Why you can’t ignore quantum computing

Quantum technologies, which take advantage of the strange fuzziness of the subatomic realm, will have a profound impact on our society—from medicine and materials science to banking and clean energy. Such technologies, which include communications, computing, quantum sensing and simulation, will bring many benefits. But they will also make necessary a dramatic shift in the global cyber-security architecture—a process that will start in earnest during 2023.

Quantum computers are still in development. But as they become more powerful and more reliable, they will pose a threat to how we transmit and store confidential data including bank transactions, sensitive government information and intellectual property. That is because unlike existing computers, quantum computers will be able to crack the encryption systems that provide secure data communication and storage, and underpin the global economy.

Criminals and other adversaries know that this will be possible one day—and they are not waiting to get their hands on sensitive data. They are already carrying out “store now, decrypt later” (sndl) attacks—stealing data for future decryption with quantum computers. According to America’s Department of Homeland Security, the decryption of this data could be feasible as soon as 2030. If this happens, any encrypted data acquired by adversaries today will have a maximum confidentiality period of eight years.

Criminal groups are targeting intellectual property and other kinds of data that will keep their value years from now when they decrypt it.

The time has come to address the security risks that quantum computers will pose when they start working, says Jack Hidary, CEO, SandboxAQ

This means that as quantum computers scale, there will be “submarine decryptions” of data troves that will surface unexpectedly, just like submarines in water.

This is not a tomorrow problem: sndl attacks are being perpetrated right now. Once stolen, there is no way to protect encrypted data. For example, an aerospace company could lose billions in future revenue if its proprietary designs are stolen. A government’s military and intelligence operations could be compromised if plans fall into an adversary’s hands.

(Several countries are actively engaged in building quantum-computing hardware for the sole purpose of defeating public-key cryptography and securing their own critical systems and data.)

In response, researchers have in recent years developed quantum-resistant cryptography schemes—new forms of encryption that even future quantum computers will be unable to crack. These are known collectively as “post-quantum” cryptography (pqc).

In July 2022 America’s National Institute of Technology and Standards (nist) announced the results of a six-year, multinational process to set the new pqc standards. Experts from more than 25 countries participated in developing and validating these algorithms. Nist also launched a National Cybersecurity Center of Excellence, composed of 12 leading companies from around the world, to develop pqc migration strategies and models for future hardware and software solutions.

With this watershed event, governments, corporations and technology providers finally have the clarity and certainty they need to begin the transition to pqc. The next two years will be critical as governments and corporations begin that process.

Identifying all the devices and systems that need to be upgraded, working out which of the multiple nist algorithms should be deployed in each case and making systems “crypto-agile” (ie, easily upgraded in the future) is a daunting task that will take several years. More than 20bn devices globally need pqc software upgrades—every mobile phone, laptop, desktop, server, website and mobile app—plus additional systems built into cars, ships, planes and operational infrastructure.

For this reason, 2023 will be a pivotal year for cyber-security and the emerging quantum-technology ecosystem. Driven by the need to protect against immediate and emerging threats, it is the year when public and private entities will start the process of migration.

The cyber-security risk has a silver lining: it will create awareness and drive adoption of quantum technologies in other areas. Forward-looking companies in financial services, health care, pharmaceuticals, telecommunications, transport, defence and other industries will explore the potential for quantum computing to accelerate r&d, enhance their offerings and bring new innovations to market—in 2023 and beyond.