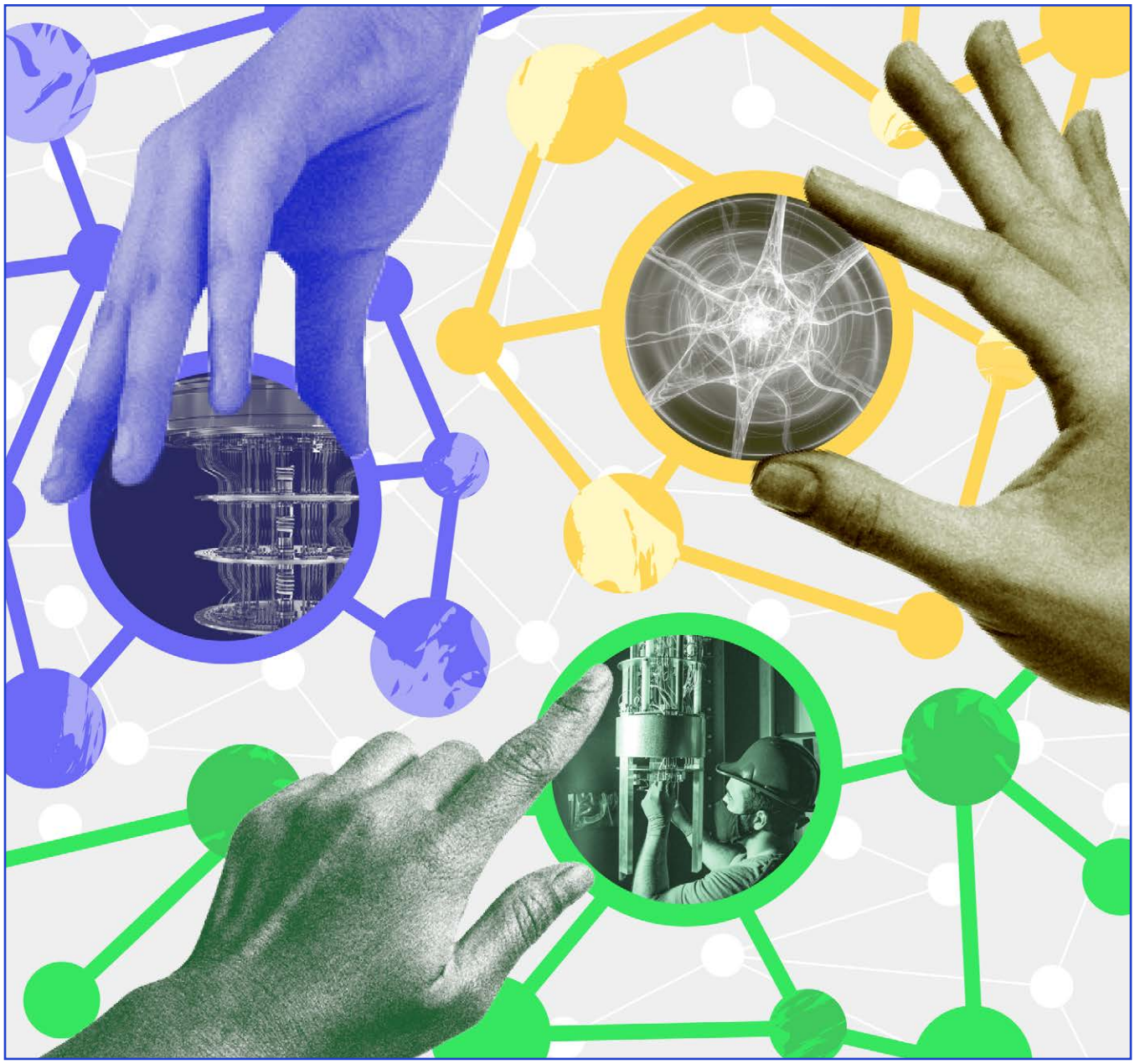


Quantum Computing 101:
Getting Ready for Tomorrow's Tech

govloop

carahsoft

Introduction

Quantum computing is a complex marriage of math, physics and IT that will take society's achievements to amazing new levels. It will allow us to break free of classical computing's limitations and explore new possibilities in science, finance, national security and realms we haven't anticipated. Researchers will develop groundbreaking drugs for infectious diseases. Artificial intelligence and machine learning will become even more powerful tools.

To encourage these advancements, the federal government enacted the National Quantum Initiative Act of 2018 and included funding in defense appropriations and in the 2022 CHIPS and Science Act. As noted in the National Quantum Initiative budget supplement for 2024, "The United States is making substantial and sustained investments in [quantum information science research and development] to explore a wide range of applications and nurture a culture of discovery."

But what quantum computing is and how it works is difficult to understand. So in this guide, we offer a 101 primer that explains the technology in clear and concise terms. We share insights from government and industry experts who have firsthand quantum computing experience. And we recognize quantum risks, including its threat to traditional encryption standards.

