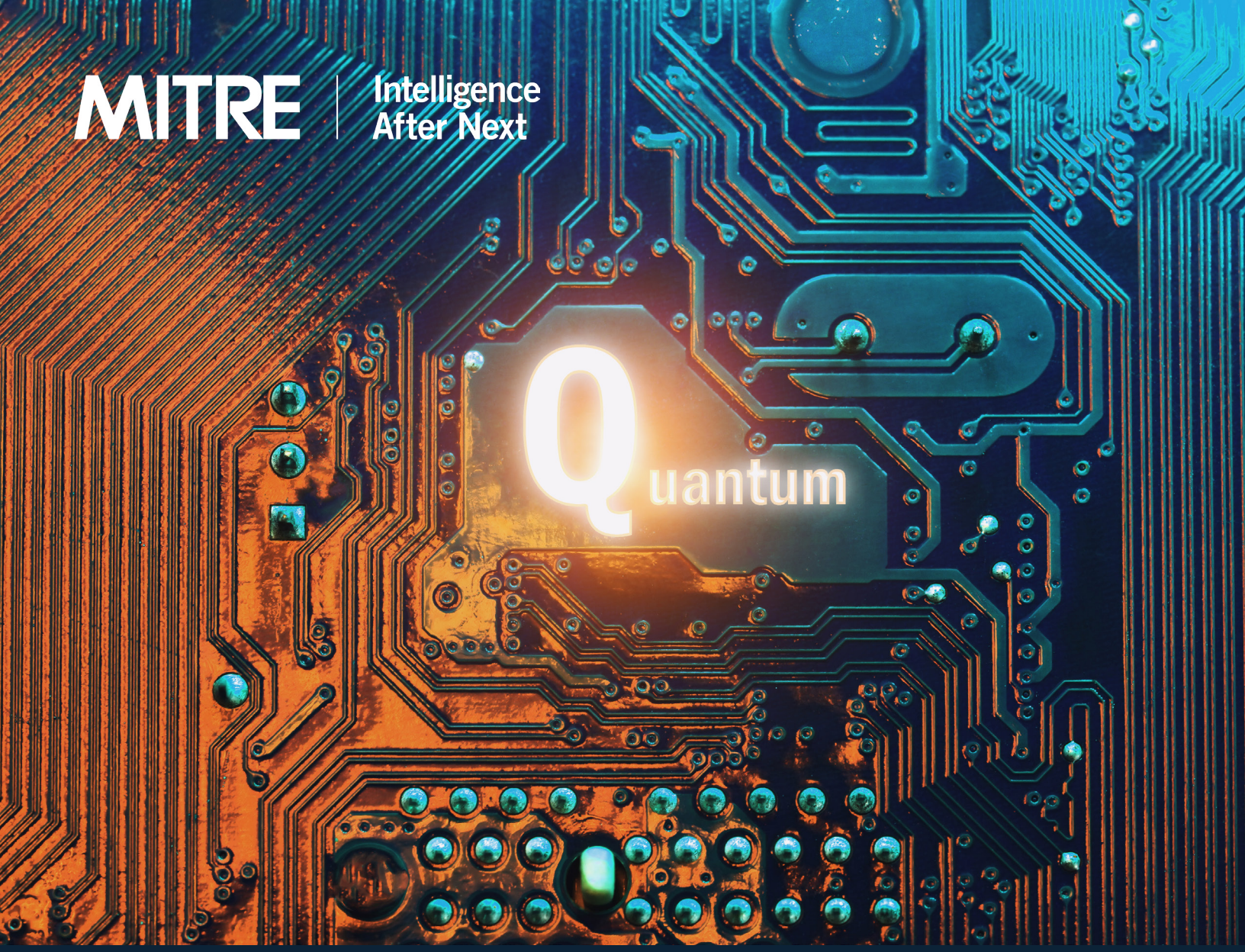
MITRE | Intelligence After Next



Intelligence After Next

SERIES # 29

QUANTUM COMPUTING: QUANTIFYING THE CURRENT STATE OF THE ART TO ASSESS CYBERSECURITY THREATS

by Yaakov Weinstein and Brandon Rodenburg

Quantum Computers—Threats, Benefits, and Cutting Through the Hype

Quantum computers are emerging computational devices that exploit the phenomena of quantum mechanics to enhance computation. Their revolutionary potential first became apparent 30 years ago with the discovery that a quantum computer could break asymmetric cryptographic protocols such as Rivest-Shamir-Adleman (RSA), a public key cryptosystem that enables any user to encode data in such a way that it can be read only by those who know a private key. Should RSA be compromised, all classified and encoded data would be immediately vulnerable. Hence, the possible existence of a quantum computer should be of great importance to the Intelligence Community (IC).

