Deloitte.
Insights

FEATURE

The realist's guide to quantum technology and national security

What nontechnical government leaders can do today to be ready for tomorrow's quantum world

Scott Buchholz, Joe Mariani, Adam Routh, Akash Keyal, and Pankaj Kishnani

THE DELOITTE CENTER FOR GOVERNMENT INSIGHTS

Though now nascent, quantum science could have significant implications for national security. By taking simple pragmatic steps today, government leaders can prepare their organizations for the coming quantum future.

The rise of computing

On December 10, 1945, a switch was flipped in Philadelphia, and the modern computer age began. That switch powered up the Electronic Numerical Integrator and Computer, or ENIAC, for the first time. As the world's first electronic, digital, reprogrammable computer, ENIAC shifted the world from mechanical calculations to digital ones and, in doing so, is the direct forerunner of every laptop, server, and smartphone today.

But with the arrival of such a powerful machine, the immediate question arose of what to do with it. How would this grand tool change modern living? A little over a decade and a half later, the World's Fair in New York would try to answer that question. Exhibitors from many different countries and companies vied to show their visions of the future, often focusing on how the new computers would change the world. There were rides where visitors in movable chairs zoomed over an exquisite 3D model of future worlds. While the fair was a hit with more than 50 million visitors, sadly for us, many of its predictions of mining the moon or permanent underwater colonies have not come to pass.[1] And this is not because its creators did not understand the technology or trends at the time—quite the opposite.

The failure of these predictions is not because people were not smart or knowledgeable—it is just that predicting the future is hard. After all, while we may have missed out on moon bases and regular submarine trips, who could have predicted the internet or next-day delivery of just about anything? Often the most hyped predictions of the future are incorrect, only to be overtaken by initially more mundane, but ultimately radically transformative uses.

And so it is with quantum information technologies, which once again offer to change the underlying basis of information processing—this

time not from mechanical to digital, but from digital to quantum. Quantum information technologies will almost certainly have significant impacts on national security—touching everything from extremely secure communications to faster code breaking to better detection of aircraft and submarines.[2] However, it is also clear that today we are unlikely to be able to predict exactly what those impacts will be. But for government leaders in national security who face significant stakes for getting things wrong, doing nothing is not an option.

So how can government leaders prepare for a somewhat unknown quantum future? The short answer is that pragmatic leaders can put in place the infrastructure to allow their organization to capitalize on whatever developments quantum may bring. However, to get more specific about what government leaders can do today to be ready for tomorrow's quantum world requires understanding what "quantum" itself is.

Quantum information technologies will almost certainly have significant impacts on national security—touching everything from extremely secure communications to faster code breaking to better detection of aircraft and submarines.

What is quantum?

The term "quantum" seems to denote something so advanced and futuristic that many TV shows and movies have appropriated the term. It may, then, be shocking to learn that technologies making use of quantum are not particularly new. In fact, today's quantum information technologies, such as quantum computers and clocks, are part of the second quantum revolution. As Dr. Marco Lanzagorta, research physicist at Naval Research Lab, puts it: "We have been exploiting quantum phenomena since the 1950s with the development of lasers and semiconductors and all of the technologies that led to modern computer technology. The previous quantum technologies may have used quantum phenomena, but developers could often describe the technology's performance in terms of classical bits of information."[3] Today, technologies have advanced to a point where we can use quantum phenomena not just to make devices but to store, process, and analyze a new type of information. This revolution is a revolution in *quantum information science*.

As seen in the introduction, quantum information science has the potential to be just as revolutionary to defense and national security as classical information science that has given us computers and the internet. While many government leaders may wish to prepare their organizations for the coming quantum revolution, the obscure and counterintuitive nature of quantum science can be a major barrier. As a result, many government leaders are unfamiliar with quantum science or technology. While government leaders certainly don't all need PhDs in particle physics, they should at least have a general idea of what quantum science is and to more fully appreciate how it will affect technological advancements in the days to come.

Quantum information technologies, such as quantum computers, cryptography, radars, clocks, and other quantum systems, rely on the properties of quantum mechanics, which describes the behavior of matter at the subatomic scale.[4] This

highly complex science often conflicts with everyday intuitions about how the world works, yet it is exactly these counterintuitive features of quantum mechanics that give the different technologies their unique strengths and weaknesses.

At a very basic level, quantum principles such as "superposition" and "entanglement" allow subatomic particles to interact and share information in ways not possible for classical electronic components. When applied in new forms of technology, these quantum principles offer novel methods of computing, sharing, and encrypting data necessary for a host of commercial, scientific, and military applications. For example, by taking advantage of superposition and entanglement in quantum computers, scientists are able to use new algorithms to solve complex problems exponentially faster than even the most advanced traditional computers in operation today.[5] Similarly, through these same quantum principles, information can be shared through quantum encryption techniques that may provide significant boosts to security. The foundational quantum principles lie at the heart of the benefits that quantum information technology may bring, but they also create distinct challenges to realizing these benefits on a large scale (figure 1). (For a more in-depth description of superposition and entanglement, see Appendix.)

