techUK
FOR WHAT COMES NEXT

Industry Perspective: Preparing for Quantum Resilience

A techUK report

September 2024

Executive Summary

At the heart of the UK's ambitions to be a world leader in quantum technologies is the need to ensure quantum deployment is safe and secure.

Quantum technologies offer a formidable opportunity to unlock innovation in the UK and internationally. Quantum computing, for example, is anticipated to enable previously unattainable technological advancements across different industries and sectors, from drug discovery, protein-folding, carbon capture, battery research and more. Such advancements will have the opportunity to have a positive impact in the UK, critical to achieving the UK's ambition to become a world leader in science and technology.

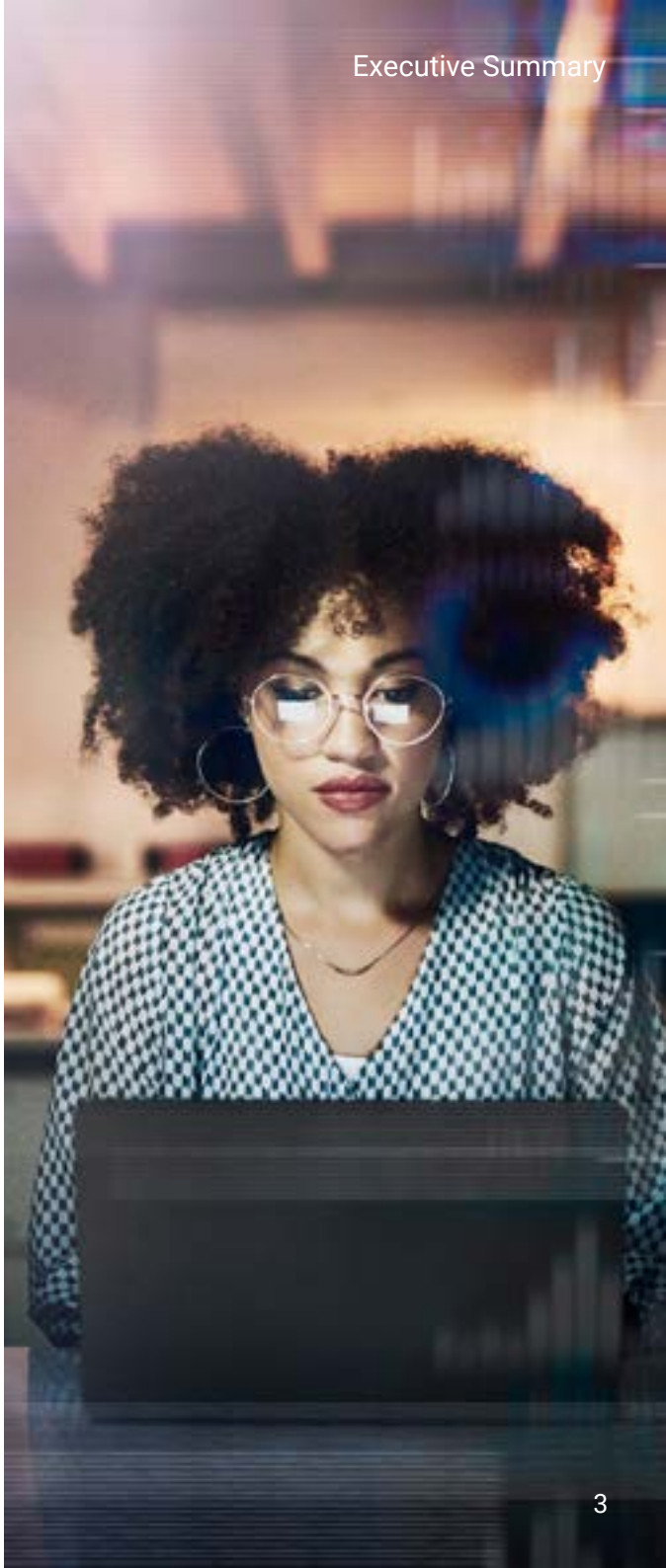
However, to realise this potential, we must ensure the resilience of quantum technologies and understand that they also pose a significant cyber threat in themselves. Though the timeframe varies from as little as five years to over ten years, quantum computers could be capable of breaking algorithms underpinning the use of cryptography that safeguards data. This could include the breach of sensitive health, financial or personal data; the interception of messages on the internet; and the undermining of the integrity of digital documents.[1]

Time is of the essence for organisations worried about the quantum threat. They will not be able to make the quantum secure transition overnight as migration to post-quantum cryptography (PQC) can be timely and costly for businesses and governments alike.

The *National Quantum Strategy,* published in March 2023, underscored a commitment to provide guidance to quantum businesses and researchers on how to work safely with others, including against cyber threats. Equally, guidance from the National Cyber Security Centre (NCSC) specifically on post-quantum cryptography has been welcomed as useful information for all businesses on this topic.[2] The UK Government and the NCSC will play an important role in co-ordinating guidance and developing clarity in this space. techUK members have expressed hope for increased collaboration and business engagement on the issues surrounding quantum resilience, to ensure that organisations understand how to become cyber secure against the quantum threat in an appropriate, orderly and timely manner.

techUK has created this short document to detangle misconceptions around the quantum computing threat to encryption, support understanding of key guidance, policy and technological development, and signpost where organisations might access more guidance on developing quantum resilience in future. This document seeks to introduce cyber security in a quantum world in simple terms, and to highlight where impartial further information can be found.

techUK welcomes the current work undertaken by the UK Government in this space and calls for further collaboration between government and industry. This public–private partnership will be a critical driver of a successful transition to quantum resilience, ensuring that organisations across all sectors in the UK have the tools and talent they need in future.



