines the differences between disruptive and convergent technologies, affirming that the former includes "those technologies or scientific discoveries that are expected to have a major, or perhaps revolutionary, effect on NATO defence, security or enterprise functions in the period 2020-2040"; whereas the latter are based on "a combination of technologies that are combined in a novel manner to create a disruptive effect.[1] In line with what above, quantum technologies can be considered both disruptive and convergent technologies, since they are expected to greatly increase in importance due to their potential and to their interrelation to other major strategic disruptors, such as Artificial Intelligence (AI) and security of infrastructures.

A common misconception is to include quantum technology as a branch of cyber security. Nevertheless, Quantum Technologies are the product of a complex mix of disciplines and subjects, spacing from physics to applied sciences. This aspect also reflects in the normative framework, which usually - and mistakenly- includes quantum technologies as a collateral aspect of cyber security. However, it must be acknowledged that current norms and regulations applied to the cyberspace do not fully overarch quantum technologies in their application scope. Thus, it is crucial to forecast the trends concerning quantum technologies both as a potential driver for new security threats, but also as a brand-new domain to be regulated.

Quantum technologies allow research to apply new interpretation lenses on the real world, applying quantum theories and processes to areas such as communication, cryptography, modelling and computation. Indeed, quantum mechanics is enhancing a worldwide innovation process through information sharing from academic labs to the industrial sectors. Among the multiple application fields, some of the potential advantages of implementing quantum technologies in our every-day lives relates to reliable navigation systems, secure communication, healthcare imaging and high-speed and powerful computing systems.[2]

At present, some of the applications of quantum technologies well go beyond the technical expertise, catching the interest of governments and the Big Tech companies. All around the world, major

[1] For further information: https://qt.eu/discover-quantum/quantum-technologies-in-a-nutshell/.

[2] For further information: https://www.nist.gov/topics/physics/introduction-new-quantum-revolution.

states begin to launch programmes based on the potentiality of quantum technologies, starting a so-called "quantum race". Among others, China,[3] the United States of America and Japan. At the basis of the "quantum race" lie also commercial interests, drivers of the quantum computing development, while defence and security interests are drivers of advancement in quantum sensing and communication. Nevertheless, the European Union,[4] acknowledging the transboundary nature of this emergent technology, decided to consolidate the European Quantum Flagship, by gathering eight European university research groups, companies and institutes, in order to build a blueprint for a future quantum Internet (Laurat, 2020).

As represented in Table 1, by comparing the eight major emergent and disruptive technologies expected to advance over the next 20-40 years, Quantum Technologies are classified as having a high impact on Communications and on Precision Navigation, as well as a revolutionary impact on Information Sciences. Moreover, it can be observed that there is a synergy related to Sensors among *Data*, *Quantum* and *Space Technologies*, allowing for further advancements across the three domains in the coming years.

Emergent and Disruptive Technologies	Technology Focus Areas	Impact	Horizon
Data	Advanced analytics	Revolutionary	2025
	Communications	High	2030
	Advanced Decision Making	Revolutionary	2025
	Sensors	High	2030
Artificial Intelligence	Advanced Algorithms	Revolutionary	2030
	Applied AI	Revolutionary	2030
	Human-Machine Symbiosis	High	2035
Autonomy	Autonomous Systems	Revolutionary	2025

[3] China recently launched a satellite and installed a Quantum Key Distribution (QKD) link between Shanghai and Beijing.

[4] For further information, please consult the European QT flagship initiative.

	Human-Machine teaming	Revolutionary	2030
	Autonomous Behaviour	High	2030
	Countermeasures	High	2025
Quantum Technologies	Communication	High	2030
	Information Science	Revolutionary	2035
	Precision Navigation	High	2025
	Sensors	Moderate	2040
Space Technologies	Platforms	Moderate	2025
	Operations	Moderate	2030
	Sensors	High	2035
Hypersonics	Platforms and Propulsion	High	2025
	Countermeasures	High	2030
Biotechnology & Human enhancement	Bioinformatics	Moderate	2025
	Human Augmentation	High	2030
	Medical Countermeasures	High	2030
	Synthetic Biology	High	2025
Novel materials and Manufacturing	Novel Materials	High	2040
	Additive Manufacturing	Moderate	2025
	Energy Storage	Moderate	2030

Table 1. Overview of the eight major Emergent-Disruptive Technologies and their impact levels. Source: D.F. Reding and J. Eaton. "NATO Science & Technology Organization Science & Technology Trends 2020-2040", NATO, Belgium. March 2020.

Nevertheless, the real nature and scope of quantum remains quite uncovered by the literature. The complexity of the topic, based on quantum mechanics (the physics of subatomic particles), makes its understanding quite tough. This policy paper aims to uncover some of the core aspects of quantum technologies, that still lie in the shadow and that should be put in the spotlight to understand the potential of such emergent technology. The research question driving the analysis consists of what are the political and security implications and potential application fields of quantum technologies over the next decades.

Moreover, the final goal of this paper is to suggest a set of recommendations in order to prepare the road for quantum technologies inclusion and application. Therefore, the paper is written according to three purposes, and each of them is reflected in one of the three sections below. In particular, the second section, named "Definitions and Global Framework" provides an overview of the definition applied to quantum technology and its scope, explaining their nature and the main features involved in the Quantum Technology processes. Thus, the third section, "Fields of implementation and the future of quantum technologies between fiction and reality", introduces the main application domains and securitarian implication of quantum technologies, with a special focus on the defence and security aspects. Section 4, "Strategies and Doctrines", aims to present current practices and strategies across the world, especially by outlining major actors in the field as well as their primary objectives and applications fields related to the quantum domain.

Finally, the last section provides a summary of the elements emerged in the previous parts, suggesting a set of recommendations on the basis of the analysis and practices observed, as well as pointing out future research subjects' perspectives.

2. DEFINITIONS AND GLOBAL FRAMEWORK

But what are quantum technologies? And how are they impacting our everyday lives? Even if the processes underlying quantum technologies are not straightforward, their advantages are already showing their success in some of our current technological devices.[5] Since the last century, thanks to the developments in quantum mechanics, scientists began to study the behaviour of matter at the atomic scale, facilitating the start of this new study domain.

Above all, two main advantages drive the potential to new quantum application: the principle of quantum entanglement and quantum superposition. In order to understand why they constitute a benefit, a brief explanation is provided about what they relate to in the following lines.

Quantum Entanglement

Entanglement might be one of the two most complex concepts of quantum technologies, and it should be intended as the property of two particles to be intertwined even if they are separated by great distances one from another. Also defined as "a sort of quantum marriage between qubits", such commodity allows to know qubit[6] values of one particle, by measuring the value for its intertwined particle. Indeed, entanglement allows a system to perform exponentially more computation simultaneously.[7]

Quantum Superposition

University of Oregon physicist Dave Wineland, Nobel Prize in physics for his experimental work in quantum mechanics at NIST in 2012, provided an explanation about quantum superposition consists of:

[5] Quantum phenomena are applied in procedures such as transistor nuclear energy, medical imaging, photoelectric detectors, lasers etc.

[6] In classical computing, the information is encoded in bits, having a value of 0 or 1. A qubit (i.e., quantum bit) is the quantum analogue of a classical bit.

[7] It is worth noting that one of the major issues of entanglement is that, the more qubits there are, the faster they will tend to decohere, thus losing the properties of entanglement. This explains the absence of a quantum computer that could perform exponential computation at the same time, since decoherence causes the system to crash at early stages of entangled calculations. NIST, "The strange world quantum physics". Available at: https://www.nist.gov/topics/physics/introduction-new-quantum-revolution/strange-world-quantum-physicshttps://www.nist.gov/topics/physics/introduction-new-quantum-revolution/strange-world-quantum-physics.

"what you can think of as a good analogy is a marble that can roll back and forth in a bowl [...] In our atomic ion experiments, we can make an atomic marble. We can make it roll back and forth just as a marble would in a real bowl. And at some instance of time then, the atom will be on the right side of the bowl and a little bit later on the left side of the bowl."[8] Nevertheless, superposition like entanglement is very fragile, and the former can be altered by stray noise, causing measuring errors.

Entanglement and superposition allow for a completely new area of study, with almost an infinite combination outcomes possibility. Over time, it has been recognized that the first quantum revolution concerned innovation such as computer chips, lasers, magnetic resonance imaging etc. This revolution provided the basis to create advanced tools, which now allow to open the road to almost unlimited technological opportunities, overarched under the category of the "second generation quantum technologies". At present, their application is still under investigation, but many believe it to be the leading innovation to a fourth industrial age.

According to many experts on the subject, even though quantum technologies are still at the early stages of their development, they will soon be able to increase C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) data collection, due to an increased sensor capability, secure communications and computing, nevertheless it will help improve faster predictive analysis when related to modelling and simulation, as well as the identification of biological organisms, novel material, and chemical properties.[9] In particular, quantum technologies will bring to the table a set of advantages and advancements as outlined in the next few lines, as well as represented in Image 1.

First of all, superposition and entanglement will provide major advancement related to quantum computers, allowing for enormous computing powers in problem solving tasks. Among others, quantum computers will enable simultaneous high-speed processing of large amounts of data and equations. This could help increase decision-making processes as well as operational issues, by providing effective ad hoc solutions to complex problems. More broadly, applying this aspect to other emerging technologies, such as AI systems, could further medical and diagnosis studies for instance. Global IT companies, such as Intel, IBM and Google, are taking advantage of this innovation, trying to overcome classical computation in a 20-years-deadline program. Quantum computers could be able to run

[8] NIST, "The strange world quantum physics". Available at: https://www.nist.gov/topics/physics/introduction-new-quantum-revolution/strange-world-quantum-physics

[9] Quantum Flagship."Big Data boosting AI". Available at: https://qt.eu/discover-quantum/applications-of-qt/big-data-boosting-ai/

algorithms, reaching approximate solutions through optimization, and this "is exactly the type of problem that quantum computers are well-suited for."[10]

The second tool potentially enabled by quantum technologies would be quantum simulators. By reproducing behaviour of materials at low temperatures, quantum simulators are designed to identify and create new chemicals and materials, applicable to an almost infinite set of sciences (e.g., medicine, agriculture, energy supply, etc.).

