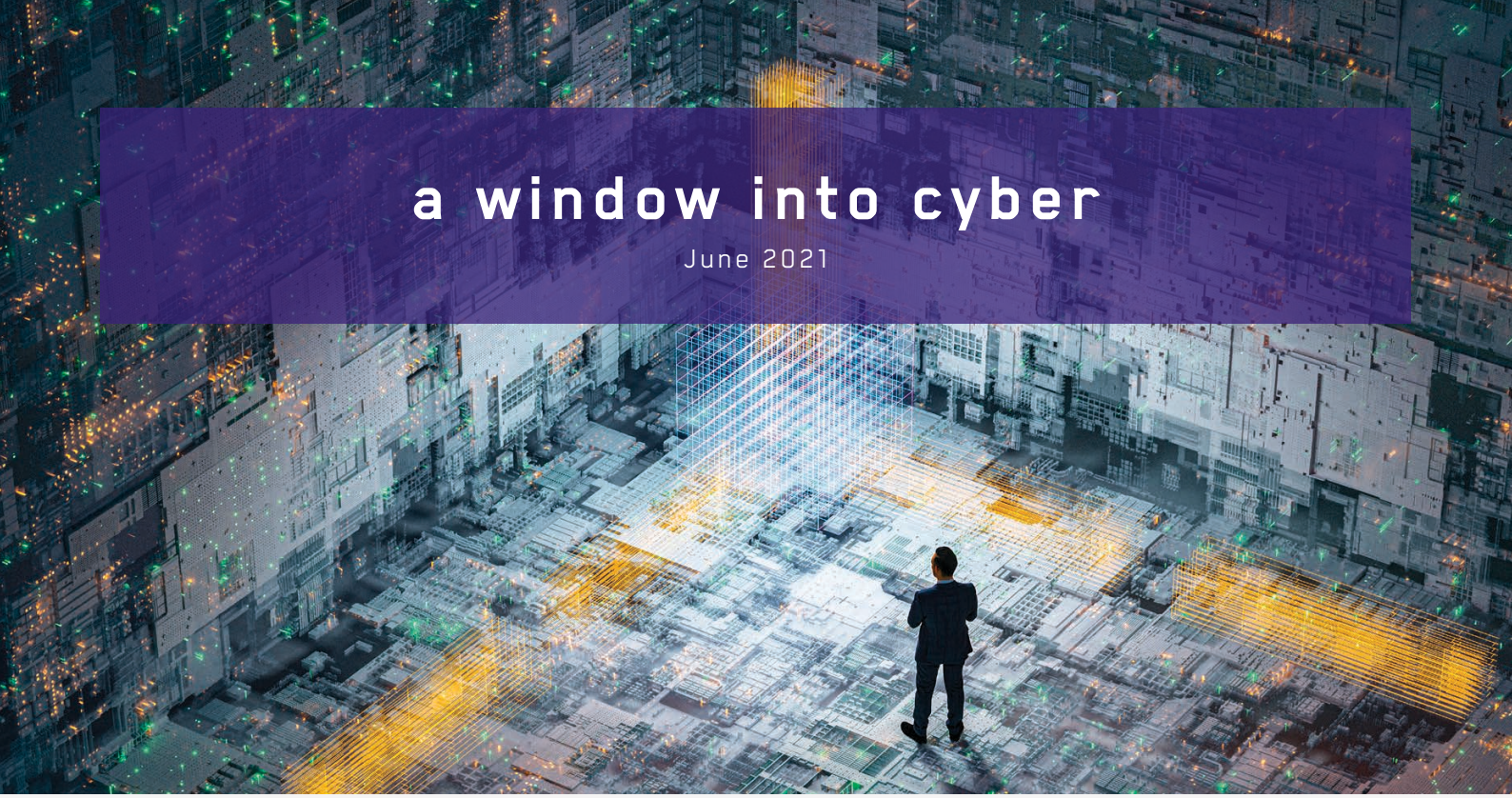
a window into cyber

June 2021



a note from Ben Maidment

Class Underwriter, Brit Cyber Services

BRIT

If you hear the word 'quantum', what springs to mind? Quantum leap? Quantum mechanics? A brand of dishwasher tablet? From now on, 'computing' should be top of our list.