1. Definitions and myth busting: an introduction to cryptography

Becoming 'quantum resilient' means a commitment to protecting our data, systems and networks against malicious actors leveraging the capabilities of a quantum computer.

However, there are several misconceptions around what it means to be quantum resilient. This often includes the assumption that businesses will need access to a quantum computer to become quantum secure.

This is not true. Quantum resilience is built using enhanced cryptography.

What is the problem?

Cryptography underpins the security of our digital infrastructure. Cryptography remains important to protecting data and users, ensuring confidentiality, and preventing cyber criminals from intercepting sensitive corporate information.[3] Cryptography is inherently both complex and mathematical in nature, and this paper does not seek to define cryptographic processes and concepts. A widely reviewed, detailed effort to explain cryptography in cyber security is included in The Cyber Body of Knowledge (CyBOK).[4]

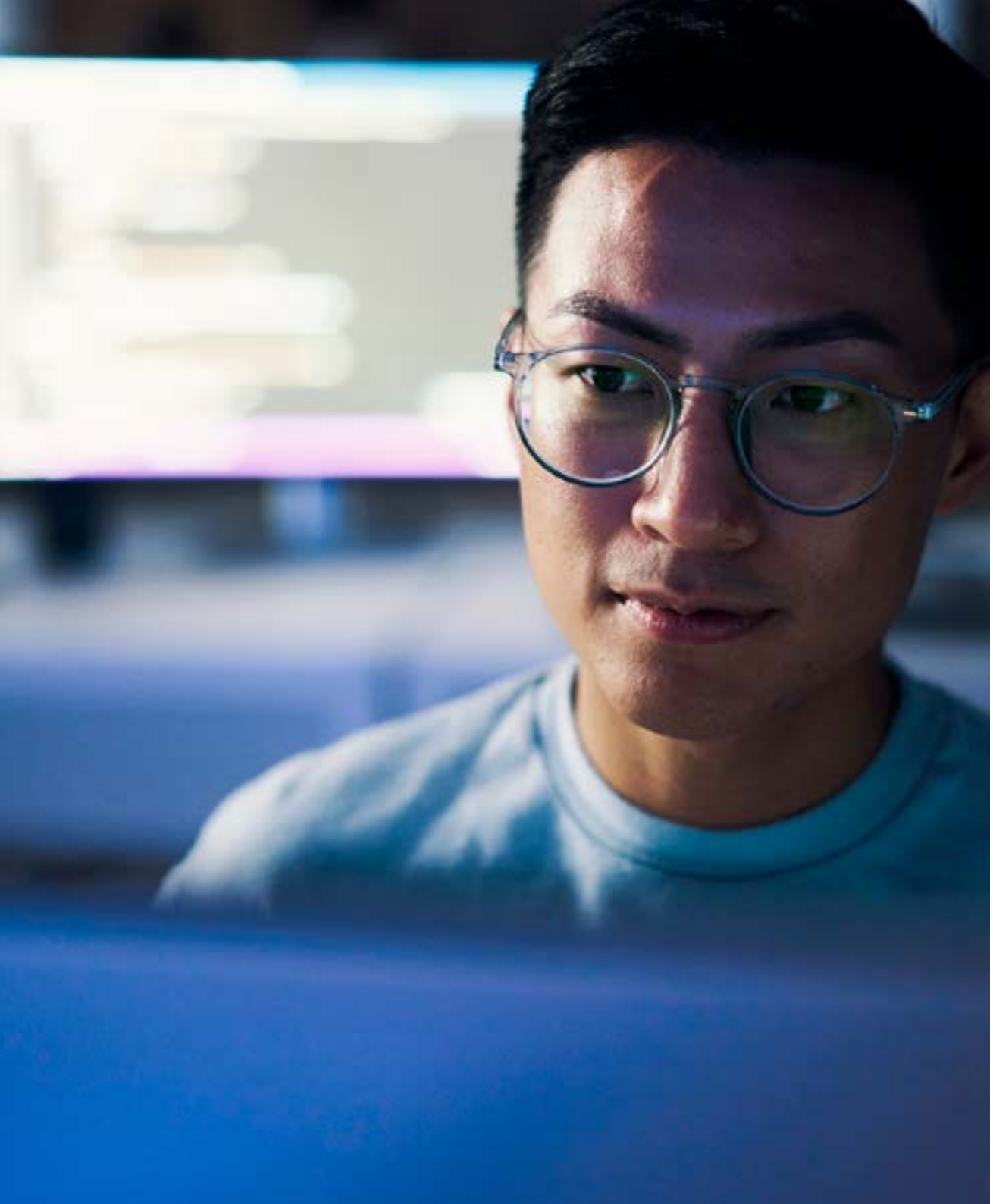
There are different types of cryptography, however, public key cryptography (PKC) is a commonly cited example. The security of the internet, electronic commerce, mobile communications and software updates are based on PKC, which allows secure communication and transactions with someone you haven't met. There are multiple types of PKC algorithms with one example being Rivest–Shamir–Adleman (RSA), which is commonly used in a range of web browsers, VPNs, chat and other communication channels, and more.

The challenge is that quantum computers could potentially break cryptography in the coming years. While there are a lot of unknowns in this claim, it is important that businesses take it seriously and prepare for quantum resilience.

When will quantum computers break cryptography?

There is no simple answer to this question. Predictions are being made, with the 2023 *Quantum Threat Timeline Report* by the Global Risk Institute revealing that more than a quarter surveyed believe it is over 50% likely by 2033.[5] This report states that there is a significant chance that the quantum threat becomes concrete in the next ten years, however, it must be stressed that this is an imperfect science. There is no set roadmap for quantum computing and, therefore, no set timeline for becoming quantum secure.