The challenges of quantum mechanics

The fundamental properties of quantum mechanics have opened new opportunities for technology, but they can also pose some fundamental challenges. Elsa Kania, adjunct senior fellow at the Center for New American Security, argues that a sober view of these challenges can help temper some of the hype around quantum information technologies: "While references to 'the race for quantum computing' do abound, it is important to recognize that this is not just a race, but rather more of a marathon."[6]

OPERATIONAL CHALLENGES

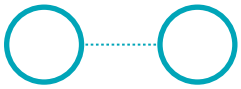
To begin with, there are some scientific challenges that are unique to quantum technology. For

FIGURE 1

Strange principles often underlie quantum information science

SUPERPOSITION

Superposition describes a particle's ability to exist across many possible states at the same time. So the state of a particle is best described as a "superposition" of all those possible states.



ENTANGLEMENT

Quantum entanglement refers to a situation in which two or more particles are linked in such a way that it is impossible for them to be described independently even if separated by a large distance.

OBSERVATION

Superposition and entanglement only exist as long as quantum particles are not observed or measured. "Observing" the quantum state yields information but results in the collapse of the system.

Source: Deloitte analysis.

The fundamental properties of quantum mechanics have opened new opportunities for technology, but they can also pose some fundamental challenges.

example, the very nature of quantum mechanics makes it impossible to "clone" or duplicate qubits, which are the quantum equivalent of a classical computer bit. This makes many common programming techniques that rely on copying the value of a variable impossible to use with quantum technology. For similar reasons, it's impossible to read the same qubit twice. While this can be a great advantage for secure communications where you want to generate unforgeable cryptographic keys, it can create tremendous difficulties in computing as it complicates the techniques necessary to test or "debug" a program before running it.[7]

ENGINEERING CHALLENGES

Along with these scientific and operational challenges to quantum, there are also significant engineering problems. As one might assume, the complicated nature of quantum science means developing quantum technology is very difficult. While research and development are underway, most quantum systems exist only in a laboratory environment, with many challenges to be overcome before these systems can operate at scale.[8]

One major hurdle includes reducing "noise." Noise is unwanted variations in data that interferes with computations and leads to errors.[9] Noise is a problem for classical computers as well, but the sensitivity of qubits to external interference and their difficulty correcting errors that arise make it an especially difficult problem for quantum computers.[10] Current attempts to overcome noise require laboratory settings that control for external vibrations and electromagnetic waves, and maintain very precise temperatures near absolute zero.[11] Without solving the problem of noise, quantum systems can't reach their full potential.[12]

Another challenge is increasing the number of qubits on a processor chip. Like a traditional computer's bit processor (i.e., 32-bit or 64-bit processor), quantum computers need qubit processors with hundreds or even millions of qubits to complete complex computations accurately.[13] Current quantum computers possess roughly 50 qubits. However, according to Dr. Jonathan Dowling of Louisiana State University, current efforts to develop quantum computers are seeing the number of quantum bits on a quantum computer's processor chips double every six months.[14] "That is four times faster than Moore's Law for classical chips, but the nature of quantum computers—[through] superposition and entanglement—means that their processing speed grows exponentially with the number of qubits. So, the processing power of quantum computers obeys *double* exponential growth," Dowling noted.[15] If this growth pattern continues, qubit processors could be capable of cracking one of the most widely used types of encryption, Rivest–Shamir–Adleman (RSA) encryption, and solving complex problems and simulations within the next decade.

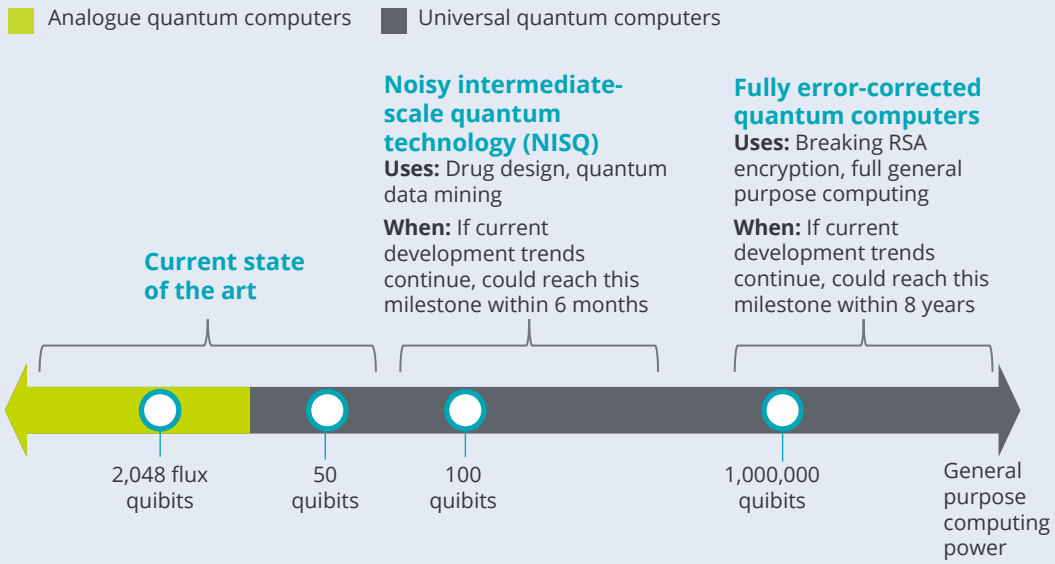
But just as with classical computers, the chip is not the only important component. New quantum computers and other such technologies also require ecosystems of supporting software, hardware, and algorithms, just as traditional computers, encryption, communications, and other technologies do. Developing these additional items will undoubtedly come with their own scientific and engineering challenges. It is important to note that quantum technologies are still in the early stages of development, which means that as these technologies mature, new problems requiring new solutions will likely come up.[16]