Thirdly, quantum technologies will push further data and communications protection, through the development of a quantum internet. Indeed, current communication systems are based on encryption, easily overcome by quantum computers. Thus, it is needed a quantum-safe cryptography, such as the key primitive commercially available today. Quantum communication applies to secure communication and long-term storage, cloud computing, thanks to the quantum key distribution (QKD) and the quantum random number generators systems, helping to produce secret keys. Nevertheless, it must be stressed out that there is a lack of common recognised certification and standards regulating quantum communication devices and systems. Indeed, it is not clear to what extent current cyber security norms would be applicable to quantum communication innovations, thus calling for an urgent recognition of this issue from the international arena (Acin, 2018).

Lastly, quantum would provide major advancement in sensors and measurements. In fact, through the creation of quantum sensing and metrology, it will be possible to exploit most accurate measurements, high resolution imaging devices (e.g., ultra-sensitive gravimetric, accurate clocks, magnetic and acoustic sensors).

Some experts have divided the evolution of quantum computing in three distinct phases or generations (The Hague Security Delta, 2019). A first generation of the development of quantum computers will include the non-commercial application of quantum computers with medium-low complexity (Grumbling and Horowitz, 2018; The Hague Security Delta, 2019). This phase would be characterized by significant advancement costs which are mainly devoted to proof of concept (The Hague Security Delta, 2019).

Second generation of quantum computers, then, would be geared towards early commercial applications, with research directed at improving the scalability of quantum solutions' complexity

[10] NIST, "Quantum Supremacy", 2018. Available at: https://www.nist.gov/topics/physics/introduction-new-quantum-revolution/quantum-supremacy

(Grumbling and Horowitz, 2018; The Hague Security Delta, 2019). Finally, the third generation of quantum computers will achieve the development of universal quantum computers, meeting quantum supremacy in a wide variety of (non)commercial applications: the research will be largely focus on the implementation of quantum applications surpassing classical computing (Grumbling and Horowitz, 2018; The Hague Security Delta, 2019).

The greater accessibility of quantum computers will allow the rapid development of new applications and show this entire disruptive impact on all the fields of security in a comprehensive roadmap as reported in the table below.

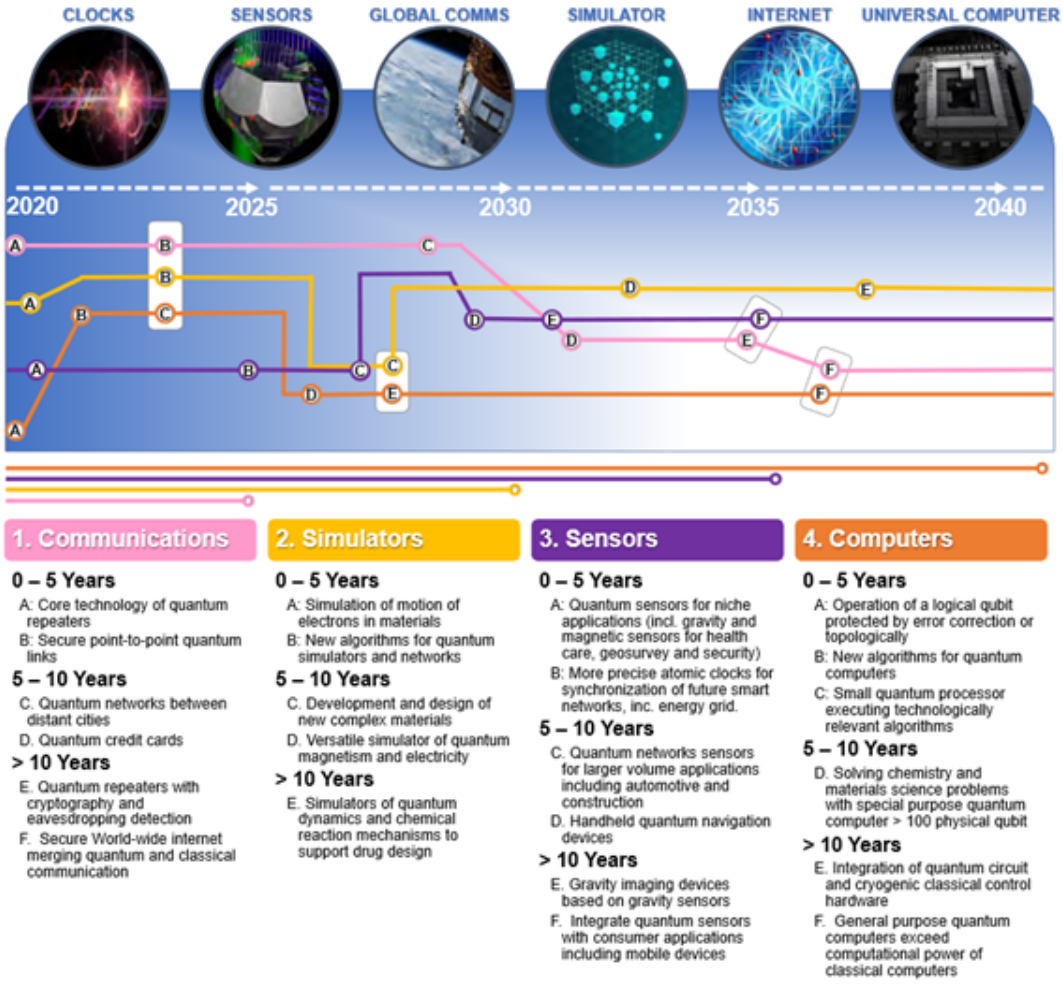


Figure 1. Prospect of main Quantum technological drivers over next years.

Source: (Reding and Eaton, 2020, p. 70)

3. FIELDS OF IMPLEMENTATION AND THE FUTURE OF QUANTUM TECHNOLOGIES BETWEEN FICTION AND REALITY

The debate on quantum computing and the technological developments related to it in the defense and security studies have found fertile ground in the path of the apocalyptic prospects of technological progress and, in a complementary way, the possibility of gaining a strategic competitive advantage thanks to it. In both cases, the awareness of the revolutionary perspectives of this type of technology involved various areas, not limited, therefore, to security, and tools including computing, communications, and sensors. On the practical side, trying to get out of the efforts to understand the technology, this section will try to explore through some empirical evidence the potential developments in this sector, selected with particular reference to the impact on international security and stability.

The tremendous potential of this development meets with two types of preliminary considerations *vis-à-vis* approaches. The first collides with the ability to think of technology as a collective perception and expectations about an imaginary future. In this sense, literature tends to hyperbolically merge different perspectives from various fields of knowledge, including political science, security studies, engineering, and computer science. The second, on the other hand, focuses on the speculations about the dynamics of quantum theory as a new model or paradigm in the social sciences and, in particular, for "quantizing international relations" in applying the fundamental notions of quantum theory to the discipline (Wendt, 2015; Smith III, 2020; Der Derian and Wendt, 2020). This debate has recently been taken up and deepened and it can be seen as an attempt to *horizontalize* the consequences for the various academic disciplines of this new scientific paradigm (Grove, 2020).

This section will not focus on the implications of this new changing paradigm which have yet to be fully explored and whose material and real consequences could also affect technological development. In this vein, this part of the paper is principally dedicated to dive into security perspectives of the quantum world.

In this analytical framework, this section aims to empirically investigate the developments between factual reality and quantum imagination of it related to international security. Along with this theoretical pathway, quantum technology will be considered not as a single monolith but in its nuances within the different applications. This attempt aims to overcome the possibility of limiting technology to

a naïve discourse on the technological supremacy of the major global players, on the one hand, and to better understand, on the other, the potential impacts of quantum.

As described in the previous section, the applications of this type of technology are usually identified with some technologies, i.e., quantum computing, quantum sensors, quantum communications, quantum sensing, quantum imaging and quantum hologram (Inglesant, Jirotka, and Hartswood, 2018, p. 6).[11]

These new developments have all highlighted the potential of applying some properties of quantum mechanics (e.g., entanglement) to achieve new capabilities with a disruptive effect in the international arena (and its understanding). In this sense, the literature has highlighted the revolutionary contribution of technology and, at the same time, the level of uncertainty about the final result from their gradual concrete implementation. To complete this comprehensive conceptualization, it is also worth noting the development in quantum biology, i.e., the possibility of replicating some quantum properties into the practice of living beings in their behaviors still incomprehensible to modern science.[12] This section is composed of three main parts. The first and the second paragraphs are characterized by a general-specific order. In light of this, on the one hand, the first part analyzes the applicability of quantum technologies in defense and security as reference sectors of the quantum developments, and, on the other, the second part focuses on cyber security as a specific field of application. Finally, the last part emphasizes the element of strength and weakness within the proposed roadmap for the implementation of quantum technologies following the preliminary caveat about expectation of the imagined future.

Overview of quantum technologies in defence and security

According to numerous reports, the areas of defence and security could be the first to adopt these technologies with particular reference to quantum-enabled clocks, quantum navigators, quantum gravity sensors and quantum imaging (Inglesant, Jirotka, and Hartswood, 2018). The applications are affected, however, by the fact that the subject treated as seen is still an *in fieri* subject or are in the initial stages of development or concept. Some of these developments, then, are not available as products (i.e., quantum gravity sensors, quantum navigation, and quantum imaging) also due to the

[11] See also: Defienne, H. (2021). Quantum leap: how we discovered a new way to create a hologram. The Conversation, 17 February. Retrieved from https://theconversation.com/quantum-leap-how-we-discovered-a-new-way-to-create-a-hologram-155056.

