A quantum of prevention for our cybersecurity

Author
Michele Mosca, *Institute for Quantum Computing*
& Special Advisor on Cyber Security to the Global Risk Institute

GLOBAL RISK INSTITUTE

Global Risk Institute (GRI) is pleased to work with Professor Michele Mosca as a Special Advisor on Cybersecurity.

Michele Mosca is co-founder of the Institute for Quantum Computing at the University of Waterloo, researcher and founding member of the Perimeter Institute for Theoretical Physics, member of the Centre for Applied Cryptographic Research (CACR), and co-founder and Director of CryptoWorks21, an NSERC CREATE training program in cryptography in an era with quantum computers. Waterloo's world-renowned expertise in cryptography and quantum computing underpin its global leadership in cybersecurity in the context of quantum technologies.

***Global Risk Institute** is funding research on quantum computing focusing on the medium and long term implications of this new technology which we believe will have a profound impact on financial services. The research will be provided to members as it becomes available.*

DISTRUPTIVE TECHNOLOGIES AND CYBERSECURITY

Cyber technologies can dramatically increase productivity and enable new capabilities that are at the centre of our current businesses, our economies, and our society.

However this increased accessibility to information assets, and our almost total dependence on cyber technologies, implies unprecedented vulnerabilities to cyber-attacks from a wide range of threat.

Cybersecurity tools are what prevent these vulnerabilities from undermining all the value that these cyber technologies bring. Organizations need to ensure the capacity to maintain and protect critical cyber systems and information assets against a growing landscape of threats, including emerging quantum computing technologies.

1 in 7 chance key cryptography tools will be broken by 2026 and a 50% chance by 2031

I have estimated a one in seven chance that some of the fundamental public-key cryptography tools upon which we rely today will be broken by 2026 and a 50% chance by 2031. [1,2] Although the quantum attacks are happening yet, critical decisions need to be taken *today* in order to be able to respond to these threats in the future, and organizations are already being differentiated by how well they can articulate their readiness.

As we see almost daily in the news, cyber attacks still occur despite many countermeasures in place, compromising information assets and disrupting business functions. Once a weakness is discovered, the relevant systems are usually repaired, preventing further compromise of information and restoring the relevant business functions. The impact of a cyber breach can range from a minor nuisance to catastrophic. Recent news reports highlight class action lawsuits against Home Depot, tens of millions of dollars of SWIFT fraud, and countless other examples of financial damage, reputational loss, and business disruptions.

As we learn to handle the currently known attacks, cybercriminals find new ways to attack our cyber systems. There are no silver bullet solutions to achieve cybersecurity. No one technology, no one vendor, no one "project" will ultimately suffice. What is needed is a strong cyber immune system, capable of quickly detecting unexpected threats and reacting quickly to deal with them.

QUANTUM COMPUTERS AND CYBERSECURITY

The advent and development of quantum physics has surely been one of most unexpected threats to cybersecurity. Quantum physics is a new set of physical laws discovered a century ago. A quantum computer is a new type of computer that harnesses the power of quantum physics in order to solve problems that were previously believed to be intractable on regular computers. We're not talking about a speed-up due to faster hardware – we are talking about a speed-up due to an entirely new paradigm for computation that uses quantum effects to solve certain problems with astronomically fewer operations.

Conventional computers work by manipulating information stored in a collection of bits, where each bit can store one of two states which we label 0 and 1. For example, those states can be a high voltage or a low voltage. Quantum physics allows for a bit to embody the 0 and 1 states *at the same time*. By manipulating a large collection of quantum bits, a quantum computer can in a special way explore the countless configurations of 0s and 1s simultaneously.

Scientists and engineers are keen to build a full-scale quantum computer since the special form of computation it enables, a special kind of parallel computation, promises to solve important computation problems with the potential to, for example, design next-generation materials, find new drugs, improve the production of fertilizers, and optimize an array of other processes. Furthermore, the tools developed along the way, as scientists and engineers harness quantum systems in a variety of new technologies, will solve important problems in fields such as high precision measurements and medical imaging.