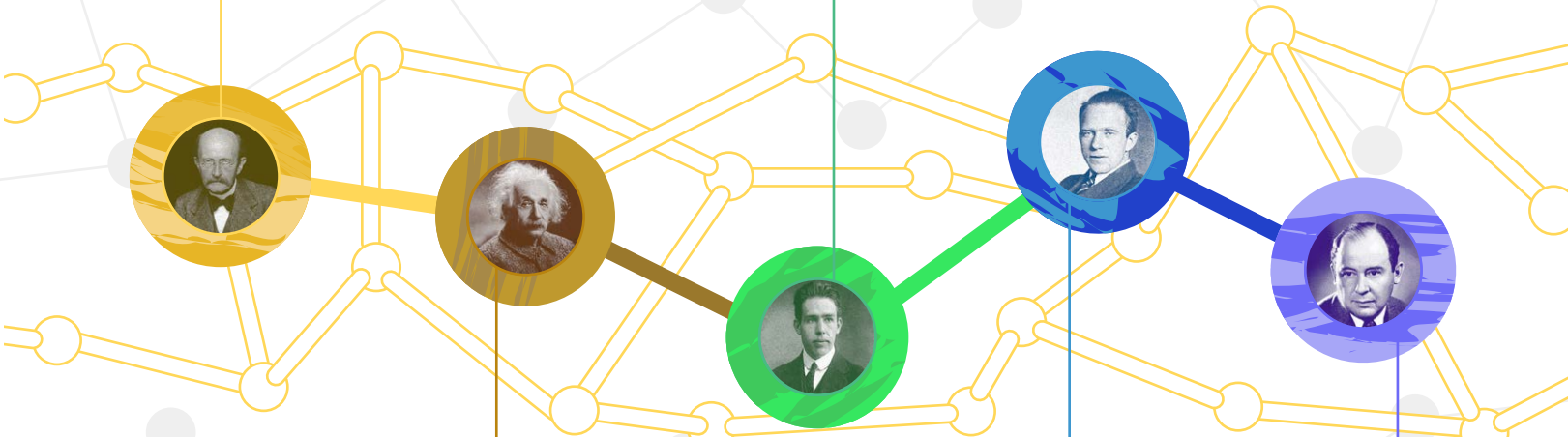
A quantum computer is unlikely to appear in your office any time soon. But you must be ready for what quantum technology will deliver — and understand how and why it will impact you.

Table of Contents

Quantum Computing: A Timeline

Although quantum computing is still a nascent technology, its history stretches back to the dawn of the last century. Its slow emergence has involved first physicists, then mathematicians and finally computer scientists. Here is a brief overview.

The theory behind quantum computing has its roots in early 20th century physics:



1900

Max Planck proposes that energy is emitted in discrete packets called quanta.

1905

Albert Einstein, building on Planck's work, says light consists of particles called photons.

1913

Niels Bohr develops a model for the atom in which electrons orbit a nucleus at quantized energy levels, emitting or absorbing photons when they jump from one level to another.

1927

Werner Heisenberg formulates the uncertainty principle, a concept in quantum mechanics that will play an essential role in the development of quantum computing.

1930

John von Neumann works out the mathematics behind quantum mechanics.

1980s

1981: Physicist Richard Feynman proposes creating a computer based on quantum mechanics to simulate quantum systems — a use case beyond the capabilities of classical computers.

1982: Physicist Paul Benioff creates a theoretical model that shows how the principles of quantum mechanics could be applied to computation.

1985: Physicist David Deutsch, building on Feynman and Benioff, describes how a quantum computer would operate.

1990s

1994: Mathematician Peter Shor writes an algorithm that would make it possible for a computer with sufficient power to break many widely used forms of encryption.

1996: Computer scientist Lov Grover writes an algorithm for quantum computers that would be more efficient for database searching.

2010s

2011: D-Wave Systems launches the D-Wave One, which it bills as the first commercially available quantum computer.

2016: IBM makes its design for prototype quantum processors publicly available, hoping to get developers to start thinking about writing quantum code.

2019: Google's quantum hardware lab, which opened in 2014, demonstrates how a quantum computer could solve a particular task in 200 seconds vs. the projected 10,000 years that a traditional computer that would need.

2020s

2020: The University of New South Wales in Australia offers the first undergraduate degree in quantum engineering to train a workforce for the budding industry.

2022: The Biden administration issues a national security memorandum highlighting the importance of advancing quantum information sciences while addressing the potential security risks.

2023: The National Institute of Standards and Technology (NIST) releases draft guidelines for developing encryption systems that quantum computers cannot crack.

Key sources: The WIRED Guide to Quantum Computing | A Brief History of Quantum Computing | The History Of Quantum Computing You Need To Know

How Quantum Computing Works

There's no easy way to explain how quantum computing works without getting deep into the kind of math that only quantum physicists can understand. But here is a brief overview that draws on numerous efforts to make quantum computing accessible to the rest of us. Click on the many hyperlinks for a deeper dive.

Classical vs. Quantum Computing

As many of us have learned along the way, a computer runs on binary code: It converts information into ones and zeros, making it incredibly efficient at running calculations and storing or communicating data.

In a classical computer, such as your laptop or phone, that information is encoded in bits, or binary digits, with each capable of representing either a one or zero.

Quantum computers also use binary code, but there's a big difference. They encode information in quantum particles — such as atoms, ions and photons — that aren't strictly binary. A quantum bit, or ***qubit***, can represent a zero, a one, or both a zero and a one simultaneously. That attribute, known as a **superposition**, makes it possible to run incredibly complex calculations very quickly.

This ability reflects the murky nature of quantum mechanics, which deals in probabilities. Think about a coin toss. As the coin spin through the air, there's an equal probability that the heads or tails side is facing up. By taking advantage of those multiple states, a quantum computer can run a massive number of calculations at one time. (To learn more, check out this article.)

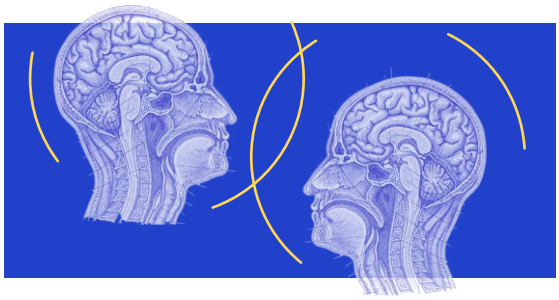
Another important quantum property is **entanglement**, which makes it possible to manipulate multiple qubits, as explained in this video.

