

THIS WEEK IN QUANTUM SECURITY

October 7, 2026

By Joel Van Dyk

Quantum Security Advisor and Strategist

By Joel Van Dyk, Quantum Security Advisor and Strategist

This week, several strands of the quantum-security story came together at once. NATO published a detailed Quantum Technology Roadmap that turns “quantum-ready” from a strategy slogan into an implementation programme; China’s new cryptographic competition became an unusually public testbed for AI-assisted cryptanalysis; Visa warned that AI is already compressing the time between vulnerability discovery and exploitation while it prepares for quantum-era payments security; and both Quantum World Congress in Maryland and the Quantum Innovation Summit in Dubai focused less on whether quantum matters than on how organisations, governments and critical infrastructure actually prepare for it. [NATO](#)

The common thread is implementation under pressure. A cryptographically relevant quantum computer has not arrived, and none of this week’s research shows that NIST’s standardised PQC algorithms have been broken. What is changing is the environment around them. AI is making cryptanalysis and vulnerability discovery faster, governments are building procurement and interoperability frameworks, and quantum hardware is moving steadily toward systems that have to work with conventional computing infrastructure. The interesting question is increasingly not whether migration should begin, but how organisations build systems that remain secure while the technology, standards and attack methods continue to move.

The Week’s Key Developments

NATO turns “quantum-ready” into an implementation roadmap

NATO published the public version of its Quantum Technology Roadmap on 29 September, translating its 2023 strategy into a much more detailed programme covering quantum computing, communications and sensing. The roadmap is organised around five lines of effort: use-case identification; testing and adoption; standardisation and interoperability; protection against quantum risks; and training and education. It also explicitly connects quantum with AI, space and next-generation communications rather than treating those technologies as separate programmes. [NATO](#)

The post-quantum security parts are unusually concrete. NATO says adoption and implementation of PQC standards is already an ongoing activity. It plans an industry-readiness study on quantum-resistant cryptography by Q2 2027, another update to its cryptographic-threat action plan by Q3

2027, and a Quantum Zero Beacon pilot between NATO headquarters in Brussels and SHAPE in Mons by Q4 2027. The roadmap also calls for a wider Alliance quantum standards roadmap and an Allied Quantum Computing Access Network concept. [NATO](#)

That matters because defence organisations have an interoperability problem that looks very similar to the one facing global financial institutions, only with different consequences. NATO systems have to work across countries, vendors, command structures and legacy environments, often for very long service lives. A migration that produces incompatible national solutions would undermine the very interoperability the Alliance depends on.

The roadmap is also careful not to pretend that every part of quantum technology is at the same maturity level. Testing and adoption are meant to remain adaptive because computing, communications and sensing are progressing at different speeds. That is a useful approach to PQC as well. Migration planning should be structured, but it cannot assume that every protocol, product and operational environment will move in lockstep.

For cybersecurity teams, the most useful signal is that another major institution has stopped treating quantum readiness as a future policy exercise. NATO is now assigning timelines, test programmes, industry studies and implementation owners.

China's cryptography competition becomes a live experiment in AI-assisted cryptanalysis

One of the most interesting cryptographic stories of the week is coming from China's Next-generation Commercial Cryptographic Algorithms programme.

China's Institute of Commercial Cryptography Standards published **119 first-round candidates** on 20 September: 34 signature schemes, 41 KEMs, nine key-exchange protocols and 35 hash functions. Within the first week, an independent evaluation effort recorded **191 active findings across 89 candidates, including 78 rated critical**. Those findings included universal signature forgeries, signing-key recovery, trivial hash collisions, broken implicit-rejection mechanisms and parameter sets that failed to deliver their claimed security level. [Cryptography ePrint Archive](#)

The number has continued to rise. As of 1 October, ngcc.dev lists **248 active findings across 101 reports**, split across implementation, design and side-channel issues. Those numbers are moving quickly because the evaluation remains active. [NGCC](#)

The AI angle is what makes this particularly relevant. Markku-Juhani Saarinen's new IACR ePrint describes an agentic workflow that discovered and verified 110 of the first week's findings, 47 of them critical. The paper says the earliest AI-assisted discoveries were mostly implementation problems, but by the end of the week the workflow was also reproducing design-level attacks including key recovery. [Cryptography ePrint Archive](#)

That does not mean AI has suddenly automated cryptography research or that every finding represents a sophisticated mathematical break. Many of the early problems were bugs that stronger negative testing should have caught: verifiers accepting malformed signatures, repeated values, weak seed handling or incorrect rejection logic.