It is important to recognise why quantum computers can threaten security. The quantum threat is based on the efficient implementation of Shor's Algorithm, where quantum computers have the potential to break much widely used public key cryptography.[6] In 1994, Peter Shor invented an algorithm which solves the mathematical problem underlying RSA in hours, rather than the many years assumed for classical compute.



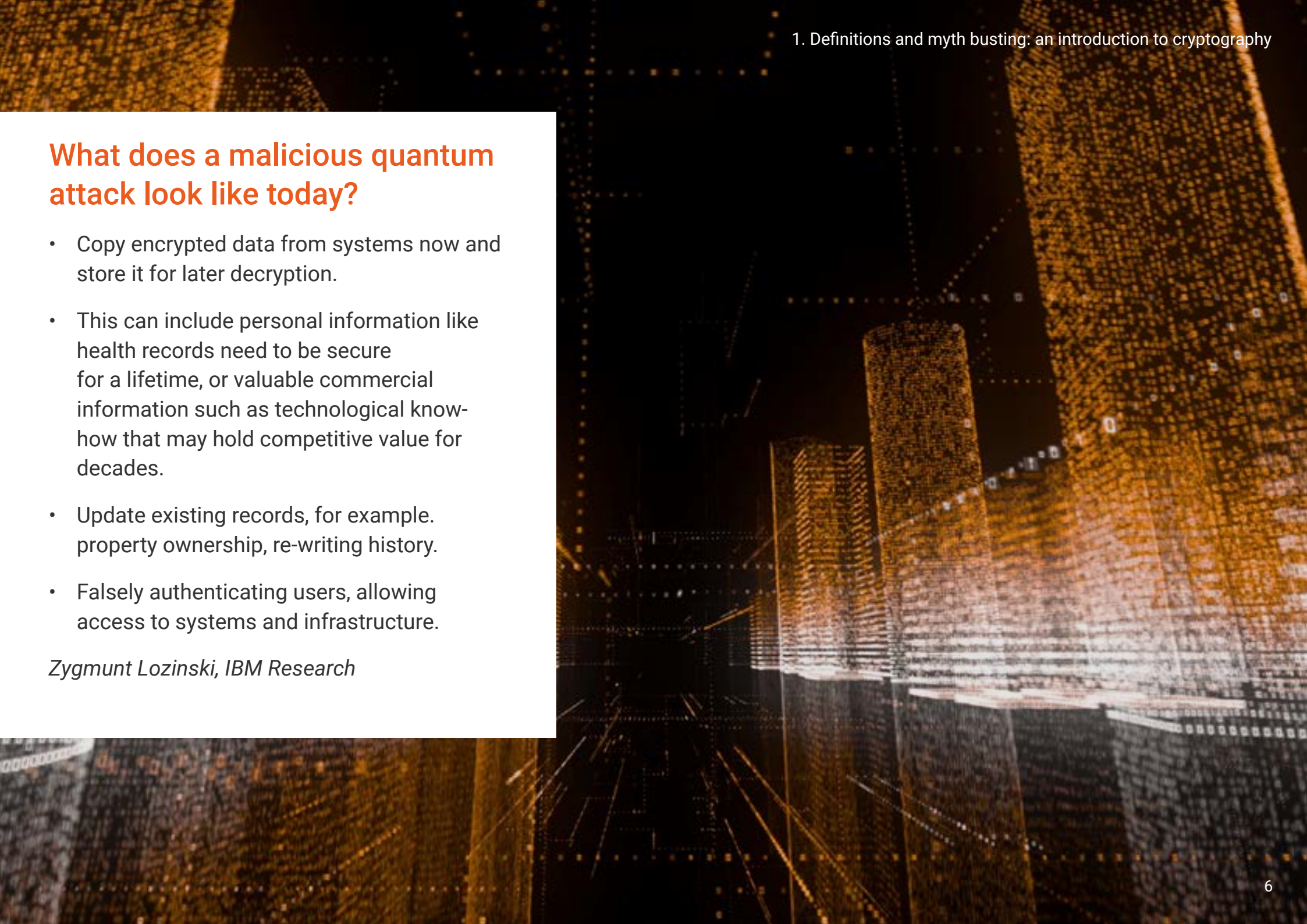
Once a quantum computer can effectively deploy Shor's algorithm, RSA is at risk.

'Harvest Now and Decrypt Later' attacks

One of the biggest risks at present is what's known as a 'Harvest Now, Decrypt Later' attack where encrypted data is captured, stored and held onto, until a quantum computer can unlock it. For sensitive data that holds value – such as in regulated industries that are required to keep sensitive customer data for long periods of time – this is a real threat now, as some estimates place the application of Shor's algorithm in 10–15 years.[7] [8]

An introduction to long-lived systems vulnerable to quantum attackers

Another risk is attacks on long-lived (10+ years) systems that have cryptography implemented in hardware, which can be common across multiple industries (including critical infrastructures, healthcare, retail, etc.) Hardware can be difficult to update once in use which means if quantum attacks became viable during its lifetime it could undermine the security of the system. To prevent long-lived systems becoming vulnerable during their lifetime, quantum-resistant cryptography should be integrated into hardware during the design phase, prior to being deployed.[9]



What does a malicious quantum attack look like today?

- Copy encrypted data from systems now and store it for later decryption.
- This can include personal information like health records need to be secure for a lifetime, or valuable commercial information such as technological know-how that may hold competitive value for decades.
- Update existing records, for example. property ownership, re-writing history.
- Falsely authenticating users, allowing access to systems and infrastructure.