It's all about math: The more qubits you have, the more ones and zeros you can use to run calculations. "While doubling the number of bits in a classical computer doubles its processing power, adding qubits results in an exponential upswing in computing power and ability," this article explains.

Quantum Concepts in Human Terms

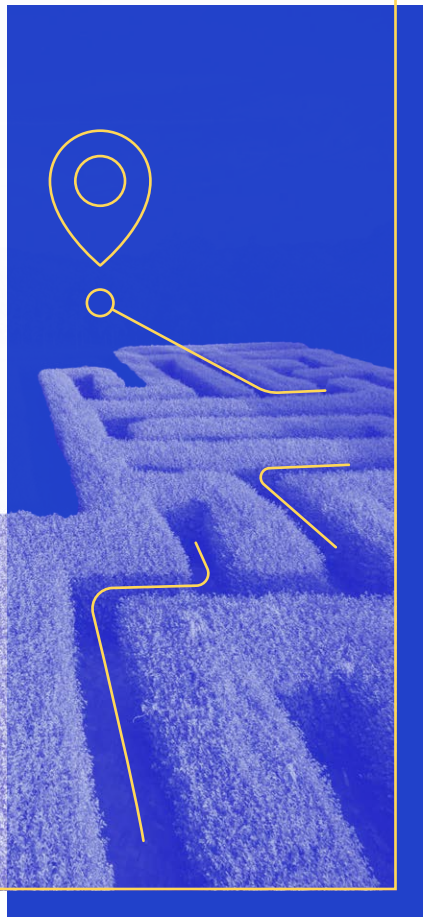
Have you ever been in love?

Two people spend time together, influencing each other, so interconnected that they act as one. When they are apart — no matter how far away — a connection remains, and they still influence each other. That's a bit like quantum entanglement.



Can you hold two opposing ideas in your mind simultaneously?

Yes, probably, but it can be difficult. Think of a classical computer as having one idea at a time — either zero or one. But a quantum computer can work with both at the same time, like holding two opposing ideas. That's similar to superposition.



Reality Check: The Quantum Advantage

A quantum computer will not always be faster than a classical computer. In fact, according to a recent article published by the MIT Sloan School of Management, classical computers "generally operate faster than quantum computers...but require more steps to accomplish a task."

Think about how a computer might solve a maze. A traditional computer would run all possible paths, one after the other, to find what works. The more power it has, the faster it can run that sequence.

But a quantum computer, using qubits in superposition, can test all possible paths at once, enabling it to arrive at the solution seemingly instantaneously. Advantage: quantum.

In fact, MIT researchers say the edge quantum computing has can be described in two ways:

+ It can solve problems traditional computers can't handle.
+ It can solve problems faster than traditional computers and costs about the same.

In some cases, solving a problem faster will provide what's known as a **quantum economic advantage**. For example, the same basic approach used to solve a maze might be applied to optimize routing and navigation in a global supply chain. Classical computers do that now, but not nearly as efficiently as quantum computers.

Early Use Cases for Quantum

Some of the domains in which agencies are expected to adopt quantum computers include:

AI/machine learning

With its ability to tackle complex calculations, a quantum computer could accelerate AI's ability to learn and evolve, according to an article in Forbes.

Cybersecurity

Yes, quantum computers eventually could crack some widely used cryptography algorithms. But the technology also could provide the basis for much stronger algorithms. Additionally, quantum computers could enhance the systems used to detect and respond to cyber threats.

Modeling and simulation

Quantum computing is expected to help scientists create more powerful and accurate computer models. This could be a boon in a wide variety of fields, from drug development and material science to transportation, finance and military operations.

A Work in Progress

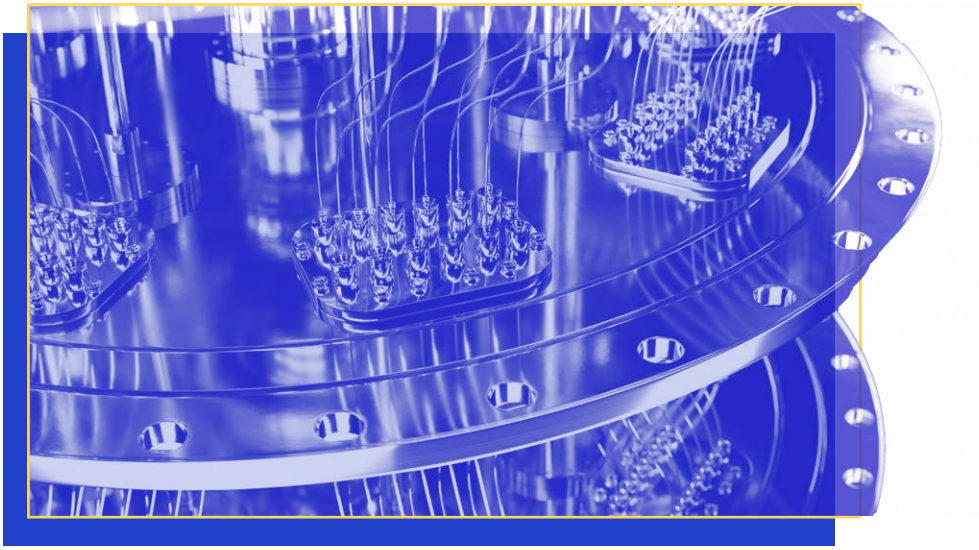
Quantum computing remains a work in progress. Here are some of the challenges that quantum scientists, computer scientists and hardware manufacturers are working to address:

Decoherence. Qubits are highly sensitive to vibrations, temperature changes and other environmental factors. A slight disturbance can knock a qubit out of superposition, resulting in errors. Some options for stabilizing qubits include supercooled refrigerators, insulation and vacuum chambers.