That is partly why this is such a useful case study.

AI is not replacing cryptographers here. It is increasing the speed and scale at which submitted implementations and designs can be challenged. A competition that might once have depended on a relatively small number of researchers manually examining dozens of schemes now has automated and AI-assisted scrutiny operating almost immediately.

For organisations implementing PQC, that has a very practical implication. The attack surface is not only the mathematics. The code, parameter choices, test harnesses and side-channel behaviour all matter, and increasingly capable AI tools may make weak implementation much easier to find.

This also shows where AI can help cybersecurity and intersect. The “Adversarial Podcast” had a similar discussion last week. AI here is helping cybersecurity SOCs and defenders make up the difference in resources, speed and initiative with the hackers. Just like Jerry, Sounil, and Mario, I don’t pretend to know where AI will wind up. I’m hoping it’s not all bad (Skynet), it probably won’t be all good, but somewhere in between. This seems a good in between use.

Visa increasingly treats AI and quantum as parts of the same payments-security problem

Visa added another useful financial-sector signal this week.

Speaking about increasingly autonomous cyber threats, Visa President of Technology Rajat Taneja said the recent behaviour of advanced AI systems had been “humbling” and warned that attackers may increasingly be able to operate without continuous human direction. Reuters reports that Visa has open-sourced parts of its AI-assisted defensive tooling while also preparing for longer-term risks from quantum computing to the cryptography supporting global payments. [Reuters](#)

Visa’s own research organisation now explicitly lists **Quantum Security, Quantum AI for Payments and Quantum Computing** among its focus areas, including work on quantum-safe payment security and future-facing architectures relevant to financial systems. [Visa](#)

The useful part of this is not that Visa has combined two fashionable technologies in the same research programme. It is that payment security increasingly has to deal with both time horizons at once.

Quantum risk is long-term but migration-heavy. AI-enabled cyber risk is immediate and compresses the time available for defenders to respond. One requires long-range planning; the other makes poor implementation and slow remediation more dangerous today.

That combination strengthens the case for crypto-agility. An organisation can choose the right post-quantum algorithm and still create a vulnerable system if key management, certificate handling, authentication, APIs or access controls are weak.

For financial institutions, the security problem is increasingly a moving target: new cryptography is being introduced into systems that are themselves facing more capable automated attackers.

Quantum World Congress: scaling now depends on infrastructure, not just qubits

Quantum World Congress in College Park closed with a message that was more interesting than the usual hardware-roadmap competition.

NIST Director Arvind Raman argued that quantum cannot scale until it can be measured consistently, pointing to the less visible infrastructure needed to support an industry: standards, metrology, manufacturing, networking, cryptography and repeatable benchmarks. Other sessions made similar points from different directions. Atom Computing focused on the need to close the speed gap in neutral-atom systems; D-Wave discussed engineering error modes that are easier to detect; and India's C-DAC argued that the country's problem has shifted from demonstrating capability to scaling access, integration and commercial use. [Quantum World Congress](#)

Microsoft also used the event to connect AI-driven scientific discovery with its new quantum research centre in Maryland, while regional announcements included a new Virginia Quantum Hub and plans to place an operational quantum computer in a Fairfax County public high school in 2027. [Quantum World Congress](#)

The important signal is not that quantum is suddenly commercially mature. It is not.

What has changed is the kind of conversation the industry is having. Manufacturing, workforce, measurement, procurement, error correction, software integration and local access are now taking up as much space as raw qubit counts.

That is probably healthy.

The closer quantum gets to becoming an industry rather than a collection of research programmes, the more those engineering details will determine whether the technology actually scales.

