

QUANTUM TECHNOLOGIES AND CYBERSECURITY

TECHNOLOGY, GOVERNANCE AND POLICY CHALLENGES

Rapporteurs: Lorenzo Pupillo

Afonso Ferreira

Valtteri Lipiäinen

Carolina Polito



TASK FORCE REPORT



This study reflects the discussions among members of the Task Force on Quantum Technologies and Cybersecurity. It was composed of industry experts, representatives of European institutions and agencies, intergovernmental organisations, academics, researchers, civil society organisations and practitioners. It met three times between March and June 2023.

The views expressed in this report do not necessarily reflect the views and positions of the members of the Task Force, or the views of their respective organisations. The members do not necessarily agree with all the positions put forward or necessarily endorse the references to academic and independent studies. A robust and clear set of principles have guided the drafting process to preserve a balanced approach to a variety of views. All members were given ample opportunity to express their views. The content of the report and any remaining errors, however, are solely attributable to the rapporteurs.

Suggested citation: Pupillo, L., Ferreira, A., Lipiainien, V. and Polito, C. (2023), *Quantum Technologies and Cybersecurity: Technology, governance and policy challenges*, Task Force Report, Centre for European Policy Studies, Brussels.

ISBN 978-94-6138-793-6

© Copyright 2023, CEPS

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, mechanical, photocopying, recording or otherwise – without the prior permission of the Centre for European Policy Studies.

CEPS

Place du Congrès 1, B-1000 Brussels Tel:32(0)22293911

email: info@ceps.eu; www.ceps.eu

CONTENTS

- List of abbreviations..... 1
- Preface 2
- Executive Summary 3
- 1. Quantum technologies..... 8**
 - The second quantum revolution 8
 - Quantum computing and quantum advantage..... 14
 - Other quantum technologies 17
 - Public funding and the economic impact of quantum technologies 18
 - Quantum technologies – A global overview 19
- 2. Quantum technologies and cybersecurity.....20**
 - The effect of quantum technologies on cybersecurity 20
 - Why we need to act now – Mosca’s inequality 24
- 3. Quantum-resistant cryptography.....28**
 - Overview of quantum-resistant cryptography 28
 - Migration to quantum-resistant cryptography 31
 - Large enterprises and cryptographic agility 34
- 4. Quantum cryptography37**
 - Quantum key distribution – Advantages and disadvantages 37
 - Quantum random number generators 39
- 5. Ethical, governance and policy issues of quantum technologies.....40**
 - Introduction 40
 - Responsible quantum technologies 41
 - Equitable access to quantum technologies 45
 - Quantum technologies and privacy 48
 - Governance of quantum technologies..... 48
- 6. Quantum technologies and cybersecurity: Policy implications50**
 - Introduction 50
 - Policies to foster the standardisation of quantum-resistant cryptography 51
 - Policy initiatives to assess the potential risks and threats of quantum technologies 53
 - Policies for the transition to quantum-resistant cryptography..... 54
 - International coordination and the sharing of best practices..... 60
 - Promotion of enhanced quantum awareness in the public and private sectors 61
 - A future-ready workforce with quantum skills 61

Openness of research	63
Dual-use export control policies	64
Civilian and military coordination and cooperation	67
Possible future research areas of quantum technologies linked with cybersecurity.....	70
7. Policy recommendations	72
Bibliography.....	79
Appendix A. List of Task Force members and invited speakers.....	83
Appendix B. Quantum technology in the EU and rest of the world	86
Appendix C. Examples of the transition to quantum-resistant cryptography in selected countries.....	97

List of Boxes, Figures and Tables

Box 1. The double-slit experiment.....	11
Box 2. NIST standardisation competition.....	30
Box 3. Migrating to quantum-resistant signatures later than quantum-resistant key exchange*	32
Box 4. Quantum exceptionalism and ethics	40
Box 5. Fostering equitable quantum access: The Open Quantum Institute	46
Box 6. Standardisation policies beyond NIST*	52
Box 7. In detail: The NCCoE PQC project	56
Figure 1. Illustration of the power of qubits	10
Figure 2. Quantum technologies – Estimated value unlocked by applying quantum technologies in various industries	18
Figure 3. Expert estimates of the likelihood of a quantum computer breaking RSA-2048 in 24 hours (different time frames)	22
Figure 4. Quantum Readiness Toolkit	35
Figure 5. Public and private financing for quantum technologies worldwide	45
Figure 6. TNO PQC Migration Handbook, post-quantum cryptography personas.....	58
Figure 7. Decision tree for migration scenarios.....	59
Figure 8. Quantum skills gap.....	62
Figure 9. Timeline for the NATO quantum strategy.....	68
Figure B1.1 Wave behaviour in double-slit experiment	11
Figure B1.2 Particle behaviour in double-slit experiment	12
Figure B1.3 Quantum behaviour of electrons in double-slit experiment	12
Figure B7.1 Timeline for NCCoE migration to quantum-resistant cryptography	57
Table 1. Principles of Responsible Quantum Technologies	43
Table B.1. Quantum funding in the EU (EUR million).....	86
Table B.2. Plans and policies implemented by the Chinese government from 1986 to 2018 ..	94

LIST OF ABBREVIATIONS

AI	Artificial intelligence
AIVD	General Intelligence and Security Service
ANSSI	Agence nationale de la sécurité des systèmes d'information
ASD	Australian Signals Directorate
BSI	Federal Office for Information Security
CISA	Cybersecurity and Infrastructure Security Agency
CRQC	Cryptographically relevant quantum computer
DOE	Department of Energy
EuroHPC JU	European High-Performance Computing Joint Undertaking
EuroQCI	European Quantum Communication Infrastructure
FDI	Foreign direct investment
IETF	Internet Engineering Task Force
IoT	Internet of Things
IPCEI	Important Projects of Common European Interest
IRIS ²	Infrastructure for Resilience, Interconnectivity and Security by Satellite
KEM	Key encapsulation mechanism
NCCoE	National Cybersecurity Center of Excellence
NCSC	National Cyber Security Centre
NDAA	National Defence Authorization Act
NICT	National Institute of Information and Communications Technology
NISQ	Noisy intermediate-scale quantum
NIST	National Institute for Standards and Technology
PQC	Post-Quantum Cryptography
QCI	Quantum communication infrastructure
QKD	Quantum key distribution
QRNG	Quantum random number generator
RSA	Rivest–Shamir–Adleman
SDG	Sustainable Development Goal
STEM	Science, technology, engineering and mathematics
TLS	Transport layer security
TTC	Trade and Technology Council
WEF	World Economic Forum



PREFACE

This report is based on discussions of the CEPS Task Force on Quantum Technologies and Cybersecurity. The Task Force was composed of industry experts, representatives of European institutions and agencies, intergovernmental organisations, academics, researchers, civil society organisations and practitioners (see the list of participants in Appendix A). The activity of the group started in March 2023; it met on three separate occasions and continued until October 2023.

The report is divided into seven chapters that explain different aspects of quantum technologies and their policy implications. While we recommend reading the entire document, Readers may wish to note that the first four chapters are best suited to a technical audience, whereas the later chapters could inform lawmakers and policymakers. Therefore, we have included a brief summary at the beginning of the first four chapters to provide an easy read for people who would like to jump to the policy chapters (5 to 7).

As Coordinator of the Task Force, I would like to acknowledge the invaluable contributions of all the participants in this work. Particular thanks go to the members of the Advisory Board: Sabrina Maniscalco at the University of Helsinki, Michael Osborne at the IBM Research Division in Zurich, Bart Preenel at KU Leuven and Tim Watson at the Alan Turing Institute in London.

I also wish to acknowledge the substantial work done by my fellow rapporteurs Afonso Ferreira, Valtteri Lipiäinen and Carolina Polito. I would further like to thank Michela Giuricich for her contribution to the preparatory work of this Task Force. This work has been a collective endeavour and, as indicated in the text itself, other Task Force participants have directly contributed their expertise by personally commenting on selected sections of the report. Thanks also go to the invited speakers who contributed to the Task Force discussions.

Lorenzo Pupillo

Coordinator and Rapporteur of the Task Force
Associate Senior Research Fellow
Head of the Cybersecurity@CEPS Initiative

CEPS, Brussels
December 2023



EXECUTIVE SUMMARY

The Centre for European Policy Studies launched a Task Force on Quantum Technologies and Cybersecurity in March 2023. The goal of this Task Force was to draw attention to the technical, ethical, market and governance challenges posed by the intersection of quantum technologies and cybersecurity. The Task Force, multistakeholder by design, was composed of nine private organisations, six EU institutions and agencies, one international, one multilateral and one intergovernmental organisation, five universities and think tanks, two national research agencies and one civil society organisation (see the list of participants in Appendix A).

The group explored ways to formulate practical guidelines for governments and businesses to ease the adoption of quantum technologies in the EU while addressing the cybersecurity risks associated with the implementation of quantum technologies. These discussions led to policy recommendations for EU institutions, Member States, the private sector and the research community for the development and deployment of quantum-safe technologies.

We are now living through a quantum revolution, with modern technology allowing us to directly manipulate individual quantum systems and fully utilise quantum phenomena. These breakthroughs, a long time in the making, are enabling a new class of technologies based on quantum mechanics. Advances in quantum technologies may drastically change the world as we know it. They are expected to positively impact on many sectors of the global economy, including pharmaceuticals, climate and weather modelling, and financial portfolio management. Specific applications could be used for molecular simulation to upgrade electric vehicle batteries, optimise traffic flows in our cities or improve generative models that create datasets to enhance machine learning. These benefits come from the computational advantages of problem-solving in totally novel and different ways compared with using traditional computers.

At the same time, this new computational power also has a negative side, which explains why quantum technologies are relevant to cybersecurity. While there are some benefits to using quantum technologies to bolster cybersecurity, the most important link is that a large quantum computer could break widely used cryptographic algorithms, breaching confidential data. Most internet applications rely on cryptography to guarantee the confidentiality, authenticity and integrity of data. A cryptographically relevant quantum computer (CRQC) that breaks cryptographic algorithms would have major implications for cybersecurity.

Currently, existing quantum computers are too small and error-prone to be a threat. According to experts, a CRQC is unlikely to surface in the next 5-10 years, but is very likely in the next 30 years. Nevertheless, responding to the threat should start long before CRQCs become available, for two main reasons. First, sensitive encrypted data can be stored and subsequently decrypted with a CRQC (hack now, decrypt later!). Second, the process of transitioning to new types of cryptography that can help mitigate this threat takes a long time.

Indeed, quantum computers only give a boost on certain classes of mathematical problems, so it is possible to develop cryptography based on mathematical problems that are resistant to attack by quantum computers. Quantum-resistant cryptography can thus help mitigate the threat posed by quantum computers.

It is lucky that these solutions exist, but there are still hurdles to overcome: quantum-resistant cryptography is not a drop-in solution, so starting to use it will require a potentially complicated process of migration. Also, standards need to be written both for quantum-resistant cryptography and for many protocols that make use of cryptography. In short, the transition to quantum-resistant cryptography is a lengthy process. It will require careful planning and must be started well in advance of the availability of CRQCs. Cryptographic agility¹ should be kept in mind during the process, to make similar transitions smoother in the future.

As the new world of quantum technologies emerges, we need to seize the opportunity to decide how quantum technologies can help us promote better societies and a more sustainable future. At present, our understanding of the potential impact of quantum technologies remains incomplete. Given the risks arising from the development of quantum technologies that we are currently unaware of and therefore not yet considering, perspectives on the impact of quantum technologies should be broadened to contemplate the wider societal implications that may arise from quantum technological advances. This means addressing several societal issues, among others equitable access to these solutions, ethical development and respect for human rights.

Furthermore, governing quantum technologies presents unique challenges. This field is not only evolving at an unprecedented speed, but also our current understanding of the technology, its use-cases and its potential interconnections with other emerging and unpredictable technologies (such as generative artificial intelligence and large language models) is still quite limited. Therefore, as we move further in the development of quantum technologies it is important to promote responsible governance of quantum technologies, where the term *responsible* refers to the use of 'quantum technologies that are aware of the power of their effects'². Some general principles for responsible quantum could include, for instance, safeguarding against risks and engaging stakeholders in the process of developing quantum technologies.

On governing the interplay of quantum technologies and cybersecurity, this report seeks to support EU initiatives to create a robust policy framework. This will facilitate the integration of quantum technologies while addressing the challenges they pose to information security.

¹ Cryptographic agility is the ability to change the cryptographic building blocks in an application in a fast and painless way. This may mean technical solutions that make switches easy, but it also encompasses measures taken at an organisational level.

² As described by Mira Wolf-Bauwens in *Ethics, Governance and Politics of Responsible Quantum Computing*, presentation at the Third Meeting of the Quantum Technologies and Cybersecurity Task Force in 2023.

The report highlights the need to funnel EU funding into quantum-resistant cryptography, including the cryptanalysis needed to test new solutions, best practices for IT system migration and cryptographic agility. The report also underscores the importance of starting the transition to quantum-resistant cryptography well in advance, considering the complexity and length of the process, and recommends a hybrid approach during the transition period. It emphasises the need for a coordinated European strategy and policy for this transition, alongside the importance of international collaboration and standardisation.

Moreover, it is crucial to encourage initiatives to assess the potential risks and threats posed by quantum technologies. Countries like the US have recognised this urgency and are requiring organisations to comprehensively assess quantum risks. Additionally, it is imperative to promote awareness, address the talent gap in the quantum sector, invest in the development of quantum and cybersecurity skills, and modernise enforcement methods, such as dual-use export controls.

More in detail, **this Task Force makes the following recommendations to policymakers, the private sector and the research community.**

Support research at the intersection of quantum technologies and cybersecurity

It is increasingly important to continue advancing research in quantum technologies and in particular to understand how the impact of quantum technologies on cybersecurity will affect the digital ecosystem. This Task Force recommends these priorities for European research funding in the short term:

- quantum-resistant cryptography, including the corresponding cryptanalysis,
- best practices for migrating IT systems,
- cryptographic agility.

Promote cryptographic agility and coordination policies at the EU level to ease the transition to quantum-resistant cryptography

Shifting to quantum-resistant cryptography is a complex and very lengthy process. It will require careful planning and must be started well ahead of the availability of CRQCs.

We recommend having **cryptographic agility as a priority** in mind when planning the transition to quantum-resistant cryptography and **using hybrid schemes**, which employ both classical and quantum-resistant algorithms.

Furthermore, policies for the transition to quantum-resistant cryptography should be **coordinated at the EU level** through **the establishment of ad-hoc projects** (like the Post-Quantum Cryptography project of the US National Cybersecurity Center of Excellence) for sharing guidelines and best practices among Member States.

Foster the standardisation of quantum-resistant cryptography

The EU could place greater emphasis on the value of **contributions by EU researchers to the standardisation process**. By highlighting the contributions of its researchers, the EU could position itself as a cornerstone of the global standardisation process. To bolster its standing and foster further innovation, it is essential to ramp up research funding within the EU.

Encourage initiatives to assess the potential risks and threats posed by quantum technologies

Organisations with their own cryptographic infrastructure should incorporate quantum-resistance planning for the future. As a starting point for the transition of an organisation to quantum-resistant cryptography, we recommend carrying out a **quantum vulnerability assessment**.

The US National Defence Authorization Act of 2021, mandating the US Department of Defence to conduct such a comprehensive assessment of potential risks, goes in this direction.

The European Commission could promote a similar initiative through recommendations to guide Member States and companies on how to approach the cybersecurity risk aspects of quantum computing technologies.

Apply a principles-based approach to quantum governance and strengthen international coordination

In light of the rapidly changing landscape of quantum technologies, we recommend a governance approach that could limit risks without stifling exploration of the potential quantum technologies hold.

In this context, a **principles-based approach to governance** could be advantageous. Some general principles for quantum-responsible governance could include, for instance, safeguarding against risks and engaging stakeholders in the process of developing quantum technologies.

In applying such principles, one governance strategy might **involve the use of [regulatory sandboxes](#)** for areas that are not yet fully understood or that may carry higher risks. This would provide a controlled environment in which government and industry could come together to develop, deploy and test quantum and quantum-hybrid applications for use in the near term.

Enhance quantum awareness in both the public and private sectors

In the report, we stress the worrisome low level of quantum awareness across sectors, especially on the interplay between quantum technologies and cybersecurity.

We recommend promoting **awareness campaigns to both public and private organisations**. In this vein, the EU could support the creation of platforms for direct interaction with quantum experts or for showcasing best practices in quantum technology applications and the quantum transition.

Implement policies to promote a future-ready workforce with quantum and cybersecurity skills

In the report, we show the huge talent gap in the quantum sector. Organisations looking to fill such a talent gap should not only identify their talent needs but also diversify the talent pipeline and focus on talent retention.

We strongly recommend that the European Commission prioritises **investment in developing quantum skills**, specifically in the **intersection of quantum technology and cybersecurity**, to foster a new generation of experts.

Update dual-use and export control policies

Openness in quantum technology research can speed up progress, but it also risks misuse by malicious actors. While open collaboration fosters innovation, there are concerns about national security and the protection of critical information. The issue of openness in research is directly related to that of dual-use export controls, which come into play when states judge that there is a need to restrict the international transfer of certain technologies.

In this context, **the EU should consider updating its export control systems**. Indeed, there is a lack of clarity on how dual-use export controls affect a non-resident using a quantum computer through the cloud. This highlights the urgency of modernising enforcement methods to ensure that tools like export controls remain relevant and effective.

Furthermore, the EU can play a valuable role through, for example, the EU-US Trade and Technology Council, in facilitating transparency, information exchange and cooperation on quantum value-chain policies.



1. QUANTUM TECHNOLOGIES

Summary

Quantum technologies use phenomena from quantum mechanics to enable new functionalities. High-value sectors in which they could be used include the life sciences, chemistry and finance. Their potential value has been estimated at USD 1.3 [trillion](#) by 2035. Today, by and large, these technologies are not ready for the market.

Governments across the world have launched initiatives on quantum technologies, including public funding for research, the procurement of devices and coordination of research efforts. The EU and its Member States have committed roughly EUR 10 billion in funding since 2016, making the EU a leader in terms of public funding.

At the beginning of the 1900s, quantum mechanics transformed the science of physics and led to a more thorough understanding of the natural world. Even though these insights have been valuable in both research and practical applications, so far we have not been able to reap all of the possible benefits of quantum phenomena. The world is on the way to being able to engineer individual quantum systems, such as a single photon, which allows the use of counterintuitive properties of quantum mechanics and gives rise to innovative technologies in the fields of communications and computing. This scientific advance is sometimes called the second quantum revolution (Dowling & Milburn, 2003)³. Recent advances in this area have driven interest from both the private and public sectors, which in turn has helped the field to accelerate even further.

This chapter covers the basics of quantum technologies, including quantum computing, and provides an overview of the status of quantum technologies in the EU and the rest of the world.

The second quantum revolution

Quantum mechanics studies the way nature behaves at the atomic and subatomic level. It describes many quantum phenomena that are counterintuitive in our day-to-day life. We are now living through a second quantum revolution, with modern technology giving us the means to directly manipulate individual quantum systems and fully utilise these quantum phenomena. These breakthroughs, a long time in the making, are enabling a new class of technologies based on quantum mechanics.

³ The first quantum revolution, in this metaphor, can refer either to the discovery of quantum mechanics, or the first wave of technologies utilising this new type of physics.

These new quantum technologies rely on very small systems, such as individual particles, exhibiting specific quantum phenomena. As a rule, quantum phenomena are fragile and can easily be disturbed. For this reason, quantum technologies require intricate, specialised technology. Especially in the case of quantum computers, this means devices that are sealed off from the outside world, often in very cold environments.

There are a variety of different quantum technologies. Probably the most famous are quantum computers that use quantum bits, called qubits, to make certain computations much faster than has been possible so far. They have applications in a wide variety of fields, including life sciences, financial services and logistics. However, this is not the only type of quantum technology. Quantum communication allows for provably secure communications; quantum sensing provides for vastly improved accuracy of measurements; and quantum random number generators can produce true randomness based on quantum phenomena.

These technologies are at different stages of development: all are based on theoretical ideas presented decades ago, but not all are yet ready for the market, with the notable exception of quantum communications and quantum sensing. There are also well-established technologies that make use of quantum mechanical properties, such as lasers and MRIs, but these are not based on manipulating the quantum state of individual particles. This report focuses on the newer kinds of quantum technology, where there is more disruptive potential.

The two main quantum properties that quantum technologies leverage are quantum superposition and quantum entanglement.

Quantum superposition refers to the idea that a quantum system, such as a particle, can assume different states at the same time. Intuitively, a single particle should only be able to be in a single state at once. For instance, it should have one specific position and momentum. Yet, in the quantum world, this is not the case. A particle can be in a superposition of two different states. When the state of the particle is measured, it has a given probability of being in either state, but until then it behaves in a way that can only be explained by it being in both states at once. An example of the use of superposition comes from quantum computing. Classical bits assume a value of either 1 or 0. Qubits, on the other hand, can assume at the same time a position of 1 and 0. This gives rise to a class of algorithms called quantum algorithms, which operate in a fundamentally different way from classical ones, giving quantum computers an edge over classical computers.

Figure 1 shows the advantages of using qubits. Using only n qubits, it is possible to simultaneously compute 2^n values. With just 270 qubits you could have more different and simultaneous combinations (base states) in a quantum computer than the number of atoms in the universe, estimated to be approximately 10^{80} (Allende López & Da Silva, 2019).

A quantum system can only be in a superposition of two states until it is measured, when it collapses to just one of the two states. This is the fundamental difficulty of using quantum superposition. Specialised hardware has to be built so that it is possible to manipulate the quantum state without measuring it. This requires isolating it from the outside world.

Figure 1. Illustration of the power of qubits



Source: Allende López & Da Silva (2019), p. 13.

Quantum entanglement refers to the ability of two quantum systems to share information even at a distance. This happens when the state of two different particles become entangled: the state of one particle determines the state of the other. ‘Entanglement is to computing what nuclear fusion is to explosives: a property of the subatomic world that can be harnessed to create technology of unprecedented power’ (Witt, 2022). Quantum entanglement is required for quantum computation: it is what allows the qubits in a quantum computer to interact in quantum algorithms. Quantum entanglement is also central to some types of quantum key distribution, where the presence of an eavesdropper is revealed by a change in the state of an entangled particle.

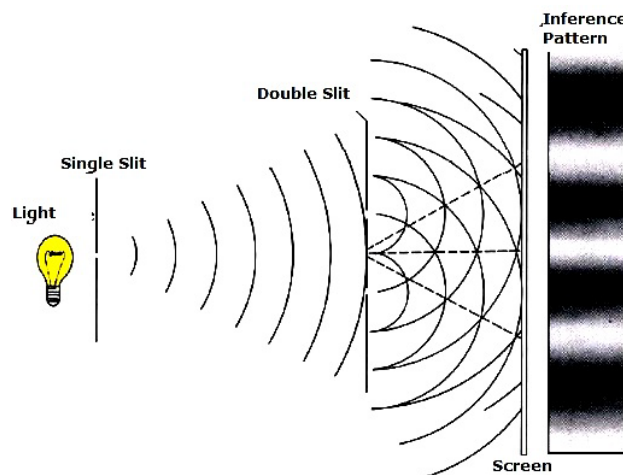
The mathematical implications of quantum physics are uniquely hard to interpret and visualise since they defy what our common sense and imagination can grasp. The very concept of the reality of microscopic particles is peculiar. One of the first problems of the founding father of quantum physics – the Nobel laureate Richard Feynman – was precisely conceiving microscopic particles as existing in the *real* world.

(Allende López & Da Silva, 2019, p. 13) A very famous experiment in quantum physics that relates to the challenges of conceiving *existence* in the quantum dimension is the double-slit experiment (see Box 1). Feynman called it ‘a phenomenon which is impossible ... to explain in any classical way, and which has in it the heart of quantum mechanics’ (Feynman et al., 1965).

Box 1. The double-slit experiment

The double-slit experiment displays the fundamentally probabilistic nature of quantum mechanical phenomena. This type of experiment was first performed by Thomas Young in 1801, as a demonstration of the wave behaviour of visible light. The experiment was originally conceived to show that light passing through a double-slit moves like a wave. As a wave, light creates an interference pattern of white and dark bands on the background screen on the right (Figure B1.1).

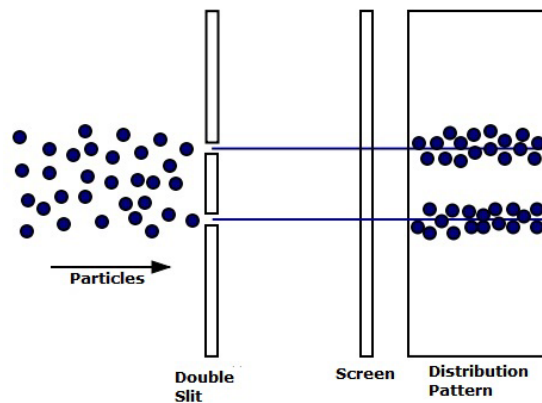
Figure B1.1 Wave behaviour in double-slit experiment



Source: '[Double Slit Experiment](#)', Mysearch Website.

In this context, it was expected that if the experiment were repeated with an electron, the electron would behave as a particle. Particles do not cross paths behind the slits and do not interfere with each other. The distribution pattern is hence very different from that of waves (Figure B1.2).

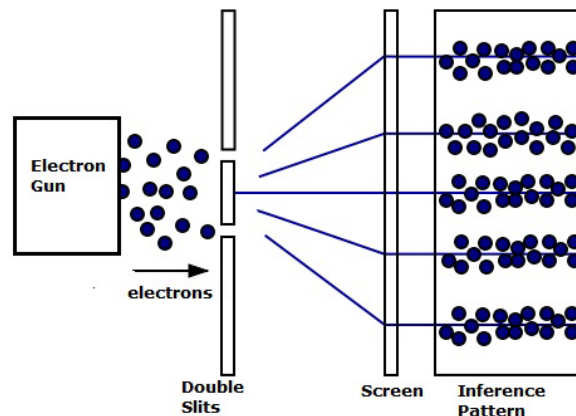
Figure B1.2 Particle behaviour in double-slit experiment



Source: 'Double Slit Experiment', Mysearch Website .

Unexpectedly, when the experiment was performed with electrons, even though the electrons were fired one after another (avoiding any waves interfering with each other) the resulting image after firing electrons was like the interference pattern created by a continuous stream of light (Figure B1.3). The only possible explanation for this distribution pattern was that a single electron was travelling through both slits at the same time, creating waves at both slits and then interfering with itself. This is intimately linked to the algebraic formula of electrons, according to which they can be described as probability waves. This probability wave explains the superposition property of quantum particles described above.

Figure B1.3 Quantum behaviour of electrons in double-slit experiment



Source: 'Double Slit Experiment', Mysearch Website.

Technological development roadmap

The development of quantum computers is accelerating, as investment leads to theoretical and engineering advances. Thus, the road towards technological readiness is getting steeper. Around 5 years ago, quantum technologies were very complex pieces of scientific apparatus held in laboratories. Nowadays, quantum computers⁴ are arriving at data centres and prototypes are being moved to different research laboratories. As such, the community of people experimenting with quantum technologies is increasing and technological progress will likely occur faster.

However, quantum technologies for commercial applications, especially quantum computing, are still far from the required readiness level. Major roadblocks include the lack of workforce and unsolved technical issues. As such, diversified and long-term investment is needed from both the private and public sectors. Among others, investment in fundamental and applied research is pivotal, as this is the building block behind all quantum technology applications. Quantum technologies face barriers to scale. In particular for quantum computers, they face barriers to scale in the form of supply chain needs and workforce needs. Industry and government must focus on these barriers to scale or risk slowing down the path to a quantum supercomputer or a universal quantum computer. Late starters, in this context, will inevitably lose the technological race.

As mentioned, quantum technologies have very different applications, including quantum computing, quantum communication and cryptography, quantum simulators, quantum sensing, quantum metrology, quantum optics, etc. They can be divided into three main families. Each of them exhibits a different level of technological readiness, although advances in engineering and control, software and theory, and education and training are needed for all these families of quantum technologies.