[12] Marais A., et al. (2018). The future of quantum biology. Journal of the Royal Society, 14 November. Retrieved from https://royalsocietypublishing.org/doi/10.1098/rsif.2018.0640.

limitations in distance coverage and usability (Inglesant, Jirotka, and Hartswood, 2018, p. 12). Although technological development may still take some time (see also the figure at the end of this section), the principles underlying these technological developments are progressing exponentially and some forms of quantum computing and quantum simulation are already available in embryonic form.[13] These technologies and their practical implications are briefly analysed below.

The quantum meter allows the detection of local gravitational fields and, therefore, the inspection with a greater degree of accuracy and sensitivity, for example in the case of the presence of nuclear submarines (Lanzagorta, Uhlmann, and Venegas-Andraca, 2015). This type of development is part of the continuous race between stealth capabilities and the ability to detect enemies and target on the battlefield. However, sensing capabilities must overcome, as emerged in various studies and reports (Reding and Eaton, 2020), various technical obstacles on the practical possibilities such as the difficulties of the specific operational theatre.

A further field of application concerns navigation systems since quantum technologies could bring greater precision of acceleration and rotation measurements compared to current gyroscopes and being complementary or alternative to satellite navigation systems (Feng, 2019). In operational terms, the change could have concrete consequences in situations of interference with the current localization systems or fill the existing gaps in situations where, usually, the localization service is not available, *a fortiori* if considered the reliance on navigation signals of modern weapon systems (Thomas, 2010). Moreover, concerning the quantum imaging developments, this type of technology is based on the possibility of using the quantum nature of light to enhance an image and thus record any alterations of light on a quantum scale (Basset et al., 2019). The application allows to see objects and movements outside the line of sight or in conditions of friction such as the presence of fog, smoke, or dust (Altmann et al., 2018).

The following image, taken from the NATO (Reding and Eaton, 2020) study on technological developments 2020-2040, contains the main applications in all operational domains of quantum technologies. As emerged from the image, quantum technologies can play a role of capacity multiplier due to the synergies and interdependencies in different domains and according to the various fields of application.

[13] Microsoft (2021). Quantum Simulators, 2 January. Retrieved from https://docs.microsoft.com/en-us/azure/quantum/user-guide/machines/.

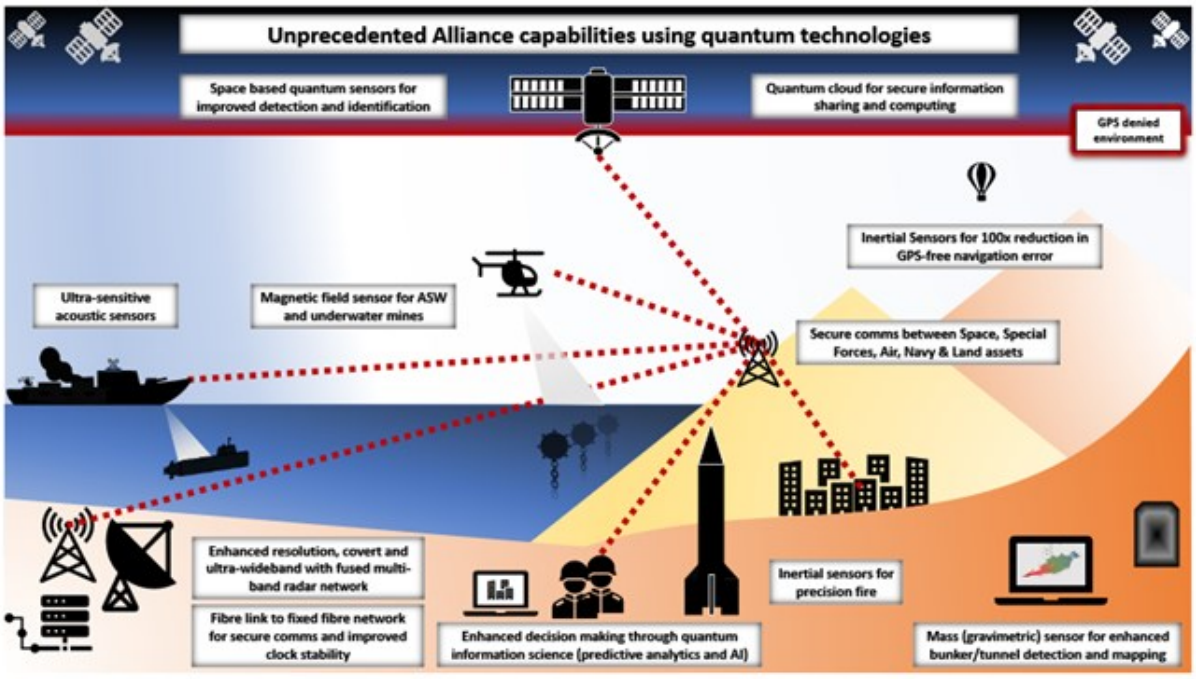


Figure 2. Quantum capabilities.

Source: (Reding and Eaton, 2020, p. 71)

Quantum technologies could increase the security capabilities of communications, which can guarantee "unbreakable" secure communications, i.e., QKD.[14] Some practical applications of this type of technology have already been explored, for instance, in the satellite transmission conducted by China in August 2016.[15] The other side of the coin of this development therefore concerns the ability of protocols responding to the continuing competition between attack and defense in cryptography to ensure combination quantum keys. In this sense, NIST (2020) started a process to evaluate through processes and standards whether a certain key is resistant to a quantum encryption algorithm or not.[16]

Quantum goes cyber: cyber security and the encryption landscape

As emerged above, the impacts of quantum technology in the sphere of cyber security lie on encryption, or rather the possibility of transforming information from a plain text into a ciphertext that can only be

[14] IBM. Quantum Cryptography. s.d.. Retrieved from https://researcher.watson.ibm.com/researcher/view_page.php?id=7242. For further details see also the video available on YouTube by the Simons Institute (2020) at https://www.youtube.com/watch?v=kNcgLqWjV0A (March 9, 2021).

[15] Broad, W.J. (2020). China Reports Progress in Ultra-Secure Satellite Transmission. The New York Times, 15 June. Retrieved from https://www.nytimes.com/2020/06/15/science/quantum-satellites-china-spying.html.

[16] See also the debate on post-quantum cryptography. Moody, D. (2020). The Future Is Now: Spreading the Word About Post-Quantum Cryptography. NIST, 2 December. Retrieved from https://csrc.nist.gov/Projects/post-quantum-cryptography/presentations.

"understood" by the recipient (Vermeer and Peet, 2020). Quantum algorithms can solve complex cryptographic issues currently used to protect data and systems. For instance, Shor's algorithms could break public key cryptography, providing faster methods to factor large integers. Common public-key cryptosystems (e.g., RSA, Rivest-Shamir-Adleman) integers solved classically are 768 bits and to break the encryption a quantum computer needs 2,400 qubits and 153 million operations with less than 0.000000006 errors per operation (Foley et al., 2021). This is still valid for RSA 2048 cryptography with a likelihood to compromise it in about eight hours with 6,200 qubits and 2.7 billion operations with less than 0.0000000003 error rate (Mosca and Piani, 2021). The coming quantum machine poses significant security challenges also for different encryption scheme such as Elliptic Curve Cryptography (ECC) (Foley et al., 2021). In general, current cryptographic methods of modern telecommunications are based, according to the Kerckhoffs principle, on the use of mathematical algorithms and secret keys and thus concern two broad categories that can be framed in systems of symmetric keys and asymmetric keys (Lewis and Travagnin, 2018, p. 6).

The distribution of quantum keys relies on a fundamental principle of quantum physics according to which under certain conditions it is impossible to obtain information on quantum states transmitted from a sender to a recipient without, therefore, altering the states themselves (Vermeer and Peet, 2020, p. 12). It is thus possible to establish symmetrical encryption (and decryption) keys allowing to detect the activity of an interceptor, evaluate the amount of information leaked and take the necessary countermeasures to guarantee the secrecy of the keys themselves (Shenk, 2018). In this perspective, QKD implementations require a public quantum channel and an authenticated public classic channel (Lewis and Travagnin, 2018). The channel authentication is, in fact, central even in the case of conventional cryptography: in order for a "classic" public channel to be encrypted, the sender and recipient must share a short initial secret key (*information theoretically secure*, ITS) with an entropy as big as the message itself (Lewis and Travagnin, 2018). In addition, the key only needs to be used once. For this type of communication, therefore, it is necessary to establish a continuous transmission of extremely long secret keys. From this point of view, QKD can be interpreted as a key expansion technique that has no classical counterparts, as it exploits quantum physics to expand the entropy of the short authentication key to any level required: in other terms, QKD can be employed to obtain a key as long as the message and then encrypt it using a timepad (Lewis and Travagnin, 2018).

Another important property of QKD is universal composability: in fact, when used in conjunction with other cryptographic protocols that are theoretically secure (ITS) and universally composable (UC), the resulting compound cryptographic protocol will also be ITS and UC. One-time pad (OTP) is universally composable, and therefore if used with a QKD expanded key the resulting protocol will be

both UC and ITS: consequently, even an opponent with unlimited computing power (even quantum) will never be able to decipher it (Chen et al., 2018).