Beyond the threat they pose to cybersecurity, quantum computers can resolve challenges of great importance to the IC. For example, quantum computers can perform complex optimization and logistical problems faster than conventional computers. In addition, quantum computers can simulate basic chemicals, materials, and pharmaceuticals more quickly than conventional computers, perhaps enabling novel and smart materials and pharmaceuticals. Finally, quantum computer algorithms for machine learning (ML) promise faster, more accurate results that can be achieved with less training data than that required for conventional computers. In fact, quantum computers can even generate more appropriate synthetic data than their conventional counterparts.

Given the revolutionary threats and capabilities of quantum computers, it is natural to wonder when such systems will become available. To assess this timeline, we invoke a commonly used metric of quantum computing power known as the quantum volume (QV). QV is defined as the minimum between the number of qubits (the quantum version of a bit) in the quantum computer, or the number of sequential computational gates those qubits can perform. By plotting quantum volume over time and extending the trend that emerges, we estimate that a quantum computer capable of breaking RSA-2048 (a current high-security version of RSA with a 2048 bit-long key) will not be available for another three or so decades. Others dispute this analysis, claiming that current trends will shift toward faster growth and that powerful quantum computers will be available much earlier.

While U.S. industry currently leads the way in quantum computing, other nations, especially China, are not far behind.

This divergence in estimates speaks to the need for the IC in the near term to (1) carefully monitor the emergence of quantum computers and (2) identify methods of protecting against the quantum computer threat to classified information. While U.S. industry currently leads the way in quantum computing, other nations, especially China, are not far behind. In fact, China is ahead of the United States in other quantum technologies, such as quantum communications and quantum key distribution. Lessons learned from those technologies may provide China with important ideas and techniques applicable to quantum computers that the United States may lack. Should China attain relevant quantum computing before the United States, it will be the first country to exploit quantum computer capabilities in logistics, optimization, ML, and materials discovery. This breakthrough could open a military and technology gap the United States will not be able to overcome.

Even if China is not able to achieve quantum computing before the United States, it will be able to read encoded U.S. intelligence it has harvested once it attains a quantum computer. Some of that information may be classified, causing a potential severe security breach.

Should China attain relevant quantum computing before the United States, it will be the first country to exploit quantum computer capabilities in logistics, optimization, ML, and materials discovery. This breakthrough could open a military and technology gap the United States will not be able to overcome.

Other adversary nations also are harvesting encrypted data from U.S. communications over physically accessible networks in hopes of compromising the encryption once a quantum computer becomes available. Given that some classified data must remain so for decades, perhaps beyond the time when quantum computers become available, it is necessary to dissolve the quantum computer threat to classified data as soon as possible.

Given the above context, this paper aims to (1) demonstrate that quantum computers are an area of significant interest and funding with predicted continued maturity and growth; (2) motivate the need for metrics of quantum computer power as a means to predict the maturity of the technology; (3) introduce quantum volume as a candidate quantum computer metric and, given the current state of the art, use it to assess when quantum computers may pose a threat to national security; (4) survey national efforts in post-quantum cryptography as a response to the emerging quantum computer threat; (5) challenge QV as an appropriate quantum metric; and (6) provide IC-relevant recommendations.

