QUANTUM THREAT TIMELINE REPORT 2023

Executive Summary

JANUARY 2024

Authors: Dr. Michele Mosca, *Co-Founder & CEO, evolutionQ Inc.*
Dr. Marco Piani, *Senior Research Analyst, evolutionQ Inc.*

evolution GRI GLOBAL RISK INSTITUTE

SUMMARY

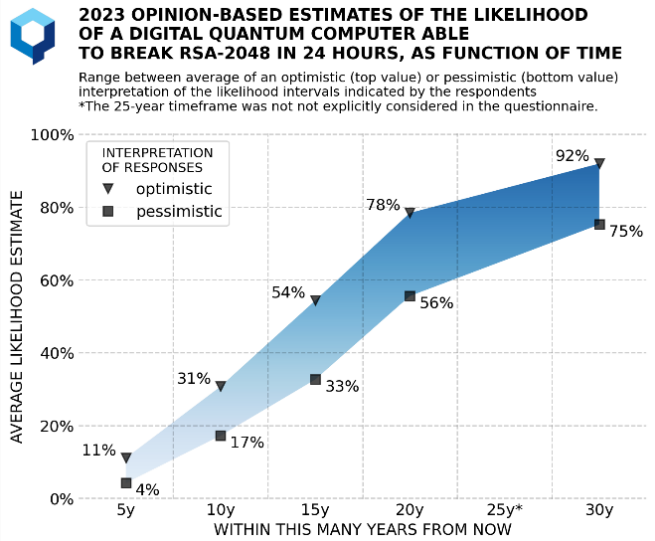
The global race to develop quantum computers[i] has critical implications for cybersecurity. A reliable "fault-tolerant" quantum computer of sufficient size will be able to break some of the most widely used cryptosystems; **hence the notion of the Cryptographically Relevant Quantum Computer (CRQC).** Today's quantum processors are still far from being CRQCs, but the technology is clearly maturing, and there is no known fundamental barrier to realizing large-scale quantum computing. Thus, cyber-risk managers should consider it more a matter of "when" than of "if".

This report synthesizes 37 leading global experts' insights on the current state of quantum computing, with focus on the threat it poses for cybersecurity. Similar reports have been produced annually since 2019, thus enabling the identification of trends in research activities and funding levels, and the tracking of milestones towards a CRQC. With these insights, businesses can better understand their level of risk and gain a quantitative basis for action.

Experts' responses suggest that a CRQC may arise faster than many anticipate. The experts indicate likelihood ranges for the realization of a CRQC[ii] for several timeframes, from 5 to 30 years. An "optimistic" interpretation of the responses that focuses on the upper bound of the likelihood ranges leads to an average estimated ~11% chance of a CRQC being developed within 5 years (up from 6% in the 2022 survey), and a ~31% chance within a decade (up from 27% in 2022). Even a "pessimistic" interpretation gives a ~33% average likelihood of a disruptive quantum threat in the next 15 years. This suggests that many organizations may already be facing an intolerable level of risk requiring urgent action.

Regardless of exactly when a CRQC becomes available, adversaries can currently use "Harvest Now, Decrypt Later" attacks to intercept, copy and archive encrypted communications for eventual decryption with a quantum computer, posing additional risk.

Figure 1



i Quantum computing harnesses quantum effects to compute in a manner completely different from today's "classical" computers. Quantum computers will be much faster and more powerful than classical computers for some types of calculations, including the kind whose complexity underpins much of current cryptography.

ii The experts provided estimates for a specific notion of CRQC – a quantum computer able to break RSA-2048 in 24h.

Quantum computers able to crack current encryption standards may arise faster than many anticipate.

Many organizations may already be facing an intolerable level of risk requiring urgent action

KEY TRENDS IN RESEARCH AND THE PACE OF QUANTUM TECHNOLOGY DEVELOPMENT

Many factors affect the Quantum Threat Timeline; one key variable is the level of investment in quantum computing and related technologies. This has skyrocketed in recent years from sources including governments, established companies, and private investors – McKinsey Digital reported $2.35 billion was invested into quantum technology start-ups in 2022 alone. While experts expect investments to continue, these could level off due to socio-economic factors, potentially slowing the Quantum Threat Timeline.

By contrast, breakthroughs in key research areas could lead to significant and unpredictable speed-ups in the Quantum Threat Timeline. The main challenge in building a CRQC lies in the fragility of physical qubits, short for "quantum bits," the building blocks of quantum computation. This can be mitigated though quantum error correction (QEC). Experts believe that major advances in QEC and/or physical architectures could suddenly accelerate the development of a CRQC, as has happened for several major technologies.

The experts report that a growing number of competing architectures show concrete potential - another signal of maturing quantum computing technologies. Superconducting systems and trapped ions remain the perceived leading architectures, but relatively new upcoming contenders include cold atoms and integrated photonics. Moreover, some promising approaches aim at combining different implementation platforms.

The relative position of global competitors in the quantum race provides another window onto the Quantum Threat Timeline. The experts still see North America as the leader, followed by China and Europe. Most consider it likely that North America will still lead five years out, but China has rising potential, with Europe lagging and Australia and Japan mentioned as possible contenders.

MITIGATING THE LOOMING QUANTUM THREAT

New "quantum-safe" cryptographic solutions exist and can be implemented to safeguard critical data and systems. Such solutions are known or at least widely considered to be immune to quantum attacks. However, transitioning to them is complex and requires substantial time to avoid pitfalls.

The Mosca inequality provides a means for quantifying the urgency of moving to quantum-safe cryptography. Organizations can relatively readily evaluate how urgent it is for them to migrate to quantum-safe systems: if the time an organization must keep its data secure ("Shelf-life Time") plus the time needed to migrate its systems ("Migration Time") is greater than the time until a CRQC emerges ("Quantum Threat Time") then an organization may not be able to continue to protect its critical assets.

Those responsible for managing cyber-risk should not wait to act, given the recent advances in quantum computing research, the high levels of investment in the field, the intense global competition, and the threat posed by 'Harvest Now, Decrypt Later' attacks. As part of their overall quantum readiness planning (see

additional references in the full report) a proactive approach to quantum cybersecurity will enable businesses to manage the transition to quantum-safe cryptographic tools and infrastructure, reducing the additional risks associated with hasty transitions motivated by crisis.

The Global Risk Institute and evolutionQ Inc. have made a quantum risk assessment methodology available to assist organizations in evaluating their individual levels of risk.