The realist's guide to quantum technology and national security

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.[1] The diversity of quantum applications across the national security domain warrants some immediate attention from governments, both for how they can harness quantum systems and for how those quantum systems may undercut national security.

One major national security concern is that quantum computers will someday be able to relatively easily break many current forms of encryption.[2] Although cryptographers are working on "quantum-resistant" algorithms that can be used to replace existing algorithms, the hard part will be implementation. Elsa Kania, adjunct senior fellow at the Center for a New American Security, notes that "the transition required in updating to new, postquantum cryptography can be extremely difficult, especially for defense and national security organizations that tend to have a significant proportion of legacy systems."[3]

On the flip side, quantum communications and quantum detection technology can improve existing capabilities. Quantum communications should be able to better protect government from losing sensitive information by creating communication methods that are potentially immune to undetected interception. These methods can also be useful in scenarios such as communicating with submarines: Some forms of quantum communications use blue-green photons, which can travel much farther and deeper in seawater than radio waves.

Other forms of quantum technology can also have a big impact on national security. For example, taking advantage of the same properties of blue-green photons, quantum LIDAR could allow submarines to detect and navigate obstacles silently, making submarines much harder to detect and track than today's, which must use noisy active sonar for the same purposes.[4]

The diversity of **quantum applications** across the national security domain warrants some immediate attention from governments, both for how they can harness quantum systems and for how those quantum systems may undercut national security.

Governments can consider taking several steps to proactively prepare for the advent of pragmatically viable quantum information technologies:

- **Educate yourself.** With a basic understanding of the science and the technology, leaders can begin to identify the areas where their organizations can benefit from or be vulnerable to different quantum technologies.
- **Practice good cybersecurity hygiene.** No matter what capabilities quantum systems may have in the future, an adversary can't decrypt information they don't have.
- **Know your data and your systems.** Managing data in the quantum era will require leaders to know what data their systems maintain and how to incorporate necessary safeguards without overloading their infrastructure.
- **Support basic research and education.** Governments can create an R&D portfolio to help balance core, adjacent, and transformational research bets to help ensure that no future contingency catches them off guard.[5]
- **Connect with others.** Government leaders should connect with experts across government, industry, and academia to help create a quantum innovation ecosystem that can enhance the ability of all of its members to meet quantum's challenges.[6]
- **Begin planning.** Finally, with the right background knowledge, connections, and preparation through workshops, government leaders can begin to explore how to best implement changes. They should 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.

To learn more, read the full article, *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,* on www.deloitte.com/insights/quantum-tech-national-security.

The realist's guide to quantum technology and national security

page 94

1. Scott Aaronson, "Why Google's quantum supremacy milestone matters," *New York Times*, October 30, 2019.
2. Duncan Stewart, "Quantum computers: The next supercomputers, but not the next laptops," *Deloitte TMT Predictions 2019*, Deloitte Insights, December 11, 2018.