Global Risk Institute **SHORT REPORT**

2021 Quantum Threat Timeline Report

Authors: Dr. Michele Mosca
Co-Founder & CEO
evolutionQ Inc.

Dr. Marco Piani
Senior Research Analyst
evolutionQ Inc.

January 2022

2021 Quantum Threat Timeline Report

This report focuses on estimates for the timeline of the threat posed to cybersecurity by quantum computers. It reflects the views of nearly fifty experts in the field of quantum computing research. The report follows versions compiled in 2019 (Mosca & Piani, 2019) and 2020 (Mosca & Piani, 2021); it provides the most recent opinions offered by these experts and examines the evolution of their views over the past three years due, for example, to scientific or technological developments or to changes in investment levels.

Contents

Quantum computing as an emerging quantum technology

Quantum computers use quantum systems, like atoms or elementary particles of light, to run computations that go beyond what is achievable by standard computers—the latter often referred to as "classical" computers (Nielsen & Chuang, 2002).

Quantum computers exploit "fragile" quantum features that are very difficult to preserve and control. This makes building a quantum computer an extraordinary challenge that requires contributions from diverse fields of expertise—including physics, engineering, and computer science—and significant investments by governments, by established companies, and by venture capital supporting start-ups.

Despite the aforementioned "fragility" of key quantum features, no fundamental roadblocks have been identified for the realizability of powerful quantum computers. On the contrary, small prototypes, capable of running rudimentary "quantum programs", have already been built. Furthermore, entire "quantum ecosystems" are emerging, which comprise both academic institutions and private companies. The private sector includes both companies involved in specific aspects of quantum technologies that are only partially related to quantum computing, and companies that instead aim at handling the "full stack" needed to build and run a quantum computer. Presently, the flourishing of such an ecosystem is favoured by investments in the field that have never been stronger and that indicate continued and increasing interest in the potential of quantum technologies and quantum computing.

Quantum computing as a threat to cybersecurity

Full-fledged quantum computers will be able to solve computational problems previously thought to be intractable by any reasonable means. This will jeopardize several elements of the current cybersecurity infrastructure that are based on the difficulty of such problems. If these widespread vulnerabilities are left unmitigated, the potential consequences are catastrophic.

Once closer to science-fiction than to science, quantum computers are assuming more and more the traits of an inevitable future technology, and certainly those of a threat that cannot be dismissed. From the perspective of anyone interested in the threat that quantum computers may pose to cybersecurity, one of the most critical questions is to understand as well as possible *when* cryptographically-relevant quantum computers might be built.

One main reason time is critical is because the quantum threat to cybersecurity can be lessened by deploying new cryptographic tools, both conventional and quantum, which are believed or are 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.

With the necessity to devote enough time to an orderly and safe transition to a "post-quantum" world, and with such complexities, the urgency for any specific organization to initiate and complete the transition to quantum-safe cryptography for a particular cyber-system depends on the organization's risk tolerance, but in general it can be estimated in terms of 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 required to safely migrate the system to a quantum-safe solution;
- and the key focus of this report: the *threat timeline*, that is, the number of years before the relevant threat actors will be able to break the quantum-vulnerable systems thanks to the availability of cryptographically-relevant quantum computers.

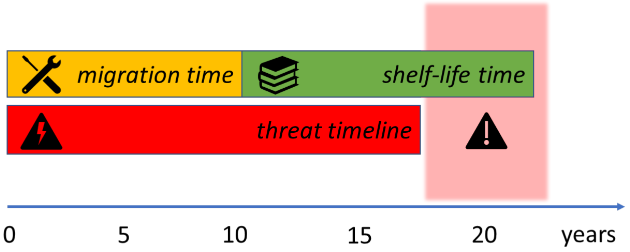


Figure 1 The quantum threat timeline determines whether a cyber-system is potentially already at risk, well before the quantum threat has become concrete, because one has also to consider the needed migration time and the desired or required (e.g., by regulations) shelf-life time.

Having spelled out these parameters, the key challenge organizations may face can be cast as follows (see also Figure 1):

> *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.*

Importantly, a safe transition is achieved through technology lifecycle management, *not* crisis management. The following should then be evident:

> *A better understanding of the threat timeline provides information on the time available to safely perform the transition to quantum-safe cyber-systems.*

This report sheds light on the quantum threat timeline by tapping into the opinions of international leaders in the field of quantum computing.