For quantum security, the same lesson applies. Migration depends on infrastructure: inventories, certificate systems, HSMs, identity, key management, monitoring, testing and evidence. The algorithm is necessary, but it is not the migration.

Dubai pushes quantum readiness into critical-infrastructure continuity

The Quantum Innovation Summit in Dubai ran from 28–30 September with an unusually explicit focus on quantum readiness and cybersecurity.

Its dedicated readiness track included the post-quantum cryptography imperative, standards and testing for quantum-safe systems, and a multi-stakeholder tabletop exercise built around maintaining critical-domain continuity during a PQC transition. Participants represented national cybersecurity leadership, regulators, telecoms, financial institutions, energy, transport and government digital services. [Quantum Innovation Summit](#)

The summit organisers framed the wider programme around moving from “quantum readiness to institutional action,” with governance, critical infrastructure, resilience and international coordination treated as part of the same problem. [Quantum Innovation Summit](#)

That is worth noting because the Middle East's quantum strategy is beginning to look broader than hardware acquisition or investment.

The region has spent much of the year building quantum-computing partnerships and sovereign capability. The readiness agenda is now beginning to ask the other half of the question: how do the

financial, telecom, transport and government systems that already exist make the transition securely?

The tabletop format is particularly useful. PQC migration is one of those programmes that can look sensible on paper until dependencies are tested under operational pressure. A simulation involving multiple sectors exposes coordination problems much earlier than a policy document can.

Global Signals

North America

The strongest North American signal this week came from Quantum World Congress and the surrounding ecosystem in Maryland. The discussion increasingly centered on measurement, manufacturing, workforce and infrastructure rather than simply proving that quantum hardware can work. Microsoft's new Maryland research centre, Virginia's new Quantum Hub and new on-premises academic deployments are all part of that build-out. [Quantum World Congress](#)

IonQ also continued to push fault-tolerant engineering into conventional computing infrastructure. The company says it demonstrated a real-time quantum-error decoder running on standard CPU hardware and is installing a Superion 256 system at NVIDIA's Accelerated Quantum Research Center, directly linking the QPU with NVIDIA accelerated-computing infrastructure. Those remain company-reported milestones, but they are useful because they address the classical-computing bottlenecks around fault-tolerant systems rather than simply increasing the physical-qubit count.

[IonQ Investors](#)

United Kingdom and Europe

The most important European signal this week is NATO's roadmap, particularly its emphasis on standards, interoperability and ongoing PQC adoption across the Alliance. NATO's public timeline now includes industry-readiness work, pilot evaluations and quantum-resilient communications activity rather than only strategic language. [NATO](#)

ETSI also published new guidance on **Quantum Random Number Generators**, warning that quantum origin does not automatically guarantee secure randomness. Side information, hardware failures, bias and drift can undermine output quality if entropy sources are not properly modelled, extracted and monitored. That is a useful reminder that "quantum" is not itself a security property.

[ETSI](#)

Asia

China produced the region's most important cryptographic story through the NGCC programme. The scale and speed of the public findings make it a rare real-time look at what happens when a national cryptographic standardisation programme is subjected to both human and AI-assisted attack from the beginning. [Cryptology ePrint Archive](#)

India's Quantum World Congress message was different but related. C-DAC argued that India's challenge has moved beyond showing that it can build quantum technology and toward connecting processors with supercomputing, secure networking and practical access. That is consistent with the

RBI's recent work on quantum-safe financial infrastructure and the broader National Quantum Mission. [Quantum World Congress](#)

South Korea also continues to build its commercial infrastructure. IonQ and SDT announced a partnership that includes a Superion 256 system and a quantum-memory module, combining computing and networking in a single regional deployment. [IonQ Investors](#)

Australia

Australia continues to use quantum as an applied-technology programme rather than only a research strategy.

The government's Critical Technologies Challenge Program is funding quantum projects tied to energy, logistics, biosecurity and healthcare, with explicit requirements around commercial pathways and real-world end users. Australia's Protective Security Policy Framework also now includes formal post-quantum transition planning, which means quantum risk is entering routine government security governance rather than remaining specialist guidance. [Industry.gov.au](#)

Australia also remains a useful example of AI and cryptographic risk converging in practice after the OpenAI-related Medicare incident prompted a government security review. That incident was not quantum-related, but it reinforces the implementation theme: increasingly autonomous systems are becoming part of the same infrastructure that must also undergo cryptographic migration.