TYPES OF QUANTUM COMPUTING SYSTEMS

Not all quantum information technologies are the same. There are a few different approaches to creating qubits and using them to store, process, and output information. Those different approaches have varied strengths and limitations that make them suitable for different uses and influence their transition from the lab to the market (figure 2).

FIGURE 2

Quantum computers vary in how they can be used



Source: Deloitte analysis.

- **Analogue quantum computers:** Most associated with adiabatic quantum computers, quantum annealers, and direct quantum simulators, these types of quantum systems are some of the most developed systems to date. Because they are less capable of reducing noise, which impairs qubit quality, their functionality is currently limited to simpler and more specific use cases.[17]
- **Noisy intermediate-scale quantum technology (NISQ):** NISQ has been described as the next evolution in quantum computing.[18] Although NISQ is unlikely to completely replace analogue quantum computers, NISQ systems are more capable of tolerating noise, meaning they may require fewer qubits before being commercially viable. While improvements against noise are a design feature of NSIQ systems, noise will still impose limitations on these systems.[19]
- **Fully error-corrected quantum computers:** By using specially designed algorithms and additional qubits, these computers emulate a noiseless system.[20] Because they require additional qubits to correct errors produced by noise, these systems are even more challenging to develop and may take longer to make commercially viable than analogue or NISQ systems. A fully error-corrected system would be able to solve a variety of complex problems and simulations.[21]

Quantum's uses in national security

The possibilities afforded by advanced quantum information technologies may affect some of the most important national security tools and tasks, such as intelligence collection, solution optimization, encryption, stealth technology, computer processing, and communications. Indeed, the diversity of quantum applications across the national security domain warrants some immediate concern, both for how we can harness quantum systems and for how those quantum systems may undercut our security. But the pursuit of quantum systems necessitates advancing an ecosystem of quantum hardware, software, and algorithms, all of which have their own unique scientific, operational, and engineering challenges. So, while some concern is appropriate, too many scientific and technological challenges remain to expect radical change due to quantum technology in the near term. Still, government leaders should be aware of the emerging opportunities, challenges, and threats posed by quantum technology and begin taking steps to prepare for the coming change. Here are some of the areas that will be impacted first:

AT A GLANCE: QUANTUM COMPUTING

What it is: Quantum computers are new machines that leverage quantum principles to compute some complex problems exponentially more quickly that existing computers. They can help solve some complex math and chemistry problems and simulations necessary to advance medicine, engineering, and other areas of science.

What it means: The ability of quantum computers to solve complex optimization problems can help solve many existing national security problems such as logistics/flow to theater optimization or wargaming. Longer-term potential benefits could include opening new frontiers for technology, improving artificial intelligence, and leading to new discoveries in science. However, the use of quantum computers will also likely require the development of new encryption techniques, as many existing techniques may be susceptible to algorithms run on quantum computers.

QUANTUM COMPUTING

Perhaps the most well-known application of quantum science to technology is quantum computing. The speed at which quantum computers will be able tackle some complex problems can offer new possibilities. Quantum computers could be used by defense planners to do large-scale simulations of military deployments, by scientists to model complex chemical reactions to design new materials, or even by computer scientists to crack cryptography or advanced artificial intelligence tools.

While the promise of quantum computing may be large, there is no exact timeline for commercial availability of a general-purpose universal quantum computer.[22] Due to complexities of science and engineering, it is difficult to predict when the first fully functional quantum computer will be available, but steady progress is being made, and some argue it could be within the next few decades.[23]

QUANTUM COMMUNICATIONS

The unique principles of quantum mechanics also offer novel methods for securing communications, collectively known as quantum cryptography or quantum communications. One of the most developed approaches to this is quantum key distribution (QKD), which most often uses attenuated laser pulses to share a classical encryption key between two users. At its core, QKD uses perhaps the oldest cryptographic technology, the shared key to a cypher. What is special about QKD is that it can securely share a key without the possibility of an eavesdropper on the quantum channel stealing it. If an adversary attempts to

intercept and read the quantum key, it will collapse the quantum state, making the intrusion known to both sender and receiver.[24] This does not mean QKD is impenetrable. It still requires that the stations where the sender and receiver operate be secure, and it may still be vulnerable to jamming and certain types of attacks on both the quantum setup or classical encryption, but it does add another layer of protection to extremely sensitive data. Dr. Joshua Bienfang of National Institute for Standards and Technology describes QKD as "sort of like a wax seal on a letter: Security is based on knowing whether someone is eavesdropping on the quantum channel, and this is fundamentally different from classical key-distribution methods."[25]