Expert opinions on the quantum threat timeline

Experts generally acknowledge that we cannot reliably predict the rate of progress towards a working quantum computer, because building one requires pushing beyond the limits of what is presently known scientifically, and/or what is possible from an engineering perspective. Despite this inevitable uncertainty, this series of reports aims at providing insight into:

- the likelihood of the quantum threat becoming real in the short, medium, or long term;
- the rate at which progress is being made towards building a cryptographically-relevant quantum computer;
- the key milestones in quantum computing research and development that cyber-risk managers should pay attention to.

In 2019, we surveyed for the first time an unprecedented breadth and depth of 22 thought leaders with questions designed to provide such an insight to those managing the cyber-risk associated with quantum cryptanalysis (Mosca & Piani, 2019). In 2020, we expanded the pool of respondents, reaching out to a total of 44 experts (Mosca & Piani, 2021). This year we have repeated an extensive survey with a total of 47 participants.

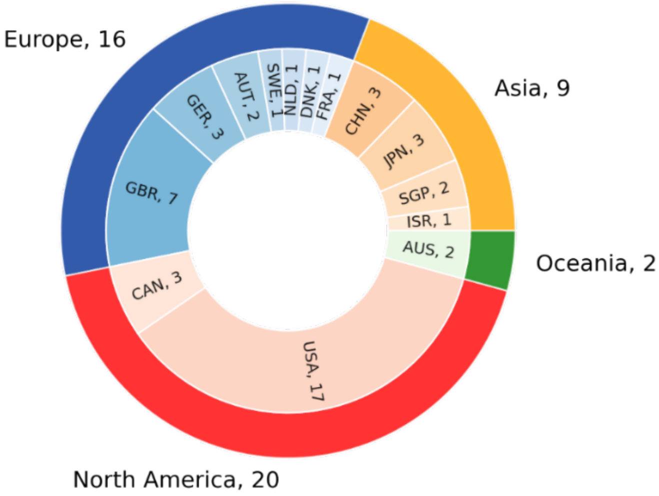


Figure 2 Number of surveyed experts by location. The respondents constitute a very international mix, with high representation from countries (like Canada, China, Japan, and the USA) and geographical areas (like Europe) where the efforts to develop quantum computers and quantum technologies have been and continue to be very strong.

The pool of respondents, from four continents (Figure 2), comprises experts from academia and industry, working on several aspects of quantum computing. Importantly, the survey secured a significant representation of some major private players in the field. This is relevant because, after the early stages of quantum computing research driven mostly by academia, progress in the field is more and more influenced by the private sector.

In our questionnaire, we asked the experts to provide estimates about the development timeline for quantum computers, specifically for quantum computers powerful enough to pose a threat to cybersecurity.

Several respondents articulated the already mentioned difficulty inherent in making such kind of prediction and it is not surprising that opinions varied significantly. Nonetheless, the results suggest that the quantum threat will become non-negligible relatively quickly, and it could well become concrete sooner than many expect (see Figure 3).

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.

