ISSUE 9

THIS WEEK IN QUANTUM SECURITY

By
Joel Van Dyk
Quantum Security Advisor and Strategist

July 31, 2026

This week produced an unusually broad mix of developments across quantum computing and quantum security. Anthropic demonstrated that advanced AI can contribute meaningfully to cryptanalysis, AT&T expanded its operational use of D-Wave's quantum technology, new enterprise research exposed the continuing gap between awareness and implementation, and the August calendar began to fill with conferences, technical workshops and corporate results.

The common thread is not that a cryptographically relevant quantum computer has suddenly arrived. It has not. The important change is that quantum is increasingly being discussed through practical outcomes: weaknesses found, workloads accelerated, certificates deployed, migration plans developed and systems tested. For people working in the sector, the conversation is becoming more operational and more global. More momentum.

The Week's Key Developments

Anthropic uses Claude to uncover new cryptographic weaknesses

The most significant quantum-security development this week came from Anthropic, whose researchers used Claude Mythos Preview to develop improved attacks against two cryptographic constructions. The first substantially weakens HAWK, a digital-signature scheme designed for a post-quantum environment in NIST's 3rd round of calls for quantum resistant cryptographic algorithms. The second presents a new attack on a reduced-round version of AES, the symmetric cipher used widely throughout digital systems.

The distinction between the research result and some of the surrounding headlines is important. Anthropic states that neither attack affects production systems today, and the work does not mean that deployed AES encryption has been broken. It does have another chink its armor. The real importance lies in demonstrating that frontier AI models can help researchers explore difficult cryptanalytic problems, improve existing attacks and identify weaknesses that had not previously been found. Anthropic also disclosed the findings to the relevant algorithm teams before publication. (Anthropic).

For the quantum-security community, this widens the discussion. Organizations have understandably concentrated on protecting cryptography against future quantum computers, but the Anthropic research suggests that AI-assisted cryptanalysis may also accelerate the rate at which cryptographic

assumptions are tested. It reinforces the need for cryptographic agility, careful implementation and continuing evaluation after an algorithm has been selected.

AT&T expands its use of D-Wave after an operational trial

D-Wave and AT&T announced an expanded agreement covering the use of quantum computing across AT&T's network operations. In an early application, AT&T reduced the processing time for a network-optimization workload from approximately one hour to less than 15 seconds. The company will now explore applications including outage response, technician routing, network-build planning and traffic management. (D-Wave Quantum)

The announcement attracted attention because quantum-computing stocks rallied. But, the more useful industry signal is the move from a limited application towards broader operational testing. AT&T plans to integrate D-Wave's annealing technology with tools already supporting its agentic-AI operations. It is also evaluating D-Wave's forthcoming gate-model systems for potential applications in quantum security and communications. (D-Wave Quantum)

The companies' language should still be read carefully. AT&T attributed a reduction of 12 million hours of customer downtime in 2025 to its wider agentic network tools, not solely to D-Wave. Nevertheless, the agreement provides a concrete example of quantum optimization being assessed against enterprise performance rather than only laboratory benchmarks. (D-Wave Quantum)

Enterprise awareness is rising faster than deployment

New research reported by IT Pro found that 85% of surveyed IT and security leaders expect quantum advances to break existing security standards within a decade, yet only 7% said their organizations had deployed quantum-safe certificates. More than 80% believed at least some of their encrypted data was already exposed to "harvest now, decrypt later" risk. (IT Pro)

The implementation picture is more nuanced than the headline numbers suggest. Nearly nine in ten respondents said their organizations were planning, testing or implementing post-quantum initiatives. Half had carried out quantum-risk assessments, 45% had developed transition plans and 44% had created cryptographic inventories. The persistent difficulty is not awareness but the complexity of changing cryptography across legacy applications, hybrid environments and edge infrastructure. (IT Pro)

The research also provides a useful geographical comparison. The United Kingdom had the largest proportion of organizations describing themselves as leading-edge at 18%, followed by the United States at 17% and Australia at 10%. These remain self-reported readiness measures, but they help show how uneven the transition remains even among relatively advanced markets. (IT Pro)