Zygmunt Lozinski, IBM Research

2. What are the potential solutions?

The quantum and cryptography communities have been preparing for the quantum threat through defining and standardising quantum-resistant solutions. These may consist of implementing updated cryptographic approaches, while quantum-based approaches are also being developed.

Post-Quantum Cryptography (PQC):

Sometimes referred to as quantum-safe cryptography, PQC simply refers to cryptography that is resistant to attack by quantum computers.[10] PQC uses different kinds of mathematics from traditional cryptography, but they are designed to run on classical computers and existing networks.

For many use cases, upgrading to PQC could be just as simple as a software update. This means that PQC can offer a straight-forward solution for businesses looking to become quantum secure, however, it is important to recognise and prepare for when this may not be the case. For example, when protocols and services need to be re-engineered, when bandwidth or compute power is insufficient, or if previous cryptographic algorithms were hardcoded.[11] For devices or infrastructure that cannot be upgraded, the NCSC recommends that businesses should plan for PQC transition as a part of scheduled technology refresh cycles.[12]

In the US, the National Institute of Standards and Technology (NIST) has, in August 2024, standardised PQC algorithms.[13] Meanwhile, in November 2023, the UK's NCSC published guidance titled *Next steps in preparing for post-quantum cryptography.* Updated in August 2024, this sets out that the best mitigation against the threat of quantum computers to traditional PKC is post-quantum cryptography (PQC) and provides useful guidance for organisations on how to begin planning for the migration to PQC.[14]

Classic symmetric encryption methods that will work in the quantum era

Symmetric cryptography is already quantum resistant, meaning this is a solution for some use cases that do not necessarily need to be updated and can be used for both encryption and key exchange.

The National Cyber Security Centre (NCSC) has said:

> *"In contrast with PKC [public-key cryptography], the security of symmetric cryptography is not significantly impacted by quantum computers, and with suitable key sizes, existing symmetric algorithms – such as AES – can continue to be used."*
>
> (NCSC, Preparing for Quantum-Safe Cryptography, 11 November 2020)[15]

Alongside PQC, the quantum community developing other quantum resilient solutions based on the application of quantum principles.

Quantum Random Number Generation (QRNG): random number generation forms the bedrock of any cryptography system. Some businesses have suggested that quantum-based solutions will enable improved random generation. The laws of quantum mechanics ensure that quantum particles are inherently truly random. This means that QRNG generators can leverage fundamental quantum properties to generate random numbers with high entropy. QRNGs are hardware devices and will be used alongside other classical and quantum-based security solutions.[16]

QRNGs in action - Simulations to security: an analogy of high-quality entropy benefits

Monte Carlo simulations are prevalent in the financial services sector, where they are used in pricing models, risk estimation, and portfolio management. Current industry standards use pseudo-random number generators (PRNGs), which are deterministic algorithms that produce only seemingly random sequences. Through an Innovate UK funded project, Quantum Dice, Hartree and HSBC have been exploring the advantages that high quality randomness from QRNGs affects financial Monte Carlo simulations. Finding that the quality of random number generators can significantly affect the accuracy and time-to-solution of simulations, Quantum Dice and HSBC are now moving forwards into a planned commercial proof of concept (PoC). This also serves to indicate the tangible increase in randomness quality offered by Quantum Dice's DISCTM QRNG, with applications spanning from simulations to security.

Quantum Key Distribution (QKD) refers to the sharing of quantum-safe encryption keys. Rather than the mathematical approach that cryptography uses, QKD relies on quantum properties of light to generate secure random keys for encrypting and decrypting data.[17] This works by light photons – each light photon representing a qubit of data – travelling across a fibre optic cable between a sender and a receiver. There are several projects underway to leverage QKD to build quantum networks, such as the quantum secured metro network in the UK.[18]

As with wide-scale adoption of many quantum-related projects, this is an area where more research is needed. As QKD technology is maturing, at this stage the UK National Cyber Security Centre (NCSC) *'does not endorse the use of QKD for any government or military applications and cautions against sole reliance on QKD for business-critical networks, especially in Critical National Infrastructure sectors'* as stated in March 2020. The NCSC has highlighted that it sees PQC as the best mitigation to the threat. The USA's National Institute of Standards and Technology (NIST) holds similar views.[19]

What is Secure Quantum Communications?

Quantum communications refers to the transfer of information across networks that is quantum secure, using the fundamental principles of quantum physics.

In 2022, the UK launched the world-first commercial quantum secured metro network. BT and Toshiba, in association with EY, connected sites in the City of London, the West End and M4 Corridor. They will be able to transfer valuable data and information between physical locations over standard fibre optic links using quantum key distribution (QKD). QKD provides an additional layer of security that complements existing and post-quantum cryptography also deployed. The network's first commercial customer, EY, will use the network to connect two of its sites in London, one in Canary Wharf and one near London Bridge, and will demonstrate how data secured using QKD can move between sites and will showcase the possibilities this network brings to its own customers. Since then, HSBC has provided world leading demonstrations of incorporating QKD into its networks, by securing encrypted and low-latency communications between its HQ site in Canary Wharf, and a Datacentre Location in Berkshire with QKD, and using it for proof-of-concept FX trading. This work provides the precursor for these businesses to explore the concept of a more general 'quantum network', as well as providing a backbone to connect together quantum computers.

The UK is continuing to push forward this work through the Quantum Missions. Mission two states that by 2035, the UK will have deployed the world's most advanced quantum network at scale, pioneering the future quantum internet.

