Quantum Personas:
A Multistakeholder Approach to Quantum Cyber-Risk Management

WORLD ECONOMIC FORUM

Foreword

Fully addressing potential cybersecurity risks posed by quantum computing will require a holistic approach which engages the global policy community and key individuals across individual organizations. This paper broadly outlines potential cybersecurity risks posed by quantum computing and illustrates those risks through the lenses of five personas, each of which brings a unique perspective to the quantum cyber-risk management discussion. Regardless of quantum computing's time horizon, these personas can begin to implement recommendations now to prepare themselves and their organizations for emerging threats from quantum computing.

Introduction

Quantum computing, often portrayed as a far-forward or fantastical technology associated with science fiction, presents a new paradigm in computation and is expected to achieve practical use within the next couple of decades[1,2]. Simply explained, in quantum computing, information is encoded in quantum bits (or "qubits"), rather than traditional bits. The unique properties of qubits, such as superposition and entanglement, enable techniques that can perform certain calculations much quicker than possible with traditional computers.

The US National Institutes of Standards and Technology estimates that within roughly 20 years "sufficiently large quantum computers will be built to break essentially all public key schemes currently in use"

Quantum computing technology advances are expected to positively impact many sectors of the global economy, including drug and materials discovery, financial portfolio management, climate and weather modelling, fabrication optimization, behavioural analytics, and more. However, the emerging capabilities of quantum computers may also present certain cybersecurity risks.

Future quantum computers are projected to be able to break some existing cryptographic algorithms, thus jeopardizing the secrets or transactions they are intended to secure. These advances in quantum computing capability have the potential to shake the foundations of some current cryptography and potentially topple the systems built on it. While quantum computers are still in their infancy, recent demonstrations have already shown that quantum computers can solve (contrived) problems exponentially faster than their classical counterparts.

The precise timeline for any emerging technology remains difficult to predict and estimates also vary for individual use cases. In contrast to some other projections, Google CEO Sundar Pichai predicted at the World Economic Forum Annual Meeting 2020 that quantum computing would achieve breaking current encryption methods "in five to ten years"[3].

The US National Institutes of Standards and Technology notes that the existing cryptography infrastructure also required 20 years to establish.

What is certain, however, is that there is a risk to data and transactional integrity, and this risk needs to be addressed. Individuals and organizations need to begin preparations immediately to mitigate quantum computing's risks.

Cybersecurity and Privacy Risks

Cryptography underpins modern transactions and communications. The security of cryptography is based on the premise that no known algorithms exist that can reverse cryptographic operations within reasonable time on the most advanced hardware available. Such timeframes may be thousands of years, with even the most advanced supercomputers using current traditional computing techniques. In the new paradigm of quantum computing, however, there are algorithms, most notably Shor's algorithm[4], which can significantly speed up the necessary calculations that undermine the security of some cryptographic algorithms. Public key cryptography, symmetric cryptography and hashing functions may all be impacted to varying degrees by quantum-based algorithms. The most dramatic effect is expected to be on public key cryptography where a quantum computer is believed to be able to break a 2048-bit RSA key in about eight hours.

As a result, advances in quantum computing may lead to the failure of modern cryptographic protections and expose information or transactions that were intended to remain confidential. This includes all manner of data, from personal medical histories and financial data to state secrets. Cryptocurrencies, as the name implies, are also often reliant on these cryptographic technologies. Quantum computing advances would allow for malicious actors to steal large quantities of cryptocurrencies[5].

Cryptography is also used in security certificates employed to verify the integrity and authenticity of software and firmware. Many devices will use such certificates to verify that updates were created by the original manufacturer and will not install

otherwise. Without this protection, malicious hackers can more easily impersonate the original manufacturer and install whatever code they desire on hardware as varied as cars to pacemakers.

What needs to be done?