Digital-asset security continues to attract institutional funding

Financial institutions and digital-asset companies are allocating more money to Bitcoin and blockchain quantum readiness. Barron's reported that BlackRock, ARK Invest and Fidelity are supporting a Bitcoin Security Consortium that has pledged $15 million over three years, while Galaxy Digital is pursuing a separate Bitcoin Quantum Readiness Initiative involving grants and advisory work. (Barron's)

The immediate risk to Bitcoin is not that a quantum computer can break it today. The practical problem is that migration in decentralised systems requires agreement among wallet providers, custodians, exchanges, developers, miners or validators and asset owners. That coordination can take considerably

longer than deploying a new cryptographic library within a single organization. In fact in the Bitcoin world that agreement is hard to come by, if at all.

> *Full disclosure:* Project Eleven is a client. I include this development because its work on understanding and prioritizing quantum exposure in digital assets sits directly within this coordination problem. The broader lesson is relevant well beyond blockchain: organizations cannot build a credible migration plan until they know which assets are exposed, how the cryptography is being used and who has authority to change it.

Global Signals

North America

The United States continues to combine government deadlines with commercial investment. The June executive order on advanced cryptographic attacks set a deadline of 31 December 2030 for federal agencies to transition their most sensitive encryption systems, followed by a 31 December 2031 deadline for post-quantum authentication. It also brings federal contractors into scope for post-quantum FIPS requirements by the end of 2030. (The White House)

This week's D-Wave and AT&T agreement shows the commercial side of that movement, while Anthropic's work illustrates how AI laboratories are becoming relevant participants in cryptographic research. Black Hat USA begins in Las Vegas on 1 August, providing an immediate opportunity to watch whether AI-assisted vulnerability discovery and post-quantum migration become more prominent within the wider cybersecurity agenda. (Black Hat)

United Kingdom and Europe

The United Kingdom performed comparatively well in the latest enterprise-readiness survey, but the deployment of quantum-safe certificates remains low across the overall respondent base. That gap between planning and live implementation is likely to remain one of the most important measures of progress. (IT Pro)

Across Europe, regulation and certification continue to drive the market. France has said it will stop certifying security products that lack quantum-resistant encryption from 2027, with broader migration expectations extending towards 2030. The policy is particularly relevant to vendors serving government, banking and critical infrastructure because it converts quantum readiness from a voluntary roadmap into a product-access and procurement issue. (Reuters)

Asia

China hosts the fifth CCF Quantum Computing Conference in Shenzhen from 2 to 5 August, followed by the International Conference on Quantum Computing and Communication Technology in Hangzhou from 7 to 9 August. Later in the month, KAIST will host the Asian Quantum Information Science Conference in Daejeon, South Korea, from 24 to 28 August. (Quantum Technology)

These meetings span computing, communication and foundational research rather than focusing exclusively on security, but they are worth watching because advances in hardware, networking and error correction will continue to influence estimates of the cryptographic risk horizon.

Australia

Australia remains one of the more established quantum markets outside North America, Europe and East Asia. The current readiness data places it behind the United Kingdom and United States in the proportion of organisations identifying themselves as leading-edge, although it remains among the countries specifically highlighted in the survey. (IT Pro)

An August meeting hosted by the Australian Research Data Commons will examine the effect of quantum technology on AI, cryptography, federated machine learning and the Australian quantum workforce. The event is useful because it reflects the same convergence highlighted by Anthropic's research: quantum, AI and data security are becoming increasingly difficult to treat as separate disciplines. (ARDC)

Africa

Publicly visible commercial quantum-security announcements remain less frequent across Africa, but research, training and standards participation are growing. Ghana hosted the African International Conference on Quantum Computing and Simulation earlier this year, while Morocco has also hosted quantum-computing and information-technology training. These initiatives are important because Africa's participation cannot begin only after standards and commercial supply chains have been established elsewhere. (Quantum Technology)

The next significant event to watch is the ITU Global Quantum Drill in Dubai in September. It will be preceded by meetings of the ITU-T Study Group 17 regional groups for Africa and the Arab region. The drill will allow governments, national incident-response teams and technical organizations to test coordination through simulated quantum-related cybersecurity scenarios. Travel-support applications close on 10 August. (ITU)