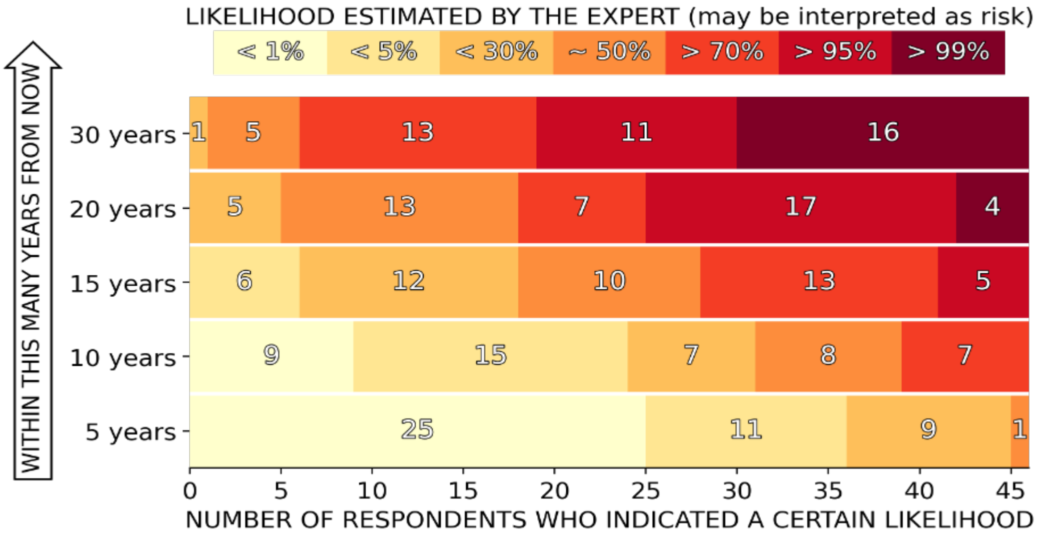


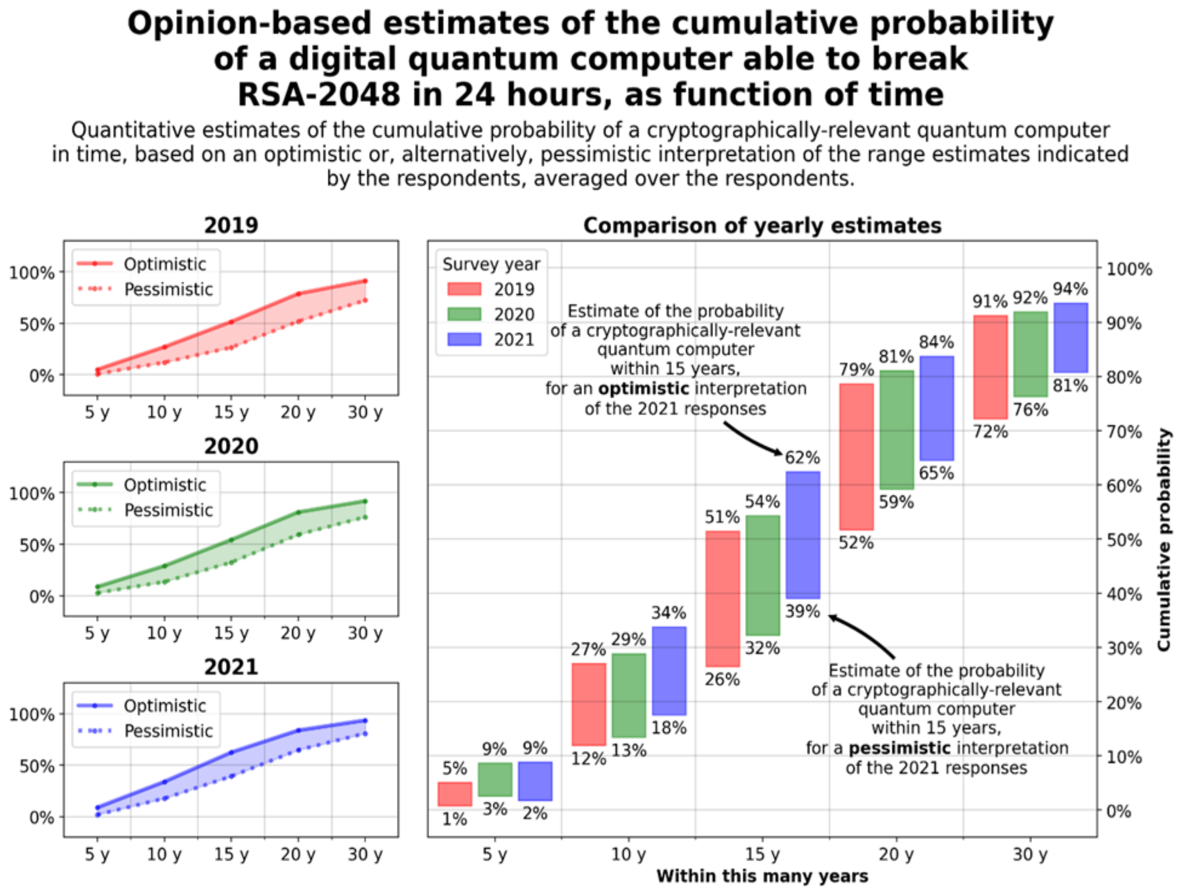
Figure 3 The responses to the key question of this year's survey—provided by 46 out of the 47 experts contributing overall—suggest that the quantum threat is becoming more and more concrete. The table below summarizes some trends that may be identified.