- **Computation.** Most prototypes today are noisy, imperfect and not fault-tolerant, with limited commercialisation. Existing applications of quantum computing include:
 - noisy intermediate-scale quantum computers
 - quantum emulators/simulators
 - quantum annealers
 - universal quantum computers.

⁴ At the moment, noisy intermediate-scale quantum machines.

- **Communication.** Companies have already started selling some quantum communication devices⁵. Nowadays, the most important applications of quantum communication are the following:
 - quantum key distribution
 - quantum clock synchronisation
 - quantum random number generation
 - quantum networking.
- **Sensing and metrology.** This market is the most advanced one in terms of technology readiness and if benchmarked with classical technologies has proven quantum advantages. Several commercial applications are already available on the market and include:
 - quantum sensing
 - quantum timing (i.e. atomic clocks)
 - quantum imaging.

Quantum computing and quantum advantage

Quantum computers operate on the quantum mechanical properties of qubits. New technological developments are trying to simulate quantum physical systems by using quantum computers. With normal computers, simulating a simple molecule of water – i.e. encoding the quantum state of water – would require a manageable number of bits (similar to what is contained in a typical message on the WhatsApp chat programme). Yet, describing more complex molecules such as penicillin at a quantum mechanical level would require a tremendous amount of memory for a classical computer – a number of bits larger than the atoms in the universe. Describing these complex molecules could only be performed by using quantum computers. For example, describing the penicillin molecule would require just 286 qubits (Langione et al., 2019). Quantum computers are much more equipped for simulating nature because nature itself works according to the rules of quantum mechanics. Against this backdrop, scientists are leveraging the properties of quantum systems to build more powerful quantum computers.

Thanks to their characteristics, quantum computers can unlock new methods of computation. Quantum computers can process information in parallel. Even so, this might be not the most important property of quantum computers. In fact, quantum computers can encode quantum information and they can be in quantum superpositions, but when we read out (i.e. measure) a quantum computer we always obtain a non-superposition value: a classical bit of either 1 or 0. The process of reading out a quantum computer is thus the *interface* between quantum and

⁵ Interestingly, a few years after ID Quantique commercialised its first quantum key distribution device, a Russian scientist, Vladimir Makarov, wrote an article stating he was able to crack the quantum cryptography device of the company. The way in which this was done was by exploiting an imperfection in the quantum cryptographic system. This started a whole field within quantum communication research aimed at closing these loopholes.

classical physics. In this respect, entanglement is possibly a more relevant property to give quantum computers the 'quantum advantage'. Quantum computers are not just faster classical computers. They are different systems.

For a quantum computer to provide a speed-up, a special quantum algorithm is required. Only a limited number of these algorithms exist at the moment. Some examples of useful quantum algorithms are Shor's algorithm, which allows for radically faster factoring of large numbers and computing discrete logarithms, and Grover's algorithm, which gives a speed-up for search problems (Montanaro, 2016). Some quantum algorithms, including Shor's, make it possible to solve problems that are practically impossible to solve on classical computers.

It is important to note that quantum computers are better than classical computers only on this limited set of tasks. As such, they are unlikely to replace classical computers, and will likely be deployed in quantum-classical hybrid systems. Then they can be used to solve the specific problems they are good at, analogous to how the graphical processing unit (GPU) in a classical computer is used to solve certain problems more effectively than the central processing unit (CPU) can solve them. Currently, a major weakness of quantum computers is data entry: since quantum states are complicated, it is hard to input large amounts of data into them.

The problem with quantum computation is that qubits are very unstable. A quantum phenomenon called decoherence can make the state of the qubits decay, rendering them useless for computation. A tightly controlled environment is needed to prevent decoherence. Since these environments are hard to create, quantum computers still are not in widespread use, even though they were theorised decades ago. An important unsolved engineering task is to build logical (or ideal) qubits that simulate a perfectly stable qubit using multiple unstable physical (or real) qubits⁶. Regardless of the technical challenges, prototype quantum computers already exist. Still, they only have a relatively small number of qubits, and those qubits have large error rates. This makes them incapable of carrying out practical computations. Building quantum computers with many more qubits is another important engineering problem.

As explained above, it is known that quantum computers, when they are advanced enough, can solve some problems much better than classical computers. But they are not yet at that point. This raises the issue of demonstrating quantum advantage – the demonstrated superiority of a quantum computer over any classical device. Quantum advantage is very difficult to prove. That is first because the classical algorithms are continuously improving, and second because quantum advantages cannot be clearly benchmarked against one single parameter. One relevant parameter is the run-time of the algorithm, but other parameters include, for example, energy consumption. It is useful to further note that quantum advantage can be shown for different types of problems: those tailored to the properties of quantum computers, purely academic problems, and problems that can be used for industrially relevant applications. Quantum advantage for the second two types have not yet been proved.

⁶ This can be achieved by using quantum error correction.

There are two main reasons quantum computers have not achieved quantum advantage for most problems: the size of the computers and their error rate. A useful dichotomy is between noisy intermediate-scale quantum computers and fault-tolerant large-scale quantum computers. At present, only noisy intermediate-scale quantum computers exist, which typically suffer roughly 1 error every 1 000 operations. Many practical applications demand error rates lower by a billionfold or more (Cheng et al., 2023; Choi, 2022). Fault-tolerant quantum computers, however, require several millions of qubits for encoding and processing and they will likely require another 10 to 30 years before commercialisation.

To keep track of the progress of quantum computing, qubit count is often used. Yet this can be a misleading metric for two reasons. First, not all quantum computers are universal. For instance, quantum annealers – a type of quantum computer for solving optimisation problems – can have a high qubit rate but are not able to use all quantum algorithms. Second, qubits can have different error rates, leading to different capabilities. One way of accounting for error rates is to measure the quantum volume of a quantum computer, which attempts to measure the capability of the quantum computer taking the error rate into account⁷.

Quantum computing is one of the most promising of the quantum technologies being developed now, and has seen large public investment. For instance, the European High-Performance Computing Joint Undertaking (EuroHPC JU) (2021) is funding the inclusion of quantum computers in European supercomputing centres, through its Digital Europe Programme. In addition, the Quantum Flagship (2023) is funding research on quantum computing and projects aimed at bringing the technology to market.

There are various policy concerns around quantum computing, in addition to the cybersecurity issues discussed in detail later in this report. For a start, there are geopolitical interests at play in terms of who leads the race to a fault-tolerant large-scale quantum computer. Quantum computing might also bring inequality: the players with access to quantum computers might see massive economic gains, while others might be left out of the quantum revolution.

⁷ An alternative metric to qubits is reliable quantum operations per second (rQOPS). The rQOPS metric considers the full system performance, as opposed to just qubit performance, so there is an assurance that an algorithm will run correctly. It is a unit of computational effort defined by the number of logical qubits in a quantum system multiplied by the logical clock frequency of the system. An rQOPS is expressed with a corresponding logical error rate, which indicates the maximum tolerable error rate of the operations on the logical qubits. The rQOPS accounts for the three key factors of scale, speed and reliability: scale through the number of reliable qubits; speed through the dependence on the clock speed; and reliability through the very small logical error rates, which are achieved by error correction. Combining these aspects provides a simple way to capture the overall capability of a system to run reliable logical quantum operations.

This note was contributed by Microsoft. See (Nayak (2021) for more details.

Other quantum technologies

While quantum computers are the most famous of the new quantum technologies, there are also others.

Quantum communication encompasses technologies that are used to transmit quantum bits over long distances⁸. A quantum communication system together with quantum processing units is often called the quantum internet. One application of quantum communication is to transmit information between quantum computers, which can be useful, for instance, for parallelising quantum computations.

A unique property of quantum communication is that it can transmit information in a provably secure way: as long as the laws of quantum mechanics hold, we can be certain that no one has eavesdropped on the messages being transmitted⁹. Quantum key distribution (QKD) leverages this property to distribute cryptographic keys. QKD has a long history, and prototype systems have existed for a long time. There are companies already selling QKD devices on the market. These devices are used to produce photons in a specific quantum state. Some limitations of QKD are that all participants in the network require these specialised devices, which have a relatively low bandwidth and can only operate over relatively short distances. We will discuss this aspect in more detail below.

Quantum sensors are a class of devices that use quantum phenomena to produce extremely accurate measurements. Some applications include biosensors and the detection of defects in metals.

Quantum random number generators use quantum phenomena to produce true randomness, which is – at least in theory – provably impossible to predict. This has applications in cryptography, where randomness is required to guarantee security.

While quantum computers use qubits to carry out general calculations, quantum simulators also use qubits, but for a more limited purpose: to simulate quantum systems. This is an easier engineering problem to solve, and as such, quantum simulators may be practically useful sooner than general quantum computers. Practical applications include materials science, where quantum simulators can be used to produce better materials than was possible before.

⁸ At the moment, the distances reached are on the order of hundreds of kilometres.

⁹ A second assumption is that the implementation process used is perfect, and not vulnerable to side-channel attacks.

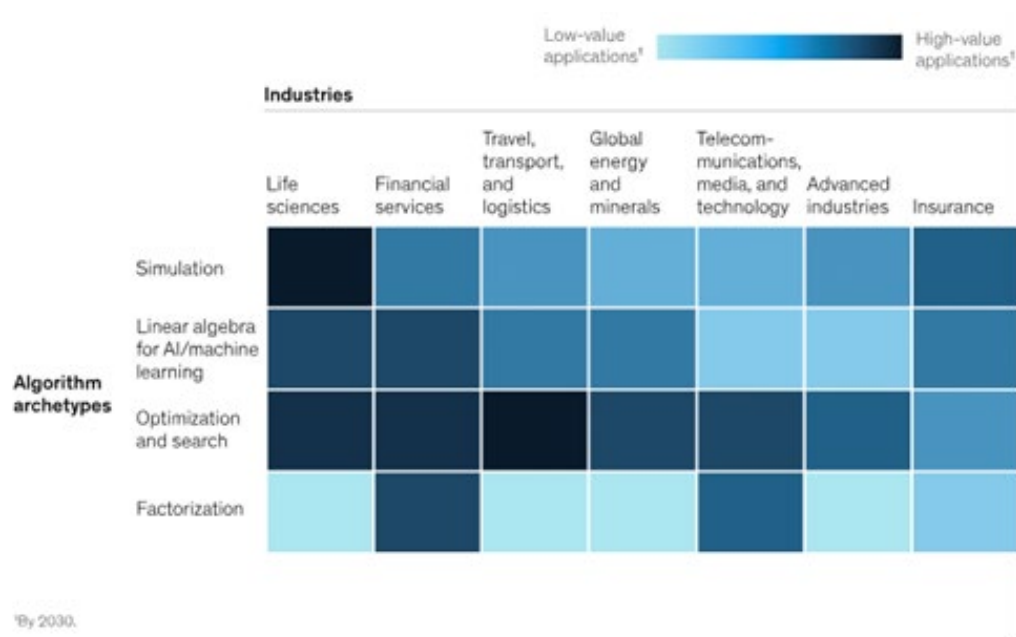
Public funding and the economic impact of quantum technologies

It is often said that the potential economic impact of large-scale fault-tolerant quantum computers is enormous, in the order of USD [1.3 trillion](#), as early as 2035 ([Bogobowicz et al., 2023](#)).

The value unlocked by the adoption of quantum technologies will dramatically vary based on the sector of application. According to McKinsey, four industries – pharmaceuticals, chemicals, automotive and finance – are to become the first beneficiaries of quantum advantages (see Figure 2). Financial services and life sciences are fertile grounds for the highest-value use cases for quantum computing over the longer term¹⁰.

The EU has invested heavily in quantum technologies, with EUR 1 billion committed through the Quantum Flagship (2023), and large programmes from Member States such as France and Germany. These programmes support quantum science and technologies across the board, from basic science to applied research in, for instance, quantum computing and communications. The EU is behind only China in the amount of public funding committed to quantum technologies. The EU also has two large-scale projects on deploying quantum technologies: (i) the EuroHPC JU intends to include quantum computing resources in supercomputing centres and make them available throughout the EU; and (ii) the European Quantum Communication Infrastructure (EuroQCI) aims to ‘build a secure quantum communication infrastructure that will span the whole EU’ as part of the Infrastructure for Resilience, Interconnectivity and Security by Satellite (IRIS²) initiative.

Figure 2. Quantum technologies – Estimated value unlocked by applying quantum technologies in various industries



Source: (Masiowski et al. (, 2022).

¹⁰ Some Task Force members believe the industries most affected will be chemistry, materials science and life sciences.

There is a large and growing international market in quantum technologies, with the quantum computing market alone valued at USD 866 million in 2023 and an anticipated size of USD 4 375 million by 2028 (MarketsandMarkets, 2023). Many companies are building prototypes of quantum computers, including both start-ups and established players in the technology sector. All major the players are involved, with US companies currently making the largest investment in the sector.

Through its heavy investment, the EU has become one of the global leaders in terms of public funding. Committed funding for quantum technologies directly from the EU has amounted to roughly EUR 2 billion since 2015. Taking into account public funding by EU Member States, the figure reaches almost EUR 10 billion in committed funding since 2015. A large share of this funding comes from Germany, which announced a EUR 3 billion action plan for building a universal quantum computer in May 2023. There was also a significant increase in public funding for quantum technologies during the Covid-19 pandemic. More detailed figures can be seen in Appendix B, Table B.1.

A large part of this public funding is for research. For instance, the EU's Quantum Flagship consists of research funding, as does the German action plan. Part of the funding is also for infrastructure, for example plans for building a Europe-wide QKD infrastructure (EuroQCI), and for procurement of quantum computers, such as in the EuroHPC JU project.

Quantum technologies – A global overview

The global landscape of quantum technologies is dynamic and rapidly evolving. Countries across the world are investing in quantum research and development although there are considerable differences in funding and approaches. The US has demonstrated a strong commitment to quantum research and development, with substantial government and private sector investment. Private companies in the US, including major tech giants, are also investing heavily in quantum technologies, driving innovation and commercialisation. China, on the other hand, has adopted a more centralised approach to funding quantum technologies.

In contrast, the funding landscape in the EU is more decentralised. The EU has taken a collaborative approach, encouraging Member States to invest in quantum research and innovation. Funding for quantum technologies in the EU comes from various sources, including national governments, the European Commission's Horizon Europe programme and public-private partnerships. While the EU has committed significant funding to quantum research through initiatives like the Quantum Flagship programme, it faces challenges in achieving unified funding strategies across Member States due to differences in national priorities and budget allocations.

Appendix B offers an overview of the specific initiatives undertaken by major quantum technology stakeholders, including the EU's Quantum Flagship programme, the US National Quantum Initiative Act and other notable national programmes.



2. QUANTUM TECHNOLOGIES AND CYBERSECURITY

Summary

A large quantum computer could break widely used cryptographic algorithms. A cryptographically relevant quantum computer (CRQC) that can break cryptographic algorithms would have major implications for cybersecurity. Today's quantum computers are too small and error-prone to be a threat. According to experts, a CRQC is unlikely to surface in the next 5-10 years but is very likely in the next 30 years.

Responding to the threat should start long before CRQCs become available, for two main reasons. First, sensitive encrypted data can be stored and subsequently decrypted with a CRQC. Second, the process of transitioning to new types of cryptography takes a long time.

The previous chapter introduced quantum computing and communication technologies, and how they are developing. But why are quantum technologies relevant for cybersecurity? While there are several advantages to using such quantum technologies for cybersecurity, the most important link is that quantum computing threatens the security of cryptographic algorithms that are widely used today. The rise of quantum computing will require major changes, and it is important to start acting now.

The effect of quantum technologies on cybersecurity

As covered in the previous chapter, quantum computers make use of quantum mechanical properties to solve certain computational problems much more efficiently than classical computers can. This new computational capability can have enormous benefits, making it possible to solve, for instance, optimisation problems that were infeasible in the past.

This new computational power also has a negative side. A large error-corrected quantum computer could break a large fraction of widely used cryptographic algorithms, breaching confidential data. Most internet applications rely on cryptography to guarantee the confidentiality, authenticity and integrity of data. Cryptography in turn can guarantee these properties only on the assumption that certain mathematical problems are intractable, meaning that they cannot be solved by a computer in a reasonable amount of time. It turns out that some of these problems are of the type that a large quantum computer can efficiently break. Current quantum computers are too small to be a threat. Still, the arrival of large quantum computers threatens a great deal of cryptography, and as a consequence, the security of the internet.

Our trust in the digital world today relies on it being possible to send data over the internet and to trust that the communication is secure. The digital economy is an increasingly large share of the world economy, and is projected to rise to account for 30 % of it by 2030. To keep the digital economy safe, cryptography is needed. Cryptography is used widely today, in applications including

- finance
- network infrastructure
- cloud services
- user devices
- IoT (internet of things)
- healthcare
- e-government
- critical infrastructure.

The number of cryptographic devices is huge: it is estimated to stand at 90 billion today, with around 60 billion being used to protect industry and around 30 billion being used to protect users.

It may be surprising that the cryptographic algorithms used so widely are insecure against quantum computers. The reason for this is that much cryptography relies on computational complexity *assumptions*. Proving unconditional security for cryptographic algorithms based on computational complexity assumptions is an open research question¹¹. Yet, the faith we have in the security of cryptography is at its core based on decades of unsuccessful attempts to break the algorithms in use.

Much of cryptography can be split into two types: symmetric and asymmetric cryptography. In the first, two participants share a secret key that they then use to guarantee security (by, e.g. encrypting messages). Symmetric cryptography was developed first, and is efficient, but suffers from the problem of requiring a pre-established secret key. Asymmetric cryptography solves this problem: it allows parties to communicate securely without having established a key beforehand. This is crucial, especially for secure communication online. It is possible to encrypt messages directly with asymmetric cryptography, but it is more common to use asymmetric cryptography to agree on a shared secret key and then use the more efficient symmetric cryptography for encryption.

The widely used public key cryptosystem RSA (Rivest–Shamir–Adleman) relies on it being infeasible to factor the product of two large prime numbers. On classical computers this assumption has held for a long time. However, this is a task that a quantum computer can solve efficiently. As a consequence, a large enough quantum computer will be able to break the security of RSA, with potentially catastrophic consequences. RSA and other asymmetric cryptographic algorithms underly the security of communications on the internet, including for financial

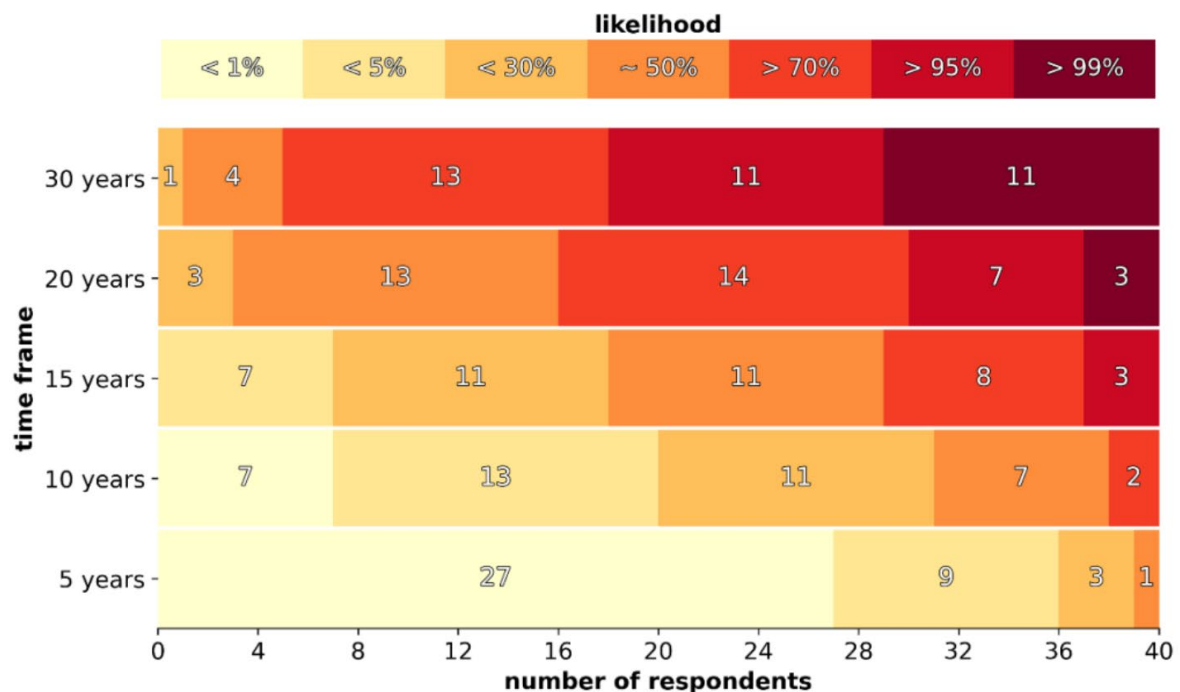
¹¹ There are cryptographic algorithms, such as one-time-pads, that are unconditionally secure. However, they are much less practical than cryptography based on mathematical problems, due to their reliance on large secret keys that have already been established.

transactions and digital signatures. A large quantum computer could break RSA-2048 in around 10 seconds (Baumhof, 2019). Another widely used vulnerable cryptosystem is the Diffie-Hellman key exchange, based on the hardness of the discrete logarithm problem, which is also efficiently solvable by a quantum computer. Both RSA and the Diffie-Hellman key exchange are used for establishing secure (https) connections on the internet.

Around two thirds of the 90 billion cryptographic devices use public key cryptography, and of those, 95-99 % rely on the computational hardness of factoring products of large prime numbers and the discrete log problem, both of which quantum computers can solve efficiently. Public key cryptography is what allows users to agree on secret keys without having met before. If these key exchange algorithms are compromised, the confidentiality of data is at risk, and the forging of signatures becomes possible. This means that a large enough quantum computer threatens the security of much of the digital economy. One estimate is that '[b]reaking the public key cryptography scheme RSA-2048 requires 20 million real qubits or around 14 000 ideal qubits' (Emerging Technology from the arXiv, 2019; Goodin, 2023).

For context, the largest quantum computers available today have on the order of 1 000 real qubits. In a survey of 40 experts, the likelihood of a quantum computer capable of breaking RSA-2048 was estimated by most to be under 1 % in the next 5 years. But in a 30-year time frame, almost all respondents believed the likelihood was at least 50 % (Mosca & Piani, 2022; see Figure 3 for details).

Figure 3. Expert estimates of the likelihood of a quantum computer breaking RSA-2048 in 24 hours (different time frames)



Source: (Mosca & Piani, (2022).

Quantum computers also have an impact on cryptographic hash functions as well as symmetric-key cryptography, which is mainly used for encryption of data. Still, the effect is not as severe as for public key cryptography. The threat to symmetric-key cryptography and cryptographic hash functions only materialises if even larger quantum devices are built. Further, it only requires a doubling of key sizes to be completely mitigated, not being a practical threat if 256-bit keys are used, as is already done in many applications. Therefore, the serious threat comes from attacks on public key cryptography.

The quantum algorithm threatening asymmetric cryptography is called Shor's algorithm, invented in 1994. This algorithm allows a quantum computer to factor large numbers *exponentially* faster than the best algorithms for classical computers (National Academies of Sciences, 2019). In essence, this means that any cryptographic algorithms relying on the hardness of factoring integers are completely insecure against a quantum computer. A similar algorithm can also efficiently solve the discrete log problem, which is also used for public key cryptography.

Grover's algorithm, discovered in 1996, is a quantum algorithm for searching for a value in a large set. One way to break symmetric encryption is to attempt every possible key. Grover's algorithm can complete this task faster than the best algorithms for classical computers. To be more precise, a quantum computer can solve these problems in time that is proportional to one square root of the time a classical computer needs (National Academies of Sciences, 2019). The same is true of hashing algorithms, which are often used to store passwords securely. In both cases, huge computers would be needed, with many more quantum gates compared with quantum computers that can factor or compute discrete logarithms.

The Advanced Encryption Standard (AES) is a widely used symmetric algorithm, used to encrypt data at rest. A quantum computer using Grover's algorithm can break AES in time proportionate to the square root of the time a classical computer can¹². This is a serious problem since it reduces the security level, but not as serious as the one for asymmetric schemes and key exchange. Grover's algorithm also threatens hashing algorithms in the same way, potentially halving their security level¹³. This problem is especially bad in the case of password hashing, since the amount of password in use is relatively low.

Symmetric cryptography is threatened due to brute-force search being faster on a quantum computer. As stated before, this speed-up merely reduces the security level, rather than making the cryptosystems completely insecure. The fix is simple: increase the security level by

¹² Since the true time needed at the moment is very large, many times the age of the universe, not all Task Force members agree that there is a relevant threat to symmetric cryptography. See National Academies of Sciences, (2019) for details on the time taken for an attack on symmetric cryptography.

¹³ As with AES, the attack in practice may be too costly to present a real threat.

using longer keys (National Academies of Sciences, 2019)¹⁴. This is already possible within present standards.

Hashes are threatened by the same attack. In normal operation, this does not significantly threaten their security. For password hashing, however, Grover's algorithm does represent a major threat. The solution is to move away from password-based authentication (National Academies of Sciences, 2019).

For asymmetric cryptography, such simple solutions do not exist. Larger changes are needed, as discussed in the next chapter.

In principle, quantum computers can easily break many asymmetric cryptosystems. In practice, however, large quantum devices with low error rates are required. Currently, we are still far from quantum computers large enough to concretely threaten public key cryptography. Even though noisy intermediate-scale quantum computers (NISQs) already exist, they only have on the order of 433 physical qubits. The gap is likely to close in the medium term. After quantum computers were theorised in the 1980s, they have seen steady interest, with progress in the 1990s (from 1 to 7 real qubits) and with the US National Security Agency spending USD 85 million on research to build a quantum computer by 2014. Today, there is a large amount of funding in this area, with for instance IBM predicting they will reach 4 158 physical qubits in 2025.

A cryptographically relevant quantum computer is large and error-resistant enough to threaten cryptography.

According to some experts in the field, the likelihood of a significant quantum threat to public key cryptography is low in the next 5 years, but becomes high within the next 20 years. Other experts disagree with this, saying that the threat will not materialise in the next 30 years (Thomson, 2023).

Why we need to act now – Mosca's inequality

The threat described above may seem to be of only theoretical interest. Currently, the only publicly known quantum computers are prototypes, with a tiny amount of computational power. The threat to cybersecurity comes from powerful quantum computers, with orders of magnitude more qubits with significantly lower error rates. So, why is it that migration to post-quantum cryptography cannot wait until such computers are built? There are two main reasons, discussed below.

¹⁴ However, no government agency has recommended longer key lengths, potentially due to the attacks being so slow in practice.

First, data can be harvested. At present, nobody can breach the confidentiality of data protected by the cryptographic algorithms used today, since no one has access to a powerful quantum computer. But a malicious actor could collect the data now and store it. They could store it long enough for powerful quantum computers to become available, which they could use to decrypt the data. That means that the confidentiality of data being sent today could be breached, even if it takes decades to do so. It is important to remember that this argument only holds for data that have to stay confidential for a long time. For instance, IoT devices often have much shorter timeframes for data that have to be kept private, and it is true that this type of attack is not a relevant threat.

Second, migration is slow. Even after quantum-safe systems have been invented and standardised, they will require a long time to implement. Historically, migration to new cryptographic standards has been very slow, as has the process of standardisation itself. Changes must be made in software as well as hardware. IoT devices might be out in the field for a long time without upgrades, requiring any changes to be made early. There is also organisational overhead, making the process slower.

Crucially, it is important that solutions to the threat of quantum computers are widely implemented. Any device can be an entry point for a cyber-attack, which can then spread.