Quantum Computer Investment

Despite the challenges of building a mature quantum computer, much progress has been made over the past few years due to significant investment by government and industry. Not surprisingly, this has led to several predictions

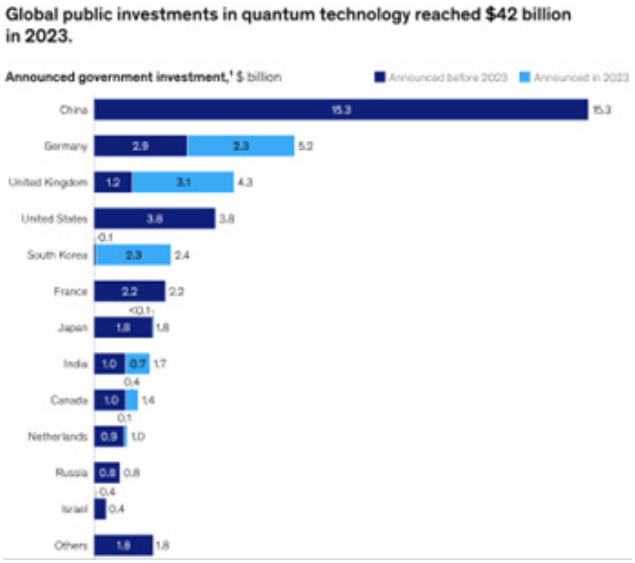


Figure 1: The Rise of Quantum Computing (McKinsey and Company; see https://www.mckinsey.com/featured-insights/the-rise-of-quantum-computing)

about the future of quantum computers, in terms of both when they will reach maturity and their potential economic impact. For example, many experts believe that practically useful quantum computers will emerge within 10 to 20 years, while others are even more (sometimes hopelessly) optimistic. Boston Consulting Group asserts that "quantum computing will create $450 billion to $850 billion of economic value globally" by 2040[1]. A 2023 Zapata AI survey found that 76 percent of companies interested in quantum technologies expect a business advantage from quantum computing within five years.[2] This is despite two years of decreased investment in quantum technology startups. Government investment, on the other hand, has continued to increase, as shown in Figure 1 (not including the CHIPS and Science Act[3] and the hoped-for reauthorization of the National Quantum Initiative Act).[4]

Quantum Computer Assessments and Predictions

Quantum computing has garnered so much interest and investment in such a short amount of time that it can

be difficult to separate hype from reality. How powerful are current quantum computers compared with how powerful they need to be to accomplish a specific task? What tools are used to make predictions about quantum computing growth? What trends in quantum computing technology are being seen, and what are possible disruptors or bottlenecks?

To address these and related questions, we must first define appropriate metrics to quantify quantum computer power. Having a well-defined, meaningful metric will enable even a casual observer to comprehend a given quantum computer's maturity; compare different quantum computers; and, with appropriate time-based data, observe trends and make predictions.

Quantum Computer Metrics

Numerous possible metrics can be applied to a quantum computer. One metric is the largest number a quantum computer can successfully factor. RSA and other asymmetric cryptographic protocols assume that factoring large numbers and similar problems is difficult—so much so that even a conventional computer cannot perform this task within a reasonable amount of time. What enables quantum computers to break these asymmetric protocols is their ability to efficiently factor large numbers. Hence, using the metric of how large a number a quantum computer can factor within a specified time is a quantifiable means of determining how close a given quantum computer is to factoring the numbers that underlie RSA-1024 or RSA-2048. The challenge with this metric, and other application-based metrics, is that quantum computers are not yet mature enough to tackle any test case of reasonable size. For now, then, a metric is needed based on system parameters.

Another possible metric is the number of qubits in a given quantum computer. Qubits are to quantum computers what bits are to conventional computers. The power of quantum computing arises because its qubits can exhibit quantum phenomena such as superposition, in which quantum systems exist in multiple states simultaneously (such as the states zero and one for qubits), and entanglement, in which quantum systems exhibit correlations between them that are not classically achievable.

The advantages of number of qubits as a metric are that it is easy to determine (simply count the qubits) and does serve as a bottleneck for quantum computing power. A small number of qubits, while capable of demonstrating various quantum phenomena, can be easily simulated on a conventional computer.

The disadvantage of using a number of qubits as a metric is that not all qubits are created equally. Qubits are error prone. Errors arise primarily due to two factors: decoherence and difficulty to control. Decoherence is a continual, natural process that causes a quantum system to lose its ability to exhibit quantum phenomena like superposition and entanglement. Decoherence arises when quantum systems interact with their environment, which may include anything from air molecules to cosmic rays. To stem the effects of decoherence, it is necessary to keep qubits as isolated as possible. Open the door to decoherence, and qubits may end up in incorrect states.

