Keeping America's Infrastructure Safe

with Quantum Technologies

leidos

Quantum technologies are quickly moving out of the lab and into the government sector. In preparation, what do public sector leaders need to know about cybersecurity and quantum technologies?

Hype from Hollywood and pop-culture magazines often creates confusion surrounding quantum sciences — leaving physicists to pick up the pieces and demystify in the aftermath.

Quantum technology, a subfield of quantum sciences, encompasses everything from quantum computers to laser pointers. This broad definition expands to touch upon any technology that leverages quantum mechanics or quantum physics — think global positioning systems (GPS), magnetic resonance imaging (MRIs) and even the transistors in classical computer chips.

For Dr. Elizabeth Iwasawa, Leidos' Quantum Technology Lead and Research Scientist, quantum technologies deal with our world, but on a much smaller scale.

"The biggest revolution enabled by quantum mechanics that everyone's familiar with was the development of solid state transistors, which are part of what allowed us to go from having really big, bulky electronics to the sleek technology we use today," says Iwasawa. "Understanding solids at the quantum level enabled electronic components to become smaller, faster and more powerful."

Unlike the hype surrounding this science, it's doubtful that we'll one day wake up in a post-quantum world: Instead, much like the evolution of mobile devices, it will be gradual as new capabilities debut. Leaders should be tracking the shifts in their threat landscapes, which could include a sudden breakthrough in quantum computing.

"It's key to avoid suddenly needing to update your encryption, digital signatures, and your standards in order to adapt to a different world enabled by quantum computing," Iwasawa explains.

Fortunately, as quantum technologies move out of the lab and into the public sector, cyber defenders will have an array of tools that can help them successfully defend and protect their data.

One such example is the development of quantum-resilient algorithms, debuted by the National Institute of Standards and Technology in July of this year. NIST's quantum-resilient algorithms are a promising development for agencies and their private sector partners.

"Our post-quantum cryptography program has leveraged the top minds in cryptography — worldwide — to produce this first group of quantum-resistant algorithms that will lead to a standard and significantly increase the security of our digital information," says NIST Director Laurie E. Locascio.

Although quantum computers seem a long way off, NIST standards will debut in 2024. With this in mind, agencies shouldn't put quantum technologies on the back burner. As Iwasawa points out, the global RSA rollout was expected to take ten years but instead took twenty. Therefore, now is the time for agencies

---

"Research what's coming, understand how it will impact your mission, and start preparing now."

—

Meghan Good

Director of the Cyber Accelerator at Leidos

and their partners to begin inventorying, prioritizing and preparing systems for migration, even if the first cryptographically-relevant quantum computer isn't expected for another ten to twenty years.

"Inventorying, prioritizing, and migrating all systems to a new encryption standard will take time and have far-ranging impacts on network speeds, storage, compute time, and budgets. Not to mention agencies will need to tackle far-reaching dependencies and institute mitigation strategies for legacy systems that cannot be migrated," says Iwasawa.

DON'T FEAR THE CRYPTOPOCALYPSE

When the discussion turns toward quantum computing, the next question often involves how this will affect standard encryption. Standard encryption keys are 256-bits long and use symmetric or asymmetric key algorithms. These keys work because they would take a classical computer too long to break, but do not pose the same challenge to a quantum computer.

Enter the cryptopocalypse, a catchy title for a mythological date when all of the government's data and military secrets will be ripe for the picking. In reality, only certain encryption types are vulnerable, like RSA, but these types are also the most widely used ones.

Quantum communications technologies hold immense promise in helping analysts see into their networks and defend in real-time. For example, it can be challenging to detect man-in-the-middle attacks on classical systems, but using quantum communications systems, it is easy to tell when someone is eavesdropping.

"They're still susceptible to man-in-the-middle attacks, but you get this extra bonus based on the laws of physics. It's almost impossible to hide that you're eavesdropping," says Iwasawa. "You can tell live. You don't have to wait for an entire transmission to end."

One of the reasons it's easy to tell a spoofed signal from the real one is because of qubits — minuscule two-state quantum systems that make up quantum computers and communications capabilities. Qubits, or quantum bits, are so fragile that when they interact with classical bits and bytes, they lose their "quantum" status as they become classical in nature.

Unlike traditional particles, quantum systems can be in a state of superposition. Superposition allows the particle to be in a linear superposition of states, meaning the bit can be 30% up and 70% down. This differs from traditional bits that are relegated to either being up or down at one fixed position in time.

Superposition, however, makes these qubits incredibly fragile. Iwasawa likens their fragility to if your cellphone lost wifi everytime you interacted with it. Qubits and quantum computing operate under a similar fragility.

So, when an eavesdropper interacts with the network, the qubits, in this case photons, react.

"Any interaction with the environment will make the qubit look classical again," says Iwasawa. And it's this change that can tip off security analysts to potential threat actors on the network.

With this improved approach to visibility, quantum technologies will be a crucial tool in helping cyber analysts close the gap between the discovery of a potential breach and its remediation.

However, despite the benefits of quantum technologies, government organizations may still have to wait five to ten years as the intricacies of quantum technologies are fleshed out. So, in the meantime, how can federal, defense and SLG leaders ready their teams to leverage quantum to secure their digital ecosystems?

For Meghan Good, Director of the Cyber Accelerator at Leidos, the answer is simple — research what's coming, understand how it will impact your mission, and start preparing now.

PREPARING FOR THE POST-QUANTUM FUTURE

With terms like superposition and entanglement, the field of quantum sciences can often seem like an entirely different language. And for government decision-makers researching quantum technologies, it can be challenging to discern hype from fact, as mentioned at the beginning of this piece. Therefore, government leaders should reach out to internal and external experts in the field of quantum technologies — ask them about what they're seeing and how that could apply to the federal government. With that being said, the inverse also applies. Physicists and scientists

should look at shaping their research toward initiatives that will help government agencies better protect and secure their data.

In short, collaboration is the key to preparing for a post-quantum future. "I think the sooner folks start on that learning journey, the better," Good explains.

Research, however, doesn't mean leaders have to understand the intricacies of Schrodinger's equation; instead, it requires agencies to have an open mind as they approach the research process. What capabilities does your organization want to see? Are there any threats that are specific to your agency?

The good thing about quantum technology is that it's in its nascent stages, so public sector organizations can work alongside physicists and scientists to address these questions and build out more secure solutions.

"A lot of people sort of wave their hands and say that quantum is very strange and complicated, but you don't need to have a Ph.D. to make an impact," says Iwasawa.

"A lot of people sort of wave their hands and say that quantum is very strange and complicated, but you don't need to have a Ph.D. to make an impact."

—

Dr. Elizabeth Iwasawa
Quantum Technology Lead and Research Scientist at Leidos

Connect with the top minds at Leidos to learn more about quantum technologies.

leidos

#22-Leidos-0913-24907