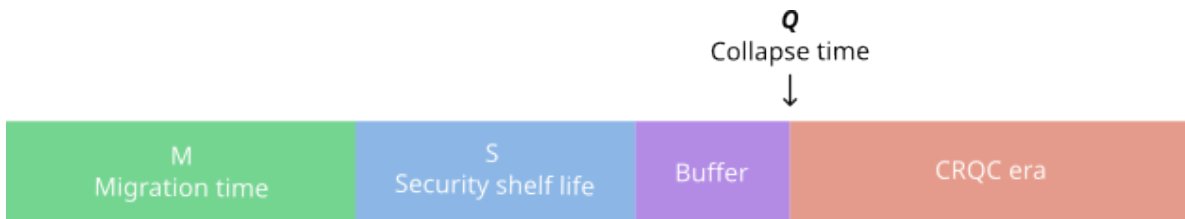
Mosca's inequality

When estimating the urgency of transitioning to quantum-safe solutions, there are three main things to take into account. First, when will CRQCs be built? The threat only becomes concrete when large quantum computers exist, but estimating when this will happen is challenging. Second, how long does it take to migrate to quantum-resistant cryptography? This creates a strong constraint, making it important to start early. The exact time will depend on many factors and differ across sectors. It is nonetheless important to remember that society-wide cybersecurity requires even the weakest link to be secure. Third, how long do the data need to stay protected? Due to store-now-decrypt-later attacks, any data transmitted before the transition is complete are unsafe. For some short-lived data this does not matter, but many types of data need to be kept secure for a long time, for instance medical data.

One way of analysing the situation is Mosca's inequality (Mosca, 2018). In this framework, the urgency of starting work on implementing quantum-resistant cryptography can be estimated based on three numbers:

- migration time – the time it takes for a post-quantum cryptosystem to be implemented;
- security shelf life – the time the information in question must remain confidential;
- collapse time – the time until a CRQC is built.

If Q is the number of years until the first large quantum computer arrives (collapse time), M the number of years it takes to migrate to quantum-resistant cryptography, and S the number of years data have to be kept confidential, then the transition must start in the year $2023 + Q - M - S$. Or, in other words, if $M + S > Q$ there is a serious problem¹⁵.



For instance, estimating that $Q = 17$, $S = 7$ and $M = 10$, the result would be $S + M = 17 = Q$, and the transition would have to start today! This creates a significant practical problem since the process of standardising quantum-resistant cryptography has not even finished yet.

Q , the amount of time until a CRQC is built, is especially hard to estimate. Quantum computing is a relatively new field, and significant engineering work is needed before quantum computers capable of breaking the RSA cryptosystem can be built. Accurate forecasts in technology are hard to make, and the field of quantum computing being new makes forecasting even harder. At this time, the best approach is likely to be tracking progress in the field, so that the breaking of RSA does not come as a surprise (National Academies of Sciences, 2019).

Nevertheless, the consensus report on quantum computing by the National Academies of Sciences (2019) estimates that ‘given the current state of quantum computing and recent rates of progress, it is highly unexpected that a quantum computer that can compromise RSA 2048 or comparable discrete logarithm-based public key cryptosystems will be built within the next decade’. The number of physical qubits in today's system is a tiny fraction of what will be needed to break RSA, and substantial improvements in error-rate and quantum error correction must also be made to break it. Major technical breakthroughs are needed before either of these are achieved.

The number of years S data must be kept confidential is an important part of the analysis and is thankfully easier to estimate. To a significant extent, it is a policy choice, and for some types of data there are existing limits on how long data must be kept confidential. It is important to note that the variable S will differ across sectors and even within a single organisation. For instance, for IoT devices S may be in the order of hours. Organisations also need to make choices on this front. The above applies to *encryption*. For signatures, S is nearly 0 since documents can simply be resigned when a CRQC is built.

¹⁵ Note that the letters used here are different from those used in Mosca's paper.

Estimating the migration time M is more tractable: it is the variable that is easiest to affect, at least in the context of a single organisation. All the same, the process to replace quantum-vulnerable cryptographic algorithms with new post-quantum algorithms is complex and consists of multiple steps. The process can be roughly divided into two halves: finding a technical solution and implementing that solution. An accurate estimate is hard to give, but the process is involved enough that it is sure to take a long time.

Similar large-scale updates to computing architecture have been made before, with a prominent example being the switch from the unsafe MD5 hashing algorithm to a secure algorithm in the SHA-2 family. An attack of practical significance was reported in 2005 (Lenstra et al., 2005), but MD5 was still used in 2019 in a quarter of major content management systems (Cimpanu, 2019). The National Institute for Standards and Technology estimates that, based on past experience, 'in the best case, 5 to 15 or more years will elapse after the publication of cryptographic standards before a full implementation of those standards is completed' (Barker et al., 2021), and notes that migrating to post-quantum cryptography might be even harder.

There are two levels at which the variable M can be analysed: how long a single organisation takes to migrate, and how long it takes for everyone to migrate. Until all actors have migrated, it is hard for anyone to remain safe; they will have to remain interoperable with outdated systems and may suffer from cyber-attacks against those outdated systems. Clearly, the time it takes for every actor to transition is longer than how long it takes for the most up-to-date organisations.



3. QUANTUM-RESISTANT CRYPTOGRAPHY

Summary

Quantum-resistant cryptography is a new type of cryptography that can withstand an attack by a large quantum computer. This type of cryptography does not require a quantum computer to operate and has already been demonstrated in practice. Quantum-resistant cryptographic algorithms are currently being standardised.

Yet, the transition to their use is not an easy task. Issues are likely to arise around interoperability, determination of exactly where changes are needed, workforce and the speed at which fixes can be made.

As the previous chapter discussed, the rise of operational quantum computers will threaten the cryptography currently in use. Fortunately, quantum computers only give a boost on certain classes of mathematical problems, so it is possible to develop cryptography based on mathematical problems that are resistant to attack by quantum computers. Quantum-resistant cryptography can thus help mitigate the threat posed by quantum computers.

It is lucky that these solutions exist, but there are still hurdles to overcome: quantum-resistant cryptography is not a drop-in solution, so starting to use it will require a potentially complicated migration process. Also, standards need to be written both for quantum-resistant cryptography and for many protocols that make use of cryptography.

In short, the transition to quantum-resistant cryptography is a lengthy process. It requires careful planning and must be started well in advance of the availability of CRQCs. Cryptographic agility¹⁶ should be kept in mind during the process, to make similar transitions smoother in the future.

An important fact is that implementing quantum-resistant cryptography does not require having a quantum computer. These algorithms can already be used today, and it is possible to start the transition immediately, as is needed for the reasons discussed in the previous chapter.

Overview of quantum-resistant cryptography

Classical cryptography, which is in use today, is threatened by large quantum computers that can crack mathematical problems thought impossible for anyone to solve. Quantum-resistant cryptography (also known as post-quantum cryptography) solves the issue at its root: it is a type of cryptography relying on mathematical problems believed to be infeasible for even quantum

¹⁶ Cryptographic agility refers to the ability to change cryptographic tools with ease. See the section on large enterprises and cryptographic agility below.

computers to solve. As long as that assumption holds, quantum-resistant cryptographic algorithms will remain secure even against CRQCs.

Luckily, quantum-resistant cryptography is backed by decades of research. The cryptographic methods it uses have been studied since the 1970s and 1980s and have stood the test of time. Concrete algorithms already exist, and since they do not require any special technology, can be used today. There are a variety of different mathematical problems believed to resist attacks by quantum computers, which can thus be used for quantum-resistant cryptography:

- **Lattice-based** cryptography has the advantage of being efficient¹⁷, but also has various drawbacks, including the fact that key lengths are much larger than in current cryptography.
- **Code-based** cryptography, for which schemes were proposed as early as the 1970s, are considered well understood and conservative in terms of their security. Depending on which one is used, they usually have larger key sizes than lattice-based schemes.
- **Hash-based** signatures are based on cryptographic hash functions, a well-understood cryptographic algorithm. Both stateless and stateful variants exist. The security of stateless hash-based signature schemes is well understood (relative to the lattice-based schemes), but they are much slower and require much larger signatures than current, classical, algorithms. Stateful hash-based signatures, on the other hand, are constrained by the sender and receiver having to keep track of which keys have been used and never reusing them, but have the advantage of being much faster and having far smaller signatures than stateless ones, at least when the number of signatures needed is relatively small.
- There are also various other mathematical problems quantum-resistant cryptography can be based on. Even though these do not seem likely to see wide use, having a diverse set of algorithms helps make quantum-resistant cryptography as a whole robust.

As discussed in the previous chapter, especially public key cryptography needs quantum-resistant alternatives. Symmetric-key cryptography and cryptographic hash functions do not require major changes to cryptography: an increase in key length is enough to completely mitigate the threat¹⁸. More specifically, two types of public key cryptography need replacing: key encapsulation mechanisms (used to transmit secret keys for symmetric encryption)¹⁹ and signature schemes (used to establish the authenticity of messages).

¹⁷ This is partly due to operations on lattices being easy to parallelise – process in a way that can take advantage of multiple processing units.

¹⁸ Even this may be unnecessary, as noted earlier in this report.

¹⁹ Most public key encapsulation mechanisms can also function as public key encryption algorithms. While public key encryption has mostly been replaced with public key exchange, public key encryption is still used.

There are many different types of quantum-resistant cryptographic algorithms, and they will need to be used in different contexts. Even without so many choices, cryptography is hard to do well. The types of attacks mounted against it are not known beforehand, and what seem like minor details can lead to devastating attacks. As such, any use of cryptography should be based on best practices and standards, which have been vetted by a large community and stood the test of time. Developing and evaluating quantum-resistant cryptographic algorithms is a complex and time-consuming process. It involves extensive research, peer reviewing and testing to ensure their security and resilience against quantum attacks.

The new algorithms need to be vetted, tested and standardised for them to be trustworthy. Standardisation bodies, such as the National Institute for Standards and Technology (NIST), are actively working to identify and evaluate candidate algorithms. The process requires collaboration and consensus among experts, which adds to the complexity and time required. NIST is running the process as a competition where teams from around the world submit candidate algorithms, which are then thoroughly vetted. The algorithms identified as the best are then standardised. The NIST Post-Quantum Cryptography competition started in 2016, and the first draft standards were published on 24 August 2023. For more details on the NIST competition, see Box 2.

The NIST competition is the leading process for standardising quantum-resistant cryptography, and most other actors are waiting for its results. This is the case for the EU and Member States, where a large portion of the underlying research has been done²⁰. However, there are also other standardisation processes, for instance in international organisations such as ISO and the Internet Engineering Task Force (IETF) (which has standardised two stateful hash-based signatures). It is important to be aware of the different ongoing processes, and foster interaction and collaboration between them.

Box 2. NIST standardisation competition

NIST has been running its competition since 2016, has found multiple promising candidates and hopes to publish a final standard in 2024 (Moody, 2022). The role of NIST is to provide a process for achieving community consensus in a transparent and timely manner. The competition has been more complicated than previous ones run by NIST and aims to find multiple good choices rather than a single winner. The main selection criteria for algorithms are that they:

- (i) are secure against both classical and quantum attacks;
- (ii) have good enough performance.

²⁰ For instance, the ML-KEM and ML-DSA solutions were developed by European researchers with European grants.

There are also various other desirable properties, such as being a drop-in replacement²¹, being resistant against side-channel attacks²² and being simple, but it is unlikely that all of these can be achieved at once.

The process has so far covered three rounds:

- *Round 1 (December 2017–January 2018)*. A total of 69 candidate solutions were submitted, based on a diverse set of mathematical assumptions. A conference was held, and almost 25 of the submitted solutions were broken.
- *Round 2 (January 2018–July 2020)*. This round started with 26 of the most promising candidates, which were investigated further.
- *Round 3 (July 2020–July 2022)*. Seven finalists and eight alternatives were chosen and evaluated. This round concluded with the selection of the first algorithms to be standardised.

The algorithms chosen for standardisation were the key exchange mechanism ML-KEM²³ and the signature schemes ML-DSA, Falcon and SLH-DSA. The mathematical basis of all of these schemes, except SLH-DSA, is the hardness of lattice problems. However, having schemes relying on different mathematical foundations would be valuable, as it would provide alternative solutions if one of them is broken. For this reason, NIST has made a new call for signature schemes based on other mathematical assumptions and will be picking key exchange mechanisms based on different mathematical assumptions in the fourth round. The algorithms under consideration were [published](#) in July 2023.

Draft standards were put up for public comment in August 2023 (NIST, 2023), with final versions expected in 2024 and Falcon expected around a year later. The standards from the fourth round are expected to be published in 2026 or 2027.

Migration to quantum-resistant cryptography

As covered in the previous section, a solution to the threat posed by quantum computers exists, and is currently being standardised. The next step is to migrate IT systems to use quantum-resistant cryptography. It may seem like the transition to new algorithms is straightforward – they just require a software update. Yet, in many situations, things will be much more difficult. For instance, embedded systems cannot simply be updated, and some devices (such as cars) will stay in operation for a long time. There are also concerns around performance: quantum-

²¹ A drop-in replacement would be possible to use in place of classical cryptographic algorithms without need for customisation.

²² A side-channel attack is a type of attack on cryptographic algorithms that relies on implementation weaknesses, for instance spikes in energy usage that reveal information.

²³ The algorithm formerly called CRYSTALS-Kyber is being standardized by NIST under the name ML-KEM. Similarly, ML-DSA is based on CRYSTALS-Dilithium and SLH-DSA on SPHINCS+.

resistant cryptographic algorithms are typically more computationally intensive compared with traditional algorithms and can require more storage space. This will become an issue for some classes of devices during deployment. Hence, the migration process itself will require significant time, effort and resources.

The process of developing quantum-resistant cryptography, nearing its end, has taken around 30 years from problem formulation to standardisation. Even when this process is complete, however, there are still many things left to do. The new algorithms are not, by and large, a drop-in replacement. They have limitations relative to the algorithms they are replacing and need careful fine-tuning and engineering to fit into existing systems. Further, they need to be incorporated into higher-level protocols such as TLS (transport layer security, which secures communication over the internet). Cryptography is used in many standards at the European and international levels, and all of these will need to be updated before a full transition can be made.

There are also different types of cryptography that need to be migrated, such as key exchange algorithms and signature schemes. One question, discussed in Box 3, is which of these is most urgent.

*Box 3. Migrating to quantum-resistant signatures later than quantum-resistant key exchange**

When CRQCs are built, they will be able to decrypt messages that were encrypted using classical key exchange mechanisms as long as the key exchange is observed and recorded. An attacker could begin to store potentially valuable key exchange messages decades before CRQCs can be built. When the attacker gains access to a CRQC, they could decrypt messages without anyone else knowing that they are doing so.

The algorithms used in digital signatures such as public key infrastructure web certificates and DNSSEC are just as susceptible to CRQCs as the key exchange algorithms used in TLS and other encryption systems. The attacks on signatures are inherently less valuable because they can be detected. That is, if an attacker were able to use a CRQC to forge a signature (such as creating a fake certificate for a high-value website), that attack would likely be discovered some time after it succeeds, and the attacked party would be able to respond by changing its signature keys. In general, impersonation is considered less valuable than message decryption.

Given this asymmetry of attack values, it is quite likely that quantum attacks on signatures will happen well after any successful attacks on secrets. This means that the technical community can take longer developing and choosing quantum-resistant signature algorithms than for key exchange algorithms. Having more time to select the best signature algorithms gives the technical community more time to evaluate the safety of the proposed new schemes, and also gives it more time to find algorithms that fit the requirements better.

The quantum-resistant signature algorithms that have been proposed so far have the negative attributes of having much larger key sizes, much larger signature sizes, or both. These increases in size have a significant effect in protocols that expect small message sizes, such as what we see with classical signature algorithms, particularly in low-power and sporadically-connected devices. Some of the proposed signature algorithms will also entail significant operational changes due to needing different types of long-term storage for the signers. It is quite likely that there will have to be many different quantum-resistant signature algorithms with different use cases.

All modern internet encryption protocols already allow different key exchange and signature algorithms. Given the considerations above, this leads to the advantage of letting the community move quickly on adopting new key exchange algorithms and more carefully on signature algorithms. However, it also has the disadvantage of extending the time it will take to complete the full migration from classical to quantum-resistant cryptography. The technical community will have to strike this balance over the coming decades, particularly with the difficulty of describing to the public whether it is alright to have protocols that use a mix of classical and quantum-resistant algorithms.

* This text was contributed by ICANN as a participant on the Task Force.

When the transition to quantum-resistant cryptography starts, there will be a period when both quantum-resistant cryptography and traditional public key cryptography will be used in hybrid implementation. There are at least two good reasons for this. First, different actors will transition at different speeds, and interoperability must be maintained. Second, quantum-resistant cryptography is still comparatively recent. There has been a relatively short amount of time to carry out cryptanalysis, leading to uncertainty about security. Implementation is likely to have security issues at first, similar to those highlighted in recent NIST activities (Gable et al., 2023). There is a high level of confidence in lattice-based cryptography, but even there, a small informal survey found that most researchers think that we need to wait for more than 5 years before obtaining a stable classical assurance level for quantum-resistant cryptographic algorithms.

Classical public key cryptography, such as RSA and elliptic-curve cryptography, has been scrutinised for a long time and a lot of experience has been gained in secure implementation. To build the same level of confidence in quantum-resistant schemes, more research and implementation experience are required. In order not to delay the migration to quantum-resistant cryptography, using hybrid schemes is a good option. Hybrid schemes allow the use of two types of cryptographic algorithms – classical and quantum-resistant – at once. This is done in a way that both algorithms need to be broken in order to break the whole scheme. Thus, hybrid schemes are as strong as the strongest one of the constituent schemes, and

possible issues with the new quantum-resistant schemes do not compromise security. For hybrid schemes, care has to be taken to ensure correct and secure implementation²⁴.

An interesting case is the US National Security Agency, which in September 2022 issued a recommendation that the transition should happen very fast (with the transition complete in some sectors by 2030), skipping hybrid systems completely (National Security Agency, Cybersecurity Advisory, 2022). It is unlikely that industry will be able to follow such a strict recommendation. Meanwhile, many European cybersecurity agencies, such as the Agence nationale de la sécurité des systèmes d'information (ANSSI) in France and the Federal Office for Information Security (BSI) in Germany, recommend using quantum-resistant schemes in hybrid mode together with classical schemes.

Large enterprises and cryptographic agility

A large part of cryptography is developed, deployed and used within the private sector, and especially within large enterprises. A wholesale transition to quantum-resistant cryptography will require coordination among all these actors, but also coordination within them. This is especially challenging for large enterprises.

This is not the first time that a transition to new cryptography has been needed²⁵. If prior transitions have taught us anything, it is that they can come on suddenly, take a decade to accomplish and are far harder than the drop-in replacement they appear to be. When practical deployment starts, various unforeseen problems are likely to arise. For instance, there are practical choices related to which algorithms to use, and organisational issues around getting everyone to agree on a migration plan.

Real-world enterprises have complicated needs: they have complex infrastructure, located in many data centres, in different sectors and geographical regions. Customer data have to be kept protected no matter where moved. This becomes a very taxing problem in a large enterprise. The transition process requires careful planning, coordination and extensive testing to ensure compatibility and minimise disruptions. Transition processes are slow, and they should not be rushed.

A single organisation may use cryptography in many of its operations. To complete an organisation-wide transition, coordination is needed. Interacting systems must be migrated in a harmonised way, with many teams across the organisation being involved. To be able to implement a fast transition in a coordinated manner, leadership is needed. Someone in the enterprise needs to take initiative and make sure the entire process runs smoothly, starting from a quantum vulnerability assessment.

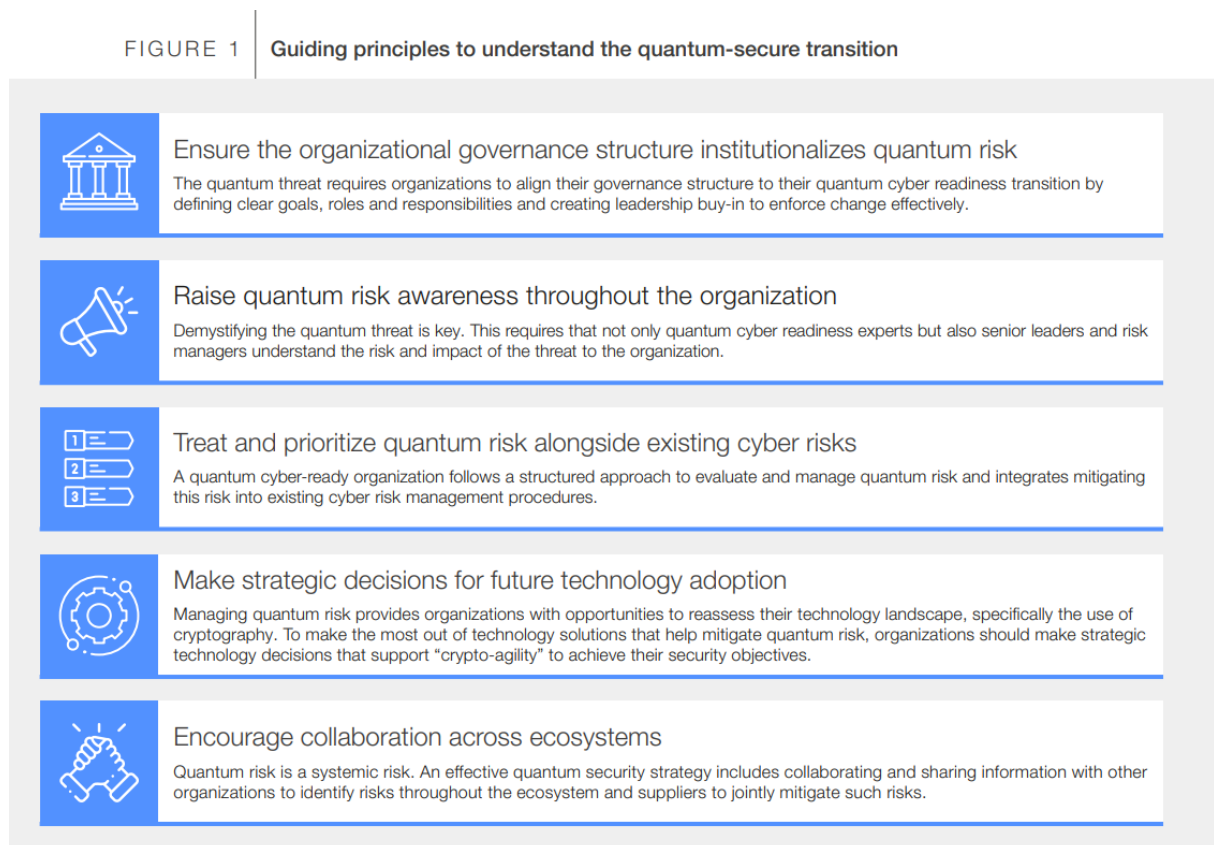
²⁴ One possible attack is a 'downgrade attack', where an attacker claims they cannot use quantum-resistant algorithms, forcing the use of classical cryptography.

²⁵ For instance, the hash function SHA-1 has been shown to be insecure since 2010, leading to the standardisation of new hash functions and a lengthy process of migration.

A workforce knowledgeable in quantum-resistant cryptography is essential for implementing the new cryptographic systems correctly. There also needs to be awareness about the quantum threat everywhere in the organisation, so that developers spot the use of outdated cryptography and migration efforts are supported.

Some guiding principles to understand the quantum-secure transitions are outlined by World Economic Forum (WEF) and Deloitte in their Quantum Readiness Toolkit (Figure 4).

Figure 4. Quantum Readiness Toolkit



Source: WEF and Deloitte (2023).

As noted above, a good starting point for the transition of an organisation to quantum-resistant cryptography is carrying out a quantum vulnerability assessment, which provides awareness of where in the organisation cryptography is used, and where it thus needs to be updated.

Large enterprises will use cryptography in many parts of their operations, and in many different applications. Cryptographic agility refers to the ability to change the cryptographic building blocks used in an application in a fast and painless way. This may mean technical solutions that make switches easy, but also encompasses measures taken at the organisational level.

The current situation with quantum computers is a good reminder of why cryptographic agility is important: cryptographic algorithms need to be replaced from time to time. In this case there is quite a bit of warning time, but it is possible that attacks on cryptographic algorithms are

discovered in the future that take a much shorter time to materialise. Having been able to use RSA for so long has been a luxury. In these situations, especially, it is important that a transition away from the compromised cryptographic systems can be completed quickly.

There is research on cryptographic agility at the library level, but there is a lack of research on the problems that arise in large modern enterprises (Ott et al., 2023). Research on cryptographic agility will likely be useful in the future: it is unlikely that the transition to quantum-resistant cryptography will be the last time cryptographic agility will be needed.

All enterprises are part of a larger network, with other companies acting as subcontractors and customers. A successful transition must take this into account and be aware that the transition will not be complete before others take action as well. As such, a migration plan has to include an analysis of the security of the entire supply chain. Coordination across the supply chain will also be needed.

During the transition to quantum-resistant cryptography, interoperability between systems that have different levels of adoption of quantum-resistant algorithms becomes crucial. Companies will need to do business with others that have not transitioned. Ensuring seamless communication and secure data exchange between systems using traditional cryptography and those using quantum-resistant cryptography requires careful consideration and the development of suitable standards and protocols. As discussed earlier in this report, hybrid modes are one possible solution to achieving interoperability during the transition.

Interoperability is also important at the protocol level. The new cryptographic algorithms need to be integrated into various protocols, where new constraints will be placed on them. This is true for both standardised protocols such as TLS and internal processes within companies.

There are some sectors where deployment of quantum-resistant cryptography is especially difficult. For instance, in the automobile sector it must be considered that cars remain in service for a long time and handle confidential user data. Embedded systems present a different sort of challenge: they have limitations that make it difficult to run modern quantum-resistant cryptographic algorithms. One example is smart card readers.

Deploying new cryptographic algorithms across a vast array of systems, protocols and applications is a significant undertaking. It involves updating software libraries, firmware, operating systems and network protocols to support the new algorithms. As it is a complex and long-lasting process, unforeseen problems are likely to come up during the transition. As such, the amount of time a transition will take is hard to estimate in advance, and it is important to be well-prepared.

Even though the transition will likely take a long time, it is required to maintain the security of IT systems. It presents an opportunity for implementing cryptographic agility in order to make similar transitions in the future faster and cheaper. It is important to start early and avoid rushing the process.



4. QUANTUM CRYPTOGRAPHY

Summary

Quantum key distribution is a type of quantum technology for the exchange of secret keys. These keys can be used to transmit messages securely. The laws of quantum mechanics can be used to prove that eavesdroppers cannot compromise the keys exchanged, even if they have access to a quantum computer. Unlike classical cryptography, QKD requires the parties exchanging keys to have special devices.

At present, QKD has various technical limitations, including the distance over which keys can be transmitted and the bandwidth. The security of QKD is only proven at a theoretical level, and implementation issues may compromise this security. QKD still requires the use of non-quantum cryptography both to authenticate the parties and to use the exchanged keys. Many cybersecurity agencies recommend using quantum-resistant cryptography over QKD.

Quantum computers pose a threat to cybersecurity by cracking many cryptographic algorithms currently in use. Quantum-resistant cryptography is a promising solution to such a threat, because it can be implemented on computers we have today. Quantum cryptography, on the other hand, uses quantum technology to improve cybersecurity. The best-known form of quantum cryptography is QKD, which uses quantum mechanical properties to securely share cryptographic keys. There are also other forms of quantum cryptography, including quantum random number generators (QRNGs).

Quantum key distribution – Advantages and disadvantages

In 1984, it was shown that it is possible to use quantum phenomena to build systems whose security is backed by the laws of physics, i.e. quantum key distribution. As the name implies, QKD allows for the sharing of keys between two parties securely. Given *perfect* implementation, it is impossible for an eavesdropper to get information about the key agreed to by the two parties. Devices implementing QKD are on the market today. Both the EU and China are investing significant amounts in R&D of QKD.

The main selling point of QKD is that it is provably secure under the correct circumstances. Its theoretical security does not rely on unproven mathematical complexity assumptions but on the assumption that the laws of quantum physics are correct and will not degrade with progress in computation. Since QKD involves sending photons between participants, it fits in well with our existing communications infrastructure, which is increasingly fibre-optics based.

Even so, QKD has various intrinsic limitations.

- (i) The parties involved need to have expensive, dedicated equipment.
- (ii) The parties need to have already established an authenticated channel using ‘conventional’ (i.e. non-quantum) cryptographic means. A possible solution is pre-sharing in-person keys, which works for large institutions and a relatively small number of devices, but is not feasible at the scale of 90 billion devices.
- (iii) It can only be used at the data link layer. This restricts the application to point-to-point links and limits the distance over which it is possible to share keys, due to the degradation in the signal over long distances. A solution is to use ‘trusted’ relay nodes, but these introduce insider risks. Hence, QKD cannot provide end-to-end security over long distances.