To date, QKD has been successfully tested using fiber optics and in satellite communications and has even hosted the first quantum-encrypted videoconference.[26] Today, many of a nation's most sensitive secrets, such as nuclear launch codes or sensitive intelligence, are protected via symmetric encryption where both sender and receiver share a key. This can be a nearly unbreakable form of encryption, but it does require the physical exchange of new code sheets or digital keys, often via truck, helicopter, or hand courier. QKD offers one way to speed up the exchange of those keys over long distances while remaining secure, making it well suited for protecting sensitive national security communications.[27]

While there may be great potential for quantum encryption to protect a government's or a company's sensitive secrets, quantum communication's real use may emerge as an enabler for quantum computing. Given the small number of quantum computers likely to exist in the foreseeable future, connecting multiple such computers together could not only improve performance but also increase access to these important quantum tools.[28] While such a network of quantum computers is likely some time off, as it would require the development of new forms of quantum communication far more advanced than today's QKD, it could introduce entirely new uses for quantum computing, much as the internet did while connecting classical computers.

AT A GLANCE: QUANTUM COMMUNICATIONS

What it is: In quantum communications, quantum principles are applied to create new forms of communication systems as well as new methods for securing communications. Quantum communications technology such as QKD is one of the most developed quantum information technologies in use today.

What it means: Most immediate uses will focus on using QKD and other methods to secure sensitive government communications such as in nuclear command and control on from shore to submarines, but long-term uses may center on creation of networks of quantum computers.

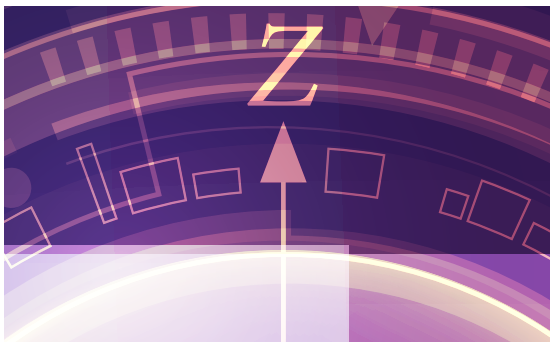
QUANTUM METROLOGY

The second quantum revolution does not end with computing and communications but extends to a variety of measurement activities as well. While we may not give it too much thought, many of our everyday tasks rely on some form of precise measurement: Taking a picture requires measurement of light, while using GPS to get directions requires precise measurement of time. So, quantum's ability to improve such measurement tasks can be a real game changer.

As with computing and communications, the new capabilities of quantum metrology are rooted in the peculiarities of quantum physics. Take quantum radar or light detection and ranging (LIDAR), for

example. Classical radar and LIDAR emit radio waves or light particles and measure their return off an object; then, by comparing the measurement to what was expected, they gather information about the speed and distance of that object. But a pair of entangled quantum particles contains twice the mutual information of a pair of perfectly correlated classical particles (the mutual information of two variables A and B is defined as the amount of information that one obtains about B from the measurement of A). That is, perfect quantum correlations are "stronger" than perfect classical correlations.[29] This means that a quantum radar or LIDAR can use fewer emissions to get the same detection result, allowing for better detection accuracy at the same power levels even for stealth or low observable aircraft, or allowing the radar/LIDAR to operate at much lower power levels that are much harder to detect and jam by an adversary.

The same principle can help improve imagery. Many forms of quantum imagery use entangled particles to measure everything from photons to disturbances in magnetic or gravitational fields. By harnessing the greater information that entangled particles can bring, these methods can be used to help find underground bunkers or submarines hiding in the depths of ocean. These gravitational principles can also be used as quantum gyroscopes, laying the foundation of very accurate inertial navigation systems that don't require jammable external signals from GPS satellites. Many of these use cases are possible using classical methods. There are classical inertial navigation systems or magnetic anomaly detectors, but the use of quantum particles just makes them more sensitive or more effective in a wider array of scenarios.



AT A GLANCE: QUANTUM METROLOGY

What it is: Quantum measurements leverage the highly precise manipulation of particles to detect minute changes in information.

What it means: Quantum metrology can help create new forms of cameras, radars, and other systems. These can provide more capable means of detecting everything from stealth aircraft (quantum RADAR) to submarines (quantum ghost imaging) to underground facilities (quantum gravimetry). Quantum metrology can also help solve many of today's most pressing defense problems by offering new forms of location and timing not reliant on GPS signals that can be easily jammed or spoofed.

What can this mean for national security?

With uses ranging from code-breaking to code-making, and imaging to navigation, quantum information science has clear military and intelligence applications. Moreover, with developed countries such as the United States, China, Russia, Austria, Australia, Canada, the United Kingdom, and commercial companies around the globe investing in quantum research, these defense applications could have significant impact on relative national security.[30] Government leaders, even those in nontechnical positions, should have a basic understanding of quantum systems and the emerging national security challenges so they can take steps to protect information and prepare their organizations, teams, and business practices for the quantum world. Here are some problem areas in national security matters where quantum science can be applied.