Any QKD system requires a quantum channel and an authenticated classic channel to connect sender and receiver. QKD therefore denies an opponent the possibility of a "store now, decrypt later" approach (Lewis and Travagnin, 2018, p. 8). Consequently, to decide which asymmetric encryption algorithm to use and its key length, legitimate parties need only make reasonable assumptions about the compute resources an adversary can deploy during the channel's first authentication. In fact, if authentication is not broken during the first round of QKD, even if it is only computationally secure, all subsequent QKD rounds will be ITS. In this sense, it is usually said that QKD allows you to build long-term unconditional security from short-term assumptions and that under these conditions provides an eternal secret. QKD can therefore be used in conjunction with a public key infrastructure that offers the necessary simplicity and flexibility: even if the asymmetric scheme is deemed secure only for a limited period of time, long-term security is therefore guaranteed by QKD (Vermeer and Peet, 2020).

Eternal secrecy is different from forward secrecy that can be achieved 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 encryption keys that are established in each session are independent of each other and if one of them is compromised at any time only the traffic exchanged during that particular session can be decrypted.

As the literature review emerged, eternal secrecy is a much stronger property and includes forward secrecy, as it only depends on the security of the first round of channel authentication. As the term "unconditional security" is used as a synonym for "information-theoretic security", it needs to be clarified that demonstrated QKD unconditional security is actually based on a number of conditions (Lewis and Travagnin, 2018). The first is to consider the laws of quantum mechanics to be *de facto* valid. As with classic cryptography, the opponent does not have access to the QKD equipment, only the communication channels. Note that the presence in QKD of a public quantum channel next to the classical one allows to exploit possible further specific quantum loopholes alongside the classical ones, while still allowing quantum hacking.[17]

[17] MIT Technology Review (2019). There's a new way to break quantum cryptography. 6 March. Retrieved from https://www.technologyreview.com/2019/03/06/136765/theres-a-new-way-to-break-quantum-cryptography/.

The implementation should be free of non-idealities that are not adequately addressed. This means that every possible side channel that could allow information leakage must be known and adequately characterized: only the so-called device-independent QKD can mitigate this problem, at least to some extent (Lewis and Travagnin, 2018). In particular, the algorithms used for the generation of pseudorandom numbers must pass specific tests of randomness, such as those included in the NIST Statistical Test Suite SP 800-22 (2010).

Elements of strength and weakness, and the future of quantum technologies

The potentiality of quantum computing could be epitomized in quantum supremacy, or the ability of quantum computers to overcome the limits of classical computers. As also described in the previous section, quantum computers are able to perform the task much faster and more efficiently than classical computers ever could, or because the quantum computer has a computing capacity that is impossible for classical devices (The Hague Security Delta, 2019). For instance, quantum simulation could allow a deeper understanding of all complex phenomena in the microcosm and macrocosm, from the folding of proteins, paving the way for greater efficiency in pharmaceutical research, to the simulation of complexity of social phenomena (Thiele, 2020; Reding and Eaton, 2020). While classical computers, in fact, have to sift through the infinite possible states one by one, quantum computers can process all the research results at the same time. Although several players are investing in quantum supremacy (or its perception), this has not yet been achieved (The Hague Security Delta, 2019). Moreover, the use case for a universal quantum computer is also more and more opaque. However, universal computers are by definition unable to solve any problem in a practical timeframe, such as the issue of prime factorization.[18] On the one hand, quantum computers are no substitute for classical computers, and, on the other, they are not simply super-powered computers.[19]

In general, quantum can test the validity of each solution at the same time, whereas a traditional computer would have to test each solution (The Hague Security Delta, 2019). These foreseen possibilities of quantum technologies, and in particular quantum computing, are potentially unlimited and this new computational paradigm can have a considerable impact on other technologies as well such as AI.[20]

[18] Chu, J. (2016). The beginning of the end for encryption schemes? New quantum computer, based on five atoms, factors numbers in a scalable way. MIT News, March 3. Retrieved from https://news.mit.edu/2016/quantum-computer-end-encryption-schemes-0303.

[19] See the seminar held by Dave Bacon (Google) on this issue, demonstrating the quantum supremacy over the world's most powerful supercomputers, and available at https://www.quantumx.washington.edu/quantum-computer-versus-supercomputer.

[20] Google. Quantum. s.d. Retrieved from https://research.google/teams/applied-science/quantum/.

According to some experts, quantum computing is impossible following the current understanding of quantum mechanics[21] Some underlies the devastating technological revolution (The Hague Security Delta, 2019; Reding and Eaton, 2020). However, attempts to answer outstanding practical applications of quantum computers are underway. As emerged from literature and to take up the Hague Security Delta report, there are, however, some significant technical obstacles such as: problems related to (a) decoherence, (b) the development of algorithms, and (c) the technical environment. Decoherence is the loss of quantum coherence, which has to be preserved to perform quantum computations (Zhang et al., 2019). This issue concerns the aspect of quantum computing functionality, while the number of quantum algorithm adaptations is still very limited (The Hague Security Delta, 2019). Moreover, technologies such as machine learning will need to ensure that current algorithms can use quantum computing (The Hague Security Delta, 2019). In this vein, research and studies on quantum machine learning are much more theoretical speculation. This also mainly affects the operationalization perspectives of quantum computing.

For the technical environment, quantum computing requires near absolute zero temperatures, which are extremely difficult, and expensive to achieve and maintain.[22] Another relevant aspect is related to the cost of components for quantum infrastructure, including the current range for terrestrial quantum communication networks limited to 100 km (The Hague Security Delta, 2019).

Moreover, quantum computers are currently non-standardized, with organizations like NIST leading the way for such effort, with an estimated timeframe for the hardware on 1-5 years and the price probabilities ranging around 1-10 billion dollars, limiting the accessibility of the technologies (The Hague Security Delta, 2019). Breakthroughs in quantum computing technology also require significant material investments, while a universal applications timeframe, according to some experts, will happen in 2030 (Reding and Eaton, 2020). Starting from the evidence emerged in this section, the following pages will focus on strategies and practices developed by the most relevant actors on the international arena to achieve a strategic advantage in the quantum technologies race.

[21] See, *inter alia*, the argument of Gil Kalai, who believed that "the effort required to obtain a low enough error level for any implementation of universal quantum circuits increases exponentially with the number of qubits, and thus, quantum computers are not possible." Moskvitch, K. (2018). The Argument Against Quantum Computers. Quanta Magazine, 7 February. Retrieved from https://www.quantamagazine.org/gil-kalais-argument-against-quantum-computers-20180207/.

[22] Microsoft (2021). Quantum Computers and quantum simulators. 2 January. Retrieved from https://docs.microsoft.com/en-us/azure/quantum/overview-quantum-computers-and-simulators.

4. STRATEGIES AND DOCTRINES

As seen in the previous sections, it is safe to state that quantum technology will be the basis of the next scientific and technological revolution. However, for the time being the idea of a diffused use of quantum computing or even quantum internet in our daily existence is still sci-fi material. And it will probably still be that for at least a decade, or even more. What has become indisputable is the necessity for nation states, international institutions, networks of experts, and any other involved stakeholders to debate the upcoming role of quantum in society. In recent years, many states have started to produce a variety of documents dealing with issues linked to quantum.

This section will present an overview of the main national strategies and papers concerning quantum technologies development. The majority of these documents aims at creating a domestic environment capable of supporting research and innovation while considering the economic interests of the state. In spite of their similarities, they still present unique characteristics, especially in the way they are framed within the institutional national framework. While a certain number of states have designed long term investments plans (e.g., UK, Japan, Australia, and even EU), there are only three states that have announced a clear national strategy, focusing on the role of the state in shaping the quantum technologies environment both at home and on the international arena. For the sake of clarity, the section will start with an analysis of the latter documents, and then concentrate on the former ones. However, the choice of a form rather than the other rarely generates any significant divergence in terms of contents. In the end, the section will try to underline any evidence of a new 'quantum doctrine' emerging from the texts.

National Strategies

China

The People's Republic of China (China) pioneered the trend of national strategy already in 2015 with the preparatory works for two capital documents, released an year later. In May 2016, the Central Committee of the Communist Party of China (CCCPC) and State Council of People's Republic of China published a National Strategy for innovation-driven development and in the August of the same year, the 13th Five-year plan was also released (State Council of People's Republic of China, 2016). The five-year plan extended the desire to modernise some aspects of the Chinese economic environment to society as a whole (e.g,, the reform of the one-child policy). What emerged from both documents was the aspiration for the state to become a leading power in disruptive technologies, including the development of quantum communications and computing. It would be wrong to suggest that quantum

played a unique role within this strategy. The so called Made in China 2025 program (State Council of People's Republic of China, 2016, p. 60) encompasses a larger objective, namely the promotion of manufacture innovation based on new, smart, green technologies through the promotion of investments and research in strategic fields and the development of competencies to match this purpose. The same can be said of the Programs for Sci-Tech Innovation 2030 (State Council of People's Republic of China, 2016, p. 25), which include quantum communication and computing as one of the main technological achievements of the country.

The importance of quantum technologies for China became more apparent in recent years thanks to the actual successes obtained in this domain. In 2017, China announced the establishment of the National Laboratory for Quantum Information Science,[23] a 10 billion dollars project, which is approaching its completion these days. Last year, the country achieved two record-breaking feats thanks to the work of a group of scientists from University of Science and Technology in Hefei. In June, the group published an article on Nature demonstrating the possibility to transmit a quantum encoded message between a satellite and two ground-based stations at a distance of approximately 700 miles (ca. 1,120 km), thanks to the application of quantum entanglement.[24] Some months later, in December, the same group declared to have achieved quantum supremacy right after Google's own claim, thus taking a step towards the production of a real quantum computer.[25]

It would be hard to assess the actual level of scientific and technological progress reached by China in this field as the majority of the documents, especially the ones concerning strategic and tactical employment of these technologies, are not disclosed. Moreover, China has just an embryonic industry, whose development will be capital for the promotion of research and innovation outside the universities and research centres where nowadays the majority of quantum experiments are carried on. It is indisputable that China has fulfilled its ambition to become a major player in the emerging technologies international race. Western countries and the United States of America have firstly recognised Chinese prominent role in the field. To some extent the US national strategy, discussed here below, can be perceived as an attempt to chase the Eastern state on the path to lead the way of the quantum revolution.