There are also other limitations.

- (iv) Any practical implementation of QKD will have imperfections and deviate from the theoretical model. Thus, like other cryptographic systems, QKD devices have to be protected against side-channel attacks. Claims about unconditional security thus cannot be made about concrete implementation of QKD.
- (v) QKD devices are still lacking evaluation criteria that can be used to obtain certification, and more work is required in this area to have assurance about the security of concrete physical systems. For instance, issues around side-channel attacks have to be taken into account.
- (vi) The speeds are presently too low for many practical applications. Optimistically, speeds of 1MB/s might currently be reached, but this is too low, for example for video streaming. As such, symmetric cryptography, such as the commonly used AES algorithm, will have to be used for most of the encryption, making the system as a whole reliant on computational assumptions. Further improvements may be expected, but are unlikely to be in the multi-gigabyte capacity.
- (vii) Performance depends on the physical characteristics of the channel.
- (viii) QKD is especially sensitive to denial-of-service attacks, since the protocol stops whenever it recognises an eavesdropper.

Various developments in the area might provide solutions to the problems described above. Device-independent QKD promises to guarantee security even in situations where some devices are not trustworthy. Quantum repeaters might enable QKD over long distances without the need for trusted nodes. However, such technologies are not yet available or practical.

Regardless of any limitations of QKD, it remains an exciting area of research. Even if QKD is not ready for widespread use in the near to medium term, research in the area may have useful spillover effects.

As QKD devices are expensive, they are unlikely to be used by consumers in the near future. Instead, once the technology is sufficiently mature, the main users could be:

- governments (military and diplomatic communications),
- financial institutions (connections between data centres and main branches),
- critical infrastructure.

Various national cybersecurity agencies have taken stances on QKD.

- The **BSI** in Germany held in 2022 that QKD is only a solution for a limited set of use cases, is currently not sufficiently mature, and the priority should be the migration to quantum-resistant cryptography (BSI, 2022).
- **ANSSI** in France said in 2022 that QKD ‘may find some use in a few niche applications’, but the use of quantum-resistant cryptography is ‘by far the preferred way’ (ANSSI, 2020; 2022).
- **AIVD** (General Intelligence and Security Service) in the Netherlands found in 2022 that due to the limitations in functionality and the current immaturity of the technology, QKD without quantum-resistant cryptography is unsuitable for securing sensitive information against the threat of quantum computing, according to the Netherlands National Communications Security Agency (AIVD, 2022).
- The US **National Security Agency**, in 2020, did not recommend the usage of quantum key distribution (NSA, 2020).
- The UK’s **NCSC** (National Cyber Security Centre), in 2020, did not endorse QKD for government or military applications. It advised against replacing existing public key solutions with QKD in commercial applications (National Cyber Security Centre, 2020).

Quantum random number generators

Random numbers are needed for cryptography, including QKD, to be secure. They are used, for instance, for generating keys. Random number generation can be divided into two main categories: pseudorandom number generation (where cryptographic tools are used to generate numbers indistinguishable from random) and true random number generation (where a non-deterministic phenomenon, such as electrical circuit noise, is used as a source of randomness). QRNGs use quantum phenomena for true random number generation. Commercial products implementing QRNG have been available for years.

Even though the randomness of QRNGs is based on physical laws, the trustworthiness of the devices is still important to check. To this end, the European Space Agency carried out an analysis of some devices on the market. Even though these tests do not constitute any form of formal security assessment of the tested devices, endorsement or disapproval, they provide insight into the quality of the devices on the market now. The study found that most QRNG devices on the market failed statistical tests of randomness unless post-processing was applied.

Even if quantum theory can provide perfect randomness in theory, imperfections in implementation of QRNGs can easily undermine the theoretical benefits. For this reason, cryptographic post-processing of randomness produced by QRNGs is mandatory.



5. ETHICAL, GOVERNANCE AND POLICY ISSUES OF QUANTUM TECHNOLOGIES

Introduction

As we delve deeper into the realm of quantum technologies, it will become paramount to thoroughly examine the societal implications and ethical considerations these technologies are likely to bring. Indeed, in line with [comments](#) by the Responsible Technology Institute, as ‘potential use cases become clearer, the importance of preparing for and anticipating [their] effects becomes more urgent’. This chapter focuses on quantum computing and societal well-being. The next chapter will look more specifically into policy issues related to the intersection of quantum technologies and cybersecurity.

At present, our understanding of the potential impact of quantum technologies remains incomplete, as there are risks arising from the development of quantum technologies that we are currently unaware of and therefore have not yet considered (see Box 4). As such, perspectives on the impact of quantum technologies should be broadened to contemplate the wider societal implications that may result from quantum technological advances that are yet to unfold.

Because of the computing power that quantum technologies will make available, their societal impacts could be beneficial, for example, in developing new antibiotics to combat drug-resistant bacteria or in creating more efficient and selective catalysts for converting CO₂ into hydrocarbons. Nevertheless, as we move forward in the development of quantum technologies, it is important to address societal issues, such as equitable access to these solutions, ethical development, and respect for human rights, among others. Many of these concerns are not unique to quantum technologies.

Box 4. Quantum exceptionalism and ethics

The realm of quantum technologies involves emerging technologies that still hold many unknowns regarding their potential impact. Among these uncertainties is the significant security concern stemming from the potential of quantum computers to decrypt protected communications, which is especially worrisome for communications that have been intercepted and stored, awaiting a future where quantum capabilities might unveil them.

While the developer community generally believes in the positive effects (quantum advantage) that will arise from the adoption of quantum technologies, there are hence unforeseeable consequences and challenges. This has sparked a normative debate about whether quantum technologies should be viewed merely as accelerators of classical computers or as entities with their own distinct ethical implications.

There seem to be distinctive ethical implications related to quantum technologies. For example, in future there may be quantum technologies that enable fundamental changes to our world, such as those manipulating fundamental particles or gene editing. Manipulating fundamental particles through quantum technologies could lead to breakthroughs in computing and materials science.

At the moment, quantum technologies in the field of biology explore the potential quantum effects in biological systems and processes. Yet, they do not involve direct manipulation of genes at the quantum level. In fact, quantum computation technologies (including quantum simulators applied in quantum biotechnologies; see Mauranyapin et al., 2022) still have a narrow commercial distribution.

However, not all quantum technologies carry the potential for such profound alterations to our environment. Other applications with less disruptive potential, such as quantum sensing or quantum timing, come with their own set of distinct ethical considerations such as those related to equitable access to quantum technologies.

Thus, understanding the distinct ethical implications associated with each quantum technology is crucial.

In this context, it is also worth noting that quantum supercomputers will not operate autonomously in the technological landscape. Instead, they will be integrated within a computational architecture that encompasses next-generation high-performance computing, advanced cloud infrastructure and emergent Machine Learning paradigms. Ethical considerations will have to be based on the cumulative capabilities of this computational framework.

Responsible quantum technologies

The field of quantum technologies provides an opportunity for proactive engagement in shaping a framework for responsible usage and developing principles prior to the widespread commercialisation of the technology. By taking a proactive approach, ethical considerations can be embedded in the development and deployment of quantum technologies, thereby promoting their *responsible* use, design and development in society.

In the context of quantum technologies, the term *responsible* refers to the use of 'quantum technologies that are aware of the power of their effects'²⁶. It encompasses considering the implications of the technology, understanding the magnitude of its effects, and taking proactive measures to prevent and mitigate potential harm. Responsible quantum technologies entail ensuring that solutions are sustainable, accessible and inclusive for both Global North and

²⁶ As described by Mira Wolf-Bauwens in *Ethics, Governance and Politics of Responsible Quantum Computing*, presentation at the Third Meeting of the Quantum Technologies and Cybersecurity Task Force in 2023.

Global South countries, explainable and accountable, and that development and use of the technology are guided by well-defined principles of responsibility.

Before delving into the governance of quantum technologies, it should be acknowledged that many of the well-established principles of good governance apply to this domain as well. That said, governing quantum technologies presents unique challenges. This field is not only evolving at an unprecedented speed, but also our mid-term understanding of the technology, its use cases and its potential interconnections with other emerging and unpredictable technologies (such as generative AI and large language models) is still quite limited²⁷. In light of the rapidly changing landscape of quantum technologies, some suggest that adopting a principles-based approach to governance might be beneficial in certain areas.

Some general principles for quantum-responsible governance merit highlighting. Scholars have divided principles for responsible governance of quantum technologies into three main areas (see Table 1): (i) safeguarding against risks, (ii) engaging stakeholders in the process and (iii) continuing to advance quantum technologies (Kop et al., 2023a; 2023b). In this chapter and the following chapter, such high-level responsibility principles will be dealt with in more detail, further developing the operationalisation of the guiding principles.

The aim of safeguarding against risks brought by the adoption of quantum technologies encompasses aspects related to information security and problems related to dual-use quantum technologies and the international quantum race. These problems are not solely related to quantum technologies but have also shaped the current discussion on AI technologies.

Both quantum technologies and AI have profound implications for information security. For instance, quantum computing has the potential to break existing cryptographic methods, thereby revolutionising the entire field of secure communication. Similarly, AI technologies are used in cybersecurity applications but can also be exploited to execute more advanced and targeted cyber-attacks. Consequently, governance frameworks for both need to prioritise information security, examining how to protect against the misuse of these powerful technologies.

The second principle suggests that engaging stakeholders – such as academia, NGOs or the private sector – with inclusive and participatory design throughout the process of developing and deploying quantum technologies should be guaranteed. Principles for inclusive stakeholder engagements have been encouraged by institutions such as the Open Quantum Institute and will be discussed more in detail below.

²⁷ Some participants on the Task Force suggested that the possible unique characteristics of quantum technologies relate to the increased market concentration in the quantum sector, which is in the hands of a few players, compared with, for example, the AI sector. What is more, according to some participants, access to quantum capabilities can be more feasibly restricted through export controls on key components.

Finally, advancing quantum technologies would require, according to the framework, cross-disciplinarity, ongoing and transparent dialogue, and inclusive education on quantum.

<i>Table 1. Principles of responsible quantum technologies</i>			
Category	Topic	Aim	Principle
Safeguarding	Information security	Addressing security threats	Consider information security as an integral part of QT
	Dual use	Addressing risks of dual use	Proactively anticipate the malicious use of quantum applications
	Quantum race	Addressing winner-takes-all dynamic	Seek international collaboration based on shared values
Engaging	Quantum gap	Engaging states	Consider our planet as the sociotechnical environment in which QT should function
	Intellectual property	Engaging institutions	Be as open as possible and as closed as necessary
	Inclusion	Engaging people	Pursue diverse R&D communities in terms of disciplines and people
Advancing	Societal relevance	Advancing society	Link quantum R&D explicitly to desirable societal goals
	Complementary innovation	Advancing technology	Actively stimulate sustainable, cross-disciplinary innovation
	Responsibility	Advancing our understanding of RQT	Create an ecosystem to learn about the possible uses and consequences of QT applications
	Education and dialogue	Advancing collective thinking and education	Facilitate dialogue with stakeholders to better envisage the future of QT

Note: QT refers to Quantum Technologies; RQT refers to Responsible Quantum Technologies

Source: Authors' elaboration based on Kop et al. (2023b).

However high level, these principles could offer a preliminary guiding framework to foster a conversation on the responsible development and application of quantum technologies, considering various ethical and societal dimensions.

World Economic Forum quantum computing governance principles

At the level of international organisations, discussions on responsible quantum technologies have been carried out foremost at the WEF. In 2021, the organisation launched an initiative among national and civil government experts to kickstart discussion on responsible quantum computing.

The primary objective of this initiative was to establish a shared understanding of the current state of technology development. Central to this effort was the identification of core values and the formulation of policy principles and related action items. The core values that emerged from these discussions are transparency, the pursuit of the common good, accessibility, non-

maleficence, equitability, inclusiveness and accountability (WEF, 2022). Albeit acknowledging that these values and practices may not always be universally applicable, the incorporation of core values into the definition of core governance themes has been regarded as a crucial aspect, as it encourages the identification of shared practices within the community.

A key governance objective identified in the WEF's work has been ensuring equitable access to the hardware infrastructure of quantum technologies, thereby avoiding the risks of knowledge monopolies among an expert elite and the exacerbation of existing inequalities.

Promoting responsible quantum technologies should also entail, according to the WEF, increasing public awareness, engagement and informed decision-making among the general public and stakeholders. This aims to demystify the hype surrounding quantum computing, which is often intentionally propagated to justify new research areas and investment. Similarly, raising awareness is crucial in countering misinformation about quantum technologies, which can lead to fear and mistrust.

To achieve this, recommended actions include a focus on scientific facts. In this context, it is essential according to the WEF to cultivate public engagement through open dialogue about quantum computing's potential and applications. This dialogue can be enhanced by showcasing responsible and ethical quantum use cases. Communication clarity is paramount: spokespeople and science communicators should be encouraged to use accurate and measured language, steering clear of hyperbole.

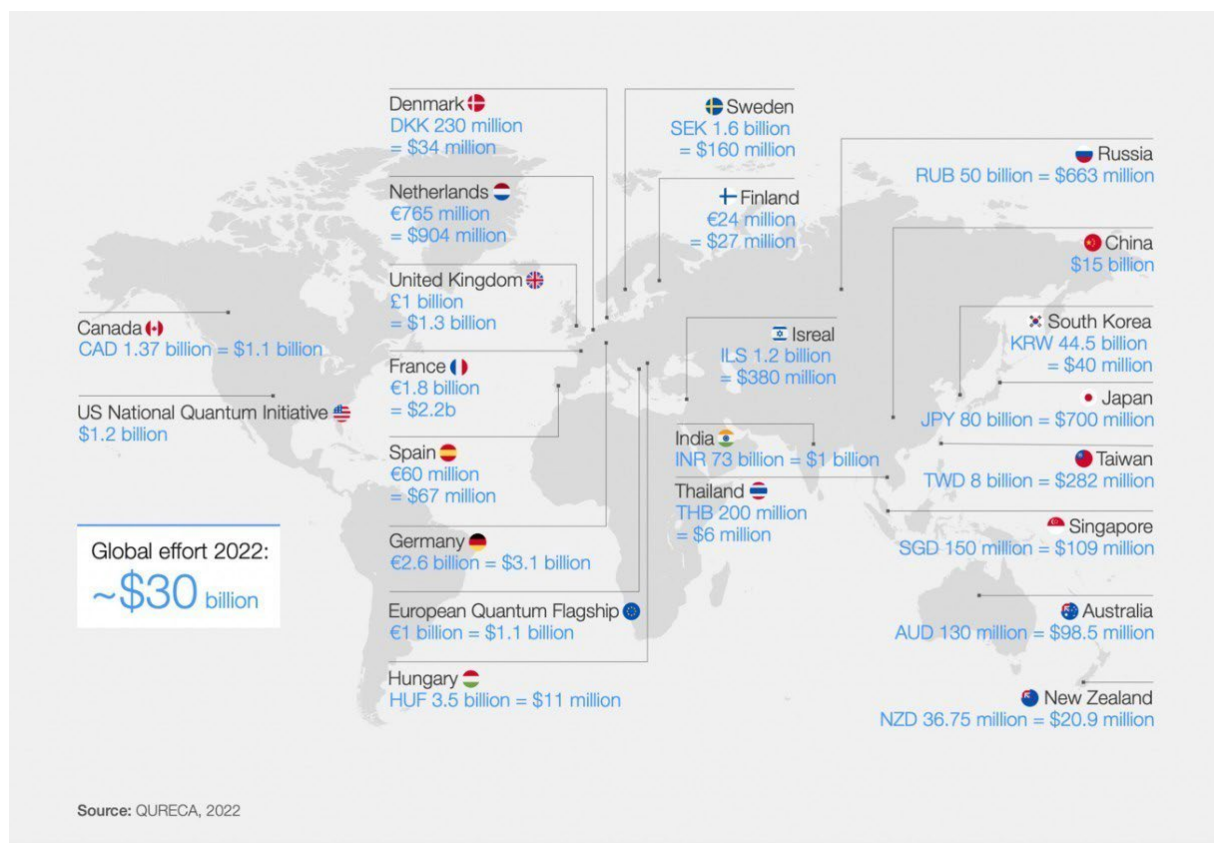
In tandem, interactive forums should bridge the gap between quantum experts and media representatives, ensuring that quantum computing is portrayed responsibly in the public domain. Furthermore, fostering platforms where diverse stakeholders can exchange views can enrich the discourse. Finally, underpinning these initiatives with data, through tools like surveys and focus groups, can help tailor public awareness campaigns and ensure they offer science-based, clear and accessible information about quantum technology.

Sustainability also emerged as one of the core governing principles. Indeed, quantum technologies have the potential to make a significant impact in the fight against climate change, by leveraging quantum advantages to reduce energy consumption. According to the WEF (2021), 'quantum computers will be capable of optimising power grids and [predicting] the environmental effect of various energy-producing and transportation methods' (see also Berger et al., 2021). The WEF also holds that 'the much higher efficiency of a quantum-based calculation device will make the energy consumption significantly smaller than if using conventional computers for the same tasks' (WEF, 2021).

Equitable access to quantum technologies

As mentioned, addressing equitable access to quantum technologies is deemed a fundamental aspect in the development of quantum-responsible technologies. When examining the distribution of global investment in quantum technologies, it becomes evident that the majority of this investment is concentrated in the Global North while there is a notable lack of investment in Latin America and Africa (see Figure 5).

Figure 5. Public and private financing for quantum technologies worldwide



Note: Some investments in Thailand, India and South Africa are not listed. According to the quantum research and consulting firm GQI, South Africa invests around USD 3.2 million.

Unsurprisingly, countries with limited investment in quantum technologies are also less likely to have established national strategies for quantum technologies. This raises concerns regarding the equitable distribution of the benefits that quantum technologies can offer, and the risk of a digital divide in view of where investment is focused. Approximately half of global investment in quantum technologies comes from China, reflecting a shift towards Beijing as the 'centre of mass' for innovation investment. These disparities have significant implications in terms of workforce development, talent acquisition and awareness raising of the cybersecurity risks associated with the increasing adoption of quantum technologies.

Multinational corporations could potentially fill this void by investing in the Global South. However, companies might fairly prioritise profit-making over equitable access. To address this, one potential strategy could be to encourage open-source development of quantum software, which could help promote more equitable access to quantum technologies in the Global South. In addition, the EU or the international community at large could create joint funds for promoting the development of quantum technology in the Global South by private actors.

Similarly, the availability of quantum computers in the cloud could represent a step towards fair quantum access. Quantum computers have been available in the cloud for a few years. This has allowed for the execution of prototype quantum software applications directly on the underlying hardware, enabling the implementation of real-world use cases. Assuming that a country has sufficient bandwidth for cloud operations, this cloud-based approach could enhance the accessibility and scalability of quantum applications (see Box 5). At the same time, they introduce potential cybersecurity risks, since the possibility of detecting attacks may be limited.

In this context, a more liberal²⁸ approach would advocate for treating quantum technologies as a common good, making them widely accessible while implementing measures to prevent malicious use. Conversely, a more realist²⁹ viewpoint would prioritise security considerations and potential risks, and would not consider access to these technologies a universal right. Hence, the question of international governance of quantum technologies is complex, requiring a balanced approach that incorporates both perspectives and identifies specific areas of cooperation among international actors.

Exploring use cases tied to sustainability, health and the UN Sustainable Development Goals (SDGs) could serve to initiate an international dialogue on the societal impact of quantum technologies.

Box 5. Fostering equitable quantum access: The Open Quantum Institute

The Open Quantum Institute, established by GESDA, a Swiss independent private not-for-profit foundation, is an initiative with the objective of ensuring global and inclusive access to quantum technologies. The primary focus of the Open Quantum Institute is to accelerate the adoption of quantum technologies aligned with the UN SDGs. It aims to achieve this by providing fair access to quantum computers through cloud-based platforms. Ultimately, the goal of the initiative is the establishment of a multilateral governance framework for leveraging quantum technologies to address the SDGs.

²⁸ *Liberal* here refers to the specific theoretical perspective of international relations theory, which emphasises the importance of states' economic and institutional cooperation in shaping the international system. Liberals believe that states can work together to achieve common goals and promote peace and stability.

²⁹ *Realist* here refers to the specific theoretical perspective of international relations theory. In contrast with liberal views, realism focuses on the competitive and power-driven nature of international relations.

The Open Quantum Institute is currently in its incubation phase. The incubation plan encompasses four key pillars.

- Establish a centre of expertise for utilising quantum technologies in addressing SDG use cases. This involves bringing together domain experts from various fields. Currently, teams of experts are working on a range of topics, including climate change, food security, biodiversity and health security.
- Secure a broad pool of resources in state-of-the-art quantum technologies and make them globally accessible.
- Upskill users and develop educational tools specific to quantum technologies. The target audience for these tools consists of two core groups: research and development professionals from quantum-underserved regions and diplomats seeking to enhance their understanding of quantum technologies.
- Actively foster diplomatic and expert meetings to facilitate discussions and collaborate in the development of effective governance mechanisms.

Within the context of the Open Quantum Institute's initiatives, a range of use case solutions aligned with the SDGs has been identified.

One such use case is the development of carbon capture materials. Quantum computers can be utilised to design and optimise materials that capture and store carbon dioxide, thereby helping to mitigate climate change and achieve SDG 13 (Climate Action).

Another identified use case concerns the presence of antibiotics in wastewater. Quantum technologies can aid in developing advanced purification methods that effectively remove antibiotics from wastewater, reducing the risk of antibiotic resistance and supporting SDG 6 (Clean Water and Sanitation).

Sustainable fertiliser production is another key use case. Quantum technologies can contribute to the design and optimisation of eco-friendly and efficient fertiliser production processes, promoting sustainable agriculture and supporting SDG 2 (Zero Hunger).

Finally, quantum technologies can optimise food production and vaccine distribution. By leveraging quantum algorithms and simulations, supply chains can be optimised to minimise waste, ensure efficient distribution of vaccines and enhance food production processes, thereby contributing to SDGs 2 and 3 (Good Health and Well-being).

Quantum technologies and privacy

The intersection of quantum technologies and privacy raises important considerations. As explained earlier, quantum technologies' computational power would render current encryption methods obsolete, potentially compromising the privacy and security of individuals' personal data, communications and sensitive information. This raises concerns about the right to privacy and the need for robust encryption algorithms that can withstand quantum attacks.

In the context of vulnerability disclosure, individuals who discover security flaws or weaknesses in software or systems may argue that they should be granted the possibility to access encrypted data to assess the security risks and report them to relevant authorities. This aligns with the principles of transparency and accountability, allowing for the identification and mitigation of potential threats.

The potential of quantum computing to break traditional encryption introduces a distinctive dimension to the tension between privacy and decryption. Indeed, decryption in the quantum context becomes critical for studying vulnerabilities in encryption methods and developing quantum-resistant cryptographic solutions.

Governments could, theoretically, undertake steps to strike a balance between these interests, namely:

- stimulate research, publish results and ensure access to quantum technologies and quantum research that is fair, reasonable and non-discriminatory;
- ensure court oversight of public decryption and the removal of keys after decryption.

Prohibiting private decryption, while auspicious, could nonetheless be particularly hard to enforce. For example, in the case of decrypting RSA, a public key cryptosystem, the key can be broken on a quantum computer with no knowledge about what it was used to encrypt, as the public key can be separated from the protected file.

Governance of quantum technologies

The rapid advance of quantum technologies has brought forth complex regulatory challenges. Possible future regulation of quantum technologies will have to encompass, as done for a number of emerging technologies, a wide range of considerations – including ethical implications, privacy concerns and cybersecurity risks.

In regulating quantum technologies, the precautionary principle is relevant. The precautionary principle enables decision-makers to adopt precautionary measures when scientific evidence about an environmental or human health hazard is uncertain and the stakes are high. One

essential question is thus whether, when confronted with technologies that are high risk, governments should apply the precautionary principle.

The precautionary principle can serve as a valuable tool to address potential risks and uncertainties associated with the rapid development and deployment of quantum technologies enabling policymakers to take proactive measures to prevent or minimise potential harm.

However, there are also potential drawbacks and challenges in adopting a precautionary approach. One concern is the potential for excessive regulation or stifling innovation. The precautionary principle, if applied too rigidly, may lead to over-cautious decision-making, slowing down technological progress and hindering the exploration of quantum technologies' transformative potential.

Mechanisms that balance both effectiveness and flexibility in regulation could be considered, allowing for more nuanced risk management strategies. One such governance strategy might involve the use of regulatory sandboxes for areas that are not yet fully understood or which may carry higher risks. Having a system in place to capture insights and lessons could help inform the adaptation of existing governance frameworks to better suit this evolving field. This approach has been discussed and, in some instances, applied in the governance of AI to explore its benefits and limitations in a controlled manner. Just as in AI, where lessons from real-world deployments and pilot programmes often inform broader governance strategies, a similar iterative approach could be beneficial for quantum technologies.

Any regulatory principle will also need to be implemented in a way that will be consistent with existing international norms and standards, and where needed with new international standards. Harmonisation across different jurisdictions will be pivotal to avoiding fragmented and conflicting approaches that could hinder the global development and deployment of quantum technologies.



6. QUANTUM TECHNOLOGIES AND CYBERSECURITY: POLICY IMPLICATIONS

Introduction

In the previous chapter, we looked at the establishment of a quantum-responsible ecosystem to ensure equitable access, and responsible and inclusive development. This chapter explores, more granularly, the policy implications of the diffusion of quantum technologies and cybersecurity.

The Task Force has highlighted the following issues that need to be addressed in order to mitigate the potential drawbacks from the diffusion of quantum technologies and to ease the adoption of these technologies in the EU:

- policies to promote the standardisation of quantum-resistant cryptography through harmonised cryptographic standards;
- policy initiatives to assess the potential risks and threats posed by quantum technologies;
- policies to ease the transition to quantum-resistant cryptography;
- international coordination and the sharing of best practices;
- awareness raising about quantum technologies among leaders in both the public and private sectors;
- a future-ready workforce with skills in quantum technologies;
- dual-use and export control policies;
- civilian and military coordination and cooperation;
- research policies.

We aim to shed light on these multifaceted policy dimensions, and on the complexities and opportunities presented by the interplay between quantum technologies and cybersecurity.

A key policy concern is the shift towards quantum-resistant cryptography. In the present landscape, it is essential to support organisations in the transition to quantum-resistant cryptography. Despite the proliferation of initiatives at the EU level, the migration to quantum-resistant cryptographic algorithms still seems to be rather uncoordinated across Europe. National guidelines sometimes diverge and propose frameworks that are at times challenging in terms of the practicality of the proposed schemes. While the US has established a clear deadline for the transition to post-quantum cryptography (2033), the EU has not yet set such a deadline .

Policies to foster the standardisation of quantum-resistant cryptography

Coordinating EU efforts in standardisation and implementation is essential to avoid fragmented approaches and to create a robust global defence against quantum threats. As mentioned, the standardisation of quantum-resistant cryptographic algorithms has involved various actors, including researchers, cryptographers, policymakers and industry experts from around the world.

The process is being led by the National Institute for Standards and Technology (in the US, which has organised a series of public competitions, conferences and workshops to solicit contributions and evaluations from the global research community. Countries and international organisations are actively participating in the standardisation effort by providing submissions and evaluations of proposed cryptographic algorithms. Some of the key actors involved in the collaboration include researchers and experts from the US, EU Member States, Canada, Japan, South Korea, Australia and a few other countries. The collaboration has extended to industry players and private sector organisations, which also provide feedback on the practicality and usability of the proposed algorithms.

Various other standardisation processes are concurrently underway (see Box 6). In this context, it is crucial to evaluate potential risks associated with what can be described as a ‘certification overload’ scenario: the anticipated surge of organisations seeking certification once the NIST standards are officially released.

While a notable amount of quantum research originates in the EU, the EU appears to be somewhat influenced by the US in the standardisation process. For example, algorithms like ML-KEM and ML-DSA were developed by European researchers with European funding. The intricate process of achieving agreement among EU Member States might contribute to a more cautious approach by the EU, which could in turn leave room for external influence, such as from the US, in shaping standards.