LOSS OF SECRETS

Information security is one of the most fundamental elements of national security. Whether it be military plans, advanced technology information, diplomatic cables, personal data, or company data, critical details related to state and business security are embedded in data being shared through public and private networks. If we can't protect this data, we can't expect any reasonable sense of national security. Cryptography is one way in which governments and private companies secure information.

Often, by utilizing highly complex math problems, cryptography can make digital information more or less unusable, unless the party concerned possesses the mathematical solution, known as a key. To decode cryptography without the key would require completing so many computations that it is unfeasible for today's computers, but not for quantum computers.[31] Quantum computers will someday be able to compute complex problems so quickly that some forms of encryption can be broken relatively easily. For even the largest classical computers yet to be built, these problems with sufficiently large crypto keys can take millions of years to solve. However, because of quantum superposition and entanglement, even a relatively slow quantum computer could break the encryption in a matter of hours (assuming an RSA cryptokey of 2,048 bits, a hypothetical 1-petahertz classical computer and a hypothetical 1-megahertz quantum computer).[32] This poses a significant problem for not just governments trying to protect state secrets but also for commercial companies responsible for protecting personal data. The seriousness of the issue seems to become only more apparent when you consider the fact that information can be downloaded today and decrypted later once quantum computers are mature.[33]

Luckily, not all types of encryption can be decoded easily by quantum computers. Many of government's most sensitive secrets are protected by symmetric encryption immune to quantum attacks, and mathematicians and cryptographers are working on improved "quantum-resistant" algorithms that can be used for everyday uses such as telecommunications.

But relying on mathematicians to develop quantum-resistant encryption is not the sole answer. In fact, it may actually be the easy part. In the words of Kania, "the tricky aspect will be implementation. The transition required in updating to new, post-quantum cryptography can be extremely difficult, especially for defense and national security organizations that tend to have a significant proportion of legacy systems."[34] Even once new algorithms are developed, the arduous process of updating keys and adding software patches can take years, if the process is possible at all. Add on top of this the regulatory and technological requirements to continue to support existing types of security, and organizations can face the challenge of having to interweave existing and post-quantum security measures on the same systems. As David Worrall of Cambridge Quantum Computing describes it, post-quantum security "is not a 'drop-in' replacement for existing measures; it likely must lay on top of existing infrastructure, updating key generation, hardware security models, and algorithms to provide additional security."[35]

This may be good news for governments looking to avoid ripping and replacing costly IT infrastructure, but it also means that government leaders need to have a detailed understanding of their data, security needs, and network architecture in order to find the right mix of classical, quantum, and post-quantum security methods. As Dowling puts it, "There is not one simple fix, but a menu of options where price, security, and data transmission distance cannot all be simultaneously optimized. The state of quantum technology is still in flux right now, and this menu will change yearly."[36]

LOSS OF INTELLIGENCE

The loss of one's own secrets is difficult enough to deal with, but when paired with the prospect of losing critical information on an adversary, it can be quite damaging to national security. Quantum communications proposes to protect government from just that. By relying on the collapsing nature of qubits once they are read, quantum communication methods such as QKD aim to make the sending and receiving of sensitive encryption keys potentially immune to undetected interception.

While these communication methods are unlikely to replace the internet or cellphones even in the mid-term, they can be incredibly useful in scenarios such as communicating with submarines. Quantum communication uses blue-green photons, which can travel much farther and deeper in sea water than the radio waves currently used to communicate with submarines.

Taking advantage of the same properties as blue-green photons, quantum LIDAR could also revolutionize underwater warfare. Currently, submarines detect obstacles and other submarines via sonar (an acronym for sound navigation and ranging). Pings from active sonar are the most accurate detection method but give away a submarine's own position. Quantum LIDAR could allow submarines to detect underwater mines and navigate obstacles silently, making submarines much harder to detect and track.[37]

These few uses of quantum technology highlight the challenge in assessing its impact on national security. Depending on the specific use case and the technology used, quantum information science can have radically different impacts. For example, while quantum communications and LIDAR can make submarines more difficult to detect, quantum gravimetry can make them easier to find. As with any technology, quantum is not inherently positive or negative; rather, its impact depends on understanding its strengths and limitations, and using it properly.

How to be ready today for quantum tomorrow

While quantum technology is certain to have a significant impact on national security, there is little clarity about when or how this impact may occur. However, a mix of education, outreach, and basic preparation can turn any organization into a quantum-ready one. Here's what you can do to get there.

TO DO TODAY

Practice good cybersecurity hygiene. No matter what capabilities quantum systems may have in the future, an adversary can't decrypt what they don't have. Staying vigilant about cyber threats, keeping systems patched, encrypting data—all of these activities are still required in a future quantum world. The "mundane" work of keeping information secure just grows in importance in a future quantum world.