[23] Kania, E. B. (2018). China's Quantum Future. Foreign Affairs,26 September ,

[24] Broad, W. J. (2020). China reports progress in ultra-secure satellite transmission. The New York Times. 15 June. Retrieved from https://www.nytimes.com/2020/06/15/science/quantum-satellites-china-spying.html.

[25] Simonite, T. (2020). China stakes its claim to Quantum Supremacy. Wired. 13 December. Retrieved from https://www.wired.com/story/china-stakes-claim-quantum-supremacy/

USA

The first national documents in the United States of America (USA) emerged in 2017 in the forms of preparatory work for the National Quantum Initiative Act published in December 2018 (Raymer and Monroe, 2019). However, quantum technologies in the USA have developed since the late 80s. The academy, the private world and even some intelligence agencies already possessed a certain degree of know-how in the field or, at least, of interest in the matter (*ibidem*). The US Congress took a move to promote a stronger collaboration among the involved stakeholders: government, private companies and academia (NSTC, 2018). The main objectives can be synthetized in two macro-category: economy and security. The strategy was delineated on a science-first approach, in order to identify the biggest challenges for the sector. To support these approaches the strategy includes steps to develop a workforce capable of dealing with quantum technologies, a new series of public-private partnerships, and new infrastructures and investments for research. The role of quantum technology in national security is addressed as a part of a bigger picture involving future and emerging threats; quantum technology could represent both a menace and an advantage for nation states. Its role depends also on the capacity of the state to understand and use these technologies in its favour; thus, the importance of developing domestic quantum capacity (*ibidem*, p.15). The Strategic Overview contained also a very short paragraph on the necessity and importance of international cooperation to promote knowledge and new discoveries (*ibidem*, p.16). The following Congress Act (2018) established a complex system of institutions, committees, sub-committees and sub-groups to attain these objectives with a specific attention to the economic and technological advancement rather than the security aspect. As a start, the Act requires a redesign of the institutional ecosystem and the whole strategy after ten years, in order to assess the attainments and progresses achieved over this period of time. Specifically, the Congress confirmed the allocation of federal funds to promote education and private entrepreneurship in this sector. However, the strategy stresses also the importance of improving the collaboration of between industry and academia; only creating a strong and continuous dialogue between these two sectors, it will be possible to develop a workforce based on necessity and to select specific ideas that can help produce scalable solutions for the future application and commercialisation of quantum technologies.

The purposes of the Chinese and US strategies are not so different. Nevertheless, the extent to which national industries and the governments are involved cannot be compared, as the economic market and business environment are so distant one from another. In the USA, the most interesting breakthroughs have been disclosed by private companies; for instance, IBM and Google are competing to develop the first full-fledged quantum computer. Moreover, as already stated above, Google has declared the achievement of quantum supremacy (Kleese van Dam, 2020). It would be wrong, however,

to brush off the public involvement in American research field. In the beginning of 2020, the US Department of Energy (DOE) held a workshop to present its blueprint to create a national quantum Internet. The main aim of the workshop was to put together all the involved stakeholders (industry, government departments, research labs, universities, and other interested parties) to promote the passage from laboratory to real-life experimentation. The DOE aims at integrating, at least in the first steps, the classical networks (particularly optical fiber networks) with quantum instruments (repeaters, communication protocols, and even new types of optical fiber). However, the next phase would be the creation of Quantum Local Area Networks (Q-LAN). Some experiments have already proved the level of knowledge and advancement of such collaboration; in December 2020, a public-private partnership between a group of American universities and the Fermilab successfully transmitted information from one photon to another at a distance of nearly 44 km with an accuracy of 90%.

France

France has been, at the least for the moment, the last county to produce a national strategy, making it impossible to assess the impact of its plan in the long run. The strategy was due already last year, but it was publicly announced only at the beginning of 2021. President Emmanuel Macron delivered a speech on January at the University of Paris (Saclay), unfolding his intention to compete with China and US for a leading position in the emerging technology arena.

The plan focused on two main topics. On one side, President Macron did not shy away from his ambition to promote the role of France in the international arena, as the main catalyst of a future European hub for emerging technology. He highlighted the necessity to mature a national strategy for quantum keeping in mind the importance of collaboration within the European Union institutions and among European countries in order to carve out a place under the sun. In the presentation, he referenced the multinational project to create the first European hybrid system computer, as one of the many conjoint efforts (Macron, 2021).

At the same time, President Macron has pointed out the inevitable domestic transformations that such a grand strategy requires. The national investments would be devoted to the promotion of public-private collaborations and partnerships, and to the development of the human capital needed to sustain such revolution (Macron, 2021). The subsequently published strategy is even more unambiguous in clarifying the exact proportions of the project. France wants to achieve its main objectives (international acknowledgement, development of the first quantum computer, integration of quantum cryptography, etc.) in five years from now, through a diffused investment of nearly 2 billion

euros (SGPI, 2021). The plan seems well-structured and bold in its aspirations. A better assumption on its efficacy and results will be possible only in the next few years.

Plans of Investments

UK

The United Kingdom (UK) has invested in quantum science and technologies since 2013, when it announced the creation of the UK National Quantum Technologies Programme with an initial £270 million investment. The Programme is overseen by the Quantum Technologies Strategic Advisory Board (QT SAB), a body created to coordinate the UK quantum community. The Programme itself established collaboration between public sector and national laboratories. The main goal of the Programme was the transformation of the know-how already achieved in this sector in marketable products. Such an objective requires a strong coordination between government institutions, academy and industry. In 2015, the QT SAB released two documents to set off the path to achieve it: a national strategy in March 2015 and a following roadmap in September 2015. The two documents are strictly correlated and based on five major areas: a strong foundation of capability, the stimulation of applications and market opportunities, the growth of a skilled workforce, the creation of the right social and regulatory context, and the maximisation of benefit through international cooperation (QT SAB, 2015a, and 2015b). In order to complete the national system, the five areas are completed by eight recommendations that outline a 10-year plan to support industry and academia, a series of incentives to encourage private investment, the promotion of collaboration among sectors and the maintenance of its competitive advantage at the international level. (QT SAB. 2015a).

In comparison with the previous mentioned national strategies, that are mostly political statements and long-term projects, the UK documents are definitely more realistic and less utopian. Although based on the same premises as the other documents, the roadmap presents a list of quantum technologies divided by the expected time period necessary for their commercial exploitation. The main objectives are the following: the development of a market for quantum components, the production of technology to improve navigation system, the introduction of quantum sensors (through gravity mapping), the improvement of communication security thanks to the introduction of quantum-safe cryptography, the progress in quantum enhanced imaging (even in medicine), and the elaboration of quantum computer to overcome the current shortcoming of classic computing. The defence and space sectors are identified in the report as some of the main areas for the application of these new quantum technologies. However, in the long run, the primary goal is to create a consumer-friendly quantum technology market. Moreover, a strong focus is pointed at the necessity to develop standards and benchmarks to sustain market growth both at the internal and international levels. The QT SAB stresses

the vital role played by the national hub, as coordinators between industrial and commercial interests and academic researchers.

In 2020, the Programme released a new Strategic Intent that reframed the main objectives of the country as follows: stimulation of industrial production and growth of internal market, preservation of research and knowhow, resilient national network and international cooperation, and environment capable of attracting and growing talents (QT SAB, 2020). Interestingly enough, the areas of applications for quantum technologies have remained unaffected. The Strategic Intent recapitulated the investments carried on in the last years and their results. Currently in the UK there are four major university hubs, concerning sensing and timing, quantum communications, quantum imaging, and quantum computing and simulation. Contrary to other countries, the UK remains strongly grounded to realistic expectations and never mentions in its documents the concept of quantum Internet but as a very futuristic idea. In conclusion, despite the lack of a real national strategy, the quantum community is undeniably thriving.

Israel

Quantum technologies have been in the radar of Israel's defence departments for more than a decade. However, Israel's structured efforts to establish a quantum technology sector only began in 2018, when The National Infrastructure Forum for Research and Development (TELEM), which is part of the Israel Academy of Sciences and Humanities, appointed a special committee to evaluate the subject. This special cohort headed by former Chief Scientist Orna Berry, gathered representatives from all the main government research departments: the Israel Innovation Authority; the Ministry of Science, Technology, and Space; the Ministry of Finance; the Council for Higher Education Planning and Budgeting Committee; and the Ministry of Defense Administration for the Development of Weapons and Technological Infrastructure (MAFAT).

In March 2019, the conclusions resulting from the committee's work led to the understanding that quantum would have dramatically impacted on computer technology as we know it, bringing about permanent disruption in a number of critical fields where Israel nowadays holds a leadership position (such as sensing, communications, cybersecurity, cryptography and computing just to name a few) due to the high quality of its research and development capabilities. It was also evident that being able to muster this new technological challenge would have allowed for the creation of new jobs and consequent economic growth. In order to embrace this paradigm shift and start building the foundations of a brand new sector, the government launched a initial five-year long national plan with an allocated investment of 1.25 billion NIS ($380 millions) that same year, and established the Israel

National Quantum Initiative, a joint venture between the Council for Higher Education, the Israel Innovation Authority, the Ministry of Science, the Ministry of Defense and the Ministry of Finance, in order to manage this programme.[26]

The main goals were to set attractive conditions to enable the growth of a high-quality research community and create an ecosystem for applied research, industrial and defence development, which could ultimately lead to the production of commercially viable applications. The committee also outlined few overarching criteria, such as the ecosystem's high competitiveness and excellence; the openness to foster collaboration at national and international level, due to the unclassified nature of the initiative; and finally the will to devote most of the budget to the direct implementation of strategic goals, therefore keeping a lean and agile management structure.