As mentioned elsewhere in this report, NIST announced, in July 2022, the first quantum-safe cryptography protocol standards for cybersecurity. By 2033, all public key cryptography in the US will be replaced following these standards. All of the US federal government, hence, will have moved to quantum-resistant cryptography by 2033, and by 2025 companies will be excluded from the procurement preferred list if their technology is not quantum-resistant. This operation entails approximately USD 100 billion per year and will represent a massive commercial incentive for companies to start offering this technology.

The implementation rate of these quantum-resistant cryptographic algorithms is still quite low, especially within the EU. Historically, migration to new cryptographic standards has taken around 10 to 15 years. Thus, it is pivotal to start having a conversation about how to foster the adoption of quantum-resistant cryptographic algorithms, especially considering that there are around 50 years of quantum-vulnerable legacy. Quantum-vulnerable legacy refers to cryptographic systems set up prior to the advent of quantum computers that are susceptible to attacks by quantum computers. There is a need to migrate from legacy cryptography to quantum-resistant cryptography.

However, many security governance frameworks have offered little or no guidance to industries on how to govern cryptographic vulnerabilities. Among the key aspects are where cryptography is being used, how to manage migration to new generations of cryptography, how to establish a policy for the retirement of older cryptography and how to enforce minimum security policy for cryptography usage.

*Box 6. Standardisation policies beyond NIST**

Much of the attention on standardising quantum-resistant cryptography is focused on NIST. But other organisations are also participating in the standardisation effort. In particular, the Internet Engineering Task Force standardises protocols that use cryptographic algorithms.

Each internet security protocol, such as TLS, IPsec, DNSSEC and S/MIME, has its own working group in the IETF. Those working groups are moving separately on their own transition mechanisms, including choosing which of the NIST standards they will use. The work is being loosely coordinated by the executive management of the IETF, the Internet Engineering Steering Group. The IETF also recently created the Post-Quantum Use in Protocols (PQUIP) Working Group to support communication within the IETF, although PQUIP is not allowed to create protocols of its own.

The NIST standardisation process will soon define one key encapsulation mechanism (KEM)³⁰ and three signature algorithms, followed by additional KEMs and signature algorithms a few years after that. The IETF's working groups are considering whether to concentrate solely on the first KEM and the first signature from NIST or to describe how to use the additional NIST algorithms. A few considerations are also being given to algorithms standardised by other organisations.

The policy issue of which algorithm to choose will significantly affect when and how the migration to quantum-resistant algorithms happens. Many organisations feel the need to start using quantum-resistant KEMs, and it is likely that the initial policy for most countries and organisations will be to use the first NIST KEM algorithms as soon as possible. It is currently unclear how rapidly the first NIST signature algorithms will be required by such policies. The software and hardware industries often move faster than government policy development, and as such, it is possible that there will be a significant amount of deployment of quantum-resistant cryptography even before the matching policy requirements.

Besides standardisation at NIST, there is an ongoing effort to standardise KEMs in ISO/IEC SC 27 / WG 2. This includes the schemes FrodoKEM and Classic McEliece, which have been candidates in the NIST standardisation process and are regarded as conservative options for key agreement, as well as ML-KEM, which will be standardised in close coordination with NIST to achieve compatible standards.

* This text was contributed by ICANN as a participant on the Task Force.

³⁰KEMs are used in secure communications protocols where endpoints use public key encryption to establish a shared symmetric key without needing secrets to be passed over an insecure communication channel.

Policy initiatives to assess the potential risks and threats of quantum technologies

As already explained in detail in Chapters 2 and 3, organisations that manage their own cryptographic infrastructure should factor a quantum-resistant transition into their long-term plans and conduct investigatory work to identify which of their systems will be a high priority for transition. Thus, organisations should conduct an assessment of quantum vulnerability. Priority systems could be those that process sensitive personal data, or the parts of the public key infrastructure that have certificate expiry dates far into the future and would take a longer time to replace.

A very important initiative for quantum vulnerability assessment is the US National Defense Authorization Act (NDAA). In 2021, Congress passed the NDAA, mandating that the US Department of Defence ‘perform a comprehensive assessment of potential risks and threats posed by Quantum Computing technologies’ (WEF, 2021). The act states that this entails the following aspects:

- identification and prioritisation of critical national security systems at risk;
- assessment of NIST standards for quantum-resistant cryptography and their application to the cryptographic requirements of the Department of Defence;
- assessment of the feasibility of alternate quantum-resistant algorithms and features;
- description of any funding shortfalls in public and private developmental efforts on quantum-resistant cryptography, standards and models;
- development of recommendations for research, development and acquisition activities, including resourcing schedules, for securing critical national security systems against quantum computing code-breaking capabilities.

In addition, the US Department of Home Affairs and NIST have developed a [post-quantum cryptography roadmap](#), which includes the identification and inventory of vulnerable critical infrastructure systems across the 55 national critical functions. These critical functions comprise provision of internet-based content, information and communication services, identity management and associated trust support services, information technology products and services, and the protection of sensitive information, as [outlined by CISA](#) (the Cybersecurity and Infrastructure Security Agency).

The European Commission could promote a similar initiative through recommendations to guide Member States and companies on how to approach the cybersecurity risk aspects of quantum computing.

Policies for the transition to quantum-resistant cryptography

Nations and organisations are recognising the urgent need to prepare their cryptographic infrastructure. At the policy level, organisations can already start taking some steps.

- Perform a quantum risk assessment. This should include producing an inventory of current cryptography protection³¹, identifying the values of S , M and Q in Mosca's inequality (the amount of time that data must remain secure (S); the time it takes to upgrade cryptographic systems (M); and when quantum computers come online with enough power to break current encryption schemes (Q))³².
- Raise and maintain awareness.
- Evaluate the quantum resistance of other vendors.
- Partner with service providers with which the organisation is intertwined.
- Develop an internal knowledge base among IT staff.
- Track the developments in quantum computing and quantum-resistant solutions.

Establish a roadmap towards quantum readiness.

Different actors have different levels of urgency for transitioning their systems. Reasons might include store-now-decrypt-later attacks, long-lived systems (such as infrastructure and IoT), and having a system that is especially time-consuming to migrate (for instance, a public key infrastructure).

As mentioned, there is a link between the types of data and how long they must be kept confidential (the S in Mosca's inequality). In some settings, long-term confidentiality is not as important, and migration is not as urgent. Similarly, when considering digital signatures, particularly in contexts where resigning is an option, the dynamics can vary. If resigning is feasible, entities can essentially renew or update their digital signatures as needed. This flexibility means that there might not be a pressing urgency for a complete migration. This resigning capability offers a safety net for certain systems, granting them a grace period to strategize their migration without compromising their security posture.

³¹ When conducting this inventory some Task Force members believe that companies should consider whether a given use of cryptography is truly fulfilling a security need. It is possible that some security needs can be fulfilled without the use of cryptography and the related costs arising out of the new quantum-resistant algorithms and of transitioning to them

³² Some members of the Task Force argued that this might be very difficult to estimate, and hence will look to either regulatory bodies or industry leaders to assess it.

Examples of the transition to quantum-resistant cryptography in selected countries

As quantum technologies are still evolving, the status of the transition to quantum-resistant cryptography varies among countries, with some leading in research and implementation, while others are in the early stages of developing strategies and policies.

Here the cases of the US and the Netherlands are presented. A more detailed overview of other countries within and outside the EU can be found in Appendix C.

United States

An Office of Management and Budget [Memorandum](#) states that the US must prioritise the transition of cryptographic systems to quantum-resistant cryptography by 2035, with the goal of mitigating as much of the quantum risk as feasible. The process to make this happen involves an inventory of cryptographic systems, an annual assessment of the funding needed, designating a migration lead and testing pre-standardised quantum-resistant algorithms.

In September 2022, the US National Security Agency released 'Commercial National Security Algorithm Suite 2.0', a cybersecurity advisory notifying operators and vendors of national security systems of a forthcoming transition to quantum-resistant cryptography. In addition to the quantum-resistant algorithms being standardised by NIST, the suite recommends the symmetric-key algorithm AES, the hashing algorithm SHA and hash-based stateful schemes for signing.

The transition to quantum-resistant cryptography in the US is a process that started long ago. In 2015, the National Security Agency sounded an alarm on the quantum threat by advising NATO partners against changing to a more modern version of classical cryptography (Suite B). Instead, the advice was to transition directly to quantum-resistant cryptography.

Moreover, CISA also announced the [Post-Quantum Cryptography \(PQC\) Initiative](#), which includes supporting critical infrastructure and government network owners and operators during the transition to post-quantum cryptography.

Importantly, the National Cybersecurity Center of Excellence (NCCoE) has developed a project on migration to quantum-resistant cryptography. The NCCoE PQC is a flagship project aimed at raising awareness, developing practices to ease migration, and delivering white papers, playbooks and demonstrable implementation (see Box 7). The NCCoE is engaging with industry collaborators, regulated industry sectors and the US federal government.

In sum, the NCCoE practice guide should help an organisation:

- identify where, and how, public key algorithms are being used in information systems;
- mitigate enterprise risk by providing tools, guidelines and practices that can be used by organisations in planning for the replacement/update of hardware, software and services that use quantum-vulnerable public key algorithms;
- develop a risk-based playbook for migration involving people, processes and technology.

This practice guide should also help product and service producers:

- perform interoperability and performance testing for different classes of technology;
- strengthen cryptographic discovery tools to produce actionable reports;
- understand the potential impact that transitioning from quantum-vulnerable algorithms could have on their products and services.

Box 7. In detail: The NCCoE PQC project

The primary objective of the NCCoE is to deliver cybersecurity capabilities based on industry standards. It seeks to address the challenges associated with the adoption of NIST-standardised algorithms. In this capacity, the NCCoE complements NIST PQC standardisation efforts. The centre assembles commercial off-the-shelf open-source technologies and builds demonstrations in the facility labs.

The NCCoE has also developed a practical guide that complements the NIST series. This guide includes a C-suite executive summary, a reference architecture, use cases, security documentation and implementation guidance. Additionally, it provides bills of material, scripts, codes and tools to facilitate the replication and adaptation of the lab demonstrations in various contexts. In other words, the centre has put together a step-by-step guide on what was done during the lab demonstrations so it can be replicated and adapted to different settings.

The NCCoE has published a playbook and cybersecurity paper on migration strategies and developed open-source codes, such as a proof of concept code. Finally, the centre engages in outreach activities.

In planning their migration process, states or organisations should first carry out an inventory of where the cryptography algorithms are implemented. In order to effectively perform the inventory, discovery tools are critical.

The NCCoE leverages automated tools to discover the use of quantum-vulnerable cryptography within an organisation in hardware, firmware, software, protocols and services and it uses a risk-based approach to prioritise their replacement. The discovery of vulnerable algorithms in an organisation is performed in three main ways. First, vulnerable algorithms can be detected in the code development pipeline. Second, they can be detected while in use by looking at the operational network services and protocols and by analysing the network traffic and protocols being used. Finally, the discovery tools can detect the usage of vulnerable algorithms on the host (i.e. for Linux machines there is a discovery tool that can scan the machine and look for programmes and/or files using vulnerable algorithms).

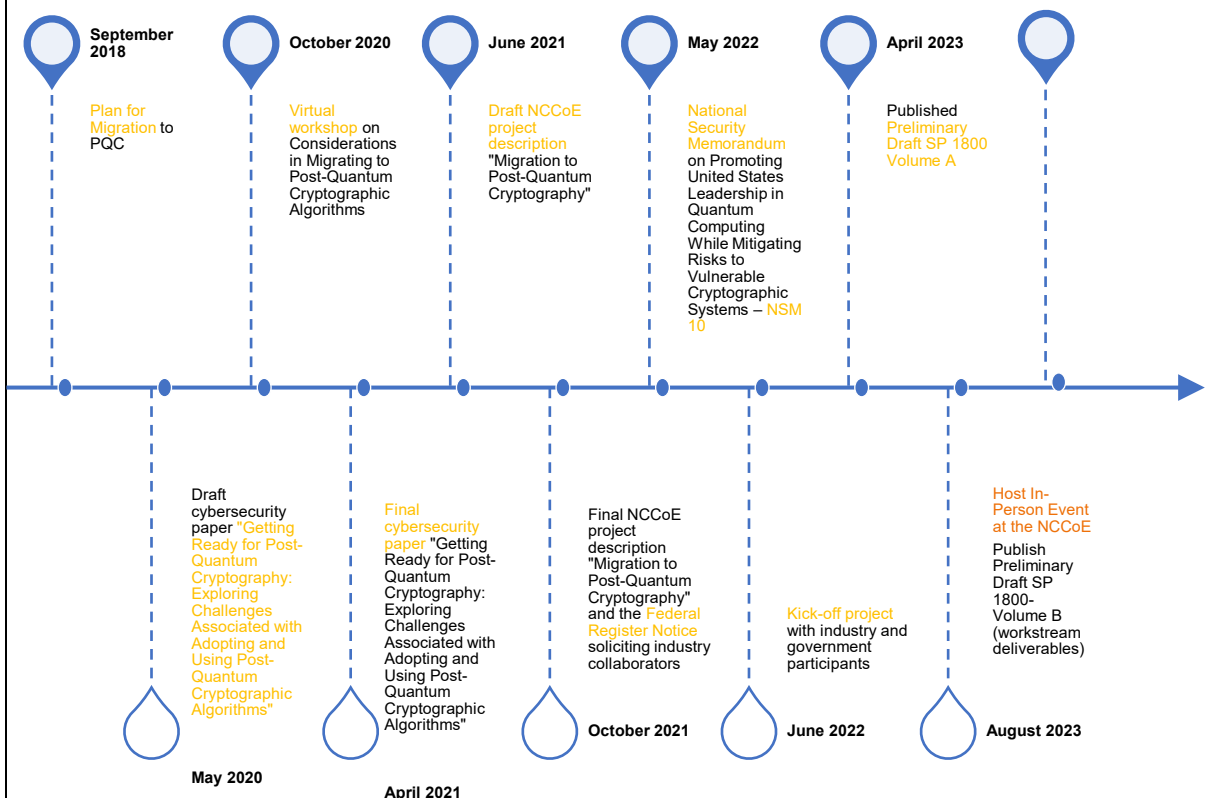
The output of this discovery system is then correlated with the system running within the organisation and fed into a risk assessment engine to establish which system needs to be migrated first. This creates a prioritisation list of the need for migration based on the risk assessment. The NCCoE works with commercial providers that have discovery tools in place and provides support in the integration phase of these tools with the system database.

Other workstreams carried out by the NCCoE relate to interoperability and performance. The interoperability workstream aims at demonstrating interoperability between collaborators’ software and hardware components implementing the same algorithm or standard. It is also developing and demonstrating known answer tests and test vectors for the NIST-standardised algorithms.

The performance workstream aims at identifying the performance metric of quantum-safe algorithms. Currently, performance tests are carried out on both quantum-resistant-only algorithms and hybrid ones.

The timeline in Figure B7.1 provides an overview of the NCCoE migration roadmap. In a later phase, the project will also look at how cryptographic agility can be realised in different contexts. It is important to recognise that not all software can be seamlessly migrated; therefore, appropriate mitigation strategies need to be devised. The use of proxies or tunnels for vulnerable algorithms that incorporate quantum-resistant cryptography may prove valuable in addressing this issue.

Figure B7.1 Timeline for NCCoE migration to quantum-resistant cryptography



Sources: US National Cybersecurity Center of Excellence; Task Force on Quantum Technologies and Cybersecurity, presentation.

The Netherlands

TNO (Netherlands Organisation for Applied Scientific Research), CWI (Centrum Wiskunde & Informatica) and AIVD's National Communications Security Agency have jointly published a [handbook](#) on migration to quantum-resistant cryptography. The process of writing the handbook also included partners from industry.

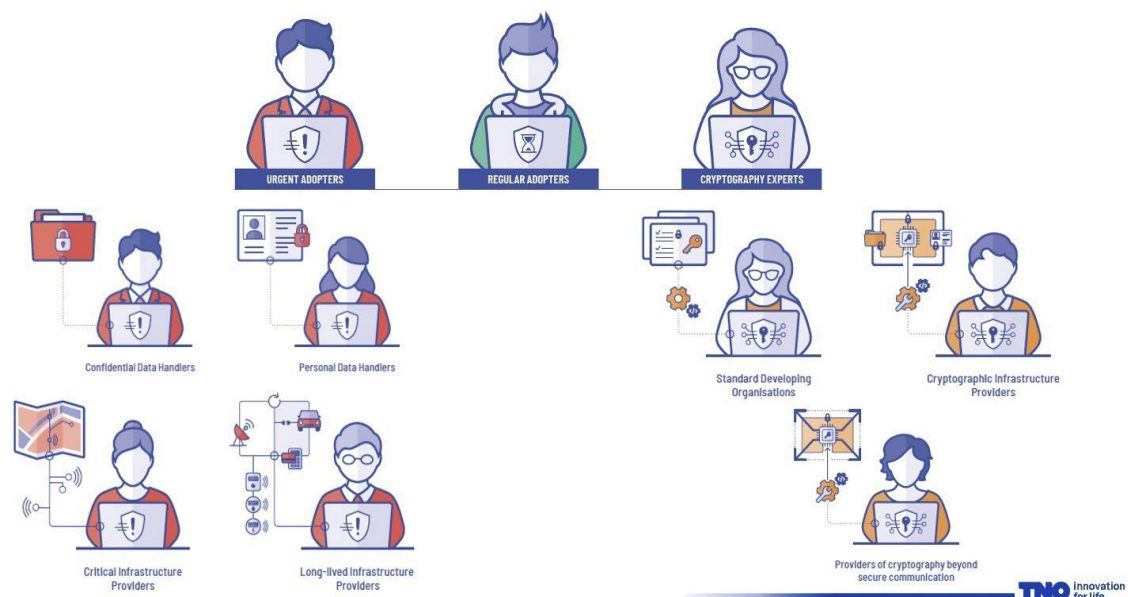
In planning, urgent cases would migrate on a fast track by early 2025 and other use cases would complete the migration by 2028.

The handbook is aligned with the three-step approach of the European Telecommunications Standards Institute – diagnosis, planning and execution.

The diagnosis step should help organisations identify whether they need to take steps towards migration as soon as possible or can wait a bit more. Different PQC 'personas', i.e. urgent adopters, regular adopters and cryptography experts (see Figure 6), are identified depending on:

- attack surface
- system types
- data types
- time pressure
- dependency on other organisations
- threat level.

Figure 6. TNO PQC Migration Handbook, post-quantum cryptography personas



Sources: TNO; Task Force on Quantum Technologies and Cybersecurity, presentation.

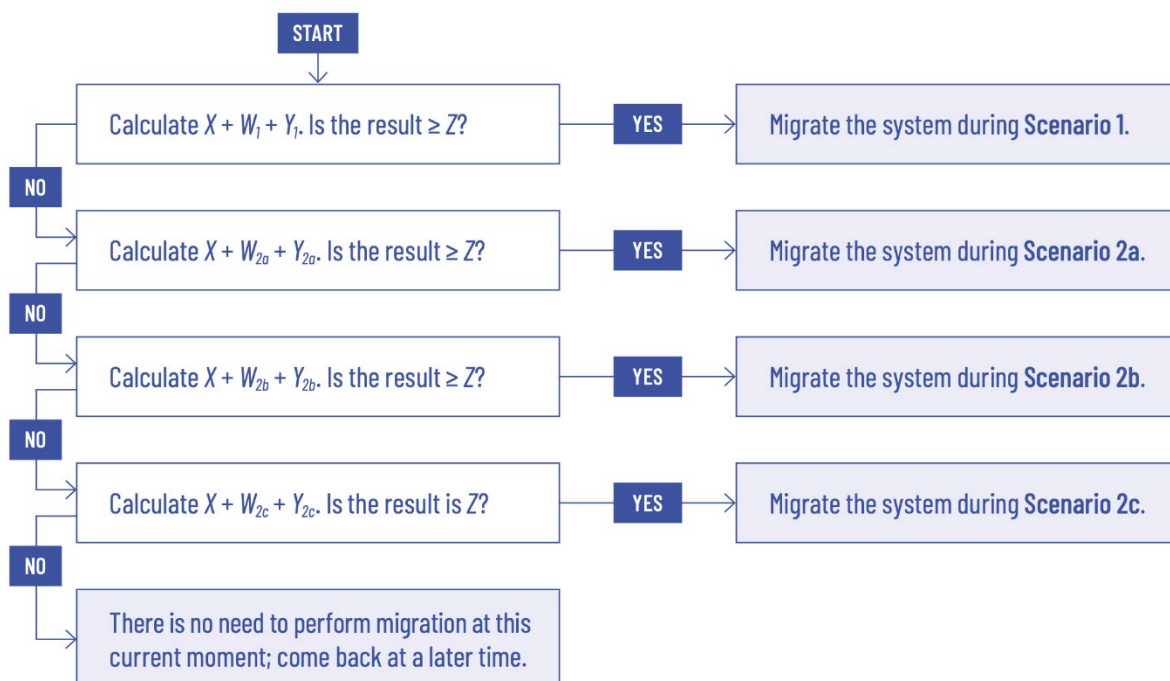
According to the handbook, there are three levels of cryptography an organisation is responsible for: (i) its own cryptographic infrastructure, (ii) its cryptographic knowledge and (iii) the cryptographic infrastructure related to supplying services or products to other organisations. Each of these three has to be considered when migrating to quantum-resistant cryptography and determining what kind of persona best fits.

Once an organisation has established what kind of PQC persona it is, it can start planning the migration. According to the handbook, knowledge of the following information is a prerequisite for the establishment of a suitable migration plan:

- risk assessment,
- inventory of all cryptographic assets used in the organisation,
- inventory of all the data handled by the organisation,
- inventory of the suppliers of cryptographic assets.

An organisation that has decided to migrate and has completed the preparatory phase must identify when to migrate by applying Mosca's inequality. In Figure 7, the application of Mosca's inequality leads to different decisions as to when to migrate. Scenario 1 is extremely urgent migration, Scenario 2a is urgent migration, Scenario 2b is semi-urgent migration and Scenario 2c is less urgent migration.

Figure 7. Decision tree for migration scenarios



Note: X , Y , and Z are variations on the usual symbols used in Mosca's inequality formula. The X is the estimated time the data must remain secret; W_i is the estimated waiting time until the milestone associated with Scenario i ; Y_i is the estimated time it takes to perform the migration in Scenario i .

Sources: TNO; Task Force on Quantum Technologies and Cybersecurity, presentation.

International coordination and the sharing of best practices

The field of quantum technology requires robust international collaboration due to its global scope. The NIST's PQC project and its standardisation effort have seen the participation of cryptographers from all over the world.

Yet, other initiatives have also brought together the participation and collaboration of multiple actors. For example, a recent initiative from the EU – the International Cooperation on Quantum Technologies ([InCoQFlag](#)) – goes in this direction. Over the next 3 years, InCoQFlag aims to facilitate workshops and networking sessions between EU and non-EU academia and industry stakeholders to support international collaboration.

Along these lines, there is another group of countries called the 'Group of 12', initiated by the US, which brings together representatives from governments and the scientific community of like-minded countries. This group aims to align national strategies in the field of quantum technology.

Overall, to coordinate the various EU Member State initiatives around quantum technologies, a foundation for consensus and collaboration has to be established. Circle of trust mechanisms, such as the Important Projects of Common European Interest Next Generation Cloud Infrastructure and Services (IPCEI-CIS)³³ developed within the EU in the field of cybersecurity, could serve as a starting point for enhancing cooperation in areas where strategic interests are particularly significant. These mechanisms could be expanded internationally to include like-minded countries, including those within the transatlantic alliance.

It is crucial to strike a delicate balance, working with countries outside the EU framework without creating an alternative to it. The IPCEI approach may provide some guidance in this regard. Ultimately, these considerations revolve around the integration of shared values into the governance of quantum technology. The closer that partners align politically and socially with these values, the easier it becomes to include them in the circle of trust.

Finally, it should be noted that quantum technology development involves a complex web of interconnected components, materials and expertise that transcend national borders. The supply chain for quantum technologies often spans multiple countries, with various stages of research, manufacturing and distribution taking place across different regions. This global interdependence highlights the necessity of harmonised standards, regulations and collaborative efforts to ensure the integration of quantum technologies. The absence of such international coordination could lead to fragmented and disjointed approaches.

³³ IPCEIs are strategic instruments for the implementation of EU industrial strategy. They materialise in large-scale consortia for research and development and the first industrial applications in strategic value chains.

Promotion of enhanced quantum awareness in the public and private sectors

The level of awareness of the quantum risk is worryingly low. A [survey](#) by BSI and KPMG on the topic received fewer responses than usual, and of the companies that responded less than half are taking the quantum threat into account in their risk management.

Many guidelines assume that companies have in-house expertise on quantum-resistant cryptography. Often, especially for smaller companies, this is not the case. It is important to provide plain communication on these issues, as the cybersecurity community has done in other areas of interest.

When drafting guidelines, it is important to take into account the diverse groups that will be reading the guidelines. This includes both different sectors (which might have different transition timelines) and different actors (that are concentrating on different aspects of the transition). For instance, the TNO *PQC Migration Handbook* starts with the diagnosis step to help organisations identify whether they need to take steps towards migration as soon as possible or can wait a bit more.

Awareness needs to be promoted at both the EU and Member State levels and in the public and private sectors. By promoting awareness and spreading the knowledge and information we have acquired thus far on quantum systems, along with the advantages and disadvantages they pose, individuals will be able to better identify if their personal data or company data are at risk of being subject to malicious behaviour.

This issue is also closely linked with that of enhancing quantum skills and promoting education, which will be analysed below. Aside from education and training programmes, other useful initiatives that the EU could promote are the creation of platforms for direct interaction with quantum experts or the showcasing of best practices in quantum technology applications and the quantum transition.

A future-ready workforce with quantum skills

The development of quantum computing will require a future-ready workforce with a strong set of specific skills. It will need not only researchers but also ‘quantum-informed workers to develop the supply chain and operational infrastructure needed to support the industry’ (Lee, 2021).

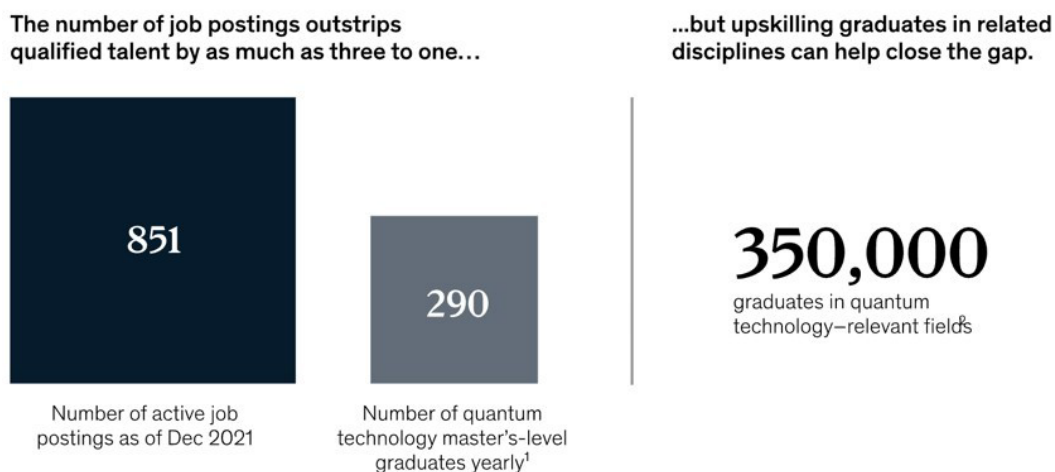
In this context, the current vast talent gap poses a significant challenge to the comprehensive development of the quantum ecosystem. When comparing the number of graduates in quantum technologies with the number of job postings in this field, the scale of this workforce gap becomes evident (see Figure 8).

This issue becomes even more relevant in the context of the intersection between quantum skills and cybersecurity skills. It prompts questions about how to retrain cybersecurity experts

to meet the demands of the evolving landscape or when considering the overall underrepresentation of women in quantum and cybersecurity fields.