The mechanisms of controlling qubits vary depending on what they are physically. Atoms or electrons, for example, are controlled by lasers. However, because qubits are very small, a laser aimed at one qubit may affect neighboring qubits as well. Similarly, if the laser is on for too long or too short a time, the qubit will perform the incorrect computational gate. The number of qubits does not reveal how error-prone or noisy the qubits are. Therefore, the number of qubits cannot alone relay the power of a given quantum computer.

With that in mind, an appropriate metric could be based on the qubits themselves. An example would be the decoherence time of a qubit—the amount of time after which a quantum system no longer exhibits quantum phenomena. Alternatively, one could examine the error probability of a qubit. An average over, or worst case of, all the qubits in the quantum computer would then serve as the quantum computer metric. The disadvantage

of looking at each qubit separately is that two-qubit computational gates are necessary to implement quantum algorithms (the algorithms implemented on a quantum computer). Hence, knowing the specifications of a given qubit is insufficient to provide insight into the ability of the quantum computer as a whole. In addition, qubit-based metrics are not system level and may disregard other properties of the quantum computer.

Quantum Volume

A more well-rounded—though harder-to-determine—metric is quantum volume, first developed by IBM.[5] QV depends on two factors: the number of qubits in the quantum computer and the number of arbitrary two-qubit computational gates those qubits can perform without error. Hence, a quantum computer with only two qubits, though it may be able to perform many computational gates, has a lower QV than a quantum computer with three qubits capable of performing three sequential arbitrary two-qubit gates. This metric has several advantages, including that (1) QV strikes a balance between the number of qubits and how many gates they can perform (this is because the noisier or more error prone the qubits, the fewer number of sequential gates that can be implemented); (2) QV disregards details about possible errors and accounts only for how large a computation (measured by number of sequential gates) the qubits can perform; (3) two-qubit gates between arbitrary qubits will increase in difficulty if the qubits are not next to each other. Hence, QV favors qubit layouts in which qubits have many nearest neighbors.

Figure 2 presents the QV of different quantum computers (from the companies IBM, IonQ, Quantinuum, and AQT) over roughly the past decade. As shown, the record QV has increased in an almost straight line between 2016 and 2024. Extending this line enables us to predict the QV of quantum computers in future years. The dashed horizontal lines signify approximately what QV would be needed to accomplish specific quantum computer milestones. For example, the line labeled Shor's algorithm (which is the algorithm a quantum computer uses to factor large numbers, discovered by Peter Shor) is the approximate QV necessary for a quantum computer to compromise RSA-2048. Hence, if we follow the trend line, we would approximate that a quantum computer will be powerful enough to do compromise RSA-2048 around the years 2055–2060.

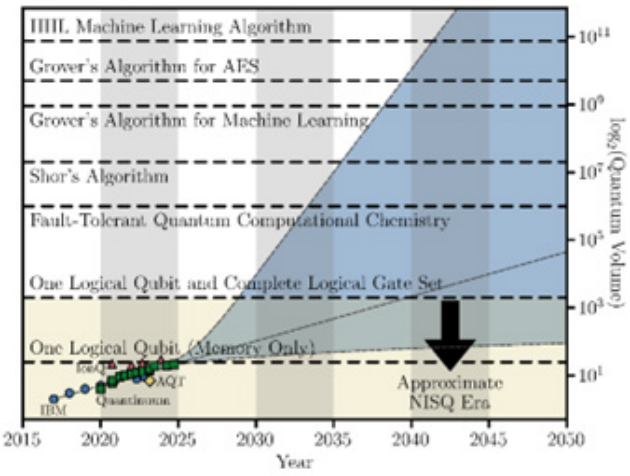


Figure 2: Growth of (logarithm base 2) Quantum Volume as a Function of Time. The different shapes represent reports of different companies: IBM (circles), IonQ (triangles), AQT (diamond), and Quantinuum (squares). Horizonal dashed lines are approximate QV values a quantum computer would need to accomplish the labeled tasks. Explanation for these tasks or milestones are found in the text. The Approximate Noisy Intermediate-Scale Quantum (NISQ) Era is the current time period, before fault-tolerant quantum computers become available. Fault tolerance is achieved when quantum computer algorithms can be implemented successfully irrespective of the presence of errors on qubits. Before that time (namely, in the NISQ era), whether quantum computers will be able to demonstrate a clear, practical advantage when compared to conventional systems is an open question and an area of intense exploration.