Know your data and your systems. At its core, responding to quantum is, as Worrall puts it, "a management problem, not a technical one; it involves a change of mindset from being reactive to being proactive."[38] The first step to proactively managing the impact of quantum is understanding what data you have today, where it is stored, and how it is secured. This includes an inventory of all systems and applications using encryption.[39] As important as knowing your data is knowing how much data your system will be able to handle. New methods for securing data in a quantum world will come with larger data flows, and many current systems differ in their capacity to process larger volumes of data.[40] Managing the problem, then, will require leaders to know what their systems can support and how to incorporate necessary safeguards without overloading their existing infrastructure.

With a clear current picture, leaders can prioritize potential future upgrades to encryption based on how long information needs to remain protected. If

the utility of data expires in a few months, then classical encryption may work even in a quantum world. If information must be protected for years or decades, it should be a high priority to transition to quantum-based or quantum-resistant encryption when those algorithms are proven in the future.[41]

Read. Government leaders can read and educate themselves on the basics of quantum. With a basic understanding of the science and the technology can leaders begin to identify the areas in which their organization could benefit from or be vulnerable to different quantum technologies. After all, who knows the mission better, and who else can tell where an organization is most vulnerable? To identify these risks and opportunities requires at least a basic knowledge of quantum and its emerging technologies.

Professional organizations such as Institute for Electrical and Electronics Engineers (IEEE) and the International Society for Optics and Photonics (SPIE) offer short training courses designed to give government and business leaders an introduction to quantum. Leaders can also take advantage of experts within their organizations to set up internal training or familiarization courses.[42]

BEGIN TODAY, TO BE READY TOMORROW

Support basic research and education. With quantum technology rapidly evolving, government organizations cannot afford to stand still. Rather, they must continue to support basic research, both in quantum science and the mathematical and engineering problems that go along with it. Create an R&D portfolio to help balance core, adjacent, and transformational research bets to help ensure that no future contingency catches the organization off guard.[43] For organizations without R&D portfolios, supporting general education in quantum information sciences can be an important contribution to ensuring a knowledgeable workforce can be in place when needed.

Connect. Quantum is still in its early stages; even programming a simple application for a quantum computer requires detailed knowledge of quantum mechanics. As a result, government leaders should not try to go it alone. They should connect with experts from government, industry, and academia to create a quantum innovation ecosystem.[44] Sharing information, problems, and solutions across this group will enhance the ability of all of its members to meet the challenges of quantum. Western defense advantage has been built on the free flow of ideas and technology for decades—even the SR-71 was built with titanium from the Soviet Union at the height of the Cold War.

Make connections with private industry and academia that are working on quantum research and uses. Also connect with companies looking at other applications, and figure out how to integrate these into different use cases. Reach out to academics doing research into quantum physics, mathematics, and engineering (especially around cryogenics). Finally, don't overlook the resources within government—such as NASA, the Naval Research Lab, and other national labs—as well as those of allied governments such as the United Kingdom, Canada, and Australia.

Begin planning. Finally, with the right background knowledge, connections, and preparation through workshops, government leaders can begin to explore how to best implement changes. This planning can pay dividends as new quantum technologies begin to come online and the organization is already primed with knowledge of how to put them to use. Creating a quantum "team of interest" can help organizations keep abreast of those new developments and advocate for including quantum in strategic planning meetings.[45] Bring quantum into the strategic planning process, integrating its potential challenges and opportunities into thinking about how the organization will execute its mission in the coming quantum world.

The planning process should also not end at the front door of the organization. Success with quantum will require collaboration across scientists, software developers, hardware manufacturers, and end users, so planning should, too. Bringing these participants together in regular planning workshops can help prepare your organization and determine how best to work with other public and private organizations. Where appropriate, sharing the findings of these workshops publicly can generate further interest and opportunities for collaboration.

Quantum technology is evolving quickly but is still in its early stages. While we can be sure that it will have a fairly significant impact on national security, even leading experts today are unsure exactly what that impact will be and when will it occur. But, even amidst this uncertainty, or perhaps even because of it, government leaders should begin thinking about and preparing today for the quantum-enabled world of the future. Tomorrow's security depends on today's preparedness.

Appendix

SUPERPOSITION

Superposition describes a particle's ability to exist across many possible states at the same time. To understand it simply, instead of a particle, imagine a coin. If the coin is just lying flat on a table, it will be either clearly heads or tails. That is like a classical *bit* of information—it can be either 0 or 1, off or on. Now imagine the coin spinning on edge. It is not clear if it is heads or tails. It appears to be both at the same time. That is like a quantum bit or *qubit*. Because a qubit can be either 1 or 0 or both 1 and 0, quantum computers can test multiple values simultaneously. Superposition, therefore, enables them to make certain types of computations exponentially faster than even the most advanced traditional computers in operation today.[46]

ENTANGLEMENT

Another complex principle of quantum mechanics is "entanglement." Quantum entanglement refers to a situation in which two or more particles are linked and share properties despite any potential distance between them. Drawing on the coin analogy, entanglement would then be akin to flipping a coin located in Texas and having another coin located in Japan flipped in exactly the same manner, at exactly the same time, and for the same duration. Applied in technology, entanglement provides a host of novel applications—from new ways of detecting interference in the flow of point to point communications, to the detection of stealthy platforms such as military aircraft and submarines, among others. Entanglement is also critical to the function of quantum computers because entangled qubits are necessary to reduce the number of logic operations associated with computing a given problem, which enables quantum computers to solve complex problems more quickly.[47]