[Prime Minister of Australia](#)

Africa

Africa's most important current signal is institutional rather than commercial.

The Africa Quantum Consortium is now explicitly publishing around post-quantum protection of the continent's digital backbone while building a network that spans dozens of countries and organisations. Combined with the formal African PQC preparedness discussions at the recent ITU regional meeting, that suggests the region is beginning to frame quantum readiness as a critical-infrastructure issue rather than only a research topic. [Africa Quantum Consortium](#)

The practical challenge will remain capacity: skilled cryptography teams, procurement expertise, standards participation and access to testing environments will determine whether migration can keep pace with larger markets.

Middle East

Dubai has now hosted both the ITU Global Quantum Drill and the Quantum Innovation Summit within two weeks.

The important shift is that the conversation has moved toward **institutional readiness**: cybersecurity resilience, standards, interoperability, critical-infrastructure continuity and national coordination. The UAE's approach is increasingly linking quantum capability with telecoms, AI and digital infrastructure rather than treating it as an isolated research sector. [Quantum Innovation Summit](#)

The next useful signal will be whether those discussions produce published national readiness frameworks, procurement requirements or sector-specific migration programmes.

Latin America

Brazil remains the strongest regional quantum signal.

IQM's first South American quantum-computer sale will put an on-premises system at the Eldorado Research Institute in Campinas in 2027, alongside access to larger cloud systems. The significance is not cryptographic threat; it is local capability. Researchers, universities and industry will be able to develop skills and applications without depending entirely on overseas infrastructure. [IQM](#)

The region still lacks the kind of coordinated PQC migration timeline visible in the UK, Australia or parts of Europe, but Brazil is increasingly building the technical ecosystem that will eventually have to support both quantum adoption and quantum-safe migration.

Research Worth Reading

“Chinese NGCC Algorithms: The First Week of AI Cryptanalysis” — Markku-Juhani O. Saarinen.

This is the paper of the week. It documents the first seven days of China's new cryptographic competition and describes an agentic AI-assisted workflow that discovered, reproduced and classified large numbers of implementation and design flaws. The obvious limitation is that these are first-round candidates rather than deployed standards, and many early failures reflect weak implementations rather than deep cryptanalytic breakthroughs. Even so, it provides one of the clearest demonstrations yet of how AI can change the speed of cryptographic evaluation. [Cryptology ePrint Archive](#)

ETSI TR 104 171 — Quantum Random Number Generator implementation guidance. The report examines modelling, entropy extraction, runtime monitoring and the effect of side information on QRNG security. Its practical value is the reminder that a quantum source does not remove ordinary implementation risk. Randomness has to be measured, monitored and validated throughout the device lifecycle. [ETSI](#)

NATO Quantum Technology Roadmap. This is not academic research, but it is worth reading as an operational document. It assigns timelines to use-case assessment, testing, standardisation, PQC implementation, industry readiness and training across the Alliance. The limitation is that the public roadmap provides only selected activities; some defence-specific implementation detail remains outside the public version. [NATO](#)

“AI-Assisted Design of a Post-Quantum Cryptographic Accelerator: A Deployed-Silicon Case Study.” The paper reports an AI-assisted hardware-development process for ML-KEM and ML-DSA and, more importantly, documents a validation failure that standard known-answer testing did not detect. The practical lesson is stronger than the AI claim: PQC hardware needs adversarial and data-dependent testing that exercises paths static test vectors do not reach. The authors' results come from one hardware development effort, so they should not be treated as a general benchmark for AI-designed silicon. [arXiv](#)

Meetings and Events to Watch

6 October — Post-Quantum Cryptography: State of the Art, Bonn, Germany. The one-day training focuses on NIST standards, cryptographic libraries and migration strategy. It is another sign that the market is shifting from quantum-awareness education toward implementation skills. [ESAT](#)

