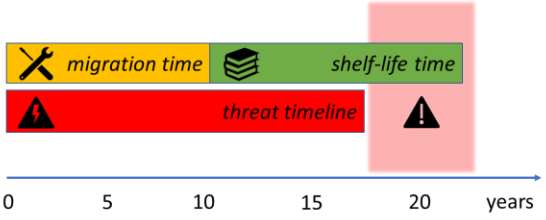
Quantum Threat Timeline Report- 2021: Executive Summary

There are computational problems presently thought to be intractable by any reasonable means and leveraged by widespread cybersecurity protocols. Such problems may soon become tractable by computers that makes use of the properties of quantum mechanics—so-called quantum computers. This may lead to potentially catastrophic consequences.

Such a cybersecurity threat can be reduced by employing new cryptographic tools, both conventional and quantum, believed or provably known to be resistant to quantum attacks. Nonetheless, the transition to quantum-safe cryptography is a challenge in itself: it requires the development and deployment of hardware and software solutions, the establishment of standards, the migration of legacy systems, and more. Most importantly, a safe transition will only be achieved through technology lifecycle management—not crisis management—and will require time.

The urgency to initiate and complete the transition to quantum-safe cryptography depends on individual organizations' risk attitude and can be evaluated in terms of three simple parameters:

- *shelf-life time*: the number of years the data must be protected,
- *migration time*: the number of years needed to safely migrate an organization's system,
- *threat timeline* (key focus of this report): the number of years before relevant threat actors can potentially access cryptographically relevant quantum computers.



If the threat timeline is shorter than the sum of the shelf-life and migration times, then organizations will not be able to protect their assets from quantum attacks.

This report sheds light on the quantum threat timeline by tapping into the opinions of 47 international leaders in the field of quantum computing. Questions posed were designed to provide insights to those managing cyber-risk associated with quantum cryptanalysis.

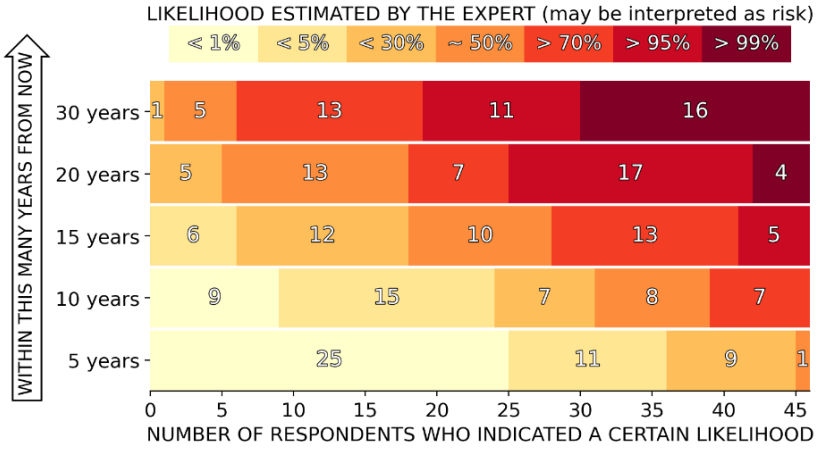
The pool of respondents, from four continents, comprises experts from academia and industry working on several aspects of quantum computing. They generally acknowledge that we cannot reliably predict the rate of progress towards developing a working quantum computer, since such an effort pushes the present limits of scientific knowledge and technological capabilities. Nonetheless, the experts we consulted provided their best estimates for the timeline of the development of a quantum computer that may pose a threat to cybersecurity.

Opinions collected suggest that the quantum threat will become non-negligible relatively quickly and it could well become concrete sooner than many expect. For example, 15 out of 46 respondents felt it was "about 50% or more" likely within a 10-year timeframe.

In comparing the opinions expressed in 2019, 2020, and now in 2021, we notice an overall trend toward estimating higher likelihoods. Such "optimism" is likely the result of significant scientific and technological progress, of "aggressive" roadmaps set by some major companies, and of levels of funding that are presently high.

EXPERTS' ESTIMATES OF THE LIKELIHOOD OF A QUANTUM COMPUTER ABLE TO BREAK RSA-2048 IN 24 HOURS

The experts were asked to indicate their estimate for the likelihood of a quantum computer that is cryptographically relevant—in the specific sense of being able to break RSA-2048 quickly—for various time frames, from a short term of 5 years all the way to 30 years.



Many countries consider quantum technologies as strategic and are engaged in what many see as a "quantum race". We have asked the experts to indicate both which geographic areas are presently ahead—North America is the perceived present leader—and which may be the leaders in five years' time—a more complex matter with answers that indicate how China is making fast strides.

As in our previous surveys of the past two years, experts indicated that the most promising physical platform for the realization of a cryptographically relevant quantum computer is presently offered by superconducting systems, followed by trapped ions. Among alternative platforms, this year's survey results point to renewed interest toward so-called optical quantum computing. In general, while there are some leading proposals, (1) the field has not identified a clear race winner, and (2) it is possible that more than one platform will eventually play an important role.

The major challenge in building a quantum computer is that physical *qubits*—the fundamental units of quantum computation—are not perfect. Multiple imperfect physical qubits can nonetheless encode more reliable *logical* qubits via *error-correction*. Experimental demonstrations of a working logical encoding constitute an important step forward. Significant results in this direction have already been achieved but have not yet demonstrated all the properties of error-correction or addressed the issue of feasible *scalability* to the many logical qubits necessary for quantum cryptanalysis. Nonetheless, the experts believe that the demonstration of one or more logical qubits that outperform the underlying physical qubits is within reach.

From threat timeline to migration timeline

The expert opinions collected in our surveys offer unique insight into the quantum threat timeline. Depending on organizations' specific shelf-lives, migration times and, most importantly, risk attitudes, all organizations should evaluate their urgency in proceeding with migration to quantum-safe systems.

The Global Risk Institute and evolutionQ Inc. have already made available a quantum risk assessment methodology (Mosca & Mulholland, *A Methodology for Quantum Risk Assessment*, 2017) on which such a process may be based.