Quantum Threat Timeline

Authors: Dr. Michele Mosca, *co-founder, President and CEO, evolutionQ Inc.*
Dr. Marco Piani, *Senior Researcher Analyst, evolutionQ Inc.*

EXECUTIVE SUMMARY

Quantum computers harness the computational power of quantum systems and offer the ability to solve computational problems previously thought to be intractable. The quantum features that quantum computers rely on are very difficult to preserve and control; this makes building a quantum computer a formidable task. However, when built, quantum computers will break some of the pillars of our cybersecurity infrastructure.

The quantum threat to cybersecurity can be mitigated by deploying new cryptographic tools (both conventional and quantum) that are believed or known to be resistant to quantum attacks. Nonetheless, the transition to quantum-safe cryptography is a challenge itself, as it requires the development and deployment of hardware and software solutions, the establishment of standards, the migration of legacy systems, and more.

The urgency for any specific organization to complete the transition to quantum-safe cryptography for a particular cyber-system relies on three simple parameters: the shelf-life time: the number of years the data must be protected by the cyber-system; the migration time: the number of years to migrate the system to a quantum-safe solution; the threat timeline: the number of years before the relevant threat actors will be able to break the quantum-vulnerable systems.

If the threat timeline is shorter than the sum of the shelf-life time and of the migration time, then organizations will not be able to protect their assets for the required years against quantum attacks. A better understanding of the threat timeline provides information on the time available to safely perform the transition to post-quantum cyber-systems.

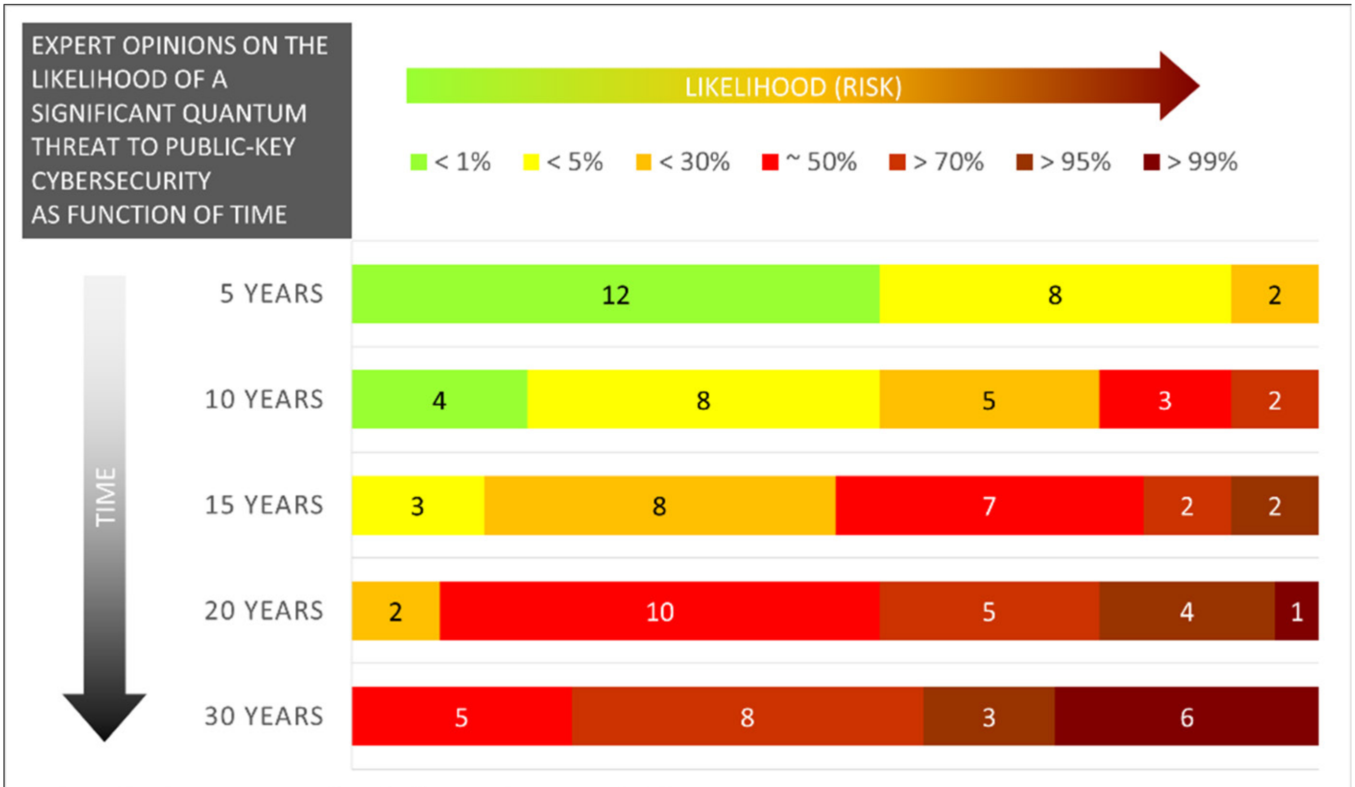
Assessing the quantum threat timeline is very challenging because of the scientific and engineering obstacles involved in building a working quantum computer. Experts generally acknowledge that they still do not know when we will have quantum computers that can threaten cyber-systems. However, it would be very helpful to gain insights into the prospects of this threat becoming real in the short and medium term, into the rate at which progress is being made, and into the key milestones cyber-risk managers should pay attention to.