7–8 October — Quantum Academy PQC and Telecommunications programmes, Dublin. The sessions cover migration fundamentals and telecom-specific quantum-safe security, including subscriber authentication and network cryptography. The telecom angle is worth watching because operators face unusually long infrastructure lifecycles. [Quantum Academy](#)

11–12 October — IAB Workshop on Accelerating the Deployment of Post-Quantum Authentication, Prague. This is probably the most important security event on the near-term calendar. Post-quantum key establishment is already relatively mature; authentication remains harder because signatures and public keys are larger and dependencies are distributed across certificates, PKI, code signing, devices and applications. The workshop is explicitly focused on real deployment experience and the obstacles preventing production adoption. [IETF Datatracker](#)

15 October — Evertrust Summit, Paris. Orange Cyberdefense, Thales and financial-sector participants are expected to discuss what organisations have actually learned while carrying out PQC migration. Practical deployment stories will be more useful than another survey of awareness levels. [Evertrust](#)

19 October — DOE Quantum Genesis Q Competition applications due. DOE's competition links public funding to fault-tolerant milestones, while the associated national-lab testbed programme is meant to create the verification infrastructure needed to evaluate those systems. The useful signal will be who applies and what architectures they believe can credibly meet the programme milestones. [GovDelivery](#)

What to Watch Next Week

The NATO roadmap deserves continued attention because its most interesting content is not the long-term vision but the implementation machinery underneath it. The industry-readiness study, cryptographic action plan, standards work and Zero Beacon pilot should begin producing evidence about what “quantum-ready” actually means across a multinational defence environment.

The China NGCC evaluation is likely to move even faster. The finding count is already changing daily, and the useful distinction will be between implementation failures that can be repaired relatively easily and design flaws that eliminate entire candidates. I will also be watching how much of that analysis is genuinely AI-generated, how much depends on human review, and whether the process begins to change how future standards competitions organise evaluation.

The IAB workshop in Prague may be even more relevant to enterprise security teams. Post-quantum key exchange has moved surprisingly quickly into real internet infrastructure. Authentication is lagging because certificates, signatures, PKI and identity are harder to change. The discussion there

should help reveal which technical constraints are genuinely blocking deployment and which are simply organisational inertia.

And the AI-security discussion is not going away.

Visa is now publicly talking about AI and quantum in the same long-term security programme, while the Chinese NGCC process shows AI-assisted analysis operating directly against cryptographic candidates. Those are two very different examples, but together they point to an important shift.

Quantum security is no longer a programme that can be planned against a static threat environment.

The migration itself will happen while the tools used to attack, test and validate cryptography are changing.

That makes crypto-agility, implementation testing and evidence more important than ever.

— Joel Van Dyk

Source Links

1. [NATO Quantum Technology Roadmap](#)
2. [NATO roadmap announcement](#)
3. [IACR ePrint 2026/2266 — Chinese NGCC Algorithms: The First Week of AI Cryptanalysis](#)
4. [ngcc.dev independent NGCC analysis](#)
5. [ngcc.dev security findings](#)
6. [Visa Research — Quantum Information and Computation](#)
7. [Visa on AI-powered cybersecurity](#)
8. [Quantum World Congress 2026](<https://www.quantumworldcongress.com/>)
9. [Quantum Innovation Summit agenda](#)
10. [Quantum Futures Forum 2026](#)
11. [IonQ real-time quantum error decoder](#)
12. [IonQ / NVIDIA Accelerated Quantum Research Center deployment](#)
13. [ETSI QRNG implementation guidance](#)
14. [Australia Critical Technologies Challenge Program](#)
15. [Australia Protective Security Policy Framework 2026](#)
16. [Africa Quantum Consortium](#)
17. [IQM Brazil quantum-computer deployment](#)
18. [IAB Post-Quantum Authentication Workshop](#)

19. [IETF — Post-Quantum Authentication: Up Next](#)
20. [DOE Quantum Genesis Q Competition](#)
21. [AI-Assisted Design of a Post-Quantum Cryptographic Accelerator](<https://arxiv.org/abs/2609.04058>)