Quantum risk should be approached like any other cyber risk. Before deciding on a course of action, the threat must be analysed and mitigation measures need to be evaluated. Due to the potentially high impact of this threat and the unknown timeline, it is imperative to start the analysis process sooner rather than later. It is also important to note that confidential information which is intercepted now can be stored by an adversary and decrypted when quantum technology becomes sufficiently mature. If confidential information must remain secret for longer than the time expected for quantum computing to mature, then immediate action is required.

Techniques are also being developed to mitigate the risks of quantum computing. Post-quantum cryptography (also known as quantum-proof, quantum-safe, or quantum-resistant cryptography) will become an important defence as standards are developed, mature and become widely available. These cryptographic systems rely on more complex mathematical problems that cannot be solved easily by quantum computers. Ideally, such systems would be interoperable with current communication protocols and networks and facilitate "crypto agility"; i.e., the seamless ability to swap to "quantum-resistant asymmetric cryptographic algorithms" when available. Clearly, the interlaced timelines of the availability of quantum computing availability and adequate deployment of post-quantum cryptography algorithms, with the expected persistency and integrity of data and transaction, mean that significant risk will likely exist for a window of time.

New standards, which take into account effective quantum computing, should continue to be developed, matured and shared internationally. First and foremost, international standards for post-quantum algorithms, key distribution and other infrastructure components are needed[6] and must be developed collaboratively, standardized and implemented. Already, the development of quantum-based attacks against traditional cryptography and computing systems may outpace the development of secure quantum-resistant cryptography.

A potential future may occur where quantum-based attacks are widely available while practical defences against them are limited. To address this, organizations such as the National Institute of Standards and Technology (NIST) in the United States have launched global standardization initiatives, mobilizing many of the world's best cryptographers who are developing and advancing quantum-safe algorithms.

However, potential disruptions or delays in development may lead to greater entrenchment of existing standards and vulnerable infrastructure, increasing the risk of quantum-based attacks. Strategic investments made now by decision-makers in the absence of quantum-aware standards can create dependencies and lead to vulnerable infrastructure lock-in. This is especially relevant as attack surfaces continue to expand due to the availability of low-cost computing. It is, therefore, imperative that organizations moving forward should consider crypto-agility – the capacity of information systems and standards to accommodate multiple cryptographic methods to allow those methods to be easily altered or swapped entirely as technology evolves, in particular to advances in quantum-based technology.

Equally important as developing the standards themselves, organizations and individuals should consider evaluating quantum risks within their existing risk-assessment processes, to include performing quantum risk-assessment and inventory. The US 2021 National Defense Authorization Act (NDAA)[7], which mandates that the Department of Defense perform a comprehensive assessment of potential risks and threats posed by quantum computing technologies, is an early example of government-led efforts to determine the overall level of risk and exposure.

This assessment should likely include an audit of both cryptographic assets and data – with an emphasis on sensitive data, its retention requirements and location (e.g., on-premises or in the cloud). The types of cryptographic keys used, along with their characteristics and their location in existing computer and communications hardware, operating systems, application programs, communications protocols, key infrastructures and access control mechanisms, are also relevant. More generally, potential future infrastructure limitations (e.g., bandwidth and latency) should also be identified.

The scope of the work that needs to be accomplished is vast and involves many individuals of varying backgrounds, specialities and perspectives.

What You Should Know and What You Can Do Today

This section proposes a role-based framework for approaching quantum risk management and identifies five personas and provides actionable recommendations to prepare themselves, their organizations and their nations for an emerging quantum computing world. The five personas identified are: policy-makers; corporate leaders; chief information security officers; cybersecurity and privacy practitioners; and customers and constituents. Each persona has information it should be aware of and actions that can be initiated now to prepare for the quantum future.

Policy-makers and standards organizations

This persona represents national and international leadership along with standards organizations which are ultimately responsible for guiding the governance of quantum technologies and efforts to mitigate their potential risk.

What should be known

The individuals and entities represented by this persona must understand the commercial and national security implications of quantum computing. Even entities within the same nation will view quantum computing from different perspectives and priorities. In the US alone, the Senate Armed Services, Commerce, Science and Transportation committees will likely each examine the issue of quantum computing with different concerns and priorities.

