

Quantum Computing Takes a Leap: Can Cyber Security Keep Up?

Kari Currence

On February 19, 2025, Microsoft unveiled its Majorana 1 chip, a groundbreaking advancement in the field of quantum computing.¹ According to Microsoft, this chip utilizes a topoconductor, known as a topological superconductor, which can create an entirely new state of matter.² This topological state of matter is used to produce more stable qubits, the units that quantum computers use to store data.³

While this marks a significant milestone in the quest for large-scale quantum computing, it also raises urgent concerns about cybersecurity. Quantum computing holds immense potential for a wide range of industries, from healthcare and finance to logistics.⁴ However, the same power that makes quantum computers so transformative also poses a serious risk to the cybersecurity frameworks that underpin our digital world. For example, encryption tools that are widely used rely on complex math problems to protect electronic information.⁵ Unlike classical computers, which are limited in their ability to process complex data, quantum computers can solve these problems exponentially faster.⁶ This means that quantum computers could break these systems very quickly, exposing sensitive information to cyberattacks and theft.⁷

This rapid leap in computational power highlights the need for swift legal and regulatory adaptation.⁸ As quantum computing becomes more advanced, American lawmakers face a critical

¹ Chetan Nayak, *Microsoft unveils Majorana 1, the world's first quantum processor powered by topological qubits*, MICROSOFT (Feb. 19, 2025), <https://azure.microsoft.com/en-us/blog/quantum/2025/02/19/microsoft-unveils-majorana-1-the-worlds-first-quantum-processor-powered-by-topological-qubits/>; Catherine Bolgar, *Microsoft's Majorana 1 chip carves new path for quantum computing*, MICROSOFT (Feb. 19, 2025) <https://news.microsoft.com/source/features/ai/microsofts-majorana-1-chip-carves-new-path-for-quantum-computing/>.

² Catherine Bolgar, *Microsoft's Majorana 1 chip carves new path for quantum computing*, MICROSOFT (Feb. 19, 2025) <https://news.microsoft.com/source/features/ai/microsofts-majorana-1-chip-carves-new-path-for-quantum-computing/>; Cade Metz, *Microsoft Says It Has Created a New State of Matter to Power Quantum Computers*, THE NEW YORK TIMES (Feb. 19, 2025) <https://www.nytimes.com/2025/02/19/technology/microsoft-quantum-computing-topological-qubit.html>.

³ Bolgar, *supra* note 2; Chuck Brooks, *Quantum Computing Has Arrived; We Need to Prepare For Its Impact*, FORBES (Feb. 22, 2025) <https://www.forbes.com/sites/chuckbrooks/2025/02/22/quantum-computing-has-arrived-we-need-to-prepare-for-its-impact/>.

⁴ *What Is Post-Quantum Cryptography?*, NAT'L INST. OF STANDARDS AND TECH. (Dec. 20, 2024) <https://www.nist.gov/cybersecurity/what-post-quantum-cryptography>; Catherine Bolgar, *Microsoft's Majorana 1 chip carves new path for quantum computing*, MICROSOFT (Feb. 19, 2025) <https://news.microsoft.com/source/features/ai/microsofts-majorana-1-chip-carves-new-path-for-quantum-computing/>.

⁵ *NIST Releases First 3 Finalized Post-Quantum Encryption Standards*, NAT'L INST. OF STANDARDS AND TECH. (Aug. 13, 2024) <https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards>.

⁶ *Id.*

⁷ *What Is Post-Quantum Cryptography*, *supra* note 4.

⁸ Gail L. Gottehrer, *International Data Privacy Compliance, Professional Perspective – The Challenges of Quantum Computing for Reasonable Security Compliance*, BLOOMBERG LAW (Apr. 2021),

challenge: how to respond to the disruptive potential of quantum computing before it becomes a security crisis. The National Institute of Standards and Technology (NIST) has already released several post-quantum encryption algorithms that are designed to withstand cyberattacks from quantum computers.⁹ However, widespread adoption of these new standards is essential.

As quantum computers render current encryption methods obsolete, cybersecurity laws must evolve to address these emerging quantum technologies. Existing cybersecurity laws and privacy regulations, such as the California Consumer Privacy Act (CCPA) and the New York Stop Hacks and Improve Electronic Data Security Act (SHIELD Act), may no longer be robust enough to address the new risks posed by quantum computing.¹⁰ Lawmakers will need to ensure that businesses and organizations adopt quantum-resistant encryption techniques and safeguard consumer data from emerging threats. Without timely legal action, quantum computing could lead to a wave of privacy violations and cybersecurity breaches that current laws are ill-equipped to handle.

<https://www.bloomberglaw.com/external/document/X24KPL64000000/international-data-privacy-compliance-professional-perspective-t>.

⁹ *NIST Releases First 3 Finalized Post-Quantum Encryption Standards*, NAT'L INST. OF STANDARDS AND TECH. (Aug. 13, 2024) <https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards>.

¹⁰ Gottehrer, *supra* note 8.