Error correction. The next challenge is to catch and correct errors as they happen, not just when an outcome looks askew. Experts have zeroed in on a few possible approaches.

Refrigeration. All large computers require cooling systems to prevent overheating, but it's an even bigger challenge with quantum computers. That's because qubits need to stay at near-absolute-zero temperatures, that is, minus-273.15 degrees Celsius, which involves large and very costly systems.

Multiqubit networking. In theory, manufacturers will be able to scale up quantum computers by having multiple chips or even multiple computers work in tandem, as is commonly done with classical computers. Unfortunately, they are still trying to figure out how to control individual qubits as their numbers increase.



When Will It Get Real?

Numerous companies have developed quantum computers that demonstrate the feasibility of the concept, even as they work on solutions to problems described above (and others). There's enough work to do that, but a timeline for a commercially viable system is elusive (as is the definition of commercial viability). Here are some predictions from industry watchers:

+ By 2035, a fully fault-tolerant quantum computer will be available, according to 72% of experts surveyed by McKinsey and Co. But the remaining 28% say that won't happen until 2040 or later.
+ Quantum computers likely will ramp up gradually, according to experts at MIT, first tackling "small-scale problems whose solutions offer smaller benefits and will only later be viable for solving more complex problems that promise larger benefits."
+ Meanwhile, some experts say quantum computers could work in tandem with classical systems, taking advantage of the strengths of each, an approach that the University of Delaware is pursuing.

When quantum computing is viable, most organizations are likely to access its capabilities via cloud services provided by major cloud providers, according to Jim McGregor, a principal analyst and partner at TIRIAS Research, a high-tech research and advisory firm. Quantum Computing-as-a-Service, you might say.

McGregor is bullish about the future of quantum computing. "You might say that quantum computing is where AI was in 2015, fascinating but not widely utilized," he writes. "Fast forward just five years and AI was being integrated into almost every platform and application. In just five years, quantum computing could take computing and humanity to a new level of knowledge and understanding."

Where Will You Be on Q Day?

An interview with Avesta Hojjati, Vice President of Engineering, DigiCert

For almost half a century, encryption algorithms have kept data safe. No matter how powerful today's classical computers get, that encryption would still take thousands — or even millions — of years to break.

The advent of quantum computing has changed all that. Put simply, some problems that are arduous for classical binary computers to solve, including the mathematical problems behind today's encryption methods, are easy for quantum computers.

What's kept classic encryption measures viable so far is that quantum computers aren't stable or powerful enough to be used to attack them. Someday soon, that will change.

"At some point — we really don't know if it's tomorrow, a week or a month from now — all these classical algorithms will be broken," said Avesta Hojjati, of DigiCert, the web's oldest certificate authority and a leading provider of digital trust.

"At DigiCert, we call it Q Day."

Not One Solution, but Many

Under National Security Memorandum 10, federal agencies must address quantum's security threat.

The good news is that there are solutions — and that's plural. "You want capabilities that allow you to move to multiple solutions because any one solution could [become] vulnerable," Hojjati said. The key is to build in agility to respond to changing threats.

"The first step is to do a discovery of [an agency's] landscape, the second step is to automate those endpoints and the third step is maintaining this posture every day," he said.

Discovery requires cataloging all the forms of encryption your system uses, he said. "Make sure you understand every single one of your cryptographic algorithms," Hojjati advised. "And this goes wide and deep in your organization. It goes wide because you should be able to integrate it with other discovery solutions, and deep to reach the silos and buckets [held] within an organization. You can't automate what you can't see."

Automating the Change

A platform such as DigiCert's Trust Lifecycle Manager begins with automating the discovery process. But automation goes much further by deploying new cryptographic standards agencywide. It can replace old algorithms with quantum-resistant ones and configure them without extensive manual intervention.

DigiCert has been helping customers prepare for Q Day since 2017, implementing its solutions for multiple use cases. Through its DigiCert Post Quantum Cryptography (PQC) lab, users can familiarize themselves with new, post-quantum algorithms for free. The company integrated those algorithms into every product it provides.

And through its Trusted Quantum Advisory Program, DigiCert educates organizations on their PQC needs, builds them a specific strategic road map to be quantum-safe and deploys specific discovery solutions for their environment, Hojjati explained.

"All of this comes in a package which is end-to-end, meaning from education to discovery to building your road map, all the way to maintaining this PQC posture," said Hojjati. "We hold the hands of customers to make sure they go through this journey without any blocks."

digicert®

digicert®

ARE YOU QUANTUM READY?

2 out of 3 security professionals worry organizations won't be ready for quantum attacks

DigiCert is at the forefront of the movement to create a quantum-safe digital world.

Working with industry leaders and policy organizations, our post-quantum cryptography innovators are developing new security technologies that stand ready for any quantum future.

GET INSIGHTS

Government Needs to Move on Post-Quantum Cryptography, Now

An interview with Philip Kwan, Director, Product Line Manager, Palo Alto Networks

Quantum computing promises to disrupt cybersecurity. In the coming years, adversaries will use this evolutionary shift in compute capability to crack the cryptography that today is the bedrock of data security.

"The threat from cryptographically relevant quantum computers — computers with enough horsepower to break cryptography as we know it today — is just around the corner," said Philip Kwan, who specializes in quantum security at Palo Alto Networks.

In some sense, the threat is already here. Adversaries are harvesting encrypted data with an eye toward breaking them as soon as the quantum capability is available. Given the immediacy of the peril, agencies need to move now toward post-quantum cryptography (PQC), Kwan said.

First Steps

It's important to start by recognizing the size and scale of the challenge.