The US NIST began soliciting quantum-resistant, public-key, cryptographic algorithms in 2016, sifting through numerous candidates with the goal of releasing an initial standard by 2022.

Standardization bodies as a whole will need to understand the relationships between different standards in order to make a timely start in transitioning to quantum-safe standards. A balance must be managed between regulating the technology too early (stifling innovation) and regulating the technology too late. However, the time horizon to implement legislation, rules, standards and policies to support quantum-risk management may be shorter than anticipated.

What can be done today

Policy-makers and standards organization can establish a quantum-security coalition[6], a global community of those who are committed to promoting the safe and secure adoption of new quantum applications for all. Such a coalition will serve as a "convener", as successful adoption of quantum risk and cybersecurity standards and policies will require a combination of industry, academia, national governments, international bodies and other forums. Through the coalition, international quantum cybersecurity and risk-management standards for quantum computing should be developed which incorporate the interests of governments, industry and individuals.

The organization should also promote enhanced quantum awareness among its leaders and accelerate a secure global ecosystem, including quantum cybersecurity technology.

Corporate leaders

This persona represents the CEO and other C-suite leaders who establish the overall direction and priorities of organizations, including initiatives pertaining to quantum computing technologies.

What should be known

One of the barriers identified regarding the development towards building a quantum-safe ecosystem is the relative lack of quantum awareness at board and CEO level[6,8]. As with the previous persona, corporate leaders must also understand there are nationalist implications in both the threat from and adoption of quantum technology, along with the individual legal and regulatory implications within their markets. It is expected that quantum-based corporate and strategic partnerships will strongly impact the organizational strategy.

The business impact of quantum computing advances and the consequential implications must be understood. For example, developments in business applications will drive enhancements in quantum computing capability (i.e., the number of qubits), which, in turn, will increase the ability of quantum computers to be a viable cybersecurity threat.

Quantum computers present both opportunities and threats that are sometimes poorly understood and are, as a result, communicated in a misleading manner to the public.

Ultimately, corporate leaders must learn how to navigate the hype – and properly evaluate the impact on their organization.

What can be done today

Organizations tend to encounter and respond to disruptive technologies initially in a siloed and ad hoc manner. However, the potential risks posed by quantum computers to the foundations of security, require a holistic approach from a leadership perspective (e.g., CTO, CDO, CPO, CIO, CISO – led by CEO and board expectations and oversight) to both realize potential opportunities and risks that quantum computing poses. In particular, understanding risks may be necessary to fulfil various regulatory and legal responsibilities.

Corporate leaders should direct investments with consideration of future advances in quantum computing. Depending on the individual organization and industry, corporate leaders may consider incorporating quantum computing technologies as a matter of corporate strategy. Such investments may include indirect investments such as relationships built and developed with standards and regulator groups, as well as international forums which are researching quantum advances. Direct investments in system and infrastructure may consider prioritizing crypto-agility to avoid lock-in and costly future changes. Perhaps no investment is more critical than the development and acquisition of knowledgeable human resources that understand the threat and technology.

Chief information security officers (CISO)

This persona represents the CISO of the organization, or whoever is the senior-most individual in the organization specifically tasked with protecting its information and technology assets.

What should be known

The CISO should be responsible for staffing the organization with personnel who are knowledgeable regarding other organizations, individuals and entities driving the regulatory and standards conversations (NIST, ENISA, etc.). The CISO should be aware of entities advancing in quantum, both security applications and quantum computing (threat). Furthermore, the CISO should serve as a bridge to individuals in the organization who should be monitoring quantum developments, such as the owner of crypto infrastructure, cybersecurity and privacy policy teams, data owners, and the data protection officer.

What can be done today?