Quantum computer enthusiasts, however, may point to recently accomplished milestones that will disrupt the current trend line.[6] For example, recent results have demonstrated that quantum error correction can successfully suppress (though by no means eliminate) errors during quantum computer implementation.[7] In

Figure 2 this milestone is signified by crossing the lowest of the dashed horizontal lines—achieving one logical qubit. A logical qubit is the set of qubits that function as one qubit from a data perspective but adds a layer of error protection. Crossing the lowest line conveys that data can be protected to some degree against errors.

U.S. industry has demonstrated the ability to outstrip the rest of the world in pushing quantum computers, but there is no guarantee that the United States will win this race.

The capability of protecting against at least some errors may enhance the ease of reaching higher-level milestones, of which the next milestone would be performing computational gates on logical qubits.[8] Hence, an optimist might say the correct prediction for quantum computer maturity is something like the upper trend line above the blue area in Figure 2, which is a notional idea of what an increased maturity timescale might look like. Along this trend line, quantum computers may be capable of breaking RSA-2048 by 2035. However, it is also possible it will prove harder to connect and control logical qubits and hence the trend will do the opposite: it might slow down.

Further milestones called out in Figure 2 include the ability for quantum computers to perform computational chemistry. This capability may enable the discovery of novel, useful materials and pharmaceuticals for a broad range of applications. Quantum computers with higher QVs can implement Grover's algorithm, originally conceived of as a means of searching disordered data sets but that can also be invoked for a range of quantum ML techniques and for attacking Advanced Encryption Standard (AES) cryptography. We note, however, that while Shor's algorithm provides an exponential speedup over conventional techniques, Grover's algorithm provides only a quadratic speedup that may be washed away once error correction and other techniques are fitted around the base algorithm (not to mention the assumed greater expense of a quantum computer). Finally, the Harrow-Hassidim-Lloyd (HHL) algorithm provides a quantum computer an exponential speedup in solving series of linear equations. This algorithm is also central in quantum ML algorithms that may provide more accurate results, in less time, and with less training data.

State of the Art

As seen in Figure 2, several quantum computing industry players have publicly announced progress in their quantum computer development, using QV as a metric. The current record is held by Quantinuum, with a value of $1{,}048{,}576 = 2^{20}$. This means that Quantinuum's quantum computer has at least 20 qubits that can sequentially implement 20 arbitrary two-qubit gates. IBM currently has two systems (Heron and Egret) with QV of $512 = 2^9$ and three (Eagle, Hummingbird, and Falcon) with QV of $128 = 2^9$. However, after assiduously reporting QV since it conceived of the metric, IBM has refrained from doing so in the past few years.

IonQ at one point announced a preliminary QV of 2^{32} but this was not verified. Instead, IonQ has developed its own benchmark called the algorithmic qubits (AQ). AQ is similar to QV except that rather than using more difficult arbitrary two-qubit gates, it tests different classes of algorithms.[9] The rationale for doing so is to provide a benchmark that is more application based and that, therefore, uses gates that are more likely to be performed in a typical quantum algorithm than an arbitrary two-qubit gate.

U.S. adversaries are seeking to weaken the U.S. supply chain for necessary components for quantum computing. The IC must identify these critical resources, such as raw material for cryocoolers and lasers, and ensure a consistent U.S. supply.

Other companies, such as Google, have not used QV but instead report more localized results, such as the success of particular error correction schemes or algorithm implementation.