The challenges of the quantum skills gap can be addressed by drawing lessons from experience with AI. In principle, organisations should clearly specify their talent needs. When building a quantum technologies team, it is recommended to focus on three key roles: quantum hardware engineers, quantum software engineers and quantum translators. Translators play a strategic role by understanding the maturity level of the technology, the potential threats related to the interplay between quantum technologies and cybersecurity, and the level of hype surrounding quantum. Still, these distinctions may oversimplify reality, as these roles often require hybrid skills. Additionally, the market is still evolving, and a clear definition of these professional roles may be more applicable to highly skilled workers rather than the broader workforce.

Figure 8. Quantum skills gap



¹ Estimate based on the number of universities with such programs and how many students graduate per year.

² Graduates of master's level or equivalent in biochemistry, chemistry, electronics and chemical engineering, information and communications technology, mathematics and statistics, and physics.

Source: OECD; Quantum Computing Report, quantumcomputingreport.com

McKinsey & Company

Source: Mohr et al. (2022).

Companies should establish pathways for a diverse talent pipeline. This involves bringing together individuals with diverse expertise, ranging from quantum experts and those knowledgeable about potential use cases of quantum technology to cybersecurity experts. It also entails fostering effective communication across different roles and tasks.

Encouraging a younger generation of scholars to pursue careers in quantum is paramount in making a significant impact on the talent pipeline. In Europe, the initiation of quantum education at primary and secondary levels is in its infancy. Furthermore, the responsibility for student education typically falls on individual nations, although the EU often plays a supporting role in driving shared educational goals.

Taking a cue from the Netherlands, a centralised approach to quantum information science in science, technology, engineering and mathematics (STEM) subjects might be a viable option for European nations. The Netherlands has recently incorporated quantum physics into its national curriculum. It is mandatory for the *voorbereidend wetenschappelijk onderwijs* track, a 6-year programme that prepares students for academic education at a research university and accounts for approximately a fifth of Dutch high school students (Omaar, 2023). This model could serve as a blueprint for other European countries aiming to introduce quantum studies at the high school level. In this context, it would be particularly important to introduce specific courses in national curricula on the implications of quantum technologies for cybersecurity.

Notably, outside of formal education, various non-profit initiatives and private sector contributions have emerged in Europe to support quantum education. To promote a wider comprehension of quantum concepts, platforms like QplayLearn.com, among others, have been developed³⁴.

Finally, talent retention should be a prime concern. Currently, there is intense competition to hire quantum experts, given the high demand and limited availability of such professionals. It is crucial to not only attract these experts but also to ensure that they stay within the EU and continue to enhance their skills. Countries like France have frameworks to attract foreign experts in technical fields. As the quantum field expands, Europe might need to further refine its immigration policies to ensure a steady influx of international quantum experts.

A wide range of professionals is required in the quantum field, and the multidisciplinary nature of the industry should be considered. This includes scientists and engineers along with professionals from fields such as law, political science and economics, among others. Training professionals from diverse backgrounds is crucial as well as prioritising funding for the development of quantum applications that demonstrate quantum advantage.

Openness of research

One important question to address in relation to quantum technologies is about the level of openness of research activities in the field. As noted above, quantum research needs collaboration and knowledge sharing to achieve better technological advances. Open research can accelerate the development of quantum technologies, leading to the discovery of new algorithms and cryptographic techniques, and improvements in quantum hardware.

³⁴ QPlayLearn.com is a platform designed to broaden understanding of quantum concepts across sectors like education, business, arts and culture. The platform offers a variety of resources, such as quantum atlases and games, targeting various levels of quantum knowledge. It uses interactive tools like games, videos and scientific descriptions to boost comprehension and active participation. Additionally, the site provides in-depth material on quantum science's mathematical foundations. Specific resources are tailored for school children, including class experiments, storybooks and guides for teachers and parents. For companies and policymakers, the platform offers courses developed by the QTIndu Project, with the European Health and Digital Executive Agency providing EUR 5.6 million in funding.

At the same time, the knowledge and techniques developed in open research can be exploited by malicious actors for cyber-attacks or unauthorised access to sensitive information. Limitations on openness would serve the need to safeguard national security interests and protect critical infrastructure. In such a view, certain aspects of quantum technologies and cybersecurity research could be restricted or classified to prevent potential misuse of knowledge.

However, while the intention to prevent potential misuse of knowledge is valid, excessive restrictions can hinder the progress of research and development. Scientific advances often thrive in an environment of open collaboration and information sharing. Restricting access to certain aspects of research could impede the flow of ideas and insights that contribute to breakthroughs.

Limitations on the right to science can be justifiable if they meet certain criteria: being prescribed by law, pursuing a legitimate purpose, and being deemed necessary and proportionate. In this vein, the role of judges becomes a crucial aspect to consider, as it may be challenging for legally trained judges to effectively assess whether restrictions on publication are proportionate (Institute for Information Law and Quantum Software Consortium, 2022).

The issue of openness of research is directly related to that of dual-use export controls, as discussed in the next section.

Dual-use export control policies³⁵

Dual-use export controls come into play when states judge that there is a need to restrict the international transfer of certain technologies, to prevent their proliferation in regions or countries that could use them in ways that undermine the judging state's national security or global stability. Yet, regimes for dual-use export controls also allow members to share important information, such as details on licensed exports and licence denials, as well as to develop and publish guidance and good practice documents.

Over the past few years, quantum computing has become a topic of discussion in multilateral regimes for dual-use export controls, and it is likely that dual-use export controls on quantum computing will be implemented in the near future. Even so, as mentioned above, introducing dual-use export controls on quantum technologies raises questions about the right to science.

Controls have the potential to interfere with the free flow of scientific knowledge and collaboration. It is crucial to closely examine the motivations behind governments' decisions to introduce such measures to ensure that they are not unduly restricting the progress and dissemination of knowledge (ibid.). For instance, much of [China's quantum research](#) is conducted at state-sponsored laboratories and institutions. This contrasts with the approach

³⁵ This section has benefited from comments by Mark Bromley, Senior Researcher, Dual Use and Arms Trade Control Programme, SIPRI.

taken by other leading players in quantum technology, where the private sector typically leads. Given the substantial involvement of governments, any decisions about export controls would likely reflect national security priorities, potentially limiting the international sharing of certain quantum breakthroughs.

For quantum technologies, the applications relevant to dual-use export control span various domains, including industrial and safety-related sectors. In the military sphere, the utilisation of quantum technologies can have dual implications, in both weakening the information security of an opponent through advanced computational capabilities and enhancing one's own security through quantum cryptography. Quantum radar, for example, offers the potential for powerful sensors that can effectively counter stealth technology. Other military applications are discussed in detail in Box 8.

Box 8. Military applications of quantum computing

Quantum computers will offer unprecedented processing power. The speed of data computation and processing, which quantum systems will greatly improve, will affect the work of unmanned and autonomous military platforms. This will enable decisions to be taken more swiftly, making work more accurate and allowing for multiple targets to be engaged at once.

An obvious military application for a functional quantum computer is the capability to engage in a near-instantaneous hack into encrypted military servers, and those controlling the national infrastructure systems of opponents. Quantum computing will dramatically improve situational awareness of multi-domain battlefields. Specific benefits for the military include AI algorithms, highly secure encryption for communications satellites – i.e. quantum key distribution – and accurate navigation that does not require GPS signals. The military sector will also be able to increase patterns and train AI systems. Quantum computing can be used at various stages of the design of new weapons systems and new materials, and even in the development of new strategies, along with operational and tactical concepts.

The further development and integration of AI into conventional weapons platforms, and the robotisation of battlefields, will progress rapidly. For example, the convergence of AI, distributed ledgers and drone technology creates formidable possibilities in respective military applications.

In addition to analysing and reporting on footage in real time, AI can power autonomous drones. These can fly entirely independently, without any human intervention or control needed. Distributed ledgers can record the data collected by AI-powered drones immutably and in real time. They can also record the flight decisions and actions taken by the drone. With each drone operating as part of a decentralised network, if it is later destroyed, whatever it has collected or performed would still be recorded on the distributed ledgers.

The Wassenaar Arrangement is one of the four multilateral export control regimes. Within the Wassenaar Arrangement, current listings for quantum technologies encompass various applications. Notably, the specific listing position for quantum computers is yet to be defined, although it is addressed indirectly under 5A004a (Systems in order to circumvent, weaken or overcome information security) and 5A002a (Systems for information security with quantum-resistant algorithms). There is an ongoing proposal for quantum computers to be included in the Wassenaar Arrangement under category 4³⁶; however, states cannot agree on which metric to use to determine whether a system falls within this category. In the 1980s, an issue similar to that emerging in negotiations on dual-use export controls for quantum technologies arose over how to draft the export control lists. The critical issue in that case was also determining the metrics to specify what constituted a powerful computer³⁷.

Quantum cryptography is already listed under 5A002c on systems designed or modified to use or execute quantum cryptography. In the case of quantum sensors, multiple general listing positions are allocated for sensors in category 6. Furthermore, the broader category of quantum technology is encompassed by controls on various supporting technologies, such as low-temperature, lasers, semiconductors and manufacturing equipment, which are covered under categories 1, 3, 4 and 6. As quantum technologies continue to evolve, these listings play a critical role in shaping international dual-use export control policies.

Within the EU, there is general agreement on the need to control the export of quantum computers. The decision on whether to adopt controls on quantum computers will be made collectively at the Wassenaar Arrangement Plenary, where most – however not all – EU Member States are represented. The EU is not directly involved in the multilateral Wassenaar Arrangement discussions, but the list of dual-use goods in the Arrangement is transposed in Community Regulation (EC) No 428/2009 establishing a Community regime for the control of exports, transfers, brokerage and transit of dual-use goods.

³⁶ The Basic List is composed of 10 categories based on increasing levels of sophistication:

- Category 1 – Special Materials and Related Equipment
- Category 2 – Materials Processing
- Category 3 – Electronics
- Category 4 – Computers
- Category 5 – Part 1 – Telecommunications
- Category 5 – Part 2 – Information Security
- Category 6 – Sensors and Lasers
- Category 7 – Navigation and Avionics
- Category 8 – Marine
- Category 9 – Aerospace and Propulsion.

³⁷ For details, see European Commission, 'Emerging Technologies Developments in the Context of Dual-Use Export Controls', Factsheets.

The EU can also play a valuable role through, for example, the EU-US Trade and Technology Council (TTC) in facilitating transparency, information exchange and cooperation on quantum value-chain policies (European Policy Center, 2023). Along these lines, in a [joint statement](#), TTC states that it has established a task force to address open questions on science and technology cooperation in quantum technologies between the EU and US. The task force is also discussing activities in quantum-resistant cryptography standardisation and potential avenues for future cooperation, feeding into the US-EU Cyber Dialogue.

It is argued that the EU's regime for dual-use export controls requires modernisation (Riekeles, 2023). For example, as quantum technologies are increasingly delivered through cloud services rather than traditional exports, this new dynamic should be addressed (ibid.). As mentioned by Rand & Rand (2022), it is almost entirely unclear how the regime for dual-use export controls 'would affect the ability of a foreign resident from executing code on a quantum computer through a cloud interface. This conundrum highlights the importance of updating enforcement regimes so that they can effectively fulfil the purpose of such traditional mechanisms as export controls.'

Finally, export control is not the only relevant mechanism in place. Technology transfer is governed by various mechanisms, including systems that screen and restrict foreign direct investment (FDI). FDI refers to investment from one nation to another, typically made by corporations rather than governments, which may entail establishing operations or obtaining tangible assets, such as shares in other companies. In recent times, several countries, including the US and multiple European nations, have enhanced their tools for screening FDI (Bromley & Brockmann, 2018). Notably, Regulation (EU) 2019/452 provides an EU framework for screening direct investment from non-EU countries on the grounds of security or public order. The framework includes quantum technologies alongside several other disruptive technologies such as artificial intelligence, robotics, semiconductor energy storage, nuclear technologies, nanotechnologies and biotechnologies.

According to Abdulrahman and Sun (2023), however, only a small percentage of transactions may fall under the regulation's screening process. Moreover, if the target of the FDI restriction is China, it should be noted that Chinese FDI has undergone changes in its internationalisation strategy and motivation, shifting from strategic asset acquisitions to a focus on advances in technology within the industrial and consumer product sectors, which could further hamper the effectiveness of the instrument.

Civilian and military coordination and cooperation

Ensuring that developments in quantum technologies align with both civilian and military needs requires a multidimensional approach. Effective civilian-military coordination hinges on clear communication, shared objectives and well-defined boundaries to ensure that the potential benefits of quantum technologies are harnessed while minimising any risks. In addition to putting in place quantum-resistant common practices and standards, it will be necessary to

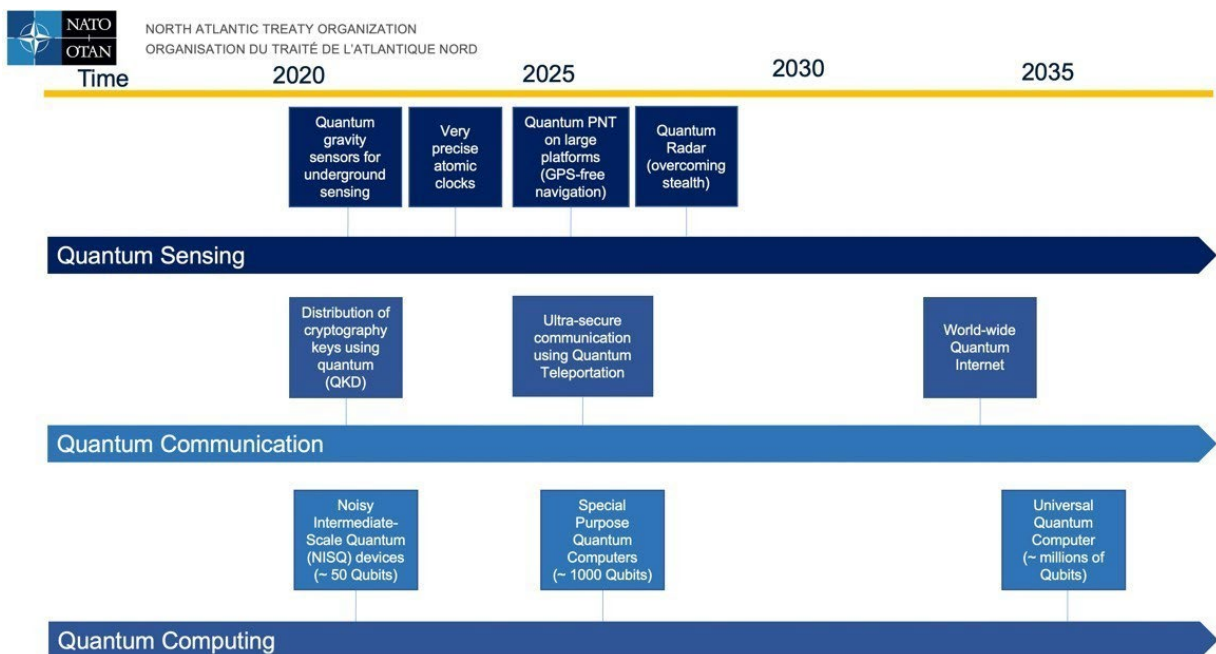
ensure that there are standards or common baselines for the quality of the implementation and level of assurance for quantum technologies, whether for civilian, military or dual-use applications.

The potential of quantum technologies to significantly enhance military capabilities and revolutionise warfare has led to the development of dedicated national and international strategies and policies in this domain. One notable undertaking in this area is the upcoming NATO quantum strategy – which will include, among others, three main technological applications, namely quantum sensing, quantum communication and quantum computing.










The increasing number of developments for military applications in these three fields is key to understanding how critical quantum will be in the military field.

NATO's quantum strategy (Figure 9) is scheduled for Q4 2023. By 2025, NATO will work towards a quantum-ready alliance, which will pilot the first use cases, potentially coming from quantum communication, sensing or computing. In 2030, NATO aims at achieving a quantum-enabled alliance³⁸. To establish a quantum-enabled alliance, several crucial issues need to be effectively addressed, including funding and financing as well as bridging the quantum workforce gap. It is essential to adopt an ecosystem approach to tackle these challenges, which involves considering the entire spectrum of stakeholders and value chains.

Figure 9. Timeline for the NATO quantum strategy



³⁸ The timeline represents a rough estimation. These figures could change over time.

	2020	2021	2022	2023	
Input	 Quantum White Paper	 Quantum Technologies: Initial Understand Phase Report	 Quantum Technologies: Final Understand Phase Report	 Quantum Strategy	
Workshops	 Workshop on Quantum Technologies	 C3B Workshop on 'Future Interoperable Capabilities using Quantum Technologies'	 Workshop on "Sprint session on NATO's Quantum Strategy" in Copenhagen, Denmark	 NATO HQ, Brussels: C3B Workshop on 'Future Interoperable Capabilities Using Quantum Technologies'	 Quantum Science & Technology Workshop in Turin, Italy

Sources: NATO Cyber and Hybrid Policy Office; Task Force on Quantum Technologies and Cybersecurity, presentation.

In this context, there are several other questions that need to be answered. Among others, we cite: how to align efforts across enterprises and allies, how to update the defined use cases, how to align different national strategies and how to leverage innovations from the private sector. With respect to the latter, NATO is developing its quantum capacities within the footprint of the Defense Innovation Accelerator for the North Atlantic (DIANA) at the quantum centre in Copenhagen. This DIANA centre will bring together operational end users, scientists and system integrators to advance technological dual-use solutions.

Moreover, NATO and the wider international community will need to find a balance between meeting states' requirements for strategic ambiguity and fostering research cooperation. Strategic ambiguity is a key aspect of technological development and refers to the deliberate lack of clarity surrounding certain aspects of technology development, allowing states to maintain flexibility and confidentiality in their decisions and actions.

During the initial phase of technological advancement, as in the case of quantum technology, the concerns surrounding strategic ambiguity become even more crucial. These concerns encompass, for example, decisions regarding the establishment of specific industries exclusively in the EU, as well as the evaluation of research openness. In this regard, early engagement of the defence sector in the initial stage of technology development would be highly advantageous. This is particularly true when considering that resilience requirements and local network requirements largely align between civil and military applications.

Possible future research areas of quantum technologies linked with cybersecurity

There are several possible areas of research that lay at the intersection of quantum technologies and cybersecurity that could have a high impact in the future. It is certain that such technologies could significantly affect cybersecurity, in terms of both introducing new challenges and enhancing security measures. But we have also seen before that it is very difficult to predict a date when quantum computers will be available, with estimates varying from 2030 to 2075, or later.

With this in mind, here are some areas of research that should be highlighted. Above all, there is the achievement of quantum computers, where research in science and engineering is still needed to provide, by a horizon still to be determined, quantum computers that show a quantum advantage over classical supercomputers. The vision in this area is perhaps to have quantum computing centres that host such computers and serve the community, like the classical supercomputing centres of today, given that it may be difficult to ship machines composed of quantum devices to every lab of every university.

This report shows that, from today's state-of-the-art perspective, **quantum-resistant cryptography** has by far the greatest potential to bring benefits to the economy and society. As quantum computers become more powerful, they could break classical cryptographic algorithms that underpin most, if not all, of our digital economy. Research is required to develop, standardise and implement new cryptographic algorithms that are resistant to attacks from both classical and quantum computers. This includes **research on best practices to perform the migration of IT systems** from current cryptographic schemes to quantum-resistant ones as well as research on networking protocols, like TLS, QUIC, IPSec/IKEv2 or space protocols like SDLS.

Because new cryptography needs to be deployed soon, a lot of resources will be spent on such migration in a hurry. Accordingly, it would be wise to have the latter implemented in such a way as to facilitate cryptographic updates and even new migrations in future. Hence, **research on cryptographic agility** has much potential for impact.

Quantum random number generation can exploit the inherent randomness of quantum mechanics to produce true random numbers, which are crucial for various cryptographic protocols and secure communications. There is still progress to be sought in this area, at both the research and innovation levels.

We have also learned that **quantum key distribution** is currently considered to have too many unresolved issues to be of immediate value. Yet, if such issues could be solved, then quantum key distribution would allow for the secure distribution of encryption keys, using the principles of quantum mechanics. It could offer a very secure method for exchanging cryptographic keys between parties, providing a higher level of security against eavesdropping and key interception. This area will probably need solutions from quantum networks, including

quantum repeaters and quantum routers. It is certainly a possible research area, but, as of today, its potential impact is rather niche due to the maturity and expected costs involved. Additionally, the complexities of supply chain management and certification further underscore the multifaceted challenges in this domain.

On the even more speculative side, **quantum and quantum-resistant blockchains** are emerging as a research area, with some papers already published. On the one hand, research is being conducted to develop quantum-resistant consensus algorithms and cryptographic primitives to build blockchains that would be secure against straightforward attacks using quantum computers, and to develop frameworks for quantum identity authentication (Allende et al., 2023). On the other hand, there are proposals to build a new generation of quantum blockchains. And evidently, there is much space in the middle, where classical blockchains are enhanced by some quantum technologies.

Even further into the future, once quantum computers start to operate, it is probable that new forms of quantum malware and cyber-attacks will emerge. Research will eventually be needed to develop **quantum-device-specific cybersecurity defences** to protect against such threats. At the same level, **quantum-resistant hardware and secure quantum hardware** will be needed to resist quantum-based attacks on devices and systems as well as attacks on the quantum components of quantum computers.



7. POLICY RECOMMENDATIONS

Based on an extensive review of the existing literature and the contributions of Task Force participants, this Task Force puts forward the following recommendations to policymakers, the private sector and the research community on the interplay between quantum technologies and cybersecurity.

Support research at the intersection of quantum technologies and cybersecurity

Quantum technologies are still at a very early stage. The EU has invested heavily in quantum technologies and a large part of this public funding goes to research. However, it is increasingly important to continue to further advance research in quantum technologies and in particular to understand how they will affect cybersecurity and the digital ecosystem. There are several possible areas of research that lay at the intersection of quantum technologies and cybersecurity that have the potential to have a high impact in future, in terms of both introducing new challenges and enhancing security measures. Here are some of the research areas that this Task Force recommends as priorities for European funding in the short term:

- quantum-resistant cryptography, including the corresponding cryptanalysis,
- best practices for migrating IT systems,
- cryptographic agility.

This report shows that **quantum-resistant cryptography** is by far the most likely area to bring benefits to the economy and society. Research is required to develop, test and analyse, standardise, and implement new cryptographic algorithms that are resistant to attacks from both classical and quantum computers. This includes research on best practices for **migrating IT systems** from current cryptographic schemes to quantum-resistant ones. We recommend that researchers and policymakers take an [evidence-based approach](#) to understanding where risk exists in this space.

We strongly recommend that the development, standardisation and implementation of new cryptographic algorithms – as well as research on best practices for migrating IT systems from current cryptographic schemes – be funded by both Horizon Europe and the Digital Europe Programme, including their work programmes for 2025.

Because new cryptography needs to be deployed soon, a lot of resources will be spent on such a migration in a hurry. Accordingly, it would be wise to implement the latter in such a way as to facilitate cryptographic updates and even new migrations in future. Therefore, we suggest funding research on **cryptographic agility**, as it has a high potential for impact.

Further in the future, once quantum computers start to operate, it is certain that new forms of quantum malware and cyber-attacks will emerge. Research will eventually be needed to

develop **quantum-device-specific cybersecurity defences** to protect against such threats. At the same level, **quantum-resistant hardware** and **secure quantum hardware** will be needed to resist quantum-based attacks on devices and systems, as well as attacks on quantum components of quantum computers. But this is not for the near or the medium-term future.

Finally, another area that has received attention in this report is **quantum key distribution**. QKD is currently considered to have too many unsolved issues to be of immediate value. This area will probably require solutions from quantum basic research, including quantum networks, repeaters and routers.

Given this landscape, it would be prudent for the EU to conduct a thorough analysis to determine the optimal allocation of research funds between QKD and quantum-resistant cryptography, ensuring a balanced and sound investment strategy.

Promote cryptographic agility and coordinating policies at the EU level to ease the transition to quantum-resistant cryptography

The rise of quantum computers challenges current cryptography, but it only affects specific mathematical problems. Therefore, we can design cryptography that quantum computers cannot easily break. While solutions exist, the shift to quantum-resistant cryptography is a complex and very lengthy process. It will require careful planning and must begin well in advance of the availability of cryptographically relevant quantum computers.

As some enterprises use cryptography in many parts of their operations, we recommend **giving cryptographic agility priority** when planning the transition to quantum-resistant cryptography. Cryptographic agility refers to the ability to swiftly modify the cryptographic components used in an application. This agility enables them to adapt to new cryptographic standards or fend off emerging threats without overhauling their entire infrastructure.

Furthermore, this report has stressed that as the shift towards quantum-resistant cryptography begins, there will be an overlap period where both quantum-resistant and conventional public key cryptography will be used together. This **hybrid approach** is necessary for two main reasons:

- different entities will transition at varying rates, necessitating interoperability;
- quantum-resistant cryptography is still in its infancy with some uncertainties about its security due to limited time for analysis.

Even though lattice-based cryptography is promising, experts believe that it may take more than 5 years to establish a solid level of trust in quantum-resistant cryptographic methods. Traditional public key methods, like RSA and ECC, have undergone extensive testing, accumulating vast experience in secure applications. To match this confidence in quantum-resistant solutions, further research and practical experience are essential.

Hence, to facilitate the shift without delay, hybrid schemes employing both classical and quantum-resistant algorithms are recommended. At the same time, careful implementation is crucial to maintain the integrity of these hybrid systems. Notably, some European cybersecurity agencies, such as ANSSI and BSI, also recommend the use of quantum-resistant systems in hybrid mode, together with classical systems.

Finally, policies for the transition to quantum-resistant cryptography should be **coordinated at the EU level**, with the establishment of ad hoc projects for sharing guidelines and best practices among Member States. So far, only a few countries in the EU have set out plans to counter emerging quantum cybersecurity threats. Furthermore, national guidelines sometimes diverge and propose frameworks that are at times challenging in terms of the practicality of the proposed schemes.

As suggested by the experience of the US NCCoE's Post Quantum Cryptography project, the European Cybersecurity Competence Centre could develop a project on migration to quantum-resistant cryptography, aimed at raising awareness, developing practices to ease migration, producing white papers and playbooks, and delivering demonstrable implementation. This should be complemented by a strong political coordination role of the EU to harmonise the transition to quantum-resistant cryptography in the Member States.

The coordination of this migration process, would be particularly relevant for the public key infrastructures (PKIs), including those of public administrations. PKIs represent a crucial area that will also be impacted once CRQC come to operation and will have to migrate to versions that use quantum-resistant cryptography as well. However, several questions must be addressed in this process, like security, performance, compatibility, and interoperability, and their relationships with general developments in the commercial sector. This Task-Force recommends that the European Commission promotes a unified and coordinated approach, in order to facilitate and accelerate the migration process of PKIs, in a way that ensures interoperability and compatibility with standard applications.

Foster the standardisation of quantum-resistant cryptography

The process of standardising quantum-resistant cryptography has been led by NIST in the US, which has been running a competition since 2016 among teams from around the world to evaluate and select candidate algorithms. Other international bodies, such as the IETF, have also taken steps to develop internationally shared standards. This is not a novelty in the process of technology standardisation. Historically, the path of technology standardisation has usually been characterised by collaborative and shared efforts. In this context, the EU should avoid both fragmentation and duplication of international initiatives.

However, as mentioned in the report, algorithms like ML-KEM and ML-DSA were developed by European researchers with European funding. Such achievements underscore the pivotal role of European scientific minds in this evolving landscape.

The EU could place **greater emphasis on the contributions of EU researchers** to the standardisation process. By highlighting the contributions of its researchers, the EU could position itself as a cornerstone of the global standardisation process. Still, mere recognition is not enough. To bolster its standing and foster further innovation, it is essential to ramp up research funding within the EU.

Encourage initiatives to assess the potential risks and threats posed by quantum technologies

Organisations with their own cryptographic infrastructure should incorporate quantum-resistance planning for the future. As mentioned in the report, a good starting point for the transition of an organisation to quantum-resistant cryptography is carrying out a **quantum vulnerability assessment**.

The urgency of addressing these quantum vulnerabilities is not just theoretical. In practical terms, it is about safeguarding vital data and infrastructure from quantum-enabled threats, which have the potential to render existing cryptographic methods obsolete. In this context, assessing vulnerabilities becomes key.