"With many technologies affected, this is going to be the largest cryptography update the industry has ever done," Kwan said. That means "you want to make sure you have executive backing and proper resources and budgets in place."

In terms of practical steps, it makes sense to begin with a thorough inventory.

"You start by identifying all of the applications, the devices, the data that potentially can be affected" either by harvesting exploits today or quantum-fueled attacks in the future, Kwan said. "Doing a very thorough crypto inventory is extremely important. It will identify potential weaknesses and help with prioritization and classification of data in order to protect it."

Know the Landscape

The vendor community has already stepped up with a variety of offerings, from PQC to quantum random number generators (QRNG) to hardware and cloud-based quantum key distribution technologies.

Government leaders should keep certain things in mind when evaluating possible solutions. Today's networks are very complex environments, with different types of devices and software applications spanning multiple versions and generations of technology, said Kwan. As a result, agencies must look for technology based on open and accepted standards.

"Organizations like [the National Institute of Standards and Technology] and [the European Technology Standards Institute] in the [European Union] are helping the industry move forward in a standardized way," Kwan said, and it makes sense to look for solutions that align with those standards, with the openness to interoperate with a wide variety of systems. "You need to think about open standards in order to develop a true end-to-end post-quantum capability to accelerate your migration efforts,"he said.

To that end, Palo Alto Networks' firewalls can prevent harvesting attacks with post-quantum VPNs and detect, block and log the use of PQC and hybrid PQC algorithms, in a way that is easy to configure and deploy.

"When we developed our products, we [made] sure that we did a very, very tight integration of the standards-based security capabilities into our security platforms," Kwan said. "Anyone using our products is going to have just a few clicks of the mouse to fully activate all of this post-quantum capability."

paloalto® NETWORKS

paloalto NETWORKS | PUBLIC SECTOR

Accelerate Quantum Readiness

Lean forward on quantum security with a strategic partner you can trust.

The threat of quantum computers is real. Nation states and bad actors are currently collecting data to decrypt later. The security of billions of global transactions, from email and online banking to internet-connected medical devices, are in jeopardy. Is your organization prepared to tackle quantum threats?

Palo Alto Networks recently participated in the White House Quantum Security Roundtable and has been selected to participate in the U.S. Cyber Center of Excellence for Post-Quantum Cryptography. Our open standards based solutions are scalable and agile to meet a variety of business and security requirements.

Ready to accelerate your quantum readiness? Check out these resources:

Palo Alto Networks — Strategic Partner on the Road to Quantum Readiness

READ THE BLOG

Palo Alto Networks helping customers in their Quantum Secure journey

READ THE BLOG

The Quantum Computing Threat

VIEW TECH DOC

A CISO's Guide to Quantum Security

WATCH NOW

5 Things to Know About Quantum Computing

Andrew Wilson is Chief of the Quantum Physics Division at the National Institute of Standards and Technology (NIST), which is developing quantum technology that aims to improve timekeeping and atomic clocks — a perhaps under-appreciated but core NIST mission. While it's true that quantum computing is complicated, Wilson offers several thoughts that help clarify where quantum is today.

"It's phenomenally exciting."

He said that it's hard to overstate how exciting this time is — when scientists and engineers are using quantum mechanics from the 1920s and '30s to re-envision our computing future. Although it's unclear when the genie will leave the bottle, practical quantum computing is on the way, he believes. In fact, it already helps with interesting mathematical and physics problems, timekeeping, and the atomic clock, and people are excited about the possibilities it holds for chemistry. "There are very serious ideas for how these kinds of things could impact and benefit society," Wilson said.

"There's all sorts of … technologies that can be at the heart of quantum computing."

Several types of quantum computers are under development, and each has advantages and disadvantages, explained Wilson. People speculate about which technology will be most successful, but he believes that "everybody's right and everybody's wrong" and that only time will tell. "The key thing," he said, "is that from a physics perspective, there's no fundamental reason why [all] these things can't work."

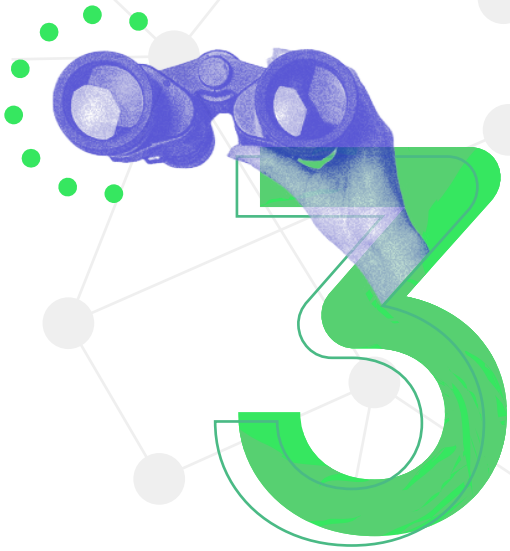
Throughout time, "humanity has learned in sometimes painful ways that if the physics says that [something] can be done, it can be done," Wilson added. That doesn't mean that the engineering will be straightforward, though.

"It's now looking like a serious proposition rather than some sort of fantastical thing."

People are making small, elementary quantum computers that are incapable of performing Shor's algorithm, for instance, but are still interesting, he said.

He believes that theories are far more advanced than what's possible to achieve in a lab — "there's kind of a disconnect that we need to close" — and that the existence of smaller quantum machines foreshadows larger ones.

"With the status of quantum computing, it's fair to say that there aren't fundamental reasons for why quantum computing couldn't work ... but the way we actually implement these things depends a bit on the hardware that's being developed," he said.



"There's an entire field of what's called 'quantum error correction.'"