This month we focus on the next generation of computers; set to far outperform today's most sophisticated machines. Quantum computers don't just solve problems billions of times faster, they're capable of tackling issues that have previously been too complex. As it becomes commercially viable, the potential applications for quantum computing are myriad: from artificial intelligence and financial modelling to drug synthesis and – crucially, as far as we're concerned – decryption.

Previously the stuff of science fiction, quantum computing also has the potential to become the stuff of nightmares, not least for cyber security specialists. My colleagues Anahita Zardoshti and Paolo Cuomo explain why we need to be prepared for a powerful new threat – and what steps we should be taking right now.

As ever, the Brit team is here for you.

this month's authors: **Anahita Zardoshti** and **Paolo Cuomo**

Anahita Zardoshti is a recent physics graduate working at Lloyd's of London, currently on secondment at Ki as a Portfolio Analyst. She previously worked in Lloyd's Innovation Team, horizon scanning for emerging risks – and authored the Lloyd's report on the impacts of quantum computing on insurance. As a Leader at Quantum London, she helps communicate the business impacts of quantum computing to professionals across different sectors.

Paolo Cuomo is Director of Operations at Brit and a Fellow of the Institute of Engineering and Technology. He identifies how evolving technologies are relevant in the insurance sector, and co-founded *InsTech* London in 2016 to drive engagement between insurtech start-ups and incumbent insurers. In 2019 Paolo established Quantum London, which aims to raise awareness of the potential benefits – and risks – of quantum computing for businesses.

Time to consider quantum computing's threat to cyber security

Anahita Zardoshti | Portfolio Analyst at Ki and quantum specialist
Paolo Cuomo | Director of Operations at Brit, co-founder of InsTech London and quantum enthusiast

Cyber security professionals are faced by immediate threats on all sides. Battling against increasingly sophisticated cyber-attacks, particularly at a time when most company IT systems are scattered around kitchen tables and living rooms, means that CISOs have limited time and budget to consider what threats the future may hold. The idea of encryption-cracking quantum computers certainly sounds like a distant, almost science-fictional concept that is not worth worrying about now. With none of their peers discussing it, why would they want to invest the little time they have adding it to their threat register? As it turns out, an increasing number of experts are seeing quantum computing as a clear and very present danger to cyber security. This means – at the very minimum – infosec professionals need to understand this threat well enough to answer the questions they'll soon be receiving from their CROs, COOs and CFOs.

Anahita Zardoshti

Paolo Cuomo

Quantum computing is a fundamentally different approach to computing, based on the mind-boggling laws of quantum physics. One of its unique features is its ability to carry out many calculations simultaneously, which can offer exponential speed advantages in solving certain computational problems. As such, quantum computing can be used to tackle problems that would otherwise be impossible to solve using our current technology. Examples include the simulation of complex molecular structures, which can help streamline the production of medicines and vaccines, or solving multivariable problems – such as the optimisation of supply chains or traffic flow – which can help improve efficiencies and reduce carbon emissions.

> "An increasing number of experts are seeing quantum computing as a clear and very present danger to cyber security."

Whilst the focus should be on the great ways in which quantum computing might revolutionise almost all aspects of our life, there is a darker side. We cannot shy away from the fact that the anticipated speed-ups it offers will be able to break the encryption that underpins much of our communications and data security. The power of many encryption systems such as RSA is based on the difficulty of solving certain mathematical problems. These 'factorisation calculations' are effectively impossible to solve (crack) using today's computers. However, it is thought that a powerful enough quantum computer could reduce the time taken to solve these problems from thousands of years to only a few seconds. In a flash, many of our encryption protocols are rendered obsolete.

continued on next page

Despite the incredibly complex hardware challenges involved, quantum computing has come a long way since its theoretical inception in the 1980s. Fierce competition and copious investment by both private and public sectors in the race to achieve quantum advantage, has elevated this revolutionary new computing paradigm out of laboratories and into commercial spheres. Recent developments and breakthroughs by tech giants such as Google and IBM, as well as national public investments of billions, has made it clear that we will one day have commercially viable quantum computers[1].