Post-Quantum Cryptography

Although Figure 2 suggests that it will be quite a while before quantum computers pose a threat to modern asymmetric cryptographic protocols, concern about future devices has already been the motivation for National Institute of Standards and Technology (NIST) and National Security Agency (NSA) efforts to create new asymmetric cryptographic protocols known as post-quantum cryptography (PQC). In addition, the need for protection against the quantum computing threat has been codified on the federal level by:

- NSA's Cybersecurity Advisory Commercial National Security Algorithm Suite 2.0,[10] which mandates timelines by which national security systems must migrate to PQC
- The Quantum Computing Cybersecurity Preparedness Act,[11] which requires each agency to maintain an inventory of information technology that is vulnerable to the threat of a quantum computer, and the Office of Management and Budget to issue guidance requiring each agency to develop a plan to migrate to PQC

Transitioning to new asymmetric encryption protocols, PQC, is the best means of doing so. PQC protocols are based on mathematical challenges that, to the best of our knowledge, cannot be easily solved even by quantum computers. While NIST and NSA have standardized a suite of PQC protocols, they are not yet deployable versions of these cryptosystems. Given the long time expected before all national security systems transition to PQC protocols and the "harvest now, decode later" tactics of U.S. adversaries, we recommend the IC begin the process of transitioning to PQC as soon as possible.

Is QV the Correct Metric?

There are a few weaknesses in QV as a metric for quantum computing power. First, many algorithms require more sequential gates or time steps than they do qubits.[12] For example, compromising RSA-2048 requires a few thousand perfect (error proof) qubits. However, doing so also requires about a trillion gates— a very noticeable difference (nine orders of magnitude). From that perspective, it may not be appropriate to treat number of gates and number of qubits on equal footing. One way to address this is to weigh the number of gates more heavily, as is done via Quantum Volumetric Classes.[13]

QV may be immediately adapted to a time when error correction has been successfully incorporated into quantum computers: by counting number of logical qubits (rather than physical) and number of logical gates. However, further analysis will be needed for quantum computers implementing error correction with only partial success.

This challenge is especially true when trying to evaluate companies like PsiQuantum that explicitly eschew NISQ devices, such as the devices currently available from other vendors, and instead aim directly at constructing fault-tolerant quantum computers. (Fault tolerance is achieved when quantum computing algorithms can be implemented without concern for the errors that may

arise.) This strategy comes with unique benefits and risks but also makes it difficult to assess progress using a metric like QV. To track the progress of companies with this approach, it may be necessary to focus on more localized benchmarks, such as the accuracy with which basic gates are performed and the time before a qubit undergoes significant decoherence.

Magic State Generators

The hardware of conventional computers can be naturally split into several parts. There are memories, control units, logic units, and so on, and each part may have appropriate metrics attached to it. Quantum computers have not yet reached the maturity level where different sections are dedicated to specific functions (though there have been proposals for utilizing different types of qubits for different functions). However, there is a unique component of a fault-tolerant quantum computer that does not have a conventional parallel and deserves attention: magic state generators.

As explained, once quantum information is encoded into an appropriate error correction code to form logical qubits, algorithms are performed by implementing logical quantum gates. These gates are specially designed such that information stays encoded and thus error protected throughout the running of the algorithm. However, there are certain necessary gates for which such an implementation requires additional resources. These resources take the form of a set of additional, ancilla qubits arranged in what is called a "magic state." Every time one of these gates is performed, a new magic state is necessary. Of course, the magic states themselves must be constructed without errors at the risk of compromising the workings of the logical gate.

Magic state generators are arrays of qubits in a quantum computer dedicated to producing magic states and sending them off to the areas of the quantum computer where they are needed. In fact, there may be multiple magic state generators in a quantum computer to limit the necessary shuttling distance of the magic states.

Due to their unique role, the metrics of the magic state generators are likely to be different from those of other qubits. Appropriate metrics would be rate of magic state generation, accuracy with which they are created, and efficiency of combining multiple magic states together to form one that is of higher quality through a process called magic state distillation.

The IC has an important role to play in protection from and the utility of quantum computers. The IC must protect its classified data from the threat of a quantum computer, and it should monitor the state of quantum computers to prepare for future threats and capabilities and determine use cases for a future quantum computer. By acting decisively and quickly, the IC will demonstrate the seriousness of the quantum computing threat.

What Next?

There is a worldwide race to construct fully mature quantum computers. Most prominently, China is outspending the rest of the world in this area with the hope of being able to "harvest now and decrypt later," once a quantum computer is available. U.S. industry has demonstrated the ability to outstrip the rest of the world in pushing quantum computers, but there is no guarantee that the United States will win this race.

