Draft Version

Q-Day, worse than Y2K

Pre-empting the quantum transition's inevitable crisis with cryptoagile post-quantum-cryptography

This is no drill. Quantum computing is no longer a dream in the distance; it is a capability that is becoming increasingly mature. By 2035, experts say, there will be a 1 in 2 chance that quantum computers will break much of today's encryption – cryptographic shields that protect our data. The threat posed is not a future hypothesis, however, it is our reality today. Every byte of encrypted data: our health records, critical infrastructure, state secrets, digital finance, the entire fossil record of our digital lives is being harvested and stored now by adversaries who know that a single future decryption breakthrough will hand them the master key – **Harvest Now, Decrypt Later (HNDL)**, also referred to as Store Now, Decrypt Later (SNDL).

The urgency is captured by the brutal, elegant logic of Mosca's Theorem[1].

$$x + y > z$$

Here, x is the shelf life of our secrets: perhaps a decade for corporate IP or a lifetime for our health data. y is the agonizingly slow time it will take to migrate our entire global digital infrastructure to quantum safe defenses[2]. z is the countdown to a cryptographically relevant quantum computing infrastructure, an unknown variable that shrinks with every billion-dollar corporate or state funded breakthrough.

> *Jillian Mascelli and Megan Rodden, US Federal Reserve, September 2025*
> *"[We] highlight [the] gap in data privacy protection and note the shortage of mitigations for the data privacy risks associated with the HNDL threat within distributed ledger [cryptocurrency] networks."*

Our expert community already recognizes $x + y$ is very much greater than z, so we are living on borrowed time, and the interest is compounding daily. This is a shock in waiting. The technological rupture would be so profound it would unravel the fabric of trust that holds our societies together. We must act.

---

[1] *Kiviharju, M. (2022). Refining Mosca's Theorem: Risk Management Model for the Quantum Threat Applied to IoT Protocol Security. In: Lehto, M., Neittaanmäki, P. (eds) Cyber Security. Computational Methods in Applied Sciences, vol 56. Springer, Cham. https://doi.org/10.1007/978-3-030-91293-2_16*

[2] *Mascelli, Jillian, and Megan Rodden (2025). ""Harvest Now Decrypt Later": Examining Post-Quantum Cryptography and the Data Privacy Risks for Distributed Ledger Networks," Finance and Economics Discussion Series 2025-093. Washington: Board of Governors of the Federal Reserve System, https://doi.org/10.17016/FEDS.2025.093*

Learning from History

We have been here before. There are lessons to be (re)learned. We must resist the temptation of authoritarian impulses, and the ghost of the NSA's Clipper Chip[3] haunts this transition.

Encryption used to lie in the hands of the state and was deployed only for military and diplomatic purposes. In the 1970s, US cryptographers Whitfield Diffie, Martin Hellman and Ralph Merkle revolutionized the field by taking encryption keys away from the state, marking the start of the "Crypto Wars". Before their concept was popularized, cryptography support outside an integrated organization (like the NSA) was not practicable. And then it was. The NSA reacted in a predictable manner, as with any enterprise that has had a long-term monopoly in a market when someone treads on their turf. They tried to recapture the market with a US government mandate to have a backdoor into all our communications. This concept has an obvious fatal flaw that would have made every citizen vulnerable: loss of the "golden keys" to the backdoor.

The immense complexity of PQC migration presents a perfect pretext to demand exceptional access or control. We must be alive to any power grab and defend against it with the same ferocity that the Clipper Chip faced. The lesson is clear, security that is architected for state or mega-corporation control is no security at all.

Our guiding light must be radical transparency and public oversight, not backdoors, black-boxes nor blind trust in a new crypto-leviathan.

Anti-resilience and choke points

The Red Sea cable chaos on September 6, the AWS outage between 11:48 pm EDT on October 19 and 2:40 am EDT on October 20, and the Microsoft DNS outage between 4:00 pm UTC on October 29 and 12:05 am UTC on October 30 of this year are *prima facie* examples of how our internet services are not built as resilient fortresses, rather they are hyper-centralized and very brittle. We might term this as "anti-resilience". Systems so complex and interconnected that a single misconfiguration in one hyperscaler's system can bring continents to a halt. Then we have choke points where a physical incident, a few anchors dragged – by accident or design – in one maritime corridor disrupts the data flows of nations.

