THE RACE IS ON - QUANTUM THREAT TIMELINE PRIMER

DECEMBER 2022

GLOBAL RISK INSTITUTE

The quest for a quantum computer has often been described as a 'quantum race', with competition at the level of nations as well as private companies. This race has heated up in recent years, with the entry of new major private players, large grants from governments, and the birth and growth of many start-ups fuelled by venture capital. It has been further described as a marathon, rather than a sprint, because of the relatively long-term nature of the research and investments needed to support it.

Additionally, as scientists and engineers race to harness the calculating power of quantum computers, cryptographers are racing to develop new encryption standards that can eventually hold up against quantum computers in the hands of "bad actors".

Risk managers will want to track developments to understand how quickly quantum computers are becoming a reality and to follow implications for cyber risk.

KEY CONCEPTS

Quantum computing is a rapidly emerging technology that harnesses the laws of quantum mechanics to solve problems too complex for classical computers. It is technology that scientists only began to imagine four decades ago, with early prototypes now available to thousands of developers, and is on its way to providing a new and powerful paradigm for computation itself.

Quantum computing's exponentially higher calculating speed for certain types of problems offers the possibility of major breakthroughs across sectors. For instance, it could be used to uncover new pharmaceutical solutions that will advance our ability to both treat and prevent illnesses; it could enable more efficient energy transmission and more rapid product innovation; it could empower us in the fight against climate change and help the world meet its' carbon reduction targets; it could help financial institutions crunch vast amounts of data at superfast speeds, enabling better decisions and yielding competitive advantage.

On the flip side, quantum computers could also be used in nefarious ways. The prospect of "bad actors" using quantum computing to interfere with cyber security is real and thought to be not far off in the future.

Quantum-safe cryptography is the process of effectively securing and transmitting data in a way that cannot be hacked by quantum computers. It endeavours to identify algorithms and tools that are resistant to attacks by both classical and quantum computers – to keep information assets and connected systems secure even after a large-scale quantum computer is built. The transition to quantum-safe cryptography is challenging. It requires the development and deployment of hardware and software solutions, the establishment of standards, the migration of legacy systems and more. The safe transition can only be achieved through technology lifecycle management – not crisis management – and will require significant time. The potential threat of quantum computers being leveraged to interfere with cybersecurity needs to be top of mind for all risk leaders.

Quantum threat timeline: In-depth research, sponsored by the Global Risk Institute, has been conducted by evolutionQ Inc., a company unique in its approach to tackling the quantum threat to cybersecurity. The research team has gathered input from a broad base of world-leading academic and industry experts, across four continents, who have weighed

in on the quantum threat timeline and offered insights which will help to manage cyber-risk associated with quantum cryptanalysis.

The urgency to initiate and complete the transition to quantum safe cryptography depends on the security requirements and risk appetite of individual organizations. evolutionQ's annual "Quantum Threat Timeline Report" explains how three simple parameters are paramount in evaluating this:

- ***The shelf-life time:*** the number of years data should be protected,
- ***The migration time:*** the number of years needed to safely migrate the systems protecting that data, and
- ***The threat timeline:*** the number of years before relevant threat actors can potentially access cryptographically relevant quantum computers.

Organizations will not be able to protect their assets from quantum attacks if the quantum threat timeline is shorter than the sum of the shelf-life and migration time. The expert opinions collected suggest that the quantum threat to cybersecurity could become concrete sooner than many expect, underscoring the urgency to transition to quantum-safe cryptography.

The expert opinions collected reflect a mix of excitement for the advancements in the field, hope based in science and technology for future progress in building a quantum computer, and the strong resolution to pursue such a goal. On the other hand, several experts expressed concern for issues (societal, geopolitical, of resource availability) that may negatively impact the development of quantum computing. As focus on progress goes, the experts agree that the next critical step for quantum computing research is to convincingly demonstrate how to overcome the inherent fragility of quantum properties to make large-scale quantum computers possible.

Mitigation of the quantum threat to cybersecurity requires a transition to cryptography that is resilient against quantum attacks. It must be implemented carefully and not rushed.

Depending on organizations' specific shelf-lives, migration times and, most importantly, risk appetites, all organizations should evaluate their urgency in proceeding with migration to quantum-safe systems. The Global Risk Institute and evolutionQ have already made available a quantum risk assessment methodology (Mosca and Mullholand 2017) on which such a process may be based.

The annual "Quantum Threat Timeline Report", continues to provide year-over-year learning and deeper insights into the world of quantum computing. Whether new to, or well versed in, the world of quantum computing, it will inform those looking to understand current perspectives on the quantum threat timeline.