It should be noted that other nations are working on QKD, including South Korea, Singapore and Japan. In Europe, all EU members have signed up to create a QKD protected quantum safe pan-EU network called EuroQCI.[20 21 22]

3. Addressing early barriers to adoption

It is important to recognise that cultural, organisational and technical challenges hinder the move towards quantum resilience. Consulting with techUK members, below are just some of the common challenges they believe need to be addressed:

Managing the need for cyber, quantum and cryptography skills

The UK suffers from skills shortfalls across both the cyber and quantum domains, evidenced in government[23] and industry reports.[24] Quantum resilience will require the development of a quantum-literate and cyber-literate workforce who have the appropriate skills to enable the deployment of resilient quantum products and services. This includes ensuring that buyers, including senior leaders in organisations, are able to make informed purchasing decisions. The sooner organisations start seeking the appropriate guidance or talent, the sooner they can move towards resilience. A key starting point could be agreeing who within an organisation is responsible for the quantum transition and equipping them with the training and resources needed.

Infancy of quantum technologies and unclear timelines

It is not clear when the quantum threat will be realised. This is because quantum computers are still in relative infancy; there is no set roadmap for quantum computing; and there is, therefore, no set timeline for becoming quantum secure. Despite this uncertainty, businesses should take this threat seriously and prepare for the eventuality. The process of becoming quantum secure will not happen overnight and will take significant investment, especially if hardware needs to be replaced. A roadmap that clearly estimates your own business timelines will place the infancy of quantum technologies in the context of how long any transition will take.

Lack of understanding around current cryptographic inventory

As cyber resilience is built over time, it can sometimes be difficult for businesses to know where, why, and how they are using cryptography, however, this needs to be understood before moving towards quantum resiliency. This is the first stage of any resiliency roadmap, and this should include a risk register, assessing the potential impacts of failure on key parts of the business in the event of a breach.

Cost to implement

For businesses recognising the quantum threat, the big question will be when to invest in scaling-up activities in quantum security. Each business will need to evaluate the cost versus impact of its quantum risk activities, with businesses that handle sensitive data needing to prioritise making this investment. Businesses should not wait until it is critical to implement. Rather, they should build quantum security into their long-term roadmap to develop a financially sustainable path towards implementation. A productive next step could be investing in updating IT systems and technical infrastructure that allows for agility so future cryptographic solutions can be embedded.

Raising awareness and a strategic understanding across the business

As the quantum threat remains intangible to most C-suite executives, it may be difficult to convey why investment is needed. This is especially true when tight budgets and other business decisions may need to take priority. However, it is critical to push for the time and ability to review how the quantum threat may affect your business, and how long it will take to prepare. Equally, scaremongering and over-hype will spread misinformation. It is important for businesses to understand that protection from the quantum threat is a cyber security problem. With this in mind, a reasonable approach would be to develop a quantum resiliency roadmap following guidance from government sources and trusted partners. One initial step is to engage with the quantum and cyber communities to develop knowledge, understanding, and critical partnerships.

4. The UK Approach

Businesses must factor in current guidance from the UK Government when developing their roadmap towards quantum resiliency, including any further guidance published after this report.

Existing UK Government Action:

National Cyber Security Centre (NCSC)

> *"There are a number of ways in which the NCSC will support the PQC migration planning process, and subsequently migration itself."* (NCSC, Post-quantum cryptography: what comes next? 14 August 2024).

In November 2023, the NCSC followed up their 2020 *Preparing for Quantum Safe Cryptography Whitepaper*[25] with guidance titled *Next steps in preparing for post-quantum cryptography*.[26] This sets out that the best mitigation against the threat of quantum computers includes post-quantum cryptography (PQC) and provided guidance for businesses.[27] It also set out work by organisations such as the US National Institute of Standards and Technology (NIST) and the European Telecommunications Standards Institute (ETSI) to counter this threat.

National Quantum Technologies Programme and the Integrated Quantum Networking Hub

The National Quantum technologies Programme has funded research into quantum communications since 2016. Originally the Quantum Comms Hub provided collaboration between universities, numerous private sector companies and public sector bodies to deliver future-proof, practical, secure communications by exploiting the commercialisation potential of existing prototype quantum secure technologies.[28] This included advanced QKD technologies across many platforms while also providing guidance on what QKD will mean across different industries including finance, defence and space.[29] Going forward, the Quantum Networking Mission and the new Integrated Quantum Networking Hub will support QKD as a stepping-stone towards the establishment of quantum networks at all distance scales, from local networking of quantum processors to national scale entanglement networks for quantum-safe communication, distributed computing, and sensing, all the way to intercontinental networking via satellites.[30]

National Quantum Strategy

While focusing on the benefits of quantum technologies, the National Quantum Strategy emphasises that 'Quantum technologies also pose potential national security challenges, not least the expectation that quantum computers will be capable of undermining the cryptography used to secure internet data'. The strategy sets out key objectives to enable UK businesses to become quantum secure, including the commitment for 75% of relevant businesses taking steps to prepare for the arrival of quantum computing by 2033.

What more could government do?

The guidance and scope from the NCSC is welcome, however, as other nations push forward towards cyber resilience, and as quantum technologies advance, the UK cannot be complacent. techUK calls for further clarity and action to address the recommendations at the end of this document. Furthermore, greater collaboration with industry to help align with US and other guidance in the global marketplace is also critical.