Understanding the current state of the art for quantum computing is thus vital in assessing the cybersecurity threat posed to RSA and similar protocols. At a minimum, it sets a timeline before which new post-quantum crypto protocols, such as those outlined in CNSA 2.0, should be

ready to go out on national security systems. Beyond that, proper metrics can assist in determining how to focus and spend research and development funds. We do not currently have a perfect metric to accomplish these tasks; however, we do provide some suggestions and thoughts here. Most importantly, these metrics provide individuals tools to make their own assessments regarding the maturity of current and future quantum computers.

The IC's Role

The IC has an important role to play in protection from and the utility of quantum computers. First, the IC must protect its classified data from the threat of a quantum computer. This means immediately determining which information systems need to be updated or replaced and setting an order of priority for doing so. In this goal of transition, the IC will set the tone for the rest of the federal government. By acting decisively and quickly, the IC will demonstrate the seriousness of the quantum computing threat.

The IC should also monitor the state of quantum computers to prepare for future threats and capabilities and to determine use cases for a future quantum computer. An adversary who builds a quantum computer is unlikely to immediately announce it to the world. Rather, it is more likely the adversary will keep this information classified, wreaking havoc on U.S. national security without revealing how the circumventions of safeguards were achieved.

Should the United States be the first to attain practically useful quantum computers, there likely will be only a short time before others, including adversaries, will achieve it as well. What can the IC do with a quantum computer that will, as quickly as possible, exploit U.S. superiority in quantum computing given that the superiority may be short lived?

To ensure the United States is the first to achieve quantum computing, it may be necessary to classify information about quantum computing hardware, and perhaps control imports and intellectual property so as to not provide U.S. adversaries with resources or information on how to build a quantum computer. Furthermore, it must be noted that U.S. adversaries are seeking to weaken the U.S. supply chain for necessary components for quantum computing. The IC must identify these critical resources, such as raw material for cryocoolers and lasers, and ensure a consistent U.S. supply.

Should the United States not be the first to achieve practical quantum computing, it becomes immediately necessary to know what information has not been protected with PQC and assume it may be compromised. In addition, the IC must consider what an adversary would do with a quantum computer and what measures should be taken to reduce damage and catch up quickly.

Finally, quantum computers are the holy grail of quantum technologies. Demonstrating exquisite control over quantum systems to build a quantum computer demonstrates the full ability to engineer with quantum systems. Other quantum technologies, such as quantum sensors and quantum communication systems, work with similar quantum phenomena. IC utilization and investment in these nearer-term quantum technologies, while providing impact in their own right, may also serve as stepping-stones along a path toward controlling quantum systems and, ultimately, quantum computers.