The business model of vendor lock-in and dependency has created single points of failure in both logic and geography. To hand these same centralized entities the keys to our quantum-safe future is to double-down on this high-risk model. We would be

[3] *CCS '94: Proceedings of the 2nd ACM Conference on Computer and communications security, pages 59 – 67, https://doi.org/10.1145/191177.1911*

building our new security on a foundation of sand. Let us not seek shelter in the eye of a hurricane that these entities helped to create.

Embedding governance

As we have said, the defense of our digital identities and patterns of life is not a task for a closed-door consortium of tech giants and three-letter agencies. **Cryptoagility**[4] and **Post-Quantum-Cryptography (PQC)**[5] are the new foundations upon which we have to pivot onto from the realm of proprietary IT upgrades, and they must be established as a non-negotiable public good, a fundamental principle of modern, digital network era governance.

True resilience in the quantum era starts with PQC, the specific mathematical or algorithmic fortifications against the known future threat. But this cannot be the single, static solution – merely swapping algorithms as a fix is not enough. The strength has to be dynamic, and the architecture of our information infrastructure must be modular to allow for easy upgrades on live systems. At the core lies a foundational philosophy, that security is a process not a product. This philosophy must be realized through enforceable policy that mandates the adoption of PQC standards – today these are NIST recommended algorithms – and moreso the architectural and operational practices that make cryptoagility possible. This implies open audits, or as open as possible, and brutal liability for technological stagnation. The policy layer, in turn, requires the technology derived from it. Systems must be architecturally designed from the chip up

Why quantum safe impacts you – we need to protect all these aspects

[4] See https://www.capgemini.com/insights/expert-perspectives/crypto-agility-the-unsung-hero-in-the-quantum-security-race/

[5] See https://csrc.nist.gov/projects/crypto-agility, https://www.fsisac.com/hubfs/Knowledge/PQC/FutureState.pdf and https://www.capgemini.com/insights/research-library/post-quantum-crypto/

Assured Service Provider — National Cyber Security Centre — Consultancy: Post-Quantum Cryptography (Discovery and Migration Planning)

Assured Service Provider — National Cyber Security Centre — Consultancy: Post-Quantum Cryptography (Advice)

to be both quantum-resistant and cryptoagile, where cryptographic suites can be swapped without rebuilding the entire digital edifice. At the edge, all of this is to be shielded by a physical, hardened infrastructure to protect against physical tampering. Each layer is interdependent, governing this framework builds a future that is robust to any single failure point – be it a mathematical breakthrough or a failure of institutional imagination.

Building Competence

This revolution in our information fabric cannot be automated. It must, at least, be audited. We must have a public whose grasp of cryptographic literacy, and responsibility is clear-eyed.

There must be an informed community of digital "sheriffs" in every sector, with clear lines of accountability. But technical experts are not enough. We must have a "Great Upskilling" across all institutional functions. Equip legal teams to understand HNDL and to enact contracts that mandate PQC plus Cryptoagility, so liability becomes a lever for change. Train procurement officers to examine bids from vendors for solutions that cryptographically evolve. Empower C-suite executives and boards to understand this is a core governance issue.

When a hospital's patient data is breached because it failed to migrate from or isolate and sensibly manage its vulnerable, legacy encrypted IT systems, the liability must land on those decision makers who treated cybersecurity as an add-on rather than a civic duty.

This is not a one-time training seminar, it is a conscious, continuous building of a new institutional DNA, to weave competence and accountability into the fabric of our organizations year-on-year until the question of "is it quantum safe?" becomes as instinctive as "what is the cost?"

Enabling the Transformation

Resilience is not a software patch. It resides in the physical world, in our silicon chips, in our optical fiber networks and in the electromagnetically shielded rooms of our critical IT infrastructure. The transformation to a quantum safe society demands the right level of public investment in the hardware that ultimately powers our democracies. We must fund the research, build the secure software foundries and re-shore the production of the cryptographic engines that protect our digital lives.