The CISO would be responsible for launching initiatives to assess quantum computing risks and exposures and to establish and/or modify processes to account for quantum computing capabilities. This crypto "inventory" includes data assets to determine which need to be re-encrypted with quantum-resistant cryptographic algorithms. Some data is so valuable that it has a long shelf life (decades) and must

be protected from those adversaries who would steal the encrypted data now and "break" it with quantum computers available in the future. This may require engagement with vendors to inquire about the robustness of their products to quantum attacks. In the event that the products are not sufficiently protective in their current form, understanding the future migration roadmap may be necessary. This engagement with vendors can serve as an impetus to developing quantum-safe solutions.

The CISO needs to champion quantum computing concerns within the organization (particularly with corporate leadership). Furthermore, the CISO's office is also likely heavily involved in developing and implementing crypto governance in accordance with legal and regulatory requirements as well as internal guidance to account for quantum risk in processes, systems and other technologies. The CISO should also coordinate communications and conversations with standards bodies as the standards are still being shaped, both to remain informed and potentially to help direct those standards as they are being developed.

The CISO should also be involved with efforts to identify and onboard practitioners to implement the cybersecurity and privacy policy. The talent pool of individuals who understand both cyber and quantum computing is extremely scarce.

Cybersecurity and privacy practitioners

This persona represents individuals who implement security policies on behalf of the organizations they service, often under the guidance of the CISO. It is anticipated that the key bottleneck in the quantum computing industry will be a lack of talent[9]. As such, it is critical for these individuals to start investing in skills which will allow them to effectively implement what is forecasted soon to be a $25 billion US quantum security market[6].

What should be known

In a manner similar to the CISO, cybersecurity and privacy practitioners must keep abreast of quantum developments, standards and products, both to advise leadership and to carry out day-to-day duties. Individuals represented by this persona must carefully consider data which requires protection and the nature of protection to be implemented with an eye on the future. What data is to be stored? For how long? Why? How will that data be encrypted or otherwise stored for that duration? How is such data currently stored and protected? A crypto inventory may be necessary and individuals with this persona are likely the individuals who must have the knowledge to perform it.

Cybersecurity and privacy practitioners must acquire and maintain high levels of quantum awareness and understand the cross-domain implications of the advancing quantum computing technologies. They must also be knowledgeable of the various quantum technology-based solutions and services available and upcoming in the marketplace. During this early stage, cybersecurity and privacy practitioners should refer to and understand the valuable lessons learned during the adoption of prior computing evolutions (e.g., personal computers, mobile computing, cloud computing), allowing them to both successfully determine effective solutions and then successfully implement them.

As with the prior evolutions, it is critical for technical personnel to maintain a connection to the overarching organizational goals. Choosing what aspects of the technology to adopt, when to adopt them and how, is a multistakeholder endeavour that requires careful deliberation. Moreover, it requires a firm understanding of the business or mission in addition to knowledge of the impending new technology. Furthermore, it requires knowledge of how the existing infrastructure is constructed and how that infrastructure supports the business or mission.

What can be done today

First and foremost, cybersecurity and privacy practitioners should research, learn and – once developed and ready for production – begin utilizing new quantum-resistant and crypto-agile tools. Ideally, they also participate in related public/private partnerships and industry events to broaden and deepen their quantum-based knowledge.

More importantly, these practitioners can also serve a critical role by participating with standards organizations and the global community as a whole. Individuals with relevant technical acumen are desired by NIST and other organizations to help define interfaces and standards for many upcoming technologies, such as quantum key distribution, which has been highlighted as an area of need. Their participation in the standards-making process may help accelerate secure and seamless quantum key distribution integration and, ultimately, a more crypto-agile future.

Customers and constituents

This persona represents typical end user and consumers of various products and services which will be impacted by quantum computing advances. Such users are likely not aware of quantum computing or are aware only at a surface level. Even so, the projected widespread impact of quantum computing on society will likely ensure the individuals will utilize technologies which may be vulnerable to quantum-based attacks.

What should be known

Quantum computing may not impact individual end users and consumers as directly as past disruptions in computer (e.g., personal computers, mobile computing, cloud computing). However, the companies and organizations that maintain your data may be subject to significant risks from quantum computing. When weighing concerns over the risks from quantum computing, individuals must balance the potential breakthrough applications (e.g., life sciences, energy and resources, banking, transportation) with the potential risks.