Wider support for business

The government intends to offer advice and support to companies from the National Protective Security Agency (NPSA) (CPNI) and the National Cyber Security Centre (NCSC) to help them to put in place protective digital and physical security measures to ensure the protection of assets which are necessary to support growth. This activity should be done in close collaboration with industry to ensure success, identifying a clear roadmap for organisations of all sizes in mitigating future threats.

techUK would contend that these efforts should be accelerated, with a collaborative approach agreed between government and industry throughout 2024 and 2025 in order to do two things:

Deliver Guidance - The guidance on PQC published in November 2023 was welcomed.[31] Building on this, the UK should, working with industry, accelerate the publication of forthcoming guidance from the NPSA and NCSC on how all organisations should prepare for the quantum transition. This should include clear steps for raising awareness of the challenges as well as more technical 'how-to' guidance for companies implementing changes. It is clear that organisations will all have unique footprints as well as unique risk profiles, and so guidance could be tiered appropriately.

Develop a Quantum Resilience Taskforce - Government and industry should convene a workstream or forum to collaborate on these challenges at the earliest opportunity, developing key metrics for success and strategy, in line with Pillar 1 of the National Cyber Strategy 2022. This should include accelerating activity to ensure that these issues are included in the procurement frameworks around Government IT and across CNI. Through this forum, the UK should seek to develop an approach aligned with its allies, to both strengthen protections and allow continued innovation in industry.

5. International Approaches and Standards Development

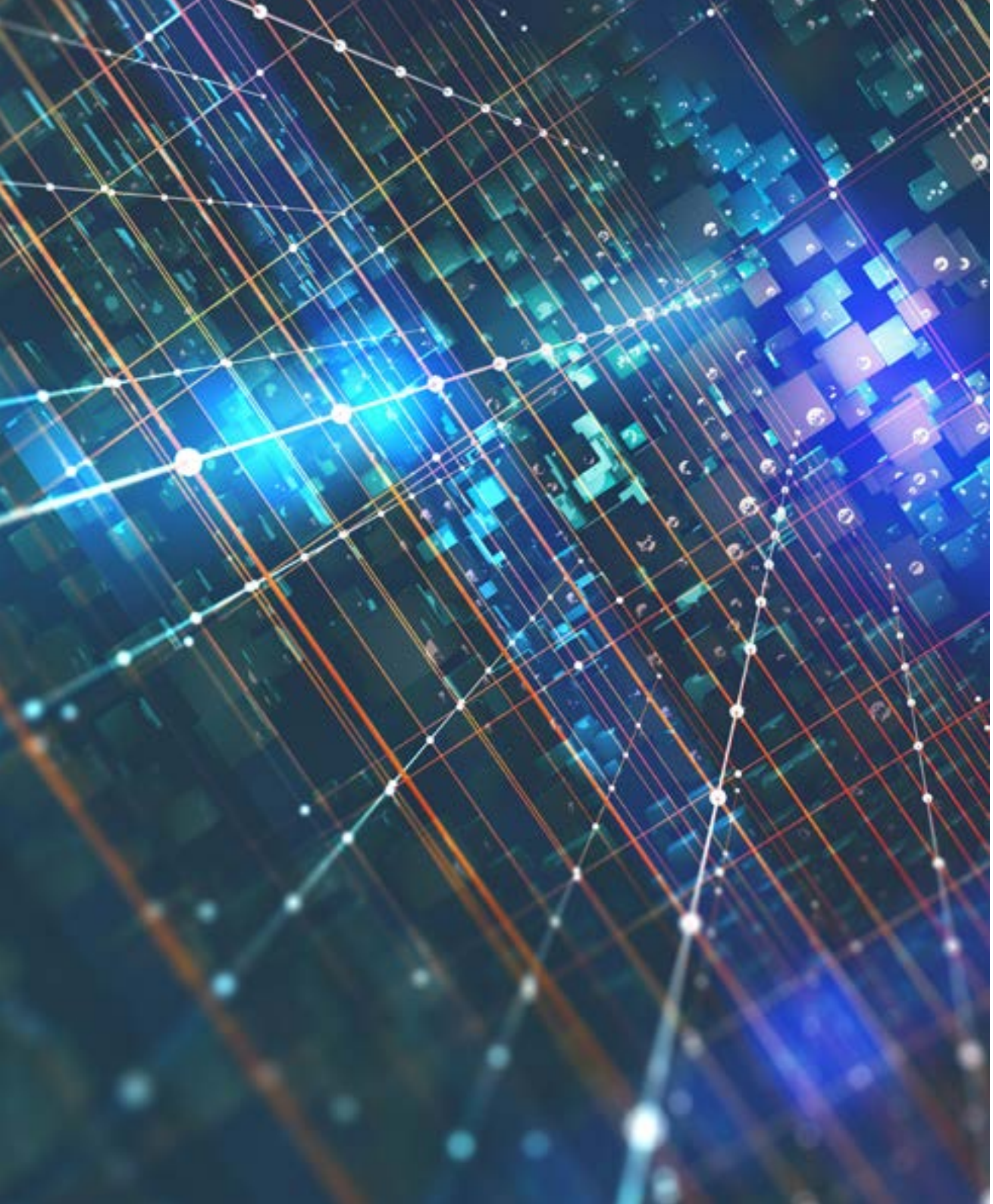
It is important that the UK engages on international standards development around quantum technologies, including quantum resilience.

Examples from International Governments

Quantum resilience is an international challenge. Several governments are publishing guidance. For international businesses, guidance in different geographies will progress at different rates, though this should be as holistic as possible. It is important to be aware of guidance across different geographies and jurisdictions. Various international governments have recognised the quantum threat and consequently developed PQC workstreams.

This is a rapidly evolving area for governments globally, meaning this should be viewed as an introduction to this area. We recommend additional monitoring as this work progresses.

On the next page there is a map containing international examples of different countries considering the standardisation and adoption of quantum resilient solutions. This is not a comprehensive list but highlights just some examples across the geographic areas many techUK members may operate. We welcome the work undertaken by the GSMA to further map international standard development in PQC in the context of the telecom ecosystem. You can view this on page 77 of this document.