Time	What to expect based on the experts' opinions
Next 5 Years	Most experts (25/46) judged that the threat to current public-key cryptosystems in the next 5 years is "<1% likely". About a quarter of them (11/46) judged it relatively unlikely ("<5% likely"). The rest selected "<30%" (9/46) or "about 50%" (1/46) likely, suggesting *there is a non-negligible chance of an impactful surprise within what would certainly be considered a very short-term future.*
Next 10 years	Still more than half of the respondents (24/46) judged the event was "<1%" or "<5%" likely, but already 15/46 felt it was "about 50%" or ">70%" likely, suggesting *there is a significant chance that the quantum threat becomes concrete in this timeframe.*
Next 15 years	More than half (28/46) of the respondents indicated "about 50%" likely or more likely, among whom 13 indicated a ">70%" likelihood, and 5 an even higher ">95%" likelihood. *This time frame appears as a tipping point, as the number of respondents estimating a likelihood of "about 50%" or larger, become the majority.*
Next 20 years	Roughly 90% (41/46) of respondents indicated "about 50%" or more likely, with 21/46 pointing to ">95%" or ">99%" likely. This indicates *there is a significant bias toward viewing the realization of the quantum threat as substantially more likely than not within this timeframe.*
Next 30 years	Forty experts out of 46 indicated that the quantum threat has a likelihood of 70% or more this far into the future, with 16/44 experts indicating a likelihood greater than 99%. Thus, *there appears to be a relatively low expectation of any fundamental show-stoppers or other reasons that a cryptographically-relevant quantum computer would not be realized in the long run.*

In comparing the opinions expressed in 2019, 2020, and now in 2021, we notice an overall trend toward higher likelihoods, as evident in Figure 4, where we calculate probability ranges for the existence of a cryptographically-relevant quantum computer, based on the experts' opinions. This is even more noteworthy given the ongoing pandemic, which the experts estimate will have had a substantial impact on progress in the short term.

The experts indicate that some of the optimism is the result of significant scientific and technological progress. Another reason may be found in the "aggressive" roadmaps toward the realization of a so-called fault-tolerant quantum computer set by some major companies. Moreover, a high level of funding and investments is presently available to speed up the development of quantum computers.

It is worth noting that both the experts we surveyed and the quantum community at large have made it clear that the "hype" that fuels some of those investments is somewhat dangerous, because, for example, it could trigger a "quantum winter" if (unrealistic) expectations are not met: a sudden drop in the level of funding could lead to a vicious loop of less investments ↔ less results.



Opinion-based estimates of the cumulative probability of a digital quantum computer able to break RSA-2048 in 24 hours, as function of time

Quantitative estimates of the cumulative probability of a cryptographically-relevant quantum computer in time, based on an optimistic or, alternatively, pessimistic interpretation of the range estimates indicated by the respondents, averaged over the respondents.

2019

2020

2021

Comparison of yearly estimates

Estimate of the probability of a cryptographically-relevant quantum computer within 15 years, for an **optimistic** interpretation of the 2021 responses

Estimate of the probability of a cryptographically-relevant quantum computer within 15 years, for a **pessimistic** interpretation of the 2021 responses

Figure 4 Evolution of the likelihood estimates by the experts. In the three graphs on the left: probability estimates based on the optimistic or, alternatively, pessimistic interpretation of the likelihood intervals of the responses to the 2019, 2020, and 2021 surveys. Large graph on the right: side by side and timeframe by timeframe comparison of such estimates. Both the lower and the upper end of the average likelihood estimate have been rising survey after survey, for each timeframe considered, the only exception being the lower end of the 5-year estimate. The increases at the 10-year and 15-year marks appear stronger in the most recent survey.

Quantum computing race

The successful development of a quantum computer would be game-changing in many ways for economy and society, not only for its impact on cryptography and digital infrastructures. For example, quantum computers, being naturally suited to simulate arbitrary quantum systems, could be used in the design of new drugs and advanced materials.

For this reason, many countries and supranational entities like the European Union appear to consider quantum technologies and quantum computing in particular as strategic, and are engaged in a "quantum race". We have asked the experts to indicate both which geographic areas are presently ahead—North America appears to be the perceived present leader—and which may be the leaders in 5-years' time—a more complex matter with more nuanced answers that indicate, for example, how China is making rapid strides (Figure 5).