To fulfil the first objective, many actions have already been focused on building human capital, by recruiting academic staff, defining academic study programs and scholarships, establishing research laboratories and attracting overseas researchers. 10% of the budget was also allocated to the creation of a direct R&D fund that would foster the birth of joint research groups from different universities. Since late 2019, when the first round of applications opened, 10 projects were funded and a second round is now being evaluated. This has already brought about a 25% increase in requests for funding from both researchers and businesses, whose areas of research cover sensing, materials, cryptography, computing and simulation.

Moreover, TELEM identified three major areas of application around which the ecosystem should build its capabilities: sensing, communication and cryptography, and quantum computing. Each field should also have a dedicated consortium who would foster collaboration among existing industry and academic groups for three years before presenting initial results. The sensing consortium began its activities in September 2019 and by now has already produced strategic collaborations among 4 major Israeli corporates and 12 academic groups in the space of atomic clocks, magnetometers, gravimeters and time networks multi sensors.

The second consortium began its work in early 2021 focusing on the R&D of quantum communications technologies across communication systems for server farms, transferring data from a single communication channel to a network, and a secure communication system for transmitting

[26] Wrobel, S. (2021). Israel joins the quantum club. Algemeiner, 26 March. Retrieved from https://www.algemeiner.com/2021/03/26/israel-steps-up-quantum-tech-race-amid-threat-of-exclusion-from-european-research-projects/.

encryption keys. The quantum communications consortium includes industry leaders such as Elisra, Mellanox Technologies, OpSys, and startup Quantum LR, which will work alongside the Ministry of Defense. Academic groups and leading researchers from the Hebrew University of Jerusalem, the Technion – Israel Institute of Technology and others will also join.[27]

Finally, the third consortium recently kicked off preliminary activities around quantum computing. Within this context the Ministry of Defense and the Innovation Authority have been taking bids from multinational companies, Israeli businesses and universities for a 198 million-shekel (50 million euros) project to build a supercomputer with 30 to 40 qubits[28].

From the activities carried out over the past few years, it seems clear that the Israeli quantum community, however small it might still be, has a high degree of expertise and is growing at a significant pace. There are in fact already more than twenty entities, including established corporates and start-ups, who are driving the sector forward by developing either software, hardware or materials, also thanks to the coordinated support provided by the multiple government initiatives whose aim will be to foster further collaboration not only at national level, but also and increasingly so on an international scale.

United Arab Emirates

The evidence is suggesting that, despite being a latecomer to technology and the Digital Revolution, the United Arab Emirates (UAE) is becoming a globally recognized forerunner in the field of new technologies and research, with a specific focus on AIs and blockchain.

In 2020, it was created the Ministry of Industry and Advanced Technology and in the same year it was founded the Advanced Technology Research Council (ATRC)[29]. Technology Innovation Institute (TII), the dedicated 'applied research' pillar of Abu Dhabi's newly established Advanced Technology Research Council (ATRC), in 2021 announced that its Quantum Research Centre (QRC) team led by its Chief Researcher Professor José Ignacio Latorre, will construct the first quantum computer in the UAE capital, in collaboration with Barcelona-based Qilimanjaro Quantum Tech researchers, ushering an

[27] Solomon, S. (2020). 3 R&D consortia seek to boost self-driving, quantum and advanced materials tech. The Times of Israel. 8 June. Retrieved from https://www.timesofisrael.com/3-rd-consortia-seek-to-boost-self-driving-quantum-and-advanced-materials-tech/.

[28] Benmeleh, Y. (2021). Israel allocates $60 million to build the first quantum computer. Bloomberg, 3 March Retrieved from https://www.bloomberg.com/news/articles/2021-03-03/israel-allocates-60-million-to-build-first-quantum-computer.

[29] Advanced Technology Research Council (ATRC) https://www.atrc.ae/

important milestone for the region in this breakthrough era in computing. The projected quantum computer will use quantum mechanics phenomena such as 'superposition' and 'entanglement' to generate and manipulate subatomic particles like electrons or photons – quantum bits also known as 'qubits' – to create exponentially stronger processing powers that can help perform complex calculations that would take much longer to solve even by the world's most powerful classical supercomputers.

Giving us a clear signal of a quite safe bet to expect a new strategy from the UAE focused on quantum technologies, as the state is clearly working to become a major player in the new technologies industry.

EU

The European Union (EU) entered the quantum competition at the end of 2018, thanks to the launch of the Quantum Technologies Flagship by the European Commission. This project represented an attempt to coordinate the Member States' research institutions, industries and even public initiatives in order to exchange knowledge and knowhow. It is part of the Horizon 2020 investment program. The willingness to boost European skills in quantum technologies and cybersecurity is evident in EuroQCI Declaration, signaling their commitment to the EuroQCI initiative signed by seven Member States (Belgium, Germany, Italy, Luxembourg, Malta, the Netherlands, and Spain)[30] during the 2019 Digital Assembly in Bucharest. The final purpose of the declaration was the development of a European quantum communication infrastructure (QCI) that will integrate quantum cryptography and innovative and secure quantum products and systems into conventional communication infrastructures (Quantum Key Distribution), enhancing them with an additional layer of security based on quantum physics. The infrastructure will consist of a terrestrial segment relying on fiber communication networks linking strategic sites at national and cross-border level, and a space segment based on satellites, and linking national quantum communication networks all over the EU and worldwide. It will also include a testing and compliance infrastructure for assessing the compliance of technologies with the new infrastructure and their certification and validation, with a view to their possible integration.

In the long run, the QCI should become the basis of a quantum Internet in Europe, connecting computers, simulators and quantum sensors. In 2020, the Strategic Advisory Board (SAB) of the European Quantum Flagship released a Strategic Research Agenda. The document blends some of the

[30] The Declaration of Collaboration is currently supported by 27 EU countries. The document is available at the following link: https://ec.europa.eu/digital-single-market/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network.

elements contained in the UK National Strategy and the ones contained in its roadmap. In fact, the Agenda is divided in nine areas to be developed: quantum communication, quantum computing, quantum simulation, quantum sensing and metrology, scientific and technological resources, innovation, international cooperation, gender equality, and education and training. Each area is complemented by a specific and thematic roadmap that addresses both the short-term and the long-term challenges for the sector. The report analyses the role of supply chain for the development of technologies and skills. In order to achieve sound results, the agenda encourages a strong integration between public investments, industry and academia.

Meanwhile, the European Commission has selected a consortium of companies and research institutes to design the future European network of quantum communication, EuroQCI. The consortium, led by Airbus, includes Leonardo, Orange, Pwc France and Maghreb, Telespazio (Leonardo 67%, Thales 33%), the National Research Council (CNR) and the National Metrology Research Institute (Inrim). In particular, the study, which will last 15 months, defines the details of the end-to-end system and the design of the terrestrial segment to support the Qkd service and provides for the development of a detailed roadmap, which includes the costs and timing of each phase of implementation. The study will also support the European Commission in implementing an advanced QCI testing and validation infrastructure, which includes standards, with the aim of launching a Euroqci pilot project by 2024 and an initial operational service by 2027.

To date the general forecast is that the Quantum science and technologies is going to receive more than 1 billion euros investments in the next few years within the framework of Horizon Europe (2021-2027).

Italy

Italy already presents some centers of excellence. The Italian National Institute of Nuclear Physics is the only partner outside America collaborating with the USA DOE and the Chicago FermiLab[31]. Moreover, Italy possesses the second longest quantum-ready communication infrastructure in the world, the so called Italian Quantum Backbone (IQB). The network travels for 1850 km from Turin to Matera. In the future, the IQB should become part of the European Quantum Communication Infrastructure (EQCI) and be financed by the European Quantum Flagship investment.

[31] Suman, F., L'Italia insegue il suo vantaggio quantistico, 4 April 2021

In the recent months, Italy has started to acknowledge its potential as a major player in the field of quantum technologies. Thanks to the publication of the National Program for Research (PNR) (2021-2027)[32], the quantum computing and technologies have been recognised as a strategic field in which Italy could have a say at the international level. The final version of the National Plan for Recovery and Resilience (NPRR) contains a chapter promoting the creation of a national reasearch centre for quantum computing. The two documents represent a first important step for Italy to recognise its potential in the field of quantum computing.

General trends and current issues

Quantum science and technologies are starting to change many sectors, from health to navigation, and they are bound to have an even more strong impact in our daily lives in the future. Even though the importance of quantum physics has been evident for decades, states around the world have started to realise the potentiality of its impact in the real world only recently. This should not come as a surprise, as the application of quantum mechanics' concepts to solve problems left behind by classical physics is a major success of current scientific progress. The aforementioned strategies and investment plans are good examples of how enterprising states are intervening to promote collaboration between industry and academia. The clear, common objective is to create a competent national workforce, as well as to achieve a high level of competency in quantum technologies through easily scale-up business ideas. The main challenge in a field as new as this is to come first and come prepared. Many other states have started their own national projects, even though they might have not published yet any political endorsement to national blueprints. Singapore, for instance, has been one of the first to address the issue with the establishment of the Research Centre for Excellence (RCE) in 2007 under the Ministry of Economy. The main focus of the RCE has been the coordination and public funding of national projects concerning quantum technologies33. Australia has also been pioneering the exploration of these innovative technologies for many year and in 2020, the Commonwealth Scientific and Industrial Research Organisation (CSIRO), a government agency, published a report containing indications and suggestions for the government to exploit the knowhow and skills acquired thanks to academia and research centers (CSIRO, 2020).