Standards Development

Standards are vital for any successful digital transformation or technology adoption, particularly when the technology is going to have global implications. It is important that countries and regions collaborate on these standards so that they are appropriate, robust, fair and safe, as well as ensuring that no unnecessary burden or misaligned approaches pose a barrier to adoption or to R&D.

The National Institute of Standards and Technology (NIST) began looking at developing quantum-resistant algorithms as early as 2016. Through the launch of the 'Post-Quantum Cryptography Standardization Project', NIST received evidence from countries around the world who submitted 69 algorithms which claimed to be quantum resistant. Cryptographers were invited to attempt to crack these algorithms, which allowed NIST to narrow down the number of candidates taking part in the project.[40] In July 2022, NIST selected four algorithms which would be eligible for inclusion in the Federal Information Processing Standard (FIPS). In August 2024, NIST published standards for three of the four algorithms:

- **Federal Information Processing Standard (FIPS) 203**, intended as the primary standard for general encryption. Among its advantages are comparatively small encryption keys that two parties can exchange easily, as well as its speed of operation. The standard is based on the CRYSTALS-Kyber algorithm, which has been renamed **ML-KEM**, short for Module-Lattice-Based Key-Encapsulation Mechanism.
- **FIPS 204**, intended as the primary standard for protecting digital signatures. The standard uses the CRYSTALS-Dilithium algorithm, which has been renamed **ML-DSA**, short for Module-Lattice-Based Digital Signature Algorithm.
- **FIPS 205,** also designed for digital signatures. The standard employs the Sphincs+ algorithm, which has been renamed **SLH-DSA**, short for Stateless Hash-Based Digital Signature Algorithm. The standard is based on a different math approach than ML-DSA, and it is intended as a backup method in case ML-DSA proves vulnerable.

The US saw a major shift in the government's attitude toward quantum computing when President Joe Biden signed the Quantum Computing Cybersecurity Preparedness Act in December 2022.[41] The bi-partisan Act outlines the US Government's commitment to address the threats posed by quantum computers and realise that action needs to be taken to mitigate risk.[42]

The UK NCSC recommends ML-KEM (Kyber) and ML-DSA (Dilithium) from the above initiatives from NIST as providing appropriate levels for general purpose use.[43] Equally, cyber security authorities in Canada, France, Germany recommend planning for the Quantum Safe transition, and beginning implementation now the NIST standards are approved.[44] This is an opportunity for 5-Eyes and European countries to ensure that their approaches are aligned in this space, supporting innovation in the sector and not over-burdening businesses with complex, different interventions.

Alongside their Post-Quantum Cryptography Standardization Project, NIST have also specified two quantum-resistant signature schemes, LMS and XMSS. Their security is already well understood and trusted but they have limited application scenarios. Typical use cases include firmware signing.[45]

International Standards on QKD and QRNGs

International standards also apply to QKD and QRNGs.[46] The paper *Current Standardisation Landscape and existing Gaps in the Area of Quantum Key Distribution* provides an overview on QKD standards from the European perspective.[47]

UK on International Standards Development

It is important that the UK is involved in standards development through standards bodies CEN, CENELEC, and ETSI, ISO, IEC and ITU-T. It is also critical that the NCSC continues to work with nations such as the US as their work on standards progresses.

In March 2021, the National Physical Laboratory (NPL) and the British Standards Institute (BSI) jointly established a quantum standards committee to help coordinate a UK position on standards activity within the UK quantum community.[48]

Furthermore, in collaboration with the Department of Science, Innovation and Technology, the NPL, the NCSC, and other quantum experts, the Quantum Standards Network Pilot has been established. One of its goals is to further enable the UK to coordinate strategic priorities and drive focused engagement with international standards systems on the standards which matter to the UK.[49]

6. Next Steps | For Business

1. Ensure access to key skills

The first step for organisations is to address one of the most prominent barriers to adoption - skills. This includes technical skills in cyber security, programme governance, change management and vendor management. All organisations are likely to have skills gaps in the quantum space, as it is still a novel and relatively unknown quantity. However, the sooner organisations start seeking the appropriate guidance or talent, the sooner they are likely to have this. A key starting point could be agreeing who within an organisation is responsible for the quantum transition.

---

2. Review current security measures and develop a Cryptographic Inventory

Organisations should assess where, why, and how they are using cryptography. This should include a risk register, assessing the potential impacts of failure on key parts of the business in the event of a breach.

3. Create a roadmap towards adoption of quantum safe technologies

Once the Cryptographic Inventory is complete, the next step should be to develop a plan for upgrading cryptography in the most appropriate and timely way. This may or may not mean engaging with quantum experts and cyber security experts outside your organisation, as well as starting pilots with quantum safe technologies. A roadmap would develop a tiered approach to implementation of quantum-based solutions, following guidance from government institutions and the cyber security community.

---

4. Engage with the quantum and cyber security communities

The UK has a thriving quantum community, with more quantum start-ups than anywhere else in Europe.[50] This is against a backdrop of world-leading government support in quantum technologies, with the National Quantum Strategy moving towards quantum commercialisation. Similarly, we also have a flourishing and innovative cyber security sector. As part of a quantum resiliency roadmap, any business should engage early with the quantum and cyber security communities to develop knowledge, understanding, and the partnerships needed to address cryptographic threats from quantum computing.

Furthermore, businesses should look for opportunities to engage through government support. This includes engaging with the quantum missions and quantum pilots mentioned in the National Quantum Strategy, that could give insights into becoming quantum secure as an end user.