The US National Defence Authorization Act of 2021, mandating the US Department of Defence to conduct such a comprehensive assessment of potential risks, goes in this direction.

The European Commission could promote a similar initiative through recommendations to guide Member States and companies on how to approach the cybersecurity risk aspects of quantum computing technologies.

More specifically, based on the NDAA blueprint, the European Commission's guidelines should indicate the following actions:

- recognise and rank national security systems that are vulnerable;
- evaluate the NIST guidelines for quantum-resistant encryption and how they apply to the cryptographic needs of the organisation;
- explore the viability of alternative quantum-resistant algorithms and features;
- identify any funding gaps in both public and private initiatives connected to quantum-resistant encryption, standards and frameworks;

craft suggestions for research, development and procurement strategies, including timelines for resource allocation, to protect vital national security systems from the decryption capabilities of quantum computers.

Apply a principles-based approach to quantum governance and strengthen international coordination

In light of the rapidly changing landscape of quantum technologies, we recommend a governance approach that could limit the risks without stifling exploration of the potential quantum technologies hold.

In this context, a **principles-based approach to governance** could be advantageous. For instance, some general principles for quantum-responsible governance could include safeguarding against risks and engaging stakeholders in the process of developing quantum technologies.

While some principles for the governance of quantum technologies have been applied to other relevant technological advances, doing so for quantum technologies presents unique challenges. Not only is this realm advancing at a remarkable pace, but our intermediate grasp of the technology, its applications and its possible ties with other emergent and unpredictable tech areas (like generative AI and large language models) remains limited.

Against this backdrop, one governance strategy might **involve using [regulatory sandboxes](#)** for areas that are not yet fully understood or that may carry higher risks. This would provide a controlled environment in which government and industry could come together to develop, deploy and test quantum and quantum-hybrid applications for use in the near term.

Regulatory sandboxes have also been envisaged within the framework of the EU AI Act. Much like in AI, where insights from real-world applications and pilot projects frequently shape overarching governance tactics, a comparable step-by-step strategy is advisable for quantum technologies.

In this vein, sharing and harmonising knowledge on standards will be crucial in the near future, when strategies for the governance of quantum technologies are put in place. Aligning governance initiatives across EU Member States and creating a framework for collaboration and consensus is thus essential. The EU's trust mechanisms, like the IPCEI on Next Generation Cloud Infrastructure and Services in cybersecurity, can be a model for fostering cooperation in critical strategic areas.

This approach could also be extended globally to involve other countries, especially those in the transatlantic alliance. Such collaboration becomes particularly important given the interconnected nature of modern tech ecosystems and could help foster accepted best practices and governance norms.

Enhance quantum awareness in both the public and private sectors

In the report, we have stressed the worrisome low level of quantum awareness across sectors, especially on the interplay between quantum technologies and cybersecurity.

Many guidelines mistakenly assume companies possess in-house knowledge of quantum-resistant cryptography, yet many – above all smaller firms – do not. Effective communication is vital given the diverse audiences reading these guidelines, which can range from different sectors to different stakeholders. In this context, the TNO [PQC Migration Handbook](#) uses a diagnostic approach, guiding organisations on migration timelines.

According to the handbook, organisations considering a transition to quantum-resistant cryptography should start by assessing their unique characteristics and needs. Organisations can typically be grouped into three main categories based on their data, systems, threat level and interdependencies: urgent adopters, regular adopters and cryptography experts.

- Urgent adopters are organisations that should prioritise migration due to the sensitive nature of their data or immediate threat levels. They either should have started the transition or should start immediately.
- Regular adopters are organisations that can take a wait-and-see approach, allowing for further developments in quantum-resistant cryptography standards before initiating the migration process.
- Cryptography experts are organisations that provide cryptographic knowledge or infrastructure services to other entities.

If an organisation identifies as an urgent adopter, it is advisable to commence the assessment promptly.

We recommend **promoting these practices in both public and private organisations** through awareness-raising campaigns. In doing so, the EU could support the creation of platforms for direct interaction with quantum experts or for showcasing best practices in quantum technology applications and the quantum transition.

Implement policies to promote a future-ready workforce with quantum and cybersecurity skills

In the report, we have shown the huge talent gap in the quantum sector. Organisations looking to fill such a talent gap should not only identify their talent needs but also diversify the talent pipeline and focus on talent retention.

We strongly recommend that the European Commission **prioritises investment in developing quantum skills**, specifically in the **intersection of quantum technology and cybersecurity**, to foster a new generation of experts.

The European Commission could utilise several funding mechanisms to invest in the development of quantum skills, including Horizon Europe and the Digital Europe Programme. In addition, Erasmus+ provides funds for collaborative projects between universities and

research institutions. It could be tapped to fund joint initiatives on quantum technology and cybersecurity training, as well as research.

Funding could also be used to incorporate quantum information science and ad hoc courses on the interplay between quantum technologies and cybersecurity in the national curricula of Member States, along the lines of the initiative carried out in the Netherlands. The latter mandates the integration of quantum physics in specific pre-university education programmes.

Update dual-use and export control policies

Openness in quantum technology research can speed up progress, but it also risks misuse by malicious actors. While open collaboration fosters innovation, there are concerns about national security and the protection of critical information. It should be noted, however, that restrictions on the openness of research are justifiable only insofar as they are prescribed by law, pursuing a legitimate purpose, and are deemed necessary and proportionate.

As argued in the report, the issue of openness in research is directly related to that of dual-use export controls, which come into play when states judge that there is a need to restrict the international transfer of certain technologies. Policymakers should consider a risk-based approach for dual-use and export controls in the quantum sector. Quantum computing is still in the early stages of development, and our ability to benchmark its progress is in its initial phase. As such, policymakers need to carefully craft new regulations to avoid unintended impacts that could hinder the advancement of this technology.

Nonetheless, there will be instances where imposing restrictions is considered necessary. In this context, **the EU should consider updating its export control systems**. For example, as quantum technologies are now frequently accessed via cloud services rather than traditional exports, this shift needs to be addressed. Indeed, there is a lack of clarity on how dual-use export controls affect a non-resident using a quantum computer through the cloud. This highlights the urgency of modernising enforcement methods, to ensure that tools like export controls remain relevant and effective.

Within the EU, there is general agreement on the need to control the export of quantum computers. The decision on whether to adopt controls on quantum computers will be made collectively through the Wassenaar Arrangement where most – but not all – EU Member States are represented.

The EU can also play a valuable role through, for example, the EU-US Trade and Technology Council in facilitating transparency, information exchange and cooperation on quantum value-chain policies. Along these lines, in a [joint statement](#), the TTC referred to the establishment of a task force to address open questions between the EU and the US on science and technology cooperation in quantum technologies. The task force will also discuss standardisation activities in quantum-resistant cryptography and potential avenues for future cooperation, feeding into the US-EU Cyber Dialogue.



BIBLIOGRAPHY

- Abdulrahman, J. & Sun, L. (2023), *The potential effects of the new FDI screening mechanism on Chinese FDI in Sweden*, Master's Thesis, Uppsala University.
- AIVD. (2022), 'Prepare for the threat of quantum computers' <https://english.aivd.nl/publications/publications/2022/01/18/prepare-for-the-threat-of-quantumcomputers>.
- Allende López, M. & Da Silva, M.M. (2019), *Quantum Technologies: Digital Transformation, Social Impact, and Cross-sector Disruption*, Inter-American Development Bank, <https://doi.org/10.18235/0001613>.
- Allende, M., León, D.L., Cerón, S. et al. (2023), 'Quantum-resistance in blockchain networks', *Scientific Reports*, 13(5664), <https://doi.org/10.1038/s41598-023-32701-6>.
- ANSSI. (2020), 'Should Quantum Key Distribution be Used for Secure Communications?', <https://www.ssi.gouv.fr/en/publication/should-quantum-key-distribution-be-used-for-secure-communications/>
- ANSSI. (2022), 'ANSSI views on the Post-Quantum Cryptography transition', <https://www.ssi.gouv.fr/en/publication/anssi-views-on-the-post-quantum-cryptography-transition/>
- Barker, W., Polk, W. & Souppaya, M. (2021), *Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms*, NIST Cybersecurity White Paper, NIST, <https://doi.org/10.6028/NIST.CSWP.04282021>.
- Baumhof, A. (2019), 'The Deal with Quantum Computing and Cryptography', *Infosecurity Magazine*, 19 April.
- Berger, C., Di Paolo, A., Forrest, T., Hadfield, S., Sawaya, N., Stęchły, M., & Thibault, K. (2021), *Quantum technologies for climate change: Preliminary assessment*, arXiv preprint, arXiv:2107.05362.
- Bogobowicz, M., Zimmel, R., Gao, S., Masiowski, M., Mohr, N., Soller, H., & Zesko, M. (2023). 'Quantum technology sees record investments, progress on talent gap', McKinsey Digital, April 24, <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/quantum-technology-sees-record-investments-progress-on-talent-gap>.
- Bromley, M. & Brockmann, K. (2018), 'Controlling technology transfers and foreign direct investment: The limits of export controls', *Non-proliferation, Arms Control and Disarmament*, Stockholm International Peace Research Institute.
- BSI. (2022). 'Quantum-safe cryptography – fundamentals, current developments and recommendations', <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.html>.
- Candelon, F., Bobier, J.-F., Courtaux, M. & Nahas, G. (2022), *Can Europe Catch Up with the US (and China) in Quantum Computing?* Boston Consulting Group.
- Cheng, et al. (2023), 'Noisy intermediate-scale quantum computers', *Frontiers of Physics*, 18(2), 21308. <https://doi.org/10.1007/s11467-022-1249-z>.

- Cimpanu, C. (2019), 'A quarter of major CMSs use outdated MD5 as the default password hashing scheme', *Zdnet*, 17 June, <https://www.zdnet.com/article/a-quarter-of-major-cmss-use-outdated-md5-as-the-default-password-hashing-scheme/>.
- Dowling, J.P. & Milburn, G.J. (2003), 'Quantum technology: The second quantum revolution', *Philosophical Transactions of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, 361(1809), 1655–1674, <https://doi.org/10.1098/rsta.2003.1227>.
- Emerging Technology from the arXiv (2019), 'How a quantum computer could break 2048-bit RSA encryption in 8 hours', *MIT Technology Review*, 30 May, <https://www.technologyreview.com/2019/05/30/65724/how-a-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hours/>.
- European High-Performance Computing Joint Undertaking (2021), 'The EuroHPC JU launched its first quantum computing initiative', https://eurohpc-ju.europa.eu/eurohpc-ju-launched-its-first-quantum-computing-initiative-2021-12-01_en
- European Policy Center (2023), *Quantum technologies and value chains: Why and how Europe must act now – A test case for the EU's technological competitiveness and industrial policies*, Discussion Paper, 23 March.
- Feynman, R.P., Leighton, R.B. & Sands, M. (1965), *The Feynman Lectures on Physics*.
- Fujitsu. (2023), 'Japanese joint research group launches quantum computing cloud service', March 24, <https://www.fujitsu.com/global/about/resources/news/press-releases/2023/0324-01.html>.
- Gable, J., Gray, S., & Mandich, D. (2023), 'Is PQC Broken Already? Implications of the Successful Break of a NIST Finalist', Cloud Security Alliance, March 4, <https://cloudsecurityalliance.org/blog/2023/04/03/is-pqc-broken-already-implications-of-the-successful-break-of-a-nist-finalist/>
- Goodin, D. (2023), 'RSA's demise from quantum attacks is very much exaggerated, expert says', *Ars Technica*, 26 January.
- High-Level Steering Committee of the Quantum Technologies Flagship (2017), *Quantum Technologies Flagship Intermediate Report*, European Commission, <https://digital-strategy.ec.europa.eu/en/library/intermediate-report-quantum-flagship-high-level-expert-group>.
- Institute for Information Law and Quantum Software Consortium (2022), *The right to science and dual-use export control*, Report of a workshop held on 26 October.
- Kania, E.B. & J.K. Costello (2018), 'China's Quantum Ambitions', *Military Cyber Affairs*, 3(2), <https://www.jstor.org/stable/resrep20450.6>.
- Kop, M., Aboy, M., De Jong, E., Gasser, U., Minssen, T., Cohen, I.G. & Laflamme, R. (2023a), *Towards responsible quantum technology, safeguarding, engaging and advancing Quantum R&D*, arXiv preprint arXiv:2303.16671.
- Kop, M., Aboy, M., De Jong, E., Gasser, U., Minssen, T., Cohen, I.G. & Laflamme, R. (2023b), *10 Principles for Responsible Quantum Innovation*, available at SSRN.

- Langione, M., Tillemann-Dick, C., Kumar, A. & Taneja, V. (2019), *Where Will Quantum Computers Create Value – And When?*, Boston Consulting Group, <https://www.bcg.com/publications/2019/quantum-computers-create-value-when>.
- Lee, M. (2021), *Quantum Computing and Cybersecurity*, Belfer Center for Science and International Affairs Harvard Kennedy School, July
- Lenstra, A., Wang, X. & de Weger, B. (2005), 'Colliding X. 509 certificates', *Cryptology EPrint Archive*, 2005/067.
- Levine, D.A. (2020), 'Made in China 2025: China's Strategy for Becoming a Global High-Tech Superpower and Its Implications for the U.S. Economy, National Security, and Free Trade', *Journal of Strategic Security*, 13(3), 1, November, <https://www.jstor.org/stable/26936543>.
- MajuLab (2022), The Quantum Priority Research Programme and Equipment (PEPR) has launched, March 7, <https://majulab.cnrs.fr/the-quantum-priority-research-programme-and-equipment-pepr-has-launched/>
- MarketsandMarkets (2023), 'Quantum Computing Industry worth \$4,375 Million by 2028'.
- Masiowski, M., Mohr, N., Soller, H., & Zesko, M. (2022). 'Quantum computing funding remains strong, but talent gap raises concern', *McKinsey Digital*, June 15 <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/quantum-computing-funding-remains-strong-but-talent-gap-raises-concern>
- Mauranyapin, N.P., Terrasson, A. & Bowen, W.P. (2022), 'Quantum Biotechnology', *Advanced Quantum Technologies*, 5(9), 2100139.
- Mohr, N., Peltz, K., Zimmel, R. & Zesko, M. (2022), *Five lessons from AI on closing quantum's talent gap – before it's too late*, McKinsey Digital, <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/five-lessons-from-ai-on-closing-quantums-talent-gap-before-its-too-late>.
- Montanaro, A. (2016), 'Quantum algorithms: An overview', *Npj Quantum Information*, 2(1), 15023, <https://doi.org/10.1038/npjqi.2015.23>.
- Moody, D. (2022), *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process*, NIST, <https://doi.org/10.6028/NIST.IR.8413>.
- Mosca, M. (2018), 'Cybersecurity in an Era with Quantum Computers: Will We Be Ready?' *IEEE Security & Privacy*, 16(5), 38–41, <https://doi.org/10.1109/MSP.2018.3761723>.
- Mosca, M., & Piani, M. (2022). '2022 Quantum Threat Timeline Report'. <https://globalriskinstitute.org/publication/2022-quantum-threat-timeline-report/>.
- National Academies of Sciences (2019), *Quantum Computing – Progress and Prospects*, edited by Grumbling, E. & Horowitz, National Academies Press, Washington, DC, <https://doi.org/10.17226/25196>.
- National Security Agency, Cybersecurity Advisory (2022), 'Announcing the Commercial National Security Algorithm Suite 2.0', September, https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_PDF.
- National Cyber Security Center. (2020), 'Quantum security technologies', <https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies>

- Nayak, C. (2021) 'Microsoft achieves first milestone towards a quantum supercomputer', Microsoft Azure Quantum Blog, June 21, <https://cloudblogs.microsoft.com/quantum/2023/06/21/microsoft-achieves-first-milestone-towards-a-quantum-supercomputer/>
- NIST. (2023). 'NIST to Standardize Encryption Algorithms That Can Resist Attack by Quantum Computers', August 24, <https://www.nist.gov/news-events/news/2023/08/nist-standardize-encryption-algorithms-can-resist-attack-quantum-computers>
- NSA. (2020), NSA Cybersecurity Perspectives on Quantum Key Distribution and Quantum Cryptography, <https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/2394053/nsa-cybersecurity-perspectives-on-quantum-key-distribution-and-quantum-cryptogr/>
- Omaar, H. (2023), *The U.S. Approach to Quantum Policy*, Center for Data Innovation, 10 October.
- Ott, D., Paterson, K. & Moreau, D. (2023), 'Where Is the Research on Cryptographic Transition and Agility?', *Communications of the ACM*, 66(4), 29–32, <https://doi.org/10.1145/3567825>.
- Querca (2021), 'Overview on quantum initiatives worldwide' (blog), 7 September.
- Rand, L. & Rand, T. (2022), 'The "Prime Factors" of Quantum Cryptography Regulation', *Notre Dame Journal on Emerging Technologies*, 3, 37.
- Riekeles, G. E. (2023), Quantum technologies and value chains: Why and how Europe must act now A test case for the EU's technological competitiveness and industrial policies, Discussion Paper, March 23rd.
- Swayne (2022), 'Infineon Participates in 6 Research Projects, Expands Commitment to Quantum Computing', *The Quantum Insider*, February, <https://thequantuminsider.com/2022/02/19/infineon-participates-in-6-research-projects-expands-commitment-to-quantum-computing/>.
- Swayne, M. (2023), 'Germany Announces 3 Billion Euro Action Plan for a Universal Quantum Computer', *The Quantum Insider*, 3 May <https://thequantuminsider.com/2023/05/03/germany-announces-3-billion-euro-action-plan-for-a-universal-quantum-computer/>.
- Thomson, I. (2023), 'You can cross "Quantum computers to smash crypto" off your list of existential fears for 30 years', *The Register*, 26 April.
- Quantum Flagship. (2023), 'Introduction to the Quantum Flagship', <https://qt.eu/about-quantum-flagship/>.
- Witt, S. (2022), 'The World-Changing Race to Develop the Quantum Computer', *The New Yorker*, 12 December.
- World Economic Forum (WEF) (2021), 'Quantum technologies can transform innovation and mitigate climate change – here's how', Article as part of the Global Technology Summit, 6 April, <https://www.weforum.org/agenda/2021/04/quantum-technologies-transform-innovation-and-mitigate-climate-change-gtgs/>.
- World Economic Forum (WEF) (2022) *Quantum Computing Governance Principles*, Insight Report, January, https://www3.weforum.org/docs/WEF_Quantum_Computing_2022.pdf.
- World Economic Forum (WEF) and Deloitte (2023), *Quantum Readiness Toolkit: Building a Quantum Secure Economy*, White Paper, Geneva, June.



APPENDIX A. LIST OF TASK FORCE MEMBERS AND INVITED SPEAKERS

Coordinator and rapporteur: Lorenzo Pupillo, CEPS

Rapporteurs: Afonso Ferreira, CNRS

Valtteri Lipiäinen, CEPS

Carolina Polito, CEPS

Advisory board

Sabrina Maniscalco, Professor of Quantum Information, Computing and Logic at the University of Helsinki, and CEO and co-founder of Algorithmiq Ltd

Michael Osborne, CTO for IBM Quantum Safe, IBM Research Division, Zurich Research Center

Bart Preneel, Full Professor at KU Leuven and Head of the Imec-COSIC Research Group

Tim Watson, Director, Defence and Security Programme, Alan Turing Institute in London, Professor of Cyber Security and Director of the Cyber Security Centre at Loughborough University

Companies and European organisations

Carmine Brancati, Cybersecurity Specialist, Cassa Depositi e Prestiti Spa

Tomas Jakimavicius, Director of European Government Affairs, Microsoft

Renata Jovanovic, Partner, Global Quantum Computing Ambassador, Deloitte

Isabella Martorina, EMEA Brand Marketing & Communication Leader, Ernst & Young

Anne McCormik, Director of EMEIA Public Policy, EU and EMEIA Digital Policy Leader, Ernst & Young

Jiri Pavlu, Mathematical Security Expert, Raiffeisen Bank International AG

Massimo Pellegrino, Partner Intellera Consulting

Florian Pennings, Director of Government Affairs, Cybersecurity and Emerging Technologies, Microsoft

Salvatore Sinno, Vice President, Innovation, Unisys Belgium

Alessandro Tatti, Head of Cyber Security, Cassa Depositi e Prestiti, SPA

Daniel Trigg, Chief Information Security Architect, Zurich Insurance Company Ltd

Jeroen Zonnenberg, Principal Consultant Security, Unisys

European institutions, agencies and intergovernmental organisations

Marcos Allende Lopez, Quantum Specialist, Inter-American Development Bank

Antonios Atlasis, Head of System Security Engineering Section, European Space Agency

Camilla Coletti, Senior Researcher, Principal Investigator and Center Coordinator, Fondazione Istituto Italiano di Tecnologia

Désirée Ehlers, Federal Ministry for Climate Action, Environment, Energy, Mobility, Innovation and Technology, Republic of Austria

Bart Groothuis, Member of the European Parliament

Harald Gruber, Head of Digital Infrastructure, European Investment Bank

Maran van Heesch, Senior Program Manager Quantum, TNO

Tobias Hemmert, Adviser, Federal Office for Information Security (BSI)

Paul E. Hoffman, Distinguished Technologist, ICANN

John Irving, Security Engineering, European Space Agency

Eva Maydell, Member of the European Parliament

Nora Mari, Government and Igo Engagement Manager, ICANN

Antonio Rossi, Project Scientist, Fondazione Istituto Italiano di Tecnologia

Kaan Sahin, Cyber and Hybrid Policy Officer, NATO

Josef Schroefl, Hybrid CoE – The European Centre of Excellence for Countering Hybrid Threats

Georgios Stamatoukos, Project Officer Cyber Defence, European Defence Agency

Suzy Wild, Accredited Parliamentary Assistant, European Parliament

Robin Wilton, Director of the Internet Trust, Internet Society

Academics/think tanks

Romain Bosc, Program Coordinator, German Marshall Fund

Joris van Hoboken, Professor of Law, University of Amsterdam

Elif Kiesow Cortez, Researcher, Stanford University

Laima Janciute, Postdoctoral Researcher, University of Amsterdam

Antonio Manganelli, Scientific Coordinator for the DEEP-IN Program, I-Com, Rome

Federica Russo, Professor of Philosophy and Ethics of Techno-Science & Westerdijk Chair, Freudenthal Institute, Utrecht University

Paul Timmers, Researcher, KU Leuven

Civil society

Dirk Bloem, Ambassador, Humanity of Things Agency

Marisa Monteiro, President, Humanity of Things Agency

Invited speakers

Christopher Brown, US NCCoE Migration to PQC Project Tech Lead, NIST

Ot van Daalen, University of Amsterdam

Oscar Diez, Head of Sector, Quantum Computing, Digital Excellence and Science Infrastructure Directorate, DG Connect

Catherine Lefevre, Senior Adviser, Open Quantum Institute, GESDA

Dustin Moody, Mathematician and Project Lead for the Post-Quantum Cryptography initiative, NIST

Melissa Rossi, Researcher in Asymmetric Cryptography, ANSSI

Mira L. Wolf-Bauwens, Lead, Responsible Quantum Computing and IBM Quantum Technical Ambassador, Responsible & Inclusive Technology

APPENDIX B. QUANTUM TECHNOLOGY IN THE EU AND REST OF THE WORLD

In recent years, countries worldwide have intensified their efforts to harness the power of quantum technologies.

This section will delve into the specific initiatives undertaken by major stakeholders in quantum technology, including the EU's Quantum Flagship programme, the US National Quantum Initiative Act and other notable national programmes. By examining the status of quantum technology development worldwide, this section gives readers an in-depth look at the global landscape in this transformative field. It offers insights into the initiatives undertaken by states and the collaborative efforts aimed at harnessing the potential of quantum technologies, while addressing the challenges and risks that lie ahead.

European Union

Europe has emerged as a key player in the field of quantum technologies, with several countries and institutions actively pursuing advances in this cutting-edge field. With significant investment and dedicated initiatives, European countries are striving to position themselves at the forefront of quantum research and development, in particular Germany and France (see Table B.1 for details on amount of funding).

At the supranational level, the EU began its active involvement in the quantum technologies field as early as 1999. It was only in 2016, however, that 4 000 EU researchers joined the 'quantum manifesto'. That document represented the first strategy of the EU on quantum technologies. It also gave rise to what has become the EU Quantum Flagship Declaration.

Table B.1. Quantum funding in the EU (EUR million)

Funder	Amount of funding	Project	Years active	Sources (website links)
EU + Member States	9 829			
Germany	5 783			
	3 000	Action Plan for Quantum Technologies	2023–2026	[1] , [2]
	2 000	Quantum Computing Roadmap	2021–2025	[1] , [2]
	650	Research Framework Programme	2018–2022	[1]
	125	QuNET	2019–2026	[1] , [2]
	8	QuaST	2023–2024	[1]
EU	1 848			
	1 000	Quantum Flagship	2018–2028	[1]
	270	EuroQCI	2023–2026	[1] , [2] , [3]
	240	IRIS*	2023–2027	[1]
	120	Quantera	2017–2026	[1]
	100	EuroHPC JU	2023–2027	[1] , [2]
	80	European Innovation Council	2022–2024	[1] , [2]

	38	Others	2022–2026	[1] , [2] , [3]
France	1 050			
	1 050	Investment Plan	2021–2026	[1]
Netherlands	750			
	615	Quantum Delta NL	2022–2029	[1] , [2]
	135	QuTech	2019–2029	[1]
Italy	116			
	116	The National Quantum Science and Technology Institute	2023–2026	[1]
Austria	107			
	107	Quantum Austria	2021–2026	[1]
Sweden	63			
	63	QACQT	2017–2027	[1]
Spain	60			
	60	Quantum Spain	2021–2026	[1]
Finland	24			
	24	Quantum computer procurement – VTT	2020–2024	[1] , [2] , [3]
Denmark	17			
	10	Quantum innovation centre	2016–2018	[1]
	4	FIRE-Q	2020–2024	[1] , [2]
	3	Crypt Q	2021–2024	[1]
Hungary	11			
	11	National Quantum Technology Programme	2018–2022	[1]

Sources: This table is based on first conducting a literature review – including (Querca, (2021) and (Candelon et al. (, 2022) – of all significant public initiatives on quantum technology in the EU, and then finding detailed information on each.

Note: For IRIS, the fraction of the total amount spent on quantum technologies has been estimated.

EU Quantum Flagship

The Quantum Flagship is a 10-year initiative of the European Commission **with a budget of approximately EUR 1 billion**. The initiative started in 2018 with the launch of more than 20 projects in the field of quantum technologies. The overall aim of the initiative is to foster research on quantum technologies as well as to transform research results for industrial exploitation and real-life applications. A roadmap was established in the context of the initiative setting out the main steps of the research agenda. The first strategic research agenda provided information on the different quantum pillars, the medium- to long-term actions and recommendations. The strategic research agenda was also complemented by a set of operational key performance indicators grouped by topic and technical pillar. These indicators are updated yearly to keep up with the pace of technological developments.

During the first phase of the initiative (2018–2022), 24 projects were financed. As a result, 1 313 scientific papers have been published, 105 patents have been filed and 25 start-ups have been founded. Notably, some of the most important EU companies in the field started as spin-offs of the initiative. In terms of research results, among others, participants in the quantum communication pillar managed to connect two quantum processors through an intermediate node and to establish shared entanglement to form a quantum network, as well as to deploy the first testbeds for quantum key distribution.

The second phase of the Quantum Flagship aims specifically at transforming the results of the first phase into industrial-ready applications. EuroQCI (on quantum communication infrastructure) and the European Quantum Computing & Simulation Infrastructure (EuroQCS) are two important initiatives launched within this framework. In this second phase, a review of the research agenda is also being carried out to include the industry perspective more comprehensively. A preliminary version of the strategic research and industry agenda was published at the end of last year.

Framework partnership agreements and flagship initiatives

To foster industrial-ready technological applications, the EU has created multiple framework partnership agreements with a larger budget and a greater number of partners compared with the projects carried out in the first phase. Two such agreements have been reached on quantum communication.

- **The Quantum Internet Alliance** involves 27 partners with a goal of building a prototype quantum internet by demonstrating quantum memories and long-distance entanglement sharing.
- **The Quantum Secure Networks Partnership** involves 42 partners and around EUR 25 million in funding. The project aims at fostering the maturity of QKD by demonstrating effective multi-node architecture.