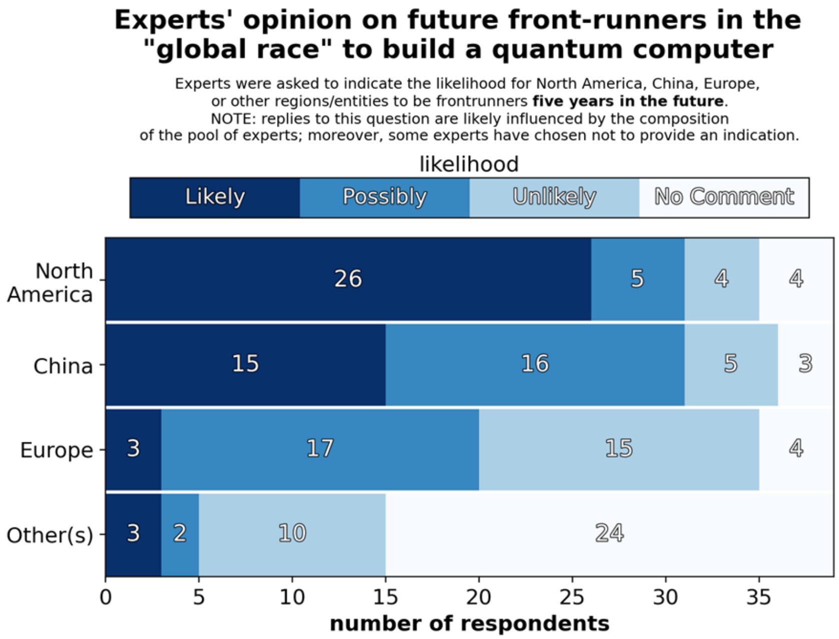


Figure 5 Number of respondents who indicated the likelihood of a given region/entity to be a front-runner in the global race to build a fault-tolerant quantum computer five years from now.

Whether pressing issues related to, e.g., the ongoing pandemic or future ones, or other challenges such as global warming, may lead to a reallocation of (public) fundings is unclear, but most of our respondents believe that the present global level of funding will remain stable or even increase in the next two years (Figure 6).

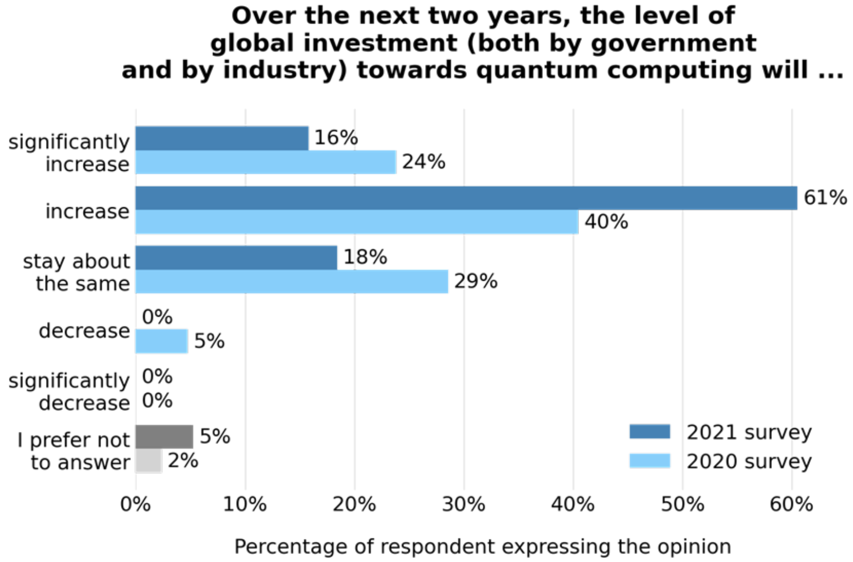


Figure 6 Expected change in the level of investment toward quantum computing in the next two years.