In August of this year, China announced its successful launch of the world's first quantum satellite communications platform, which will enable an host of new quantum experiments, with benefits including advancing the development of quantum cryptography. Europe's recently released "*Quantum Manifesto*" states [3]:

> "As is now happening around the world, developing Europe's capabilities in quantum technologies will create a new knowledge-based industrial ecosystem, leading to long-term economic, scientific and societal benefits."

Canada made substantial early investments starting nearly two decades ago to establish itself as a research leader in quantum information science and technology, with an aim to leverage this intellectual capital and expertise to realize the grander vision of being home to a new economic engine dubbed "*Quantum Valley*". Australia, Japan, Singapore, UK, USA, and other jurisdictions worldwide have similar large-scale efforts to advance quantum science and technology.

Not surprisingly, as the ideas continue to move toward working technologies and then to solutions for real problems, there is a global race for industry leadership in quantum technologies. However, one unintended consequence of quantum computation is breaking some of the cryptographic tools currently underpinning cybersecurity. For example, a fundamental requirement for online security is a digital signature. A digital signature allows a verifier (e.g. your browser) to confirm that a piece of code it is downloading comes from the alleged source (providing origin authentication) and has not been tampered with (providing data integrity). Another fundamental tool is the establishment of a secret key by communicating through a public channel. Encryption algorithms use such secret keys to provide confidentiality.

CONSEQUENCE OF QUANTUM COMPUTATION

One critical difference with breaking cryptography versus the countless other possible "hacks" of cybersecurity systems impacting the world today is that cryptography is a fundamental building block

that takes many years to replace. In contrast, once discovered, a corrupt insider is removed from their position of trust. One discovered, malware is removed. Once discovered, a software bug is patched. But when the cryptographic foundations upon which a cyber system is built are fundamentally broken, unless a failover replacement (which generally takes years to develop) is in place, the system will crumble with no quick fixes.

Right now, our cyber immune system is not ready for the quantum threat. There is a pending lethal attack, and the clock is ticking to design and deploy the cure before the threat is realized.

One consideration is the security shelf-life of information. Systems protecting information requiring long-term confidentiality, such as personally identifiable information (PII), need protection sooner since information recorded today can be decrypted tomorrow. Another consideration is the time it will take to migrate to new solutions.

Designing systems to be more cryptographically agile, that is, ready to quickly replace one cryptographic tool with another would facilitate the eventual transition to cryptography designed to be safe against quantum computers. Such "quantum-safe" cryptography includes protocols that resist known quantum attacks and are designed to run on conventional information and communication technologies. It also includes quantum cryptography protocols that are immune to mathematical cryptanalysis but require access to a quantum communication channel such as optical fibre or free-space communication. Importantly, this cryptographic agility would also facilitate changes to protect against other new threats.

Will the current risk management paradigms and the current accountability structures lead to the necessary decisions and investments?

The quantum threat is very well-defined, the approaches for solving it are also relatively well-defined, and very importantly we are not being caught off-guard and forced to fire-fight against a threat that takes years of preparation to properly defend against.

Responding to this threat not only mitigates this specific threat, but can also identify weaknesses in our current cyber immune system and lead us to build a stronger system that will allow us to handle the fast growing cyber threat landscape better than we currently do.

Meeting the challenge of preparing our cyber systems to be secure in an era with quantum computers requires migrating to new cryptographic tools. Timely and cost effective management of this risk starts today with understanding and assessing the impact of these quantum vulnerabilities, mapping out a strategy for mitigating this risk, and updating this strategy in light of ongoing advances in technology.

References

[1] "Cybersecurity in an era with quantum computers: will we be ready?", Michele Mosca

[2] "Cybersecurity in the Quantum World," ISACA Journal, volume 5, 2015.

[3] "Quantum Manifesto" QUROPE, Quantum Information Processing and Communication in Europe

About the Author

Michele Mosca is co-founder and deputy director of the Institute for Quantum Computing at the University of Waterloo, researcher and founding member of the Perimeter Institute for Theoretical Physics, and professor of mathematics in the department of Combinatorics & Optimization at the University of Waterloo.

He has held a Tier 2 Canada Research Chair in Quantum Computation since January 2002, and has been a scholar for the Canadian Institute for Advanced Research since September 2003. Mosca's principal research interests concern the design of quantum algorithms, but he is also known for his early work on NMR quantum computation together with Jonathan A. Jones.