What can be done today

First and foremost, individuals should be aware of which entities retain their data and its intended purpose. End users and consumers should understand the data protection policies and rights of organizations to which they give their data, including banks, healthcare providers and social media. While such recommendations are generally accepted as sound practice, the projected paradigm shift from quantum computing advances could make organizations that are unprepared especially vulnerable. Therefore, it behoves individuals to begin reading about quantum technology and its impact on cybersecurity, and asking service providers about quantum risks and their plans to address it.

Harnessing Quantum Mechanics to Enhance Cybersecurity and Privacy

While posing the discussed potential cybersecurity risks, quantum technologies also offer a number of techniques which have the potential to impart unique and meaningful cybersecurity benefits:

- **Quantum key distribution** – enabling secure key exchange by transmitting photons which resist eavesdropping
- **Quantum communications** – utilizing multiple quantum techniques, including quantum key distribution to enable secure communications
- **Quantum random number generators** – can be used to generate truly random numbers (such as keys) instead of keys in use today, which are pseudo-random and more predictable
- **Quantum machine learning** – integrating quantum computing with machine learning to better analyse vast amounts of data, such as organizational network traffic, which can better detect malicious intrusions

These technologies have varying maturity levels. However, all are expected to rapidly develop and advance in the near future towards commercial application and create impact in cybersecurity.

Conclusion

The future of quantum computing offers many potential advantages and risks. A new, quantum-aware foundation of cybersecurity and privacy, upon which both current and future international, organizational and personal systems can rest, needs to be built. Much work remains to be done to leverage the advantages for humankind while minimizing the risks.

As outlined in this paper, accomplishing this feat will require many individuals filling disparate roles and, ultimately, contributing to a greater whole.

Acknowledgements

This work was developed by members of the World Economic Forum's Global Future Council on Cybersecurity within the Disruptive Technologies work group, which was led by Colin Soutar. Members of the Global Future Council on Cybersecurity also wish to thank Lim Soon Chia, of the Cybersecurity Agency of Singapore, and John Beric, Mastercard Corporation, for their expert review and commentary. Thanks also to Itan Barmes, Drew Herrick, Keith Pham, and Matt Caccavale of Deloitte & Touche LLP.

Endnotes

1. NIST (n.d.). Post-Quantum Cryptography. Retrieved from https://csrc.nist.gov/projects/post-quantum-cryptography
2. Michele Mosca and Marco Piani, "Quantum Timeline Threat Report 2020," Global Risk Institute, 27 January 2021, pg. 40, https://globalriskinstitute.org/publications/quantum-threat-timeline-report-2020/
3. Harris, B. (2020, 23 January). This is the biggest risk we face with AI, by Google CEO Sundar Pichai. Retrieved from https://www.weforum.org/agenda/2020/01/this-is-how-quantum-computing-will-change-our-lives-8a0d33657f/
4. P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," Proceedings 35th Annual Symposium on Foundations of Computer Science, 1994, pp. 124-134
5. Barmes, I., & Bosch, B. (n.d.). Quantum computers and the Bitcoin blockchain. Retrieved from https://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/quantum-computers-and-the-bitcoin-blockchain.html
6. Sharma, V., & Dixon, W. (2020, 11 August). We need to build a quantum security coalition. Here's why. Retrieved from https://www.weforum.org/agenda/2020/08/we-need-to-build-a-quantum-security-coalition
7. H.R.6395 - National Defense Authorization Act for Fiscal Year 2021. (2021). Retrieved from https://www.congress.gov/bill/116th-congress/house-bill/6395
8. Buchholz, S., Golden, D., & Brown, C. (2021, 15 April). A business leader's guide to quantum technology. Retrieved from https://www2.deloitte.com/us/en/insights/topics/innovation/quantum-computing-business-applications.html
9. Lipman, P. (2021, 4 January). How Quantum Computing Will Transform Cybersecurity. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2021/01/04/how-quantum-computing-will-transform-cybersecurity/