Another "race" pertains to physical architectures. A major challenge in building a quantum computer is that of creating reliable fundamental components that encode quantum information in a way that parallels how, say,

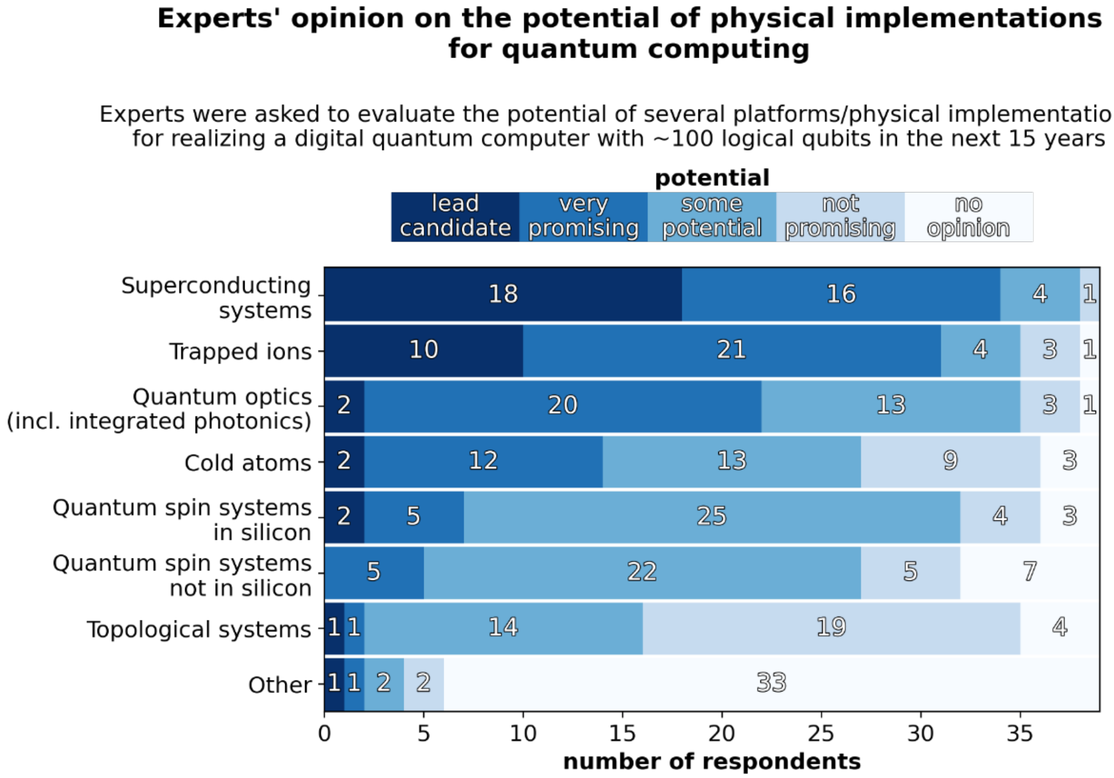


Figure 7 Similarly to previous years, superconducting-system implementations, followed by ion-trap implementations, are perceived as presently having some edge over other physical realizations.

switches encode classical information. Such fundamental components are called (physical) *qubits*, and any cryptographically-relevant quantum computer will require many of them—in the millions, for several proposed platforms. In general, it is exceedingly important for any physical/technological implementation to allow the realization and manipulation of many (physical) qubits, in a way that can be scaled up while maintaining control and quality.

Like in the surveys of the last two years, 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 by trapped ions (Figure 7). Among other promising platforms, this year's survey results point to renewed interest towards the potential of optical quantum computing. More generally, while there are some leading proposals, the field has not identified a clear winner of this race, and there is the possibility that more than one platform will have an important role.

Many respondents have emphasized the significance they expect modularity—the combination of many separate devices, rather than few large monolithic ones—to have. There is also the belief that it might be possible to make use of different physical platforms that may excel at different aspects of quantum computing, such as storage, manipulation, and transmission of quantum information. In this sense, hybrid systems that utilize more than one physical platform may play an important role, particularly if combined with the just mentioned modularity. On the other hand, hybrid systems come with their own challenges, related to making different physical implementations work effectively with one another.

Quantum error-correction and logical qubits as the next major step

The major drive of the necessity of being able to create and handle *many* qubits is that neither the qubits themselves nor their manipulation are ever perfect. Physical errors cannot be eliminated completely, for reasons very much related to the fragility of quantum features. Multiple imperfect physical qubits can nonetheless encode more reliable *logical qubits* via *error-correction*.

A very important step forward will be experimental demonstrations that error-correcting schemes lead to logical qubits that are more reliable than the underlying physical qubits. For this to happen, it must be possible to prepare, manipulate, and measure the underlying physical qubits well enough. In general, the required precision in preparation and control depends on the best-known error-correcting schemes, which may themselves be superseded by new and better schemes.