The list of countries with similar settings is constantly increasing. In spite of the fact that each state has produced peculiar documents, it appears evident that they are all focused on creating a national environment able to produce innovation and expertise. Moreover, the international race to

[32] Ministero dell'università e della ricerca (2021), Programma nazionale per la ricerca, https://www.mur.gov.it/sites/default/files/2021-01/Pnr2021-27.pdf, pp. 105-108
[33] For further information: https://www.nrf.gov.sg/programmes/research-centres-of-excellence

quantum computers and quantum internet is still open and crowded; private companies, governmental projects, university hubs are all competing at each step. Communication, defence and space sectors will be strongly influenced by these technologies. Nevertheless, it would be hard to conceive such progress in less than a couple of decades. Another important issue that should be addressed in the future is the necessity to discuss and produce international standards and benchmarks. Currently, states are announcing strategies and plans to take a political stance, on one hand, and to either unite the skills already existing, or push their development, on the other. It is fair to assume that in the next years the foreseeable, scientific and technological progresses will make it possible for stakeholders to concentrate on governance and standards.

5. CONCLUSIONS AND RECOMMENDATIONS

This paper aimed to introduce the current state of the literature related to quantum technologies, especially aiming to outline what are the main implications and applications fields. Below we briefly point out the main features emerged during the analysis, suggesting useful recommendations in order to fill the existing gaps in this domain.

Quantum appears in many ways to be the next step beyond cyber security, thus stressing the need for a broader understanding, as well as an in-depth gap and risks analysis by decision makers about the topic. The increasing interest demonstrated by both the academia and worldwide governments, the understanding of quantum technologies potential calls for a solid capability of policymakers to develop innovation processes also in relation to cyber security aspects of quantum developments. Moreover, the disruptive effects of quantum in the various fields are highly unpredictable and they could affect other technologies, e.g., enabling functionalities in AI which could lead to social changes or transform the way to conduct war and conflicts. This technological evolution has also cultural, political, and ethical dimensions, which introduce new perspectives on social phenomena. In this view, the threat of quantum computing as the product of a quantum race between the actors of the international arena, including cyber security firms and high-tech companies, could have serious implications for international stability and reshape the current balance of power in the area of new technological advancements.

Nevertheless, quantum technologies are still quite a niche topic, but their advancements are increasingly making steps forward in the political agendas, as the US and Chinese examples demonstrate. There already exists a set of best practices to be used as a role model in analysing quantum technologies further. Currently, the most innovative national frameworks put the main emphasis on the creation of a social, economic and political environment capable of embracing the new industrial revolution and, even more importantly, putting the state among the most innovative ones. As the common objective emerges from the analysis of the various national documents, so does the set of best practices and short-term goals deployed to achieve it. Firstly, great importance is given to multistakeholderism; national institutions, private sectors and academia have to collaborate to achieve an operative equilibrium between theoretical research and marketable innovation. The creation of inter-sectoral, national hubs is, therefore, the second cornerstone on which quantum strategies rely. National hubs are especially significant as tools to review the current state of the art and know-how already achieved by states. Finally, private and public investments are structured as to develop national skill sets and to attract students, researches and experts from abroad. It is clear that the frameworks

are still in their early stages, but the states working on them are contributing in shaping future developments and being part of the next steps for the incoming quantum revolution. Next strategies and related documents will surely be less concerned with preliminary elements and more with the effective standards and norms for the use and marketability of quantum elements.

Overall, it is possible to provide the reader with a set of three major recommendations on the basis of what has been outlined above. First of all, there is a strong necessity to acknowledge the lack of a common security framework applicable to quantum technologies. It is therefore crucial to stress this point in order to provide at an international and institutional level the need to regulate the quantum domain in order to prevent a lack of common guidelines and standards over the coming years. It is important to evaluate the extent to which current cyber security practices and rules related to the IT & Information Systems sectors could be applicable to the quantum revolution as well.

Secondly, there is a need for flexible regulatory strategies in order to adapt to data privacy and intellectual property regulations. This aspect is indeed strictly correlated to the encryption processes and steps forward provided by quantum technologies. At this point, it is strongly recommended to work towards the development and implementation of standards regulating the so-called post-quantum cryptography.

Lastly, another major issue to be dealt with is the interoperability among different national quantum technologies, which will primarily depend on rates of investment and the level of improvements in quantum innovation. Technical standards can give government and industry a common language to speak by creating agreed-upon definitions and ways of measuring quantum computers' performance capabilities. Among the documents and strategies reviewed, very few list 'interoperability' as an issue to be dealt with. The most recent versions of the UK strategy highlight the necessity to produce technical standards for quantum technologies and suggest to open the debate at the international level. International standard, recommendations and norms will surely be required in future to develop and maintain a globalised quantum technologies market and to push the exchange of information among major players. An international normative framework is still a long term scenario, as many states are still struggling to grasp the magnitude of these new technologies, nonetheless a strict necessity. Numerous states, universities and private companies are claiming ground-breaking results from their research and investment programs, but without a commonly accepted framework the operability of these achievements will remain relegated to scientific publications.

Modern societies rely more and more on digital infrastructure and data and securing them from quantum threats is a today challenge for mitigating tomorrow cyber risks. In this vein, quantum

computing poses security issues related to the use of quantum algorithms for breaking classical cryptography. The secure development of quantum methods should arise from the collaboration among governments, academia, and industry. This collaboration should target research in quantum theory, hardware and software, leading to the implementation of new methods to increase the performance of qubits and develop a broader understanding of the ability to affect other advanced technologies. Government, academia and the private sector should together provide a strategic value to the development of quantum technologies, especially if this takes place through a pre-established roadmap with continuous monitoring to guarantee a concrete and efficient execution phase. The roadmap should also have to take into account the cyber security risks with the aim of establishing, for the players in the international arena, an era of quantum-safe cryptography through the development of shared standards and mitigation frameworks.

Concerning the Italian case, the government should acknowledge the vast potential of the country. A national strategy for quantum would lead to three main advantages. First of all, it will be necessary to map in advance the level of know-how already existing, as per the British and French cases, in order to assess strength and weakness of the system. Secondly, the strategy will give a common and organic view on the development of quantum technologies outside the research and university area. In spite of the fact the many Italian universities have projects and plans concerning quantum computing, very few business companies are working on the commercialization of these new technologies, with the exception of the big ones, In order to develop an internal market and to be competitive in the future globalized quantum market, Italy needs to push for the creation of a SMEs' environment. To do so, the government needs to invest largely on valid and concrete projects. Finally, a national document will help Italy to take its place in the international arena. Italy can boast a high level of national competence for quantum technologies and it is up to the political willingness to help capitalize and take advantage of these capabilities.

The impacts of quantum computing on encryption are imminent. Following the proposed framework of the NIST, dealing with post-quantum cryptography at the technical level and from the perspective of the development of quantum-resistant systems has become a security priority for all stakeholders. Moreover, the attention of decision makers should also focus on the capacity of quantum computing on new security attack surfaces. In this view, not only investments in new infrastructures but new skills are required to achieve a decisive strategic advantage in a new evolving international scenario.

Bibliography

Acin, A., et al. "The Quantum Technology Roadmap: a European Community view", *New Journal of Physics*. 21 September 2018, available at: https://iopscience.iop.org/article/10.1088/1367-2630/aad1ea/pdf (March 22, 2021).

Altmann, Y., et al., "Quantum-inspired computational imaging", *Science*, vol. 361, no. 6403, 2018.

Bacon, D., "Quantum Computer Versus Supercomputer", 10 December 2021, available at: https://www.quantumx.washington.edu/quantum-computer-versus-supercomputer/ (March 22, 2021).

Basset, M.G., et al., "Perspectives for Applications of Quantum Imaging", Laser & Photonic Reviews, vol. 13, no. 10, 2019, available at: https://onlinelibrary.wiley.com/doi/full/10.1002/lpor.201900097 (March 22, 2021).

Broad, W.J., "China Reports Progress in Ultra-Secure Satellite Transmission", The New York Times, 15 June 2020, available at: https://www.nytimes.com/2020/06/15/science/quantum-satellites-china-spying.html (March 22, 2021).

Central Committee of the Communist Party of China (CCCPC) and State Council of People's Republic of China, National strategy for innovation-driven development, 19 May 2016, http://www.xinhuanet.com/politics/2016-05/19/c_1118898033.htm (Chinese), https://cset.georgetown.edu/research/outline-of-the-national-innovation-driven-development-strategy/ (English translation) (January 24, 2021).

Chen, F., et al., "Public-key quantum digital signature scheme with one-time pad private-key", *Quantum Information Processing*, vol. 17 no. 10, 2018.

Chu, J., "The beginning of the end for encryption schemes? New quantum computer, based on five atoms, factors numbers in a scalable way", MIT News, March 3, 2016, available at: https://news.mit.edu/2016/quantum-computer-end-encryption-schemes-0303 (March 22, 2021).

Commonwealth Scientific and Industrial Research Organisation (CSIRO), Australia's National Science Agency, *Growing Australia's Quantum Technology Industry*, May 2020.

Defienne, H., "Quantum leap: how we discovered a new way to create a hologram", The Conversation, 17 February 2021, available at: https://theconversation.com/quantum-leap-how-we-discovered-a-new-way-to-create-a-hologram-155056 (March 22, 2021).

Der Derian, J., and Wendt, A., "'Quantizing international relations': The case for quantum approaches to international theory and security practice", Security Dialogue, vol. 51, no. 5, 2020, pp. 399-413.

European Telecommunications Standards Institute (ETSI), "Quantum-safe Cryptography (QSC)". Available at: https://www.etsi.org/technologies/quantum-safe-cryptography (February 22, 2021)

Feng, D., "Review of Quantum navigation", *Earth and Environmental Science*, no. 237, 2019, available at: https://iopscience.iop.org/article/10.1088/1755-1315/237/3/032027/pdf (March 22, 2021).