Classical computers don't make mistakes very often because the technology is phenomenally robust. But quantum systems are much more fragile, and "errors propagate in nasty ways," he said. Error correction is basically a scheme "where you detect whether you've got errors as you go, and you fix them as you go," said Wilson.

You start by adding more qubits, then distribute information among them using entanglement and superposition. Next, you take measurements to check for errors — in a way that "doesn't disturb the quantum computing algorithm" — and fix any mistakes, Wilson said.

You ultimately can make something called a logical qubit that, theoretically, is protected from errors. "There's been lots of very nice results recently on quantum error correction," he said.

"Quantum computing has been a good problem for government labs to work on."

Government labs are helpful in dealing with difficult, long-term, large-scale problems. "A lot of the big discoveries and things that [achieve] real progress [are] often done in large, multidisciplinary, diverse teams where you've got lots of different, varied expertise," Wilson said. Quantum collaboration may be easier in a government environment than in an academic setting.

At NIST, the desire to make a better atomic clock drove the agency's exploration of quantum computing. The organization pioneered laser cooling, which traps and slows atoms and molecules to measure them more precisely. Eventually, someone at a conference mentioned the possibility of using trapped ions for quantum information processing as well, Wilson recalled. "There's many things that we do that help clocks that also help quantum information," he said. "It all really comes back to our desire to improve international timekeeping."

Cracking Encryption: The Quantum Threat

An interview with Michael Redding, Chief Technology Officer, Quantropi

There's no doubt that quantum computing offers great promise: Mathematical problems that are impossible today will be trivial tomorrow, allowing for drug discoveries and other breakthroughs. But just as radiation can be used both for good — to treat cancer, for example — and bad, quantum computing poses risk, said Michael Redding, Quantropi CTO.

"We can start to guess at all the potential ways a powerful [quantum] computer can be misused," he said, "but one that is clear and ... very specific is the fact that it will break current encryption."

The initial industry consensus was that quantum would realistically threaten encryption in 10 to 20 years, but artificial intelligence (AI) has dramatically shortened that window to three to five years, he said.

AI Revolution

That's because AI is great at extracting patterns in massive datasets. Research shows, said Redding, that we can use AI as a data pre-processor to "chew on the ciphertext" and vastly reduce how much data a quantum computer must analyze. That means the quantum computer can be smaller than anticipated because it's working with less information.

Without AI, you might need 8 million qubits to break a single encryption; using AI, you might need less than 400, he said.

Here and Now

The first problem when trying to quantum-proof your encryption is locating it — because encryption, Redding said, is "literally sprinkled throughout every system." It's like trying to identify all the rubber in your car and decide whether to replace the parts or retrofit them, and whether you or a third party will perform the work.

Although federal standards for quantum-safe encryption are still pending, agencies can take steps today to be quantum-ready, Redding said. They should inventory their network systems, establish security priorities and work with vendors on a quantum-security transition plan.

Agencies also can make the random numbers their encryption relies on — that comprise the digital keys that encryption algorithms use — even more unpredictable, he said.

And third, organizations need only minutes, he stressed, to quantum-harden the IPsec VPN channels that are the backbone of secure communication, connecting one data center to another, for instance. In other words, even if "all the [agency] applications themselves are [not secure]," he said, "as they go over the wire ... they're protected."

Being TrUE

There are three elements — what Redding collectively calls "TrUE" — to a complete cryptographic system. First, you must **Tr**ust that you're engaging in a secure discussion; the technology underlying that is asymmetric encryption, he said.

Then you need **U**ncertainty, based on symmetric encryption, so hackers don't know if they've accessed data in motion or at rest. And you need **E**ntropy, which means having truly unguessable, incalculable random numbers, he explained.

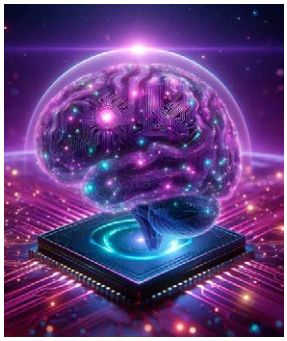
Quantropi offers a platform, QiSpace, that delivers quantum security by providing all three "TrUE" quantum solution components — as an "upgrade [or] addition to what you have," Redding said, "vs. a rip-and-replace."

One thing is certain, he said: "The next few years will be unprecedented."

quantropi®
Bring it on.

QiSpace™

Quantum-secure your data & communications today



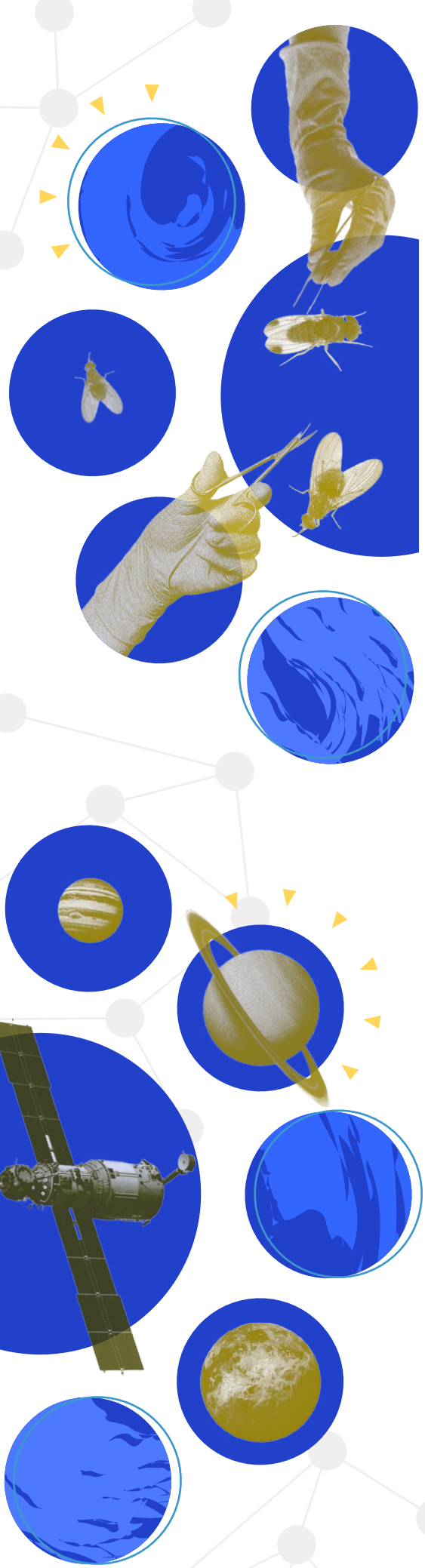
Advancements in Quantum Computing and AI are accelerating at alarming speeds, making the prospect of breaking classical cryptography a near term reality.