This is also a chance to build a decentralized, robust and democratically controlled digital estate, to push back against the other vision of the future – where information security is a luxury good, available only to those who can afford the subscription.

Securing our data future

We will know that we are succeeding, not by the press releases from Palo Alto, but by the public benchmarks we set and meet within Europe and European nation-states. The measure may be a more evolved version of Mosca's clock. This is a ground war against time itself and it demands an historic mobilization of capital. The question is not *if* we need public-private funding, rather it is *on whose terms*? We must discover the optimal ways to deploy capital as a strategic lever to enable a democratic outcome. We need a firewall against the capture of our cryptographic future.

We must establish ways to publicly track the progress of every critical agency, bank, utility or service in our societies. Measuring their *y* against the terrifying advance of *z* in Mosca's language. We must be able to see the scoreboard, to know which institutions are building true resilience and which are falling short. This is nothing less than the creation of a new social contract for the data age built on verifiable, resilient and democratic trust – a digital commons worthy of the name.

In conclusion

Cryptoagility and PQC are complex technical upgrades which we need to protect our most valuable information from the quantum computing age that is en route. They are also part of a policy choice. We can use it to build a truly resilient, democratic digital future, or we can allow it to be part of a power grab, centralizing control and deepening digital inequality. The time to make this decision is now.

For more information contact the Q-PreP team: https://qprep.eu/contact/

Appendix

Historical precedent of HNDL occurrence

February 1943[6] – Codename Venona, by the USA's National Security Agency/Central Security Service. It was intended to examine and exploit Soviet diplomatic communications. Approximately 3,000 VENONA decrypted translations have been made public.

Circumstantial evidence for HNDL occurring today

6 June 2019[7] - a large amount of European mobile network traffic was rerouted via China Telecom for nearly two hours. This was due to BGP route leak from a Swiss-based data center colocation company, Safe Host (AS21217) and it led to over 70,000 Traffic rerouted to China Telecom (AS4134). 70,000 Internet routes is roughly 300 million IPs. The most impacted European networks included Swisscom (AS3303) of Switzerland, KPN (AS1130) of Holland, Bouygues Telecom (AS5410) and Numericable-SFR (AS21502) of France.

1 April 2020[8] - Rostelecom diverted the traffic from more than 200 networks, including Google, Amazon, Facebook and Cloudflare, to Russian servers. Potentially this was accidental, but it need not have been. The incident occurred when an internal traffic optimization system exposed incorrect routes to the public internet rather than simply within its own private network. Once this happened, Border Gateway Protocol (BGP) ensured the errors spread round the internet within minutes.

Known weaknesses

November 2022[9] - 5G standard's unpatched design vulnerabilities identified (and are still valid today). These vulnerabilities are straightforward to take advantage of.

Supplementary motivation

18 September 2023[10] - we do not even have to wait till quantum computers are mature. Evidence that a very popular cryptographic algorithm RSA-2048 can be (theoretically) compromised in minutes using an ASIC (Application Specific Integrated Circuits), a custom chip, running conventional decryption attack algorithms has been published.

---

[6] https://www.nsa.gov/Helpful-Links/NSA-FOIA/Declassification-Transparency-Initiatives/Historical-Releases/Venona/

[7] https://gbhackers.com/european-traffic-rerouted-through-china-telecom/

[8] https://www.securityweek.com/russian-telco-hijacked-internet-traffic-major-networks-accident-or-malicious-action/

[9] https://haic.fi/wp-content/uploads/2022/12/Unpatched-design-vulnerabilities-in-cellular-standards_YK.pdf

[10] https://ieeexplore.ieee.org/document/10386235 or https://arxiv.org/pdf/2309.08198

Capgemini


Assured Service Provider
National Cyber Security Centre
Consultancy: Post-Quantum Cryptography (Discovery and Migration Planning)
Assured Service Provider
National Cyber Security Centre
Consultancy: Post-Quantum Cryptography (Advice)