Middle East

The UAE Cyber Security Council will host the ITU Global Quantum Drill on 17 and 18 September at Expo City Dubai. Unlike a conventional conference, the event is designed around preparedness exercises, coordination mechanisms and practical experience with quantum-safe communications. Participation is open to ITU members, academic institutions and relevant technical teams, with a particular emphasis on national CERTs and incident-response authorities. (ITU)

Latin America

Brazil will host the Quantum Thermodynamics Conference in Natal from 10 to 14 August. Although it is primarily a scientific meeting rather than a security conference, its inclusion matters because a genuinely global view of the quantum sector must follow foundational research as well as commercial and regulatory developments. (Quantum Technology)

Research Worth Reading

Anthropic, "Discovering cryptographic weaknesses with Claude." This is the essential paper and accompanying explanation for the week. It describes the improved attack on HAWK and the work on reduced-round AES, while clearly stating the limits of the results and their lack of impact on current production systems. (Anthropic)

"Measurement Study of Post-Quantum Readiness of Internet: 2026." The researchers examined 32,011 domains and found that 49.3% supported hybrid post-quantum key exchange, but none used hybrid post-quantum certificates. The result suggests that key exchange is progressing faster than authentication, leaving an important gap in end-to-end migration. (arXiv)

"Toward Quantum-Safe 6G: Experimental Evaluation of Post-Quantum Cryptography Techniques." This study assesses ML-KEM, ML-DSA and Falcon in wireless and resource-constrained environments. It finds that computational performance can be acceptable, while larger ciphertexts and signatures create challenges for bandwidth, handshake reliability and edge deployment. (arXiv)

"Securing Cryptography in the Age of Quantum Computing and AI." This review is particularly timely after the Anthropic announcement because it considers quantum attacks and AI-enhanced cryptanalysis together. Its central conclusion is that no single cryptographic approach addresses both sets of threats, making implementation hardening and crypto-agility essential. (arXiv)

Meetings and Events to Watch

1–6 August — Black Hat USA, Las Vegas. Training takes place from 1 to 4 August, followed by Summit Day on 4 August and the main briefings on 5 and 6 August. The event is not devoted specifically to quantum security, but it remains one of the best places to track how quickly post-quantum migration and AI-assisted security research are entering mainstream cybersecurity practice. (Black Hat)

2–5 August — CCF Quantum Computing Conference, Shenzhen. This is an early-August signal from China's research and technical community and should provide insight into hardware, algorithms and the country's wider quantum priorities. (Quantum Technology)

3–5 August — Quantum Computing and Sensing for Weather and Climate Applications, Boulder and online. This workshop is worth monitoring as a practical example of quantum computing and sensing being evaluated against real scientific and public-sector workloads. (Quantum Technology)

3–14 August — Fault-Tolerant Quantum Technologies, Benasque, Spain. Fault tolerance remains one of the critical variables in estimating when quantum computing could become cryptographically relevant, making this meeting more consequential to security planning than its academic framing might initially suggest. (Quantum Technology)

17–21 August — Quantum Physics and Logic, Amsterdam. QPL brings together academic and industry researchers working on the foundations of quantum computing, communication and future fault-tolerant systems. (QPL)

24–28 August — Asian Quantum Information Science Conference, Daejeon. Hosted by KAIST, AQIS is one of the month's most important Asian research meetings and covers quantum information, computation and cryptography. (aqis-conf.org)

16–18 September — ITU regional meetings and Global Quantum Drill, Dubai. The Africa and Arab regional cybersecurity groups meet on 16 September, followed by the practical drill on 17 and 18 September. Organisations seeking travel support need to apply by 10 August. (ITU)

What to Watch Next Week

The next week will provide an unusually concentrated look at the commercial state of publicly listed quantum companies. IonQ reports second-quarter results after the market closes on 5 August. D-Wave reports before the market opens on 6 August, while Rigetti reports after the close on the same day. (IonQ Investors)

The most useful indicators will not be daily share-price movements. Investors and industry observers should look at bookings, remaining performance obligations, revenue derived from actual customers, hardware roadmaps, acquisition integration and evidence that commercial trials are expanding into repeatable deployments.