Protect your data and communications today with **QiSpace™** – The only "**TrUE**" platform with all three cryptographic capabilities for complete security:

- **Tr**ust: Asymmetric encryption
- **U**ncertainty: Symmetric encryption
- **E**ntropy: Quantum entropy generation & distribution

quantropi®
Bring it on.

Learn more about Quantropi's QiSpace™ Platform



Quantum Computing: **Dissecting How, Why and When**

An interview with Sterling Thomas, Chief Scientist, Government Accountability Office

Many students of high school biology learned about fruit flies: the tiny, winged creatures with red or white eyes that teach us about chromosomes, DNA, and dominant and recessive genes. It's the study of genetics at a basic level. But to understand complex gene interactions — the kind of knowledge that leads to breakthrough drugs for infectious diseases, for instance — you need a lot more math, which humans and traditional computers can't handle.

Sterling Thomas, Chief Scientist at the Government Accountability Office (GAO) and a trained geneticist, first used quantum computers about five years ago to explore how the technology might accelerate computations of things such as genetic mutations. But it was a little tricky, he said, and much of the work remains experimental.

"It's not like we take [an algorithm] and recompile it, and it runs on a quantum computer," he explained. "You actually have to rethink how the math will be implemented."

It is true, Thomas said, that quantum technology today is only somewhat helpful. "When people talk about no one using it, there aren't any use cases, they're talking about the current state of quantum computing," he said. "It's just not fast enough [where] the advantages you get from it ... outperform what you already have."

But there is great potential in biotechnology, orbital space research and some other fields, and as quantum technology improves — and Thomas believes it will — new use cases will become clear.

Why Quantum

With supercomputers, scientists today can run, for example, 50 iterations of the same calculation in parallel to see which one works best. But some problems you can't break into pieces like that, Thomas explained. You have to perform the complex calculations all at once. Supercomputers aren't suited for it, but quantum technology is, he said.

That's because it opens up a new realm of math. Instead of computations based on either zero or one, quantum computing creates a third option: both zero and one. Thomas said that superstate "significantly expands and accelerates how you can store information and [perform] different types of calculations."

What's Holding It Back

One reason why today's quantum computers are not faster than supercomputers, he said, is because the **quantum technology must spend time identifying and correcting its errors**. Superconductors used in quantum computing rely on brutally cold temperatures — around absolute zero — and anything above that introduces mistakes.

Ion capture, another type of quantum technology, among several, requires less cold but uses magnets to move atoms around, which causes interference between qubits.

People don't realize that traditional computing requires error correction also: It just goes unnoticed because traditional systems have become so good at adjusting for mistakes, Thomas said. "Now we're going through that process in the quantum world of [saying], 'OK, if it's too energetically expensive to make [the environment] absolutely cold, where we could have no error, then let's come up with a way to correct that error,'" he said.

Quantum's energy use is truly a concern. Generative AI and other technologies consume tremendous electricity, Thomas noted, and "the hope was that quantum, because you have this third state, the superstate, you wouldn't need quite as big [data] centers to do the computations." But if it takes more energy to power smaller quantum computers, that benefit doesn't exist.

The Encryption Issue

One way to protect sensitive data is through encryption, in which complex mathematical algorithms scramble the data into a secret code, and only the correct encryption key can transform it back. Right now, encryption is an effective, widely used cybersecurity tool.

Quantum computing threatens that because, as GAO's Sterling Thomas said, quantum can perform big calculations at once rather than individually. Using Shor's algorithm, for instance, quantum might take days, not years, to identify the right key to crack an encryption code.

NIST is developing quantum-proof encryption, and Thomas said agencies should be aware of the challenges quantum poses and be ready to transition to new standards. But he believes the issue is not as dire as some people fear.

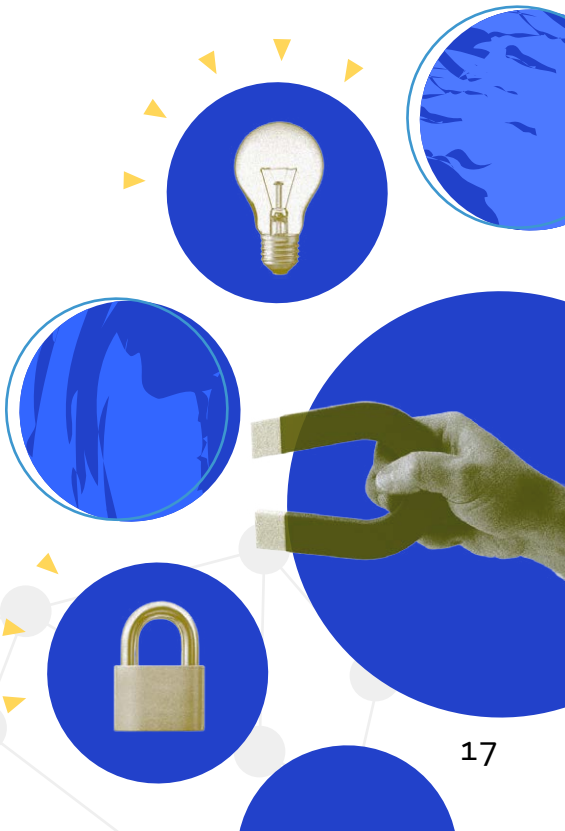
"I don't think it's Armageddon," he said. "I think it's just a matter of us developing technology that is safe within this new realm. And this won't be the last time we have to do that."