QUANTUM OBSERVATION

If trying to understand superposition and entanglement wasn't hard enough, these quantum states can only exist so long as they aren't fully observed. "Observing" the quantum state, also called measuring, extracts information from the quantum system and results in the collapse of the system.[48] To illustrate this with the coin example, measuring qubits is akin to slapping the spinning coins down flat on the table. They can now be easily read, but they are also no longer spinning, that is, they are no longer in a quantum state.[49]

Endnotes

1. Alan Taylor, "1964: The New York world's fair," *Atlantic*, June 2, 2014.
2. Scott Aaronson, "Why Google's Quantum Supremacy Milestone matters," *New York Times*, October 30, 2019.
3. Marco Lanzagorta (research physicist, US Naval Research Laboratory), interview with authors, October 18, 2019.
4. California Institute of Technology, "Quantum behavior," Feynman Lectures on Physics, 2013.
5. Sara Gamble, "Quantum Computing: What It Is, Why We Want It, and How We're Trying to Get It," *Frontiers of Engineering: Reports on Leading-Edge Engineering from the 2018 Symposium (2019)* (Washington DC: National Academy of Engineering, 2019).
6. Elsa B. Kania (Center for a New American Security and Harvard University), interview with authors, October 10, 2019.
7. Marco Lanzagorta interview.
8. Elsa B. Kania interview.
9. Klon Kitchen, *Quantum science and national security: A primer for policymakers*, The Heritage Foundation, February 5, 2019.
10. National Academics of Sciences, Engineering, and Medicine, *Quantum Computing: Progress and Prospects* (Washington DC: The National Academics Press, 2019).
11. The Qubit Report, "Using your beats to cancel the noise," May 27, 2019.
12. National Academics of Sciences, Engineering, and Medicine, *Quantum Computing: Progress and Prospects*; The Qubit Report, "Tough errors are no match: Optimizing the quantum compiler for noise resilience," September 17, 2019.
13. Jonathan Dowling (Louisiana State University), interview with authors, October 24, 2019. Jonathan Dowling suggested a million qubits would be necessary to develop a quantum computer capable of cracking RSA public key encryption.
14. Ibid.
15. Ibid.
16. Ibid.
17. Arthur Herman and Idalia Friedson. "Quantum computing: How to address the national security risk," Hudson Institute, August 6, 2018, p. 8; National Academics of Sciences, Engineering, and Medicine, *Quantum Computing: Progress and Prospects*.
18. John Preskill, "Quantum computing in the NISQ era and beyond," *Quantum* 2 (2018): p. 79.
19. Ibid., p. 5.
20. National Academics of Sciences, Engineering, and Medicine, *Quantum Computing: Progress and Prospects*, pp. 38 and 71.
21. Ibid., p. 52.

22. Elsa B. Kania and John K. Costello, "Quantum hegemony? China's ambitions and the challenge to U.S. innovation leadership," Center for a New American Security, September 12, 2018; National Academics of Sciences, Engineering, and Medicine, *Quantum Computing: Progress and Prospects*.
23. Kitchen, *Quantum science and national security: A primer for policymakers*.
24. Emerging Technology from the arXiv. "Chinese satellite uses quantum cryptography for secure videoconference between continents," *MIT Technology Review*, January 30, 2018.
25. Dr. Bienfang (National Institute for Standards and Technology), interview with authors, October 31, 2019.
26. Quantum Xchange, "Quantum Xchange tests Toshiba's Quantum Key Distribution System; doubles network capacity with optical multiplexing," April 25, 2019; Institute of Physics, "Study proves viability of quantum satellite communications," Phys.org, June 6, 2017.
27. Jonathan Dowling interview.
28. Marco Lanzagorta interview.
29. The mutual information of two variables A and B is defined as the amount of information that one obtains about B from the measurement of A. For more see: "The future of quantum sensing & communications," https://www.youtube.com/watch?v=5uqiQ_mP3PM, posted September 1, 2018.
30. Ibid.; Kitchen, *Quantum science and national security: A primer for policymakers*.
31. National Academics of Sciences, Engineering, and Medicine, *Quantum Computing: Progress and Prospects*.
32. Marco Lanzagorta interview: The current limitation on quantum computers is not the speed of the processor, but rather how many entangled qubits can be used. Current machines operate at about 100 qubits, but to achieve the code breaking we describe in the text would require around 1,000.
33. Andreas Baumhof, "The perfect 'harvest now - decrypt later' attack—or how to steal 10 billion USD in bitcoin with a quantum computer," Linkedin.com, May 30, 2019.
34. Elsa B. Kania interview.
35. David Worrall (Cambridge Quantum Computing), interview with authors, November 1, 2019.
36. Jonathan P. Dowling and Michael J. Dowling, "Quantum computing: Dream or nightmare," *CIO review*, accessed January 22, 2020.
37. "The future of quantum sensing & communications."
38. David Worrall interview.
39. Arthur Herman, *The executive's guide to quantum computing and quantum-secure cybersecurity*, Hudson Institute, March 2019.
40. David Worrall interview.
41. Cloud Security Alliance, *Preparing enterprises for the quantum computing cybersecurity threats*, May 2019.
42. Michele Mosca and Bill Munson, "The quantum threat to cyber security," Centre for International Governance Innovation, accessed January 7, 2020.
43. Alan Holden et al., *Developing innovation portfolios for the public sector: Portfolios for public good*, Deloitte Insights, August 15, 2018.
44. Gerald C. Kane, *Accelerating digital innovation inside and out: Agile teams, ecosystems, and ethics*, Deloitte Insights, June 4, 2019.