This study aims to provide such deeper insights into the threat timeline, by surveying an unprecedented breadth and depth of thought leaders with questions designed to help those managing the cyber-risk associated with quantum cryptanalysis.

We targeted a diverse set of 22 trusted thought leaders in key relevant areas of quantum science and technology. The respondent pool, from academia and industry, spans four continents. Employees of some major companies declined to take part in the survey at this time. In the future, as a greater proportion of activity in building scalable fault-tolerant computers likely moves to industry, it will be valuable to gain additional industry perspectives.

Expert opinions on the likelihood of the quantum threat to current public-key cryptosystems

The experts were asked to express their opinions about the development timeline for quantum computers. It is not surprising that opinions varied significantly, and several experts articulated the difficulty inherent in making such predictions. Nonetheless, some valuable patterns emerged.



Numbers reflect how many experts (out of 22) assigned a certain probability range.

Next 5 years: Most experts (12/22) judged that the threat to current public-key cryptosystems in the next 5 years is "<1% likely". The rest selected "<5%" (8/22) or "<30%" (2/22) likely, suggesting there is a small non-negligible chance of a short-term surprise.

Next 10 years: Still more than half of the respondents (12/22) judged this was "<1%" or "<5%" likely, but 5/22 felt it was "about 50%" or ">70%" likely, suggesting that the quantum threat could very well become concrete in this timeframe.

Next 15 years: Half (11/22) of the respondents indicated "about 50%" likely, or more likely, with two experts indicating a ">95%" likelihood.

Next 20 years: About 90% (20/22) of respondents indicated "about 50%" or more likely, with 5/22 feeling it was ">95%" or ">99%" likely. This suggests that the chances of the quantum threat are more than even at the 20-year mark.

Next 30 years: All the experts responded that the quantum threat has a chance of "about 50%" or more, with 17 out of 22 experts indicating that the quantum threat will be likely (">70%"), very likely (">95%") or extremely likely (">99%").

Expert opinions on the technical realization of quantum computers

A major challenge in building a quantum computer is that of creating reliable fundamental components, so-called physical qubits, whose number can be scaled while maintaining control and quality. In this respect, the experts indicated that the most promising physical platform for the realization of a cryptographically relevant quantum computer is presently offered by superconducting systems, followed relatively closely by trapped ions, and with several other physical implementations having significant potential.

A very important step forward will be the experimental demonstration that error-correcting schemes improve the reliability of so-called logical qubits as compared to physical qubits. For this to happen, it must be possible to prepare, manipulate, and measure the underlying physical qubits well enough. How 'well' this 'well enough' needs to be depends on the best-known error-correcting schemes, which may themselves be superseded by new and better schemes.

Another milestone will be the demonstration of so-called "quantum supremacy" that is of the ability for a quantum device to perform some computation that would be practically impossible even for the most powerful classical supercomputer, independent of the usefulness of such computation. While the achievement of quantum supremacy will not necessarily lead to decisive progress towards a cryptographically relevant quantum computer, it will signify having achieved a relatively high level of control on a relatively large number of physical qubits, which is a necessary ingredient for quantum computing. The experts agreed that this milestone is likely to be passed in the next couple of years.

From the threat timeline to the migration timeline

The expert opinions collected in our survey, and summarized in this report, offer unique insight into the quantum threat timeline. Depending on its own specific shelf-life times and migration times, each organization will have a longer or shorter time at its disposal to implement post-quantum cryptographic solutions. The Global Risk Institute and evolutionQ Inc. have already made available a quantum risk assessment methodology for taking estimates of the threat timeline and assessing the overall urgency of taking action (Mosca & Mulholland, 2017).

The Global Risk Institute and evolutionQ Inc. will provide an update of this survey in approximately one year. This will allow us to track the evolving opinion of experts and any changes in the expected timeline for the quantum threat to cybersecurity.

Michele Mosca

Michele Mosca serves as a Special Advisor on Cyber Security to the Global Risk Institute. He obtained his doctorate in Mathematics in 1999 at Oxford on the topic of Quantum Computer Algorithms. He joined the University of Waterloo faculty in 1999. He is co-founder of the Institute for Quantum Computing, a Professor in the Department of Combinatorics & Optimization of the Faculty of Mathematics, and a founding member of Waterloo's Perimeter Institute for Theoretical Physics. He conducts research in quantum algorithms, quantum software, and cryptographic tools designed to be safe against quantum computers. He co-founded the CryptoWorks21 quantum-safe cryptography training program and the not-for-profit Quantum-Safe Canada.

In 2015 he started the company evolutionQ Inc. with Norbert Luetkenhaus in order to help organizations evolve their quantum-vulnerable systems and practices to quantum-safe ones. evolutionQ delivers quantum-risk management strategies and robust cybersecurity tools designed to be safe in an era with quantum computing technologies.

Marco Piani

Marco Piani has worked as Senior Research Analyst at evolutionQ Inc. since 2018. He obtained his doctorate in Physics in 2005 at the University of Trieste, Italy, studying the relation between quantum entanglement and the dynamics of quantum systems interacting with their environment. He is an expert on how quantum properties like entanglement can be certified and used as resources for practical tasks, for example in precise measurements and in communication. In the past, he held positions as Research Assistant Professor at the Institute for Quantum Computing of the University of Waterloo, and as Lecturer and Chancellor's Fellow at the Department of Physics of the University of Strathclyde, in Glasgow, United Kingdom.