When to Expect It

Before joining GAO in October 2023, Thomas' work — related to genetics as well as cybersecurity, machine learning, data science, material science and other fields — focused largely on national security. In his view, federal security agencies are the only government entities likely to have on-premises quantum technology — because of the cost and the nature of their work. Most quantum calculations will take place in the cloud, he believes.

It's reasonable that in five to eight years, quantum will become available in a more reliable way, with systems that have larger and larger qubits. **Just like other technology with relatively humble beginnings, quantum computers will improve, Thomas predicted, and society will find use cases it hadn't envisioned.**

It will come down to two simple questions, he said: "What uses do you have in your specific role where quantum might make sense, and how will you access it?"



Time to Start Fighting Quantum Threats

An interview with Chris Hickman, Chief Security Officer, Keyfactor

One thing is certain: The day will come when quantum computers are powerful and reliable enough to render traditional encryption obsolete. What's less certain is when it will arrive.

But it's imperative that agencies prepare today. Wait too long, said Keyfactor's Chris Hickman, and "you won't have enough runway to keep your organization safe while you go through all the planning steps. It has to be done now."

The National Institute of Standards and Technology (NIST) is set to release its post-quantum cryptographic standards later this year, which will mean better tools for quantum-resistant encryption.

But people aren't always aware their data is already at risk of a quantum attack, according to Hickman. "We know data is being stolen now for decryption later," he said. Hackers don't need to invade your system to steal encrypted files; they can grab encrypted traffic from the internet and store the information until quantum can crack it, he explained.

The First Step Is Discovery

The Office of Management and Budget's Memorandum M-23-02 offers guidance for federal agencies in meeting the requirements of the National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems. It calls for inventorying and prioritizing all cryptographic systems because every encrypted resource is vulnerable if it's not upgraded to post-quantum cryptography (PQC).

"The reality is, you're only as good as your weakest link," Hickman said. "And the problem we've seen most is that organizations still lack visibility. [Encryption] is in everything, and now you've got to go find it."

That's difficult because certificates and certificate authorities are salted throughout systems, such as in individual Internet of Things (IoT) devices in the field and inside open source code. "It's important that you find [all of them] and that you continue to have that visibility," Hickman said.

Keyfactor's Command platform "has the ability to inventory certificate authorities from a number of different points," Hickman said. "It's able to connect to appliances and applications on the back end that may have certificates and inventory what's present in those devices as well."

Agile Encryption for an Uncertain Future

But it's not one and done. The federal mandates call for agility in dealing with PQC, because cybersecurity remains an arms race with bad actors.

That requires continuous solutions. Keyfactor's platform includes a lifecycle manager for encryption certificates that "detects them, finds them, brings them all in, and is able to manage them on an ongoing basis," Hickman said. Keyfactor also offers an open source cryptography stack that allows organizations to implement post-quantum into their own custom software development, he said.

But the key is to start now.

"Don't look at it as a tomorrow problem. The analogy I would use is the best time to plant a tree is 20 years ago," said Hickman. "The next best time is today."

KEYFACTOR

3-2-1...
QUANTUM!

Prepare for Quantum Today

Post Quantum Cryptography

Pqc

Because your agency's data deserves the best defense

Did you know that hackers steal encrypted federal data because they plan to decrypt it later?

Fight back! Make it harder for them by adding post-quantum cryptography into your agency's existing technologies.

Start planning today! You can get "quantum ready" in Keyfactor's PQC Lab and explore open-source toolkits, free trials, videos, and much more.

Go ahead, explore:
https://www.keyfactor.com/post-quantum-cryptography-lab/

KEYFACTOR

One solution stack to issue and manage machine IDs

www.keyfactor.com

Conclusion

Similar to AI's relatively humble beginnings, quantum computing has spent many years offering much promise but limited current benefits. However, experts say that's about to change, and government agencies at all levels must understand why and what quantum computing will impact.

About Carahsoft

Carahsoft Technology Corp. is The Trusted Government IT Solutions Provider®. As a top-performing GSA Schedule and SEWP contract holder, Carahsoft serves as the master government aggregator for many of its bestof-breed technology vendors, supporting an extensive ecosystem of manufacturers, value-added resellers, system integrators and consulting partners committed to helping government agencies select and implement the best solution at the best possible value.

Visit www.carahsoft.com, follow @Carahsoft, or email sales@carahsoft.com for more information.

About GovLoop

GovLoop's mission is to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to the public sector.

For more information about this report, please reach out to info@govloop.com.

Thank You

Thank you to DigiCert, Keyfactor, Palo Alto Networks, and Quantropi for their support of this valuable resource for public-sector professionals.

Authors

John Monroe, Director of Content
Candace Thorson, Managing Editor
Lauren Walker, Senior Staff Writer
Susan Kirby-Smith, Senior Staff Writer
Adam Stone, Contributing Writer

Designers

Kaitlyn Baker, Senior Creative Manager
Kelly Boyer, Motion Graphics Team Lead
Marc Tom, Junior Graphic Designer