6. Next Steps | For Government

5. Accelerating guidance

The UK should accelerate the publication of forthcoming guidance from the NCSC on how all organisations should prepare for the quantum transition. This should include clear steps for raising awareness of the challenges, as well as more technical 'how-to' guidance for companies implementing changes. To empower more non-technical businesses to recognise they are carrying risk, guidance should also identify common use cases, making it easy for businesses to recognise when those use cases are present in their organisation, as well as identify common steps towards resilience for the near and medium term.

---

6. Develop a Quantum Resilience Taskforce

Government and industry should convene a workstream or forum to come together to collaborate on these challenges at the earliest opportunity, developing key metrics for success and strategy, line with Pillar 1 of the National Cyber Strategy 2022. This should include accelerating activity to ensure that these issues are included in the procurement frameworks around Government IT and across CNI.

Through this forum, the UK should seek to develop an approach aligned with its allies, to both strengthen protections and allow continued innovation in industry.

References

1. https://www.deloitte.com/global/en/services/risk-advisory/research/managing-the-quantum-cybersecurity-threat.html
2. https://www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography
3. https://www.fortinet.com/resources/cyberglossary/what-is-cryptography
4. The Cyber Security Body of Knowledge (cybok.org)
5. https://globalriskinstitute.org/publication/2023-quantum-threat-timeline-report/
6. RSA relies on a public key that is the product of two large prime numbers. RSA presumes that a computer cannot factor a very large number into its prime components, called factoring. However, Shor showed how a quantum computer could do this relatively easily, taking advantage of quantum mechanical properties of superposition and interference to find possible solutions. An introduction to the mathematics behind this can be found here https://www.classiq.io/insights/quantum-algorithms-shors-algorithm
7. https://www.weforum.org/publications/transitioning-to-a-quantum-secure-economy/
8. https://security.apple.com/blog/imessage-pq3/
9. https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF
10. https://www.ncsc.gov.uk/blog-post/migrating-to-post-quantum-cryptography-pqc
11. https://threatresearch.ext.hp.com/anticipating-the-quantum-threat-to-cryptography
12. https://www.ncsc.gov.uk/blog-post/migrating-to-post-quantum-cryptography-pqc
13. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
14. https://www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography
15. https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography
16. https://www.toshiba.eu/pages/eu/Cambridge-Research-Laboratory/quantum-random-number-generators
17. https://www.toshiba.eu/quantum/products/quantum-key-distribution/
18. https://business.bt.com/insights/quantum-computing-network-security-whitepaper/
19. https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/
20. https://www.koreatechtoday.com/quantum-security-arrives-in-south-korea-thanks-to-sk-broadband/
21. https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci
22. https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2023/sg-launches-southeast-asias-first-quantum-safe-network-infrastructure

23. DSIT Cyber Security Skills in the UK Labour Market
24. www.techuk.org/resource/techuk-report-quantum-commercialisation-positioning-the-uk-for-success.html
25. https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography
26. https://www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography
27. https://www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography
28. https://www.quantumcommshub.net/
29. https://www.quantumcommshub.net/industry-government-media/our-technologies/what-does-qkd-mean-for-the-economy/
30. https://www.hw.ac.uk/news/2024/heriot-watt-university-to-lead-uks-pioneering-quantum-internet-research
31. https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography
32. http://NSA, Quantum Computing and Post-Quantum Cryptography, 4 August 2021
33. https://media.defense.gov/2021/Aug/04/2002821837/-1/-1/1/Quantum_FAQs_20210804.PDF
34. https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation
35. https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography
36. https://www.nato.int/cps/en/natohq/news_221601.htm
37. https://www.mas.gov.sg/-/media/mas-media-library/regulation/circulars/trpd/mas-quantum-advisory/mas-quantum-advisory.pdf
38. https://www.cyber.gov.au/sites/default/files/2023-05/PROTECT - Planning for Post-Quantum Cryptography %28May 2023%29.pdfhttps://www.kpqc.or.kr/competition.html
39. https://www.kpqc.or.kr/competition.html
40. https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms
41. https://www.infosecurity-magazine.com/news/biden-quantum-cybersecurity-law/
42. https://www.infosecurity-magazine.com/news/biden-quantum-cybersecurity-law/
43. https://www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography
44. Lozinski, Z., 2023 'Quantum Security Call for Information' IBM
45. https://www.ncsc.gov.uk/pdfs/whitepaper/next-steps-preparing-for-post-quantum-cryptography.pdf
46. For QRNGs, some members recommended exploring FIPS 140-3 guidance.
47. https://openqkd.eu/wp-content/uploads/2021/03/OPENQKD_CurrentStandardisationLandscapeAndExistingGapsInTheAreaOfQuantumKeyDistribution.pdf
48. https://www.npl.co.uk/quantum-programme/standards
49. https://www.npl.co.uk/quantum-programme/standards/network-pilot
50. There are at least 160 companies active in the UK quantum ecosystem. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1142746/quantum-strategy-technical-annexes.pdf
While not all of these will be start-ups, in other metrics the UK still races out ahead of European competitors. https://sifted.eu/articles/europe-quantum-startups-mapped/?utm_source=sailthru&utm_medium=email&utm_campaign=flagship_newsletter&utm_content=22-02-23&utm_term=wants_main_newsletter

techUK
FOR WHAT COMES NEXT

linkedin.com/company/techuk

@techUK

youtube.com/user/techUKViews

info@techuk.org

Image credits | iStock by Getty Images

anyaberkut | Delmaine Donson | pixdeluxe | Aliaksandra | Just_Super | KrulUA | Dizzo | Shaxiaozi | damircudic | imaginima | Panuwat Srijantawong | Siarhei | Muhammet Camdereli