The power of quantum computers is measured in qubits. Current quantum computers are measured as having low hundreds of qubits. To be useful – for positive and nefarious purposes – quantum computers will need to have millions of qubits. As always, there is a range of views on how fast the technology will develop. However, given the current speed of development, there is a strong belief that quantum computers capable of breaking encryption could be available as soon as 2035[2]. Some experts believe it could be significantly sooner. It is important to note that quantum computers will typically be accessed remotely via the cloud, so the barriers to access will be low.

"Quantum computers capable of breaking encryption could be available as soon as 2035. Some experts believe it could be significantly sooner."

Since the realisation that quantum computers could one day break our encryption systems, there has been a concerted effort to find quantum-secure solutions to encrypting data, referred to as post-quantum cryptography (PQC). Unfortunately, the mere existence of these solutions does not automatically eradicate quantum computing's threat to cyber security. The reason for this is two-fold.

Firstly, the implementation of any new encryption standard will be an expensive and lengthy process. This is often down to the incompatibility of legacy systems already in place, the inadequacy of a company's inventory of all the vulnerable nodes in their IT system that require upgrading (made even more difficult when third party vendors are involved), and efforts to make these changes over

continued on next page

longer periods to help manage costs. This is even before considering the resistance of management to changing out expensive systems for a purely theoretical future risk. Given that we don't even have a set of standardised PQC schemes in place yet, it is therefore unlikely that companies could be confident that all their systems, and those of all their partners and suppliers, would have adopted fully quantum secure solutions before the mid-2030s. This means that we might already be behind in the race to secure our data and systems!

Secondly, there is an even more immediate threat: *Harvest Today, Decrypt Tomorrow*. Encrypted data stolen by adversaries today is of no use to them, since the encryption has mathematically scrambled the underlying information. However, if data stolen today is kept until a quantum computer capable of breaking the encryption becomes available, this information is clearly no longer secure. Hence this 'retroactive' type of attack already poses a real threat to many organisations' cyber security, particularly those that hold data with a long shelflife. Trade secrets, intellectual property, medical records and government or military secrets for example, would likely need to be kept secure for more than ten years. Therefore, the emergence of a quantum computer even in a decade or more's time could mean that during data breaches today, the stolen encrypted data is no longer guaranteed to remain secure over its lifetime.

So, even though cyber security professionals may feel too busy to consider longer-term risks, the threat posed by quantum computing is not something they can completely ignore. At the very minimum, infosec professionals should:

- Include quantum computing in their **risk assessment** and develop a roadmap for how to manage this risk;
- Identify whether quantum computing **is being investigated elsewhere in the business** (for positive purposes) to make use of that expertise;
- Define the **route to cryptographic agility** within their organisations to ensure a swift transition to PQC protocols once they are standardised and available;
- Factor in that encrypted data today is **not guaranteed to remain safe in the case of a breach**.

[1] Boston Consulting Group, 2018. The Next Decade in Quantum Computing – And How to Play. Available here

[2] RAND Corporation, 2020. Securing Communications in the Quantum Computing Age: Managing the Risks to Encryption. Available here

news from Datasafe

Datasafe provides the latest risk management resources, enabling Brit's clients to proactively manage their data protection and privacy risks.

Cyber Attack Surface Assessment (CASA)

Unpatched software and unsecured RDP ports account for over half of all ransomware attacks. Datasafe's CASA scan/report reveals these areas of known attack vectors – the 'attack surface' – and many other cybersecurity concerns, so you can fix them before it's too late.

CASA only needs your organisation's website domain. Go to the Datasafe website, complete a CASA request form and the report will be emailed to you within 1-2 business days.