Significant results revolving around error correction and fault tolerance have already been achieved in at least some architectures but have not yet demonstrated at once all the properties of error-correction, or quite addressed the issue of feasible *scalability*. The latter concept is about the implementation and the handling of multiple logical qubits within the same architecture, with reasonable resources—for example, not requiring a control of the physical qubits that is too complex and hence unfeasible.

Progress in both hardware and error-correcting schemes make the experts believe that the demonstration of one or more logical qubits that outperform the underlying physical qubits in terms of both storage and manipulation of quantum information for several steps of computation and error correction is within reach (see Figure 8). On the other hand, some experts have expressed the

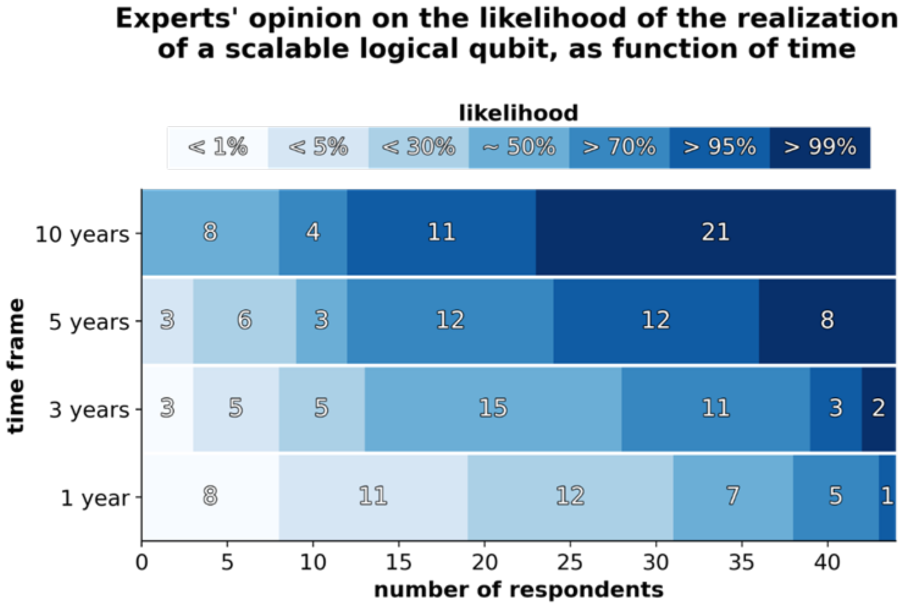


Figure 8 Quantum information is fragile, and its manipulation imperfect. Nonetheless, the experts appear to be of the general opinion that we will soon see the realization of logical qubits which make use of error correction to counteract such issues. Most importantly this appears to be likely even considering the requirement of scalability *of the encoding scheme, that is the possibility of realizing and handling a growing number of such logical qubits through a manageable increase in resources and complexity of operations.*

perspective that the notion of an individual logical qubit that is scalable is not necessarily a well defined or sensible milestone. Some of the reasons provided go from the opinion that focusing on the realization of an individual logical qubit—with, say, the idea/intuition that it might be possible to combine many instances of it afterwards—may not quite capture how quantum computing implementations are intended to work, to the opinion that claims of scalability are relatively vacuous until scaling is actually realized.

We anticipate that future realization of one or more (scalable) logical qubits will be subject to high levels of scrutiny by the community, even if celebrated as a major milestone in quantum computing research and development.

Summary and outlook

A fully working quantum computer can be seen as the 'holy grail' of quantum technologies, but also as a major threat for cybersecurity.

Building a quantum computer requires scientific and engineering advances that will take several years to be developed and implemented, as well as focused effort and resources. The key challenge to overcome is the natural "fragility" of the quantum features that we think make quantum computing more powerful than classical computing.

The quest for a quantum computer has been often described as a "quantum race" (Hsu, 2019), with competition at the level of nations as well as of private companies. This competition, which has substantially heated up in recent years, has also been described as a marathon, rather than a sprint race, because of the relatively long-term research and investments that will be needed.

Nonetheless, there could be sudden accelerations, which may come in the form of scientific or engineering breakthroughs. We expect improvements both in hardware implementations and from new schemes for error correction and fault tolerance, that is, from schemes intended to overcome the fragility of quantum features. Cyber-risk managers may want to track developments in that direction to understand how quickly quantum computers are becoming a reality.