References

1. Jean-Francois Bobier, et al, "Quantum Computing on Track to Create Up to $850 Billion of Economic Value by 2040." July 18, 2024. Available: https://www.bcg.com/press/18july2024-quantum-computing-create-up-to-850-billion-of-economic-value-2040.
2. Dan Brennan, "New Study: More than Two-thirds of Quantum-Adopting Global Enterprises Dedicated at Least $1M to Quantum Computing Initiatives in 2022; a 2.5x Increase Over 2021," New Study: More than Two-thirds of Quantum-Adopting Global Enterprises Dedicated at Least $1M to Quantum Computing Initiatives in 2022; a 2.5x Increase Over 2021 - Zapata AI
3. H.R. 4346—117th Congress (2021-2022): CHIPS and Science Act. Available: https://www.congress.gov/bill/117th-congress/house-bill/4346
4. H.R. 6213—118th Congress (2023-2024): National Quantum Initiative Reauthorization Act. Available: https://www.congress.gov/bill/118th-congress/house-bill/6213
5. Andrew W. Cross, Lev S. Bishop, Sarah Sheldon, Paul D. Nation, and Jay M. Gambetta. "Validating Quantum Computers Using Randomized Model Circuits," Phys. Rev. A, 100(3), 2019: 032328. arXiv:1811.12926. Available: https://journals.aps.org/pra/abstract/10.1103/PhysRevA.100.032328
6. Emily Conover, "How to Stop Quantum Computers from Breaking the Internet's Encryption." June 28, 2023. Available: How to stop quantum computers from breaking the internet's encryption; Paul Smith-Goodson, "IBM Prepares for a Quantum-Safe Future Using Crypto-Agility." August 8, 2024. Available: https://www.forbes.com/sites/moorinsights/2024/08/08/ibm-prepares-for-a-quantum-safe-future-using-crypto-agility/
7. Google Quantum AI Team, "Quantum Error Correction Below the Surface Code Threshold." August 24, 2024. Available: https://arxiv.org/html/2408.13687v1#abstract; Matt Swayne, "Breaking the Surface: Google Demonstrates Error Correction Below Surface Cold Threshold." August 27, 2024. Available: https://thequantuminsider.com/2024/08/27/breaking-the-surface-google-demonstrates-error-correction-below-surface-code-threshold/.
8. See this paper for a first step in that direction: Dolev Bluvstein, et al, "Logical Quantum Processor Based on Reconfigurable Atom Arrays," Nature. December 6, 2023. Available: https://www.nature.com/articles/s41586-023-06927-3
9. IonQ Staff, "Algorithmic Qubits: A Better Single-Number Metric." January 18, 2024. Available: https://ionq.com/resources/algorithmic-qubits-a-better-single-number-metric
10. National Security Agency, "Announcing the Commercial National Security Algorithm Suite", September 2022. Available: https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF
11. H.R. 7535—117th Congress (2021-2022): Quantum Computing Cybersecurity Preparedness Act." Available: https://www.congress.gov/bill/117th-congress/house-bill/7535/text
12. For example: Craig Gidney and Martin Ekera, "How to Factor 2048 Bit RSA Integers in 8 Hours Using 20 Million Noisy Qubits," Quantum, April 15, 2021. Available: https://quantum-journal.org/papers/q-2021-04-15-433/
13. Keith Miller, et al, "An Improved Volumetric Metric for Quantum Computers via More Representative Quantum Circuit Shapes." July 14, 2022. Available: https://arxiv.org/pdf/2207.02315

Authors

Dr. Yaakov S. Weinstein is the Chief Scientist for Quantum Technologies in MITRE's Emerging Technologies division. In that role, he designs and implements MITRE's Quantum Horizon Strategy, interacts with sponsors across the government, and cultivates collaborations with academia and industry. In addition, Dr. Weinstein is the Department Head for the Quantum, Imaging, and Optics Department, comprising 40+ staff dedicated to impactful, technical work for federal sponsors and the nation. Dr. Weinstein received his Ph.D. in Nuclear Sciences and Engineering from the Massachusetts Institute of Technology and was awarded a National Research Council Research Associateship at the Naval Research Laboratory. Outside of MITRE, Dr. Weinstein is the Editor-in-Chief of the Springer journal Quantum Information Processing and an Editor of the Quantum Science and Technology book series.

Dr. Brandon Rodenburg is a physicist and quantum information scientist with a background in quantum optics. Dr. Rodenburg is Quantum Technologies Group Leader at MITRE, where he is responsible for technical and strategic leadership in quantum technologies across multiple programs supporting the Department of Homeland Security, Depart of Defense, and the IC. In addition to his role at MITRE, Dr. Rodenburg is also an Ambassador for OPTICA (previously The Optical Society), where he engages in outreach and mentorship to students and early career professionals within the optics and photonics community.

Intelligence After Next

MITRE strives to stimulate thought, dialogue, and action for national security leaders developing the plans, policy, and programs to guide the nation. This series of original papers is focused on the issues, policies, capabilities, and concerns of the Intelligence Community as it prepares for the future. Our intent is to share our unique insights and perspectives surrounding a significant national security concern, a persistent or emerging threat, or to detail the integrated solutions and enabling technologies needed to ensure the success of the Intelligence Community. The views expressed in this publication are those of the author(s) and do not imply endorsement by the Office of the Director of National Intelligence or any other U.S. government department/agency.

You can receive all of MITRE's Intelligence After Next papers by subscribing to the series at mitre.org/IntelligenceAfterNext

About MITRE

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded research and development centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.