45. Jonathan Dowling interview.
46. Gamble, "Quantum Computing: What It Is, Why We Want It, and How We're Trying to Get It."
47. National Academies of Sciences, Engineering, and Medicine, *Quantum Computing: Progress and Prospects*.
48. Ibid., p. 26.
49. Ibid., p. 26.

Acknowledgments

The authors owe a special debt to the experts who contributed to this report: **Dr. Marco Lanzagorta**, US Naval Research Lab; **Elsa Kania**, Center for a New American Security; **Dr. Jonathan Dowling**; Louisiana State University; and **Dr. Joshua Bienfang**, National Institute for Standards and Technology.

We also must thank the dedicated team that helped bring the article to life: **Aditi Rao** and **Blythe Hurley** of Deloitte Services LP.

About the authors

Scott Buchholz | sbuchholz@deloitte.com

Scott Buchholz is a managing director with Deloitte Consulting LLP and serves as the chief technology officer for the Government and Public Services practice and the National Emerging Technologies research director. A leader and visionary with more than 20 years' experience in consulting, Buchholz advises clients on implementing technology innovations, solution architecture, and legacy systems modernization to transform their businesses, increase IT productivity, and improve customer experience.

Joe Mariani | jmariani@deloitte.com

Joe Mariani leads research into defense, security, and law enforcement for Deloitte's Center for Government Insights. His research focuses on innovation and technology adoption for both national security organizations and commercial businesses. His previous work includes experience as a consultant to the defense and intelligence industries, high school science teacher, and Marine Corps intelligence officer.

Adam Routh | adrouth@deloitte.com

Adam Routh is a research manager with Deloitte's Center for Government Insights and a PhD student in the Defence Studies Department at King's College London. His research areas include emerging technologies, defense, and security with a focus on space policy. Routh previously worked for the Defense Program at the Center for a New American Security (CNAS). Prior to CNAS he worked in the private sector where he facilitated training for Department of Defense components. He also served as a team leader with the US Army's 75th Ranger Regiment.

Akash Keyal | akeyal@deloitte.com

Akash Keyal is a senior research analyst with the Deloitte Center for Government Insights. He focuses on delivering key insights on topics related to defense, security, and justice.

Pankaj Kishnani | pkamleshkumarkish@deloitte.com

Pankaj Kishnani of Deloitte Services LP is a researcher with the Deloitte Center for Government Insights. He specializes in emerging trends in technology and their impact on the public sector.

Contact us

Our insights can help you take advantage of change. If you're looking for fresh ideas to address your challenges, we should talk.

Industry leadership

Scott Buchholz
Chief technology officer, Government & Public Services | Managing director | Deloitte Consulting LLP
+ 1 571 814 7110 | sbuchholz@deloitte.com

Scott Buchholz is a managing director with Deloitte Consulting LLP, with more than 20 years' experience advising clients on implementing technology innovations, solution architecture, and legacy systems modernization.

Center for Government Insights

Joe Mariani
Manager | Center for Government Insights
+ 1 240 731 1985| jmariani@deloitte.com

Joe Mariani leads research into defense, security, and law enforcement for Deloitte's Center for Government Insights. His research focuses on how government agencies can cultivate innovation and emerging technologies.

About the Deloitte Center for Government Insights

The Deloitte Center for Government Insights shares inspiring stories of government innovation, looking at what's behind the adoption of new technologies and management practices. We produce cutting-edge research that guides public officials without burying them in jargon and minutiae, crystalizing essential insights in an easy-to-absorb format. Through research, forums, and immersive workshops, our goal is to provide public officials, policy professionals, and members of the media with fresh insights that advance an understanding of what is possible in government transformation.

Deloitte.
Insights

Sign up for Deloitte Insights updates at www.deloitte.com/insights.

Follow @DeloitteInsight

Deloitte Insights contributors
Editorial: Aditi Rao, Aparna Prusty, Blythe Hurley, and Rupesh Bhat
Creative: Sonya Vasilieff
Promotion: Alexandra Kawecki
Cover artwork: Sonya Vasilieff

About Deloitte Insights

Deloitte Insights publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.

Deloitte Insights is an imprint of Deloitte Development LLC.

About this publication

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or its and their affiliates are, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

None of Deloitte Touche Tohmatsu Limited, its member firms, or its and their respective affiliates shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.