IonQ is also expected to complete its acquisition of SkyWater Technology on 31 July, subject to the remaining closing arrangements. The combined company's earnings call on 5 August should provide an early indication of how IonQ intends to connect quantum-system development with domestic semiconductor manufacturing. (IonQ Investors)

Black Hat may also produce relevant research or product announcements during the week. Following the Anthropic results, particular attention should be paid to work involving AI-assisted vulnerability research, cryptographic testing, software-supply-chain security and practical post-quantum deployment.

The most important lesson from this week is that quantum security is no longer moving along a single track. Advances in AI are changing cryptanalysis, enterprises are testing quantum systems against operational workloads, and governments and standards bodies are beginning to exercise the coordination required for migration. The purpose of this briefing is to make those connections visible while giving readers the sources they need to go deeper.

— Joel Van Dyk

Source Links

The links below reproduce the source list included in the locked Issue 9 text.

[1] Discovering cryptographic weaknesses with Claude \ Anthropic - https://www.anthropic.com/research/discovering-cryptographic-weaknesses

[2] www.dwavequantum.com - https://www.dwavequantum.com/company/newsroom/press-release/at-t-signs-agreement-to-expand-use-of-d-wave-s-quantum-computing-technology/

[3] Enterprises aren't moving fast enough on post-quantum cryptography preparations – 'harvest now, decrypt later' attacks mean it could cost them | IT Pro - https://www.itpro.com/security/enterprises-arent-moving-fast-enough-on-post-quantum-cryptography-preparations-harvest-now-decrypt-later-attacks-mean-it-could-cost-them

[4] Quantum Is Coming for Crypto. Wall Street Is Spending Millions to Stop It. - https://www.barrons.com/articles/quantum-bitcoin-computing-security-f4d5c9f8?utm_source=chatgpt.com

[5] Securing the Nation Against Advanced Cryptographic Attacks - https://www.whitehouse.gov/presidential-actions/2026/06/securing-the-nation-against-advanced-cryptographic-attacks/?utm_source=chatgpt.com

[6] Black Hat USA 2026 - Cybersecurity Conference Las Vegas - https://blackhat.com/us-26/?utm_source=chatgpt.com

[7] France to stop certifying products without quantum-safe encryption - https://www.reuters.com/legal/litigation/france-stop-certifying-products-without-quantum-safe-encryption-2026-06-16/?utm_source=chatgpt.com

[8] 2026 Confs - https://quantum.technology/conf/index.html

[9] ML4AU Community of Practice Meeting (June 2026) - https://ardc.edu.au/event/machine-learning-community-of-practice-ml4au-meeting-august-2026-quantum-technology-and-its-impact-on-ai-and-machine-learning/

[10] ITU Global Quantum Drill 2026 - https://www.itu.int/en/ITU-T/studygroups/2025-2028/17/Pages/2026-09-16.aspx

[11] Measurement Study of Post-Quantum Readiness of Internet: 2026 - https://arxiv.org/abs/2606.16473?utm_source=chatgpt.com

[12] Toward Quantum-Safe 6G: Experimental Evaluation of Post-Quantum Cryptography Techniques - https://arxiv.org/abs/2605.06881?utm_source=chatgpt.com

[13] Securing Cryptography in the Age of Quantum Computing and AI: Threats, Implementations, and Strategic Response - https://arxiv.org/abs/2603.06969?utm_source=chatgpt.com

[14] QPL | Official Website for the QPL 2026 Conference - https://qplconference.org/

[15] AQIS26 | 26th Asian Quantum Information Science Conference - https://aqis-conf.org/

[16] IonQ to Report Second Quarter 2026 Financial Results on … - https://investors.ionq.com/news/news-details/2026/IonQ-to-Report-Second-Quarter-2026-Financial-Results-on-August-5-2026/default.aspx?utm_source=chatgpt.com

[17] IonQ Receives Regulatory Approval to Complete … - https://investors.ionq.com/news/news-details/2026/IonQ-Receives-Regulatory-Approval-to-Complete-Acquisition-of-SkyWater-Technology/default.aspx?utm_source=chatgpt.com