Foley, C.P., et al., "Is your cybersecurity ready to take the quantum leap?". World Economic Forum, May 2021, available at: https://www.weforum.org/agenda/2021/05/cybersecurity-quantum-computing-algorithms/ (June 1, 2021).

Google, "Quantum", s.d., available at: https://research.google/teams/applied-science/quantum/ (March 22, 2021).

Grove, J., "Bringing the world back in: Revolutions and relations before and after the quantum event", *Security Dialogue*, vol. 51, no. 5, 2020, pp. 414-433.

Grumbling, E., and M. Horowitz, *Quantum Computing: Progress and Prospects*, Washington DC, The National Academies Press, 2018.

IBM, "Quantum Cryptography", s.d., available at: https://researcher.watson.ibm.com/researcher/view_page.php?id=7242 (March 22, 2021).

Inglesant, P., Jirotka, M., and M. Hartswood, "Responsible Innovation in Quantum Technologies applied to Defence and National Security", NQIT (Networked Quantum Information Technologies), 2018.

Johnson, W.J. "Quantum Supremacy and the Regulation of Quantum Technologies", *The Regulatory Review*. 2019

Kania, E. B., "China's Quantum Future", Foreign Affairs, 26 September 2018,

Kleese van Dam, K., 2020, *From Long-distance Entanglement to Building a Nationwide Quantum Internet: Report of the DOE Quantum Internet Blueprint Workshop*, July 2020, U.S. Department of Energy.

Lanzagorta, M., Uhlmann, J., and E. Venegas-Andraca, "Quantum sensing in the maritime environment", OCEANS 2015-MTS/IEEE Washington, 19 October 2015, available at: http://faculty.missouri.edu/uhlmannj/QuantumSensing.pdf (March 22, 2021).

Laurat, J., "World's record entanglement storage sets up a milestone for the European Quantum Internet Alliance", Quantum Flagship, 5 November 2020, available at: https://qt.eu/about-quantum-flagship/newsroom/record-entanglement-storage/ (March 22, 2021).

Lewis, A.M., and Travagnin, M., "The Impact of Quantum Technologies on the EU's future policies", European Commission – Joint Research Centre Science for Policy Report, 2018.

Macron, E., *Présentation de la stratégie nationale sur les technologies quantiques*21 January 2021, Saclay, available at: https://www.elysee.fr/emmanuel-macron/2021/01/21/presentation-de-la-strategie-nationale-sur-les-technologies-quantiques (January 28, 2021).

Marais, A., et al., "The future of quantum biology", Journal of the Royal Society, 14 November 2018, available at: https://royalsocietypublishing.org/doi/10.1098/rsif.2018.0640 (March 22, 2021).

Microsoft, "Quantum Simulators", 2 January 2021, available at: https://docs.microsoft.com/en-us/azure/quantum/user-guide/machines/ (March 22, 2021).

Microsoft, "Quantum Computers and quantum simulators", 2 January 2021, available at: https://docs.microsoft.com/en-us/azure/quantum/overview-quantum-computers-and-simulators (March 22, 2021).Ministero dell'università e della ricerca, (2021), *Programma nazionale per la ricerca (PNR) 2021-2027*, 23rd January 2021, https://www.mur.gov.it/sites/default/files/2021-01/Pnr2021-27.pdf (June 02, 2021)

Mosca, M., and M. Piani, *Quantum Threat Timeline Report*, Global Risk Institute, January 2021.

Moskvitch, K., "The Argument Against Quantum Computers", Quanta Magazine, 7 February 2018, available at: https://www.quantamagazine.org/gil-kalais-argument-against-quantum-computers-20180207/ (March 22, 2021).

MIT Technology Review, "There's a new way to break quantum cryptography", 6 March 2019, available at: https://www.technologyreview.com/2019/03/06/136765/theres-a-new-way-to-break-quantum-cryptography/ (March 22, 2021)

Moody, D., "The Future Is Now: Spreading the Word About Post-Quantum Cryptography", NIST, 2 December 2020, available at: https://csrc.nist.gov/Projects/post-quantum-cryptography/presentations (March 22, 2020).

National Institute of Standards and Technology (NIST), "Post-Quantum Cryptography", 2020, available at: https://csrc.nist.gov/projects/post-quantum-cryptography (March 22, 2021).

National Institute of Standards and Technology (NIST), "The strange world quantum physics", available at: https://www.nist.gov/topics/physics/introduction-new-quantum-revolution/strange-world-quantum-physics (March 22, 2021).

National Institute of Standards and Technology (NIST), "Quantum Supremacy", 2018, available at: https://www.nist.gov/topics/physics/introduction-new-quantum-revolution/quantum-supremacy (March 22, 2021).

National Science & Technology Council (NSTC), *National Strategic overview for Quantum Information Science*, September 2018, available at: https://www.quantum.gov/wp-content/uploads/2020/10/2018_NSTC_National_Strategic_Overview_QIS.pdf (January 21, 2021).

Quantum Flagship. "Big Data boosting AI", available at: https://qt.eu/discover-quantum/applications-of-qt/big-data-boosting-ai/ (March 22, 2021).

Quantum Flagship's Strategic Advisory Board (SAB), *Strategic Research Agenda (SRA)*, 3 March 2020, available at:: https://ec.europa.eu/digital-single-market/en/news/new-strategic-research-agenda-quantum-technologies (January 24, 2021).

Quantum Technologies Strategic Advisory Board (QT SAB), *Strategic intent*, 6 November 2020, available at: https://uknqt.epsrc.ac.uk/files/strategicintent2020/ (January 24, 2021).

Quantum Technologies Strategic Advisory Board (QT SAB), *National strategy for quantum technologies. A new era for the UK*, March 2015a available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/414788/Strategy_QuantumTechnology_T15-080_final.pdf (January 21, 2021).

Quantum Technologies Strategic Advisory Board (QT SAB), *A roadmap for quantum technologies in the UK*, September 2015b, 21 January 2021, available at: https://epsrc.ukri.org/newsevents/pubs/quantumtechroadmap/ (January 21, 2021).

Raymer, M. G., and C. Monroe, *The US National Quantum Initiative*, Quantum Science and Tecnology 4 (2019), available at: https://iopscience.iop.org/article/10.1088/2058-9565/ab0441 (January 21, 2021).

Reding, D. F., and J. Eaton. "NATO Science & Technology Organization", NATO, Belgium. March 2020.

Rukhin, A., et al., "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications", NIST Statistical Test Suite SP 800-22, 2010.

Secrétariat Général pour l'Investissement (SGPI), *Stratégie nationale sur les technologies quantiques*, 21st January 2021, Saclay, available at: :

https://www.gouvernement.fr/sites/default/files/contenu/piece-jointe/2021/01/dossier_de_presse_quantique_vfinale.pdf (February 7, 2021).

Shenk, M., *The Quantum Countdown Quantum Computing And The Future Of Smart Ledger Encryption*, Zug, Cardano Foundation, 2018.

Simonite, T., "China stakes its claim to Quantum Supremacy", *Wired*, 13 December 2020, available at: https://www.wired.com/story/china-stakes-claim-quantum-supremacy/ (February 8, 2021).

Simons Institute, "Quantum Cryptography (Beyond QKD)", YouTube Video, 27 April 2020, available at: https://www.youtube.com/watch?v=kNcgLqWjV0A (March 22, 2021).

Smith III, F.L., "Quantum technology hype and national security", *Security Dialogue*, vol. 51, no. 5, 2020.

State Council of the People's Republic of China, The 13th five-year plan for economic and social development of the People's Republic of China (2016-2020), 8 August 2016, available at: http://www.gov.cn/zhengce/content/2016-08/08/content_5098072.htm (Chinese), https://en.ndrc.gov.cn/newsrelease_8232/201612/P020191101481868235378.pdf (English translation) (January 24, 2021).

Suman, F., (2021), 'L'Italia insegue il suo vantaggio quantistico', Nature Italy, 4th April 2021, https://www.nature.com/articles/d43978-021-00041-6, (June 01, 2021)

The Hague Security Delta, *Understanding the Strategic and Technical Significance of Technology for Security IImplications of Quantum Computing within the Cybersecurity Domain*, 2020.

Thiele, R., "Quantum sciences – A disruptive innovation in hybrid warfare", The European Centre of Excellence for Countering Hybrid Threats, Working Paper 7, March 2020.

Thomas, M.L., "Evolution of GPS Systems Architecture and Its Impacts", Communications of the IIMA, vol. 10, no. 4, 2010, pp. 27-40, available at: https://scholarworks.lib.csusb.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1148&context=ciima (March 22, 2021).

Vermeer, M.J.D., and Peet, E.D., *Securing Communications in the Quantum Computing Age. Managing the Risks to Encryption*, Santa Monica, Rand Corporation, 2020.

Wendt, A., *Quantum Mind and Social Science*, Cambridge, Cambridge University Press, 2015.

Zhang, Y., et al., "Optimizing Quantum Programs against Decoherence: Delaying Qubits into Quantum Superposition", 13th International Symposium on Theoretical Aspects of Software Engineering (TASE), July 29 – August 1, 2019, available at: https://arxiv.org/pdf/1904.09041.pdf (March 22, 2021).

115th Congress House, *H.R. 6227 – National Quantum Initiative Act*, 21 December 2018, available at: https://www.congress.gov/bill/115th-congress/house-bill/6227/actions?KWICView=false (January 21, 2021).

Center for Cyber Security and International Relations Studies (CCSIRS)

Interdepartmental Center for Strategic, International and Entrepreneurial Studies (CSSII)

Department of Social and Political Sciences
University of Florence
Via delle Pandette 32
50127 Firenze

www.cssii.unifi.it
cyber@cssii.unifi.it