As shown below, framework partnership agreements are also underpinning quantum computing and simulation.

- **MILLENION** involves 14 partners and has a budget of EUR 20 million. Its focus is on building scalable and accessible quantum computers based on trapped ions and advancing technology from the current lab prototype of 50 qubits to industry-grade quantum computers of 100 qubits and towards 1 000 (TRL 8+).
- **OpenSuperQPlus**, with 28 partners, is building a full-stack quantum computer based on superconducting qubits of high fidelity.
- **Pasquans2** involves 25 partners and is building a platform for programmable quantum simulators with over 1 000 neutral atoms.

Another important initiative is the **Quantum Computing & Simulation Infrastructure (EuroQCS)**. The aim of this project is to work on the deployment of quantum systems that are integrated with high-performance computers (HPC). This key infrastructure initiative is carried out

together with the EU High-Performance Computer Joint Undertaking centre. The first phase was the launch of the HPC and Quantum Simulator hybrid (HPCQS), which combines two quantum simulators, each handling about 100+ qubits. HPCQS also serves as a testing ground for quantum-HPC hybrid computing. Subsequently, six locations in the EU have been chosen to house and manage the initial quantum computers of the EuroHPC JU.

Two centres of excellence are also being established, one dedicated to research and another to industry, accelerating the discovery of quantum-oriented applications and developing technology-agnostic quantum applications for end users.

Quantum key distribution projects: EuroQCI

EuroQCI is among the most relevant project currently funded by the European Commission in the field of quantum technologies. This project involves 27 Member States, and is being carried out together with the EU Space Agency. Its infrastructure is composed of a terrestrial segment relying on a fibre communication network and a space segment based on satellites. EuroQCI will be the first operational system providing QKD in Europe. It started in June 2019. The goal is to provide an integrated satellite and terrestrial system spanning the whole EU for the secure exchange of cryptographic keys. The project is part of the European cybersecurity strategy and has been integrated into the new IRIS².

The space segment entails the distribution of quantum-secured encryption keys on a global scale, whereas the terrestrial segment concerns the establishment of a federation of national terrestrial QCI networks with cross-border connections. The deployment of terrestrial and space components is currently moving to the pre-validation phase. In terms of funding, the main common infrastructure, the space equipment and most of the governmental services will be procured by the EU. The terrestrial infrastructure will be procured by each Member State. Some elements will also be procured by the private sector. Both segments should rely exclusively on EU-27 industries³⁹.

The roadmap of the project includes three phases.

- (i) *Preliminary validation.* This demonstration phase aims at showing the effectiveness of EuroQCI. This phase will require having a network of Member States making the terrestrial segment available for demonstration, as well as demonstrating the space segment in a real environment.
- (ii) *First generation.* In this phase, non-classified keys for public stakeholders should be delivered. This phase should rely on EU-27 industries alone. It also includes the deployment of the first generation of a space constellation.
- (iii) *Second generation.* The project should reach its final capacity and the quantum key should be delivered, meeting SECRET UE/EU SECRET requirements. Similarly, this

³⁹ The infrastructure must come from an EU-27 company: the headquarters of the company should be in the EU and most of the company's shares should be controlled by people in the EU. The distinction is not strictly made with respect to device components.

phase will solely rely on EU-27 industries and include deployment of the second generation of a fully operational space constellation.

As mentioned, the terrestrial segment is currently in the preparatory and first deployment phase, with the first national networks being established to experiment with QKD technology. The space segment, coordinated by the EU Space Agency, is also in the first phase, which is mainly concerned with the deployment of a LEO (Low Earth Orbit) satellite for demonstration and early test.

Finally, the [PETRUS Consortium](#) is coordinating the deployment of EuroQCI, capturing relevant data on system design and architecture, deployment and network operations. It is also evaluating the data with existing EuroQCI studies and educating national QCI project points of contact.

Other EU initiatives and agencies working on quantum technologies

The European Innovation Council is providing funding for projects focusing specifically on quantum technologies. In its [2022 work programme](#), they ran a Pathfinder challenge on 'Alternative approaches to Quantum Information Processing, Communication, and Sensing'. In the 2023 work programme, there is an Accelerator challenge on 'Emerging semiconductor or quantum technology components'. Calls for both challenges are still open.

The EuroHPC JU was established in 2018. The undertaking has no clear end date, but the current mission runs until 2027, with a total budget of EUR 7 billion. Its [first quantum initiative](#) was launched in December 2021, and the sites for the first European quantum computers were chosen in October 2022. As part of the EuroHPC JU, a call for pilot projects, including on building quantum simulators, was launched in 2020. The work plan for 2023 includes various projects in quantum computing, as well as follow-ups from the previous year.

The European [Chips Act](#) aims at boosting Europe's competitiveness and resilience in semiconductor technologies and applications. One of the five operational objectives of the Chips Act is 'building advanced technology and engineering capacities for accelerating the innovative development of quantum chips', so it has considerable interest in quantum technologies.

National quantum initiatives: Germany

Among EU countries, Germany has emerged as a prominent player in the field of quantum technologies, making significant strides in research, development and deployment. As mentioned, as part of the German Covid-19 stimulus programme, in 2020 the German federal government launched a [quantum initiative](#) entailing 'stimulus and future package providing a total of 2 billion euros for the development of quantum technologies and in particular for quantum computing' (Swayne, 2022). Among the recipients of funding from this initiative is Infineon, a multinational corporation providing semiconductors and system solutions, which is taking part in six projects mostly around quantum computing (Swayne, 2022). In March 2023,

an action plan was announced that will invest EUR 3 billion in the development of a universal quantum computer by 2026 (Swayne, 2023).

National quantum initiatives: France

France is supporting research and development efforts through initiatives like the national quantum plan, which intends to advance quantum technologies and foster collaboration between academia, industry and government. In collaboration with the Agence Nationale de la Recherche, France is funding various projects related to post-quantum cryptography, seeking to develop secure cryptographic solutions that can withstand attacks from quantum computers.

In 2021, the French government announced an investment plan for quantum technologies. The plan will run for 5 years, with a total budget of [EUR 1.8 billion](#) (with EUR 150 million earmarked for quantum-resistant cryptography), of which EUR 1 billion is investment by the French government. [Ten projects](#) to be funded were announced in March 2022, covering a wide range of areas, including 'error correction codes, cold-atom, superconducting and silicon-spin qubits, gravimeter-type sensors, and quantum communication with the ambition of deploying operational networks' (MajuLab, 2022).

In 2022, a memorandum was signed by Minister of Higher Education and Research Sylvie Retailleau and Dr Arati Prabhakar, Director of the US Office of Science and Technology Policy. This memorandum underscores support for the joint efforts of France and the US on quantum computing research. In this context, the French embassy in the US sent to Paris its first [encrypted diplomatic message](#) leveraging post-quantum cryptography.

National quantum initiatives: Italy

Italy, like many of its EU counterparts, is investing in quantum technologies. In its [Recovery and Resilience plan](#), the Italian government has allocated EUR 1.6 billion for fostering national R&D champions in key enabling technologies, including quantum computing, big data, climate, energy, biopharma and other significant technological advances. On 19 July 2022, it set up a new [body](#), the National Centre for Research on High-Performance Computing, Big Data and Quantum Computing.

A notable achievement in Italy's quantum initiative is the establishment of the [Padua Quantum Computing and Simulation Center](#). Its plan of action includes the acquisition of a quantum computer and the creation of an international-level scientific research centre to host it. The aim of the Padua Center is to develop a general-purpose quantum computer using 'trapped ion' technology. Furthermore, in collaboration with SEEQC, the Federico II di Napoli University is actively involved in a [project](#) to develop a quantum computer.

*United States*⁴⁰

The US has emerged as a global leader in the development and deployment of quantum technologies, driven by a strong commitment to maintaining its technological dominance. The US government, in collaboration with academia, industry and national labs, has launched several initiatives to accelerate the advancement of quantum technologies. Currently, most of the quantum technology policies and acts concern R&D and funding.

In addition to federal initiatives, individual states within the US have been proactive in fostering quantum technology ecosystems. In this context, several states, including California, New York and Maryland, have established quantum centres that bring together academia, industry and government to accelerate research and development in quantum technologies. These state-level initiatives seek to cultivate regional expertise, attract talent and promote collaboration among stakeholders.

National Quantum Initiative Act of 2018

One of the key initiatives in the US is the [National Quantum Initiative Act](#), signed into law in 2018. This comprehensive legislation aims to bolster the research, development and commercialisation of quantum technologies. The act of 2018 established a coordinated federal programme to accelerate quantum research and development with USD 1.275 billion in funding over 5 years. This act was one of the first on quantum technology to be passed in the US. It assigns specific roles to different departments and institutions:

- National Institute for Standards and Technology
- Department of Energy (DOE)
- National Science Foundation.

This act further established responsibilities for the following departments:

- National Science and Technology Council
- National Quantum Coordination Office
- National Quantum Initiative Advisory Committee.

CHIPS and Science Act of 2022

The passage of the CHIPS and Science Act (CHIPS+) of 2022 ‘signifies a concerted US government effort to coordinate a national renewal in science and technology’, in the [assessment](#) of the Center for Strategic and International Studies. The CHIPS Act grants significant funds to US DOE offices. Previously, the 2018 Department of Energy Research and Innovation Act provided the DOE with some funding, leading to the creation of five Quantum Information Science Research Centers. The CHIPS+ Act amends and expands the centres’ mandate in the following ways:

⁴⁰ This section partially draws from preparatory work by Michela Giuricich, Research Assistant Intern at CEPS.

- authorises USD 500 million for a DOE Quantum Network Infrastructure R&D programme;
- tasks the DOE to work to improve accessibility to quantum computing resources for US-based researchers and laboratories;
- reauthorises the Computational Science Graduate Fellowship programme within the Advanced Scientific Computing Research initiative;
- authorises USD 80 million in funding for NIST;
- increases up to USD 45 billion the authorised budget for the National Science Foundation and expands its mandate with the tasks of incorporating quantum information science and engineering into STEM curricula and implementing the Next Generation Quantum Leader Pilot.

[The Directorate for Technology, Innovation and Partnership 2022](#)

This directorate was formed to help ensure that American university researchers can translate theoretical advances into political breakthroughs via the best-engineered supporting infrastructure. [The Brookings Institute](#) sums up the main purpose of this directorate: to ‘advance science and engineering research and innovation leading to breakthrough technologies ... and accelerate the translation of fundamental discoveries from lab to market’.

*China*⁴¹

China has emerged as a highly relevant player in the field of quantum technologies, showcasing significant progress and an unwavering commitment to achieving quantum supremacy. The Chinese government has been actively investing in research and development.

China has allocated substantial funding and resources to accelerating the development of quantum technologies. Notably, the country accounts for over 50 % of the estimated global public investment in quantum technologies, which is allocated to research and Chinese quantum companies. Up to 2023, [estimated funding](#) for quantum technologies in China was approximately USD 15 billion. Some, for instance Levine (2020), have stated that ‘China would channel 25 per cent of the nation’s total GDP to research and development in areas of strategic importance to future economic development and national security’.

Compared with the US, China has committed significantly more public spending, extending beyond simply R&D. However, in the US private investment in quantum technologies, research and start-ups is substantially higher than in China (Levine, 2020).

[China’s quantum timeline](#)

China, along with the US, has been at the forefront of the quantum computing race. Kania & Costello (2018) observe that since the 1980s, China has been implementing policies to ensure the development of its science and technology sector. Below is a timeline of the plans and

⁴¹ This section partially draws from preparatory work by Michela Giuricich, Research Assistant Intern at CEPS.

policies implemented by the Chinese government from 1986 to 2018, as identified by Kania and Castello.

Table B.2. Plans and policies implemented by the Chinese government from 1986 to 2018

<i>Year</i>	<i>Chinese Plans and Policies</i>
1986	The National High Technology Research and Development Plan/Programme was introduced. This plan supported dual research in quantum science and technology.
1997	The National Key Basic Research and Development Plan was unveiled. The plan provided early support for basic research in quantum control, communication and information technology.
2006	The National Medium- and Long-Term Science and Technology Development Plan was put in place. It was the first official plan by China to strengthen its quantum computing sector.
2015	The Made in China 2025 strategic plan was launched, for actively advancing quantum computing.
2016 (February)	The National Key Research and Development Plan replaced the plans introduced in 1986 and 1997 to support R&D in quantum control and quantum science.
2016 (August)	The Thirteenth Five-Year National Science and Technology Innovation Plan called for results in the innovation of the quantum computing sector and set objectives for 2030.
2016 (December)	The Thirteenth Five-Year National Strategic Emerging Industries Development Plan further highlighted the importance of an overall approach that included quantum chips, quantum programming, quantum software and related materials and devices, promoting the realisation of the physics for quantum computing and application for quantum simulations.
2017	The Thirteenth Five-Year Science and Technology Military-Civil Fusion Special Projects Plan introduced quantum satellites among a series of new military civil-fusion development projects in science and technology.
2018	the State Council's Several Opinions Regarding Comprehensively Strengthening Basic Research called for boosting basic research in quantum science and urged the faster implementation of the 'Science and Technology Innovation 2030 Megaproject', which aims to enhance and improve quantum computing and quantum communications.

Source: Kania, E.B. & J.K. Costello (2018), 'China's Quantum Ambitions', *Military Cyber Affairs*, 3(2), <https://www.jstor.org/stable/resrep20450.6>.

United Kingdom

The UK is another important international player in the race for quantum technologies. The National Quantum Technologies Programme was founded in 2014 as a 10-year programme by the government's scientific research agencies. Government, academia and industry partnered for about GBP 1 billion to set up the programme. In the context of the programme, the Engineering and Physical Sciences Research Council and the Science and Technology Facilities Council led the establishment of the National Quantum Computing Centre (NQCC). The [NQCC](#) represents an investment of GBP 93 million over 5 years and has the key objective of delivering 100+ qubit NISQ-era user platforms by 2025.

This year, the UK government also published its first national quantum strategy, setting aside GBP 2.5 billion in funding for quantum research and naming the quantum computing industry as a strategic priority for the UK. Moreover, Parliament has appointed a committee to monitor how the UK's quantum industry compares with other nations with strengths in quantum, such as the US and China.

In 2022, the UK government reportedly acquired its [first quantum computer](#). The Ministry of Defence is working with ORCA Computing to explore the potential of quantum to enhance national defence. ORCA Computing's mission is to develop scalable quantum computers that integrate with real-world technologies. This is a challenge for current prototypes, primarily because, as described, they must keep the qubits on which they run at extremely cold temperatures or become unstable. ORCA Computing claims to have found a way to operate quantum computing that does not require this. Moreover, optical fibre can be used for networks rather than silicon, further enhancing scale and reliability.

Japan

In recent years, Japan has revamped its quantum technology strategy to catch up with the US and China. In 2019, the US and Japan signed the 'Tokyo Statement on Quantum Cooperation'. This was the first bilateral diplomatic agreement regarding quantum information and science cooperation. In 2020, the Japanese government laid out a quantum technology and innovation strategy. In April 2022, the Japanese government formulated a new strategy, the 'Vision of Quantum Future Society', that expanded on initiatives for social innovation through quantum technology from the 2020 strategy.

Fujitsu will become the first domestic company to produce a quantum computer in Japan, with the help of the Riken research institute. Japan's first homegrown quantum computer was opened for cloud access in March 2023 (Fujitsu, 2023). The government aims for [10 million users](#) by 2030. Fujitsu's computer is expected to be powered initially with 64 qubits, but plans are to ramp up that qubit number to about 1 000 within 3 years.

Australia

Australia has emerged as a promising hub for quantum technologies. The Australian government has shown a strong commitment to advancing them. The Commonwealth Scientific and Industrial Research Organisation and the Australian Research Council are key players in driving quantum research and development.

Australia has recently launched its [quantum strategy](#). Specifically, the Australian Department of Industry, Science, Energy and Resources has prepared a National Quantum Roadmap, a comprehensive strategic plan that outlines the country's vision and priorities for quantum technologies. The roadmap includes measures to foster collaboration between academia and industry, develop a skilled quantum workforce, attract investment in quantum research and commercialisation, and secure access to essential quantum infrastructure and materials.

Australia also participates in international collaboration and partnerships to accelerate the development and adoption of quantum technologies. The country is a member of the Quantum Flagship programme of the EU and the Quantum Industry Consortium.



APPENDIX C. EXAMPLES OF THE TRANSITION TO QUANTUM-RESISTANT CRYPTOGRAPHY IN SELECTED COUNTRIES

As quantum technologies are still evolving, the status of the transition to quantum-resistant cryptography varies among countries, with some leading in research and implementation, while others are in the early stages of developing strategies and policies. This appendix gives an overview of the transition status of countries across the world.

China

China has carried out its quantum-resistant standardisation process like the US National Institute for Standards and Technology. The Chinese competition received submissions between 2018 and 2019. It was open to Chinese developers, who submitted a total of 36 applications that were analysed over the course of a year. The applications covered the main areas of modern quantum-resistant cryptography. Experts argue that China has selected encryption algorithms for quantum-resistant cryptography standards based on the same mathematical models (Lattice-based solutions) as the US while choosing a [slightly different scheme](#).

Notably, China is also a global leader in the field of quantum key distribution. The country has made important advances in quantum communication, with the successful launch of the world's first quantum satellite, Micius, in 2016. This satellite can enable secure quantum communication over long distances. Since then, Chinese researchers have made significant progress in the deployment of QKD networks, with several large-scale QKD trials conducted across the country accounting for over 10 000 km⁴².

The country has outlined its vision for a quantum internet – an interconnected network that harnesses the power of quantum communication to enable secure and efficient data transmission. China aims to develop a comprehensive infrastructure for quantum communication that spans cities and provinces. The exact number of quantum computers that China has is not publicly disclosed.

European Union

The primary ways to counter threats posed by quantum computing should be a combination of conventional solutions, quantum-resistant cryptography and possibly QKD in hybrid approaches, according to a [resolution](#) of the European Parliament.

The EU launched a specific call for proposals in its 2022 programme for increased cybersecurity through the package 'Transition towards Quantum-Resistant Cryptography'. The total budget for the track is EUR 11 million. Two proposals will be selected at the end of the call. The expected outcomes of the project include assessing and standardising/certifying future-proof cryptography and identifying quantum-resistant cryptographic primitives, protocols, solutions

⁴² European Commission, presentation at the Quantum Technologies and Cybersecurity Task Force.

and methods that could be used to migrate from current cryptography towards future-proof cryptography. The applicants are expected to design, build and deploy quantum-resistant infrastructure and to include in their proposals an assessment of the transition from current cryptography towards future-proof cryptography. Hybrid solutions, whenever bringing higher security protection, should also be included in the scope of the project.

Finally, ENISA has worked extensively on quantum-resistant cryptography and produced two high-level studies on the state of the art, standardisation and protocols related to the technology.

Germany

The working assumption of the German BSI on high-security applications is that with non-negligible probability, there will be a cryptographically relevant quantum computer by the beginning of the 2030s. This is not a forecast on the timeline for the development of large-scale quantum computers, but a working hypothesis for risk assessment.

In this context, the BSI has been evaluating post-quantum alternatives since before the launch of NIST's standardisation process, according to an [ENISA study](#). In BSI's view, the NIST standardisation process is the most prominent international effort. In addition to this, the ISO/IEC JTC 1/SC 27/WG 2 is working on adding FrodoKEM, Classic McEliece and ML-KEM to an existing standard (ISO/IEC 18033-2). FrodoKEM and Classic McEliece standards may be particularly interesting for use cases where more conservative security assumptions are desirable.

BSI has issued [general recommendations](#) on migration to quantum-resistant cryptography, including the points below.

- It is important to raise awareness of the quantum threat, especially among industries.
- Store-now-decrypt-later is a threat today. Hence, organisations should take steps now by creating a cryptographic inventory and by prioritising and developing a migration plan.
- The migration of key agreement schemes is more urgent than signatures due to the store-now-decrypt-later scenario.
- Migrating public key infrastructure takes a long time, so preparations should be made early on for the migration to new signature schemes.
- Continuing research in quantum-resistant cryptography is important to gain confidence in the security of schemes and in their implementation.

BSI further recommends using quantum-resistant cryptography only in hybrid mode together with classical schemes or pre-shared keys. An exception to this is hash-based signatures, which may be used without hybridisation because their security is based on well-understood

assumptions about hash functions. Furthermore, when designing new products and protocols, cryptographic agility should always be taken into account as much as possible. For symmetric cryptography, the symmetric encryption scheme AES-256 is regarded as quantum-safe.

Alongside the effort towards establishing relevant standards, BSI is also conducting projects integrating quantum-resistant cryptography into open-source schemes and a study on the status of quantum computer development.

BSI is planning a migration of Germany's administrative public key infrastructure (the 'Verwaltungs-PKI' or V-PKI) to quantum-resistant cryptography. This is an interesting use case, where security, performance, interoperability and compatibility with standard applications are important criteria, and migration times are long (15+ years) due to the complexity of the ecosystem and the long validity periods of current certificates. The plan is to build a new public key infrastructure in parallel to the current one and transit smoothly to guarantee business continuity.

Applied research organisations such as the [Fraunhofer AISEC](#) Competence Center for Post-Quantum Cryptography specifically focus on assisting companies with quantum-resistant migration. Finally, the German [Industrial Association for Quantum Security](#) (DIVQSec) promotes industrially usable solutions for quantum-resistant cryptography.

France

In collaboration with the Agence Nationale de la Recherche, France is funding various projects related to post-quantum cryptography, seeking to develop secure cryptographic solutions that can withstand attacks from quantum computers.

Even though the NIST competition has helped foster attention and research on quantum-resistant cryptography, according to ANSSI the algorithms are not yet mature enough to ensure security alone. Research is still at an early stage on the underlying mathematical problems, choice of parameters, integration in protocols and secure implementation (including research on side-channel attacks). As such, ANSSI strongly recommends avoiding any drop-in replacement of pre-quantum with post-quantum, except for systems whose security relies only on hash-based signature schemes. Since quantum-resistant cryptography is not yet mature, ANSSI strongly recommends using hybrid protocols in the short and medium term.

The agency also encourages any progress towards crypto agility. For any security products aimed at offering long-lasting protection of information (after 2030), ANSSI recommends starting the transition with hybrid quantum-resistant cryptography as soon as possible. For symmetric cryptography, ANSSI encourages the use of a conjectured post-quantum security level consistent with the quantum-resistant algorithm selected for asymmetric cryptography. ANSSI does not recommend a closed list of algorithms for public key cryptography. This is to avoid proscribing innovative state-of-the-art algorithms that could be well-suited for some particular use cases. Nevertheless, ANSSI recommends a set of quantum-resistant

cryptographic algorithms largely aligned with NIST (ML-KEM, FrodoKEM, ML-DSA, Falcon, XMSS/LMS and SHL-DSA).

ANSSI also recommends the use of hybridisation modes and has various warnings about technical issues involved in setting up a hybridisation mode securely. In general, when using hybridisation modes, ANSSI recommends using standards or modes with validated security proofs. For security visas⁴³, ANSSI has a three-phase transition plan, which first builds in hybridisation as an add-on, then as a quantum-resistant mitigation and finally makes hybridisation optional. Currently, phase 1 is nearing its end. As such, ANSSI is updating its agenda on certificate delivery, including developing skills in the evaluation of hybrid mechanisms and of quantum-resistant cryptographic algorithms that are well known, as well as additional side-channel evaluation of them. The first phase-2 certificates are expected in 2024–2025. The date for moving into phase 3 has not yet been set.

United Kingdom

In short, the recommendation made in an NCSC [white paper of November 2020](#) on responding to the threat posed by quantum computing is to wait for the NIST standardisation process to finish, and then transition to the standardised algorithms.

According to the NCSC, quantum-resistant cryptography is currently the most viable avenue available for responding to the threat posed by public key cryptography. According to the NCSC's latest [guidance](#) published in November 2023, ML-KEM and ML-DSA are algorithms suitable for general-purpose use. The NCSC recommends ML-KEM-768 and ML-DSA-65 as providing appropriate levels of security and efficiency for most use cases.

There are standardised stateful hash-based signature algorithms, like XMSS and LMS, that have niche applications, such as signing firmware. However, in an earlier [white paper of March 2020](#), the NCSC argues that these are not suitable for general-purpose use.

Early adoption of non-standardised quantum-resistant cryptography is not recommended by the NCSC. Transition to any form of new cryptographic infrastructure is an inherently complex and expensive process that must be planned and managed with care. There is indeed no guarantee that non-standardised solutions are safe.

Finally, if a hybrid scheme is chosen, the NCSC recommends it be used as an interim measure that allows a straightforward migration to PQC-only in the future.

⁴³ ANSSI security visas are a way of certifying the security of a product or service. They are mandatory in some contexts.

Japan

The National Institute of Information and Communications Technology (NICT) in Japan has led efforts to explore and develop quantum-resistant cryptographic algorithms. Notably, in October 2022 NICT developed, in collaboration with the private sector, a PQC CARD for individual payment and personal authentication, equipped with post-quantum cryptography. The PQC CARD uses ML-DSA, a digital signature algorithm selected as a potential standard technology by NIST. NICT has also launched a programme, Photonics and Quantum Technology for Society 5.0, leveraging QKD systems.

NICT and a consortium of academic and industrial partners have developed a quantum-cryptography integrated system that has recently been tested on a hospital database of 10 000 sensitive medical records. The new system, called LINCOS (Long-term Integrity and Confidentiality Protection System) exchanges data using a dedicated optical fibre network with end-to-end encryption protected by quantum key distribution technology, building a [fortress](#). It uses a distributed storage technique called ‘secret sharing’, in which the data are split into pieces for storage and several pieces must be gathered for reconstruction. Notably, the effectiveness of the PQC CARD has been tested by applying it to smart card authentication and control of access to digital medical records on LINCOS.

The Japanese Cryptography Research and Evaluation Committees (CRYPTREC) are also active in evaluating and monitoring secure, quantum-resistant cryptography techniques in Japanese e-Government systems. CRYPTREC recommended cyphers that are approved in terms of their security and implementation aspects as well as current and future market deployment.

Australia

The Australian Signals Directorate (ASD), the country's leading authority on cybersecurity, has been actively involved in researching and evaluating quantum-resistant cryptographic algorithms. The outcome of these evaluations informs updates to ASD-approved cryptographic algorithms in the *Information Security Manual* (ISM). At this stage, ASD assesses whether the currently approved cryptography within the ISM provides the most effective method of securing communications. The ASD mentions on its website that it will continue to monitor alternate methods of securing communications such as QKD. However, in its planning, the ASD notes that ‘the practical limitations of QKD (including transmission distances, specialised hardware requirements and concerns around availability) mean that ASD does not support its use for secure communications at this time’.

PRINCIPLES AND GUIDELINES FOR THE TASK FORCE

The Task Force process is a structured dialogue among experts, (former) politicians, diplomats, policymakers, NGOs, academia and think tanks who are brought together for several meetings. Task Force report is the final output of the research carried out independently by CEPS and SWP in the context of the Task Force.

Participants in a Task Force

- The Chair is an expert who steers the dialogue during the meetings and advises CEPS as to the general conduct of the activities of the Task Force.
- Members provide input as independent experts.
- Rapporteurs are CEPS researchers who organise the Task Force, conduct the research independently and draft the final report.

Objectives of a Task Force report

- Task Force reports are meant to contribute to policy debates by presenting a balanced set of arguments, based on available data, literature, and views.
- Reports seek to provide readers with a constructive basis for discussion. They do not seek to advance a single position or misrepresent the complexity of any subject matter.
- Task Force reports also fulfil an educational purpose and are drafted in a manner that is easy to understand, without jargon, and with any technical terminology fully defined.

Drafting of the report

- Task Force reports reflect members' views.
- However, there does not need to be consensus or broad agreement among Task Force members for every recommendation that features in the report. Recommendations which triggered significant dissent are marked accordingly.
- Task Force reports feature data that are considered both relevant and accurate by the rapporteurs. After consultation with other Task Force members, the rapporteurs may decide either to exclude data or to mention these concerns in the main body of the text.

Centre for European Policy Studies

Place du Congrès 1, 1000 Brussels