The expert opinions we have collected and summarized in our reports offer unique insight into the quantum threat timeline. This year have more than doubled the number of respondents since the first report in 2019, also tracking changes in opinions.

Forty-six experts estimated the likelihood of the realization of a quantum computer that could break a scheme like RSA-2048. While most of the experts (25/46) judged that the development of such a quantum computer within the next 5 years is very unlikely ("<1%"), several (21/46) indicated the likelihood as non-negligible. We find it remarkable that only 24/46 judged the likelihood as small as "<1%" or "<5%" within 10 years; within the latter timeframe, the rest of the respondents indicated already a significant likelihood, to the extent that 8/46 judged it about as much likely as unlikely ("about 50%") and 7/46 considered it even likely (">70%"). The risk aversion/appetite of companies and institutions can vary significantly, but we think that for critical systems such likelihoods already represent a serious concern. We note that the logical possibility that consequential quantum cryptanalysis is, for some reason, infeasible or impossible is captured in the small but non-negligible likelihood implicitly assigned in our survey to the event that quantumly breaking RSA-2048 will take more than 30 years. While it is up to each institution, company, and manager to decide what risk they are ready to accept, we think cyber-risk managers are naturally more concerned about the chance that the quantum threat materializes early / earlier than could be expected, rather than never.

The likelihood the experts assign to the quantum threat may change from yearly survey to yearly survey, because several factors—from recent results in the field, to changes in investment levels—influence both the actual threat timeline and the opinion the experts have on it. Comparing this year's opinions to the results of the surveys we conducted in 2019 and 2020, the experts appear to be more confident about the quantum threat becoming concrete in the medium-to-long term.

Whenever one deals with opinions rather than hard facts, it is appropriate to consider how reliable or partisan such opinions might be. Quantum computing corresponds to changing the paradigm of computation itself. Working in a field that pushes the conceptual and practical limits of what humans and human-made tools are capable of requires some optimism, but it also requires a deep critical capacity that is necessary to identify and overcome roadblocks. The experts we surveyed are leading scientists also because they excel at such critical thinking, and we are confident that our respondents have tried to provide the best possible estimates, based on their expertise.

While building a cryptographically relevant quantum computer is a formidable task, it is important for people managing cyber-risk to understand that there is nothing close to a scientifically convincing or established argument for why the efforts currently underway are likely to fail, especially in the medium-to-long term. Progress in the last year, including the demonstration of several aspects of quantum error correction and further realizations of the quantum advantage of a programmable quantum processor over classical devices—so-called "quantum supremacy"—as well as the significant momentum of the field—in terms of activities, results, and resources—should probably trigger caution, directed to developing crypto-agility and resilience against quantum attacks. A respondent wrote:

> *It is important to stress — not least given the roadmaps presented by industry — the importance of migrating to post-quantum secure cryptography. In particular, this is important in applications where long-term confidentiality is sought.*

In a similar spirit, John Martinis, a pioneer of superconducting implementations and leading the first demonstration of "quantum supremacy", suggests a corresponding prudent timeframe for action, based on the rate of progress he is seeing:

> *[T]he takeaway message is that quantum safe encryption needs to be developed and deployed in the next 5 years to be reasonably safe. Right now would be better.*

The Global Risk Institute and evolutionQ Inc. have already made available a quantum risk assessment methodology for taking estimates of the threat timeline and evaluating the overall urgency of taking action (Mosca & Mulholland, A Methodology for Quantum Risk Assessment, 2017).

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

References

Hsu, J. (2019). *The Race to Develop the World's Best Quantum Tech.* Retrieved from https://spectrum.ieee.org: https://spectrum.ieee.org/tech-talk/computing/hardware/race-for-the-quantum-prize-rises-to-national-priority

Mosca, M., & Mulholland, J. (2017). *A Methodology for Quantum Risk Assessment.* Retrieved from Global Risk Institute: https://globalriskinstitute.org/publications/3423-2/

Mosca, M., & Piani, M. (2019). *Quantum Threat Timeline.* Global Risk Institute. Retrieved from https://globalriskinstitute.org/publications/quantum-threat-timeline/

Mosca, M., & Piani, M. (2021). *Quantum Threat Timeline Report 2020.* Global Risk Insitute.

Nielsen, M. A., & Chuang, I. (2002). *Quantum computation and quantum information.* Cambridge University Press.