ENTROKEY INSTITUTE™

In collaboration with eXponential academy

Zenia Tata,
Head of The
Entrokey Institute

Loki's Shield

Nishan Degnarain,
Managing Partner,
The Exponential
Academy

How Chaos, Entropy and the Science of Randomness Can Protect Organizations from AI and Quantum Cybersecurity Threats

January 2026

Table of Contents

Disclaimer

This White Paper was developed by The Exponential Academy, in collaboration with The Entrokey Institute, Entrokey Labs and Cambridge Frontier Technologies Lab, as an independent contribution to the global dialogue on quantum security. The views expressed do not necessarily represent those of all contributors, partner institutions, or affiliated organizations. This publication is for informational purposes only and does not constitute legal, financial, or technical advice. Reproduction for non-commercial use is permitted with proper attribution.

Acknowledgements

This White Paper was developed through the collaboration of The Entrokey Institute, Entrokey Labs and Cambridge Frontier Technologies Lab, supported by a network of experts in cybersecurity, quantum science, and public policy. The authors gratefully acknowledge the leadership and strategic guidance of David Harding, Eric Dresdale and Patrick Hearn from Entrokey Labs, whose vision helped shape the initiative's direction and ambition. Their collective expertise made *Loki's Shield* a shared effort to accelerate the world's readiness for the quantum era.

About Entrokey Labs

Entrokey Labs is pioneering the next generation of AI- and quantum-resilient cybersecurity. Built on advanced entropy science, the company delivers a stateless, software-only cryptographic platform that strengthens the security of critical infrastructure, enterprise systems, and government networks without requiring expensive or disruptive hardware upgrades. Its approach reflects a broader industry shift toward high-assurance, software-defined security layers capable of scaling across global digital ecosystems.

At the core of Entrokey Labs' technology is a crypto-agile architecture that combines high-fidelity entropy generation with continuous entropy verification, including sophisticated pattern-recognition techniques that detect predictability or drift before they evolve into systemic weaknesses. This entropy engine supports stateless key orchestration, reducing reliance on traditional key stores and shrinking operational attack surfaces. Integrated as a unified protective layer, the platform reinforces the integrity of data, identities, and machine-to-machine communications, providing durable protection against emerging AI-driven threats and the accelerating risks posed by quantum computing.

Guided by a mission to safeguard the world's most sensitive digital operations, Entrokey Labs offers security that is simple to deploy, cost-efficient, and engineered for the growing complexity of modern networks. As institutions confront an era defined by increasingly automated cyberattacks and the looming challenge of quantum decryption, the company provides a practical, future-proof foundation for trust—one that aligns with global movements toward quantum-safe infrastructure and resilient digital governance.

Foreword

David Harding
CEO
Entrokey Labs

Eric Dresdale
President
Entrokey Labs

Patrick Hearn
CCO
Entrokey Labs

The world is approaching a turning point in digital trust.

Quantum computing and artificial intelligence are redefining the limits of what can be decoded, predicted, and breached. For every new leap forward, the cryptographic foundations of the global economy grow more fragile.

At Entrokey Labs, we believe the coming years will mark a once-in-a-generation transformation in cybersecurity; one where randomness itself becomes the new source of resilience.

Traditional AI and post-quantum strategies, based on hardware retrofits and algorithmic patchwork, are too slow and too costly to scale. The pathway explored in *Loki's Shield* shows that by securing entropy, the true engine of cryptographic strength, organizations can achieve quantum-grade protection at over 90% lower cost and in a fraction of the time required by conventional transitions.

This approach does more than mitigate risk. It redefines the paradigm: from one of constant reaction to one of predictive, measurable trust. Entropy assurance, trust in verifiable entropy, turns cybersecurity from a defensive wall into a renewable system: one that evolves as fast as the threats it faces.

We sponsor this paper not to issue a warning, but to outline a path forward. *Loki's Shield* brings together leading researchers, technologists, and policymakers to chart a realistic roadmap toward a secure quantum future. The urgency is real, but so is the opportunity; to rebuild digital confidence, safeguard critical industries, and design a world where chaos itself becomes our protection.

Founding Team, Entrokey Labs

Executive Summary

A new storm is forming at the intersection of Artificial Intelligence and Quantum Computing, a collision that threatens the cryptographic foundations of global commerce, finance, and governance.

Within the next decade, advances in artificial intelligence and quantum computing could crack critical cybersecurity systems in everyday use by most companies and governments in the world (what's known as RSA-2048 encryption), exposing more than 99 % of current cybersecurity infrastructure. Simultaneously, AI-driven and nation-state adversaries are accelerating reconnaissance, exploiting patterns, and shortening attack cycles from months to hours. Some cybersecurity experts go further and predict that sometime within the next four years, the global economy could come grinding to a halt within a matter of weeks at a cost of over $20 trillion, equivalent to two months' disruption to global GDP. Already critical infrastructure industries are facing 'Harvest-Now-Decrypt-Later' attacks on important systems harboring sensitive data on citizen health, finance and communications.

This convergence has created an urgent, systemic risk known as Q-Day, the point at which today's encryption standards fail in real time. The U.S. National Institute of Standards and Technology (NIST), U.K. National CyberSecurity Center (NCSC), and the European Union Agency for Cybersecurity (ENISA) now treat quantum preparedness as a Top Five national security imperative with expert-led roadmaps for quantum-secure transitions[1]. Yet most organizations remain in early awareness phases. Current mitigation approaches are expensive and forecast to cost the global economy over $1.8 trillion if pursued via hardware-intensive or algorithm-only approaches.[2]

Even recognizing the importance of this technology and potential hazards associated with quantum computing, the U.S. risks falling behind nations like China which spends over four times as much as the U.S. Government on quantum technologies ($15.3 billion vs $3.8 billion[3]).

But the weakness is not just in algorithms; it is in the randomness of the keys that secure them. Without verifiable entropy, even post-quantum algorithms are vulnerable to pattern prediction by AI or quantum machines.

Entropy, the measure of unpredictability, is the new trust infrastructure.

New approaches to this quantum threat, such as those by Entrokey Labs, addresses this gap through a software-only Entropy Integrity Score[4] (EIS) that continuously scores and synchronizes randomness across cryptographic systems at a fraction of current industry hardware-only approaches. Delivered as a more agile, software update, EIS provides AI and quantum-grade protection without new hardware, aligns with the highest levels of U.S. policy (U.S. Presidential Executive Order 14144 and OMB M-24-04) on federal cryptographic resilience. The EIS layer meets and exceeds randomness test requirements found in NIST SP 800-22 exceeding the current suite's limitations in detecting certain complex, non-linear patterns that intelligent adversaries might exploit. This presents a leapfrog leadership opportunity for the U.S.

For leaders, quantum readiness is no longer a technical choice; it is a strategic one. Acting now delivers speed, cost efficiency, and compliance advantages that will define digital sovereignty for the next century.

Entropy is Loki's Shield: turning chaos into control.

In mastering randomness, we secure the foundations of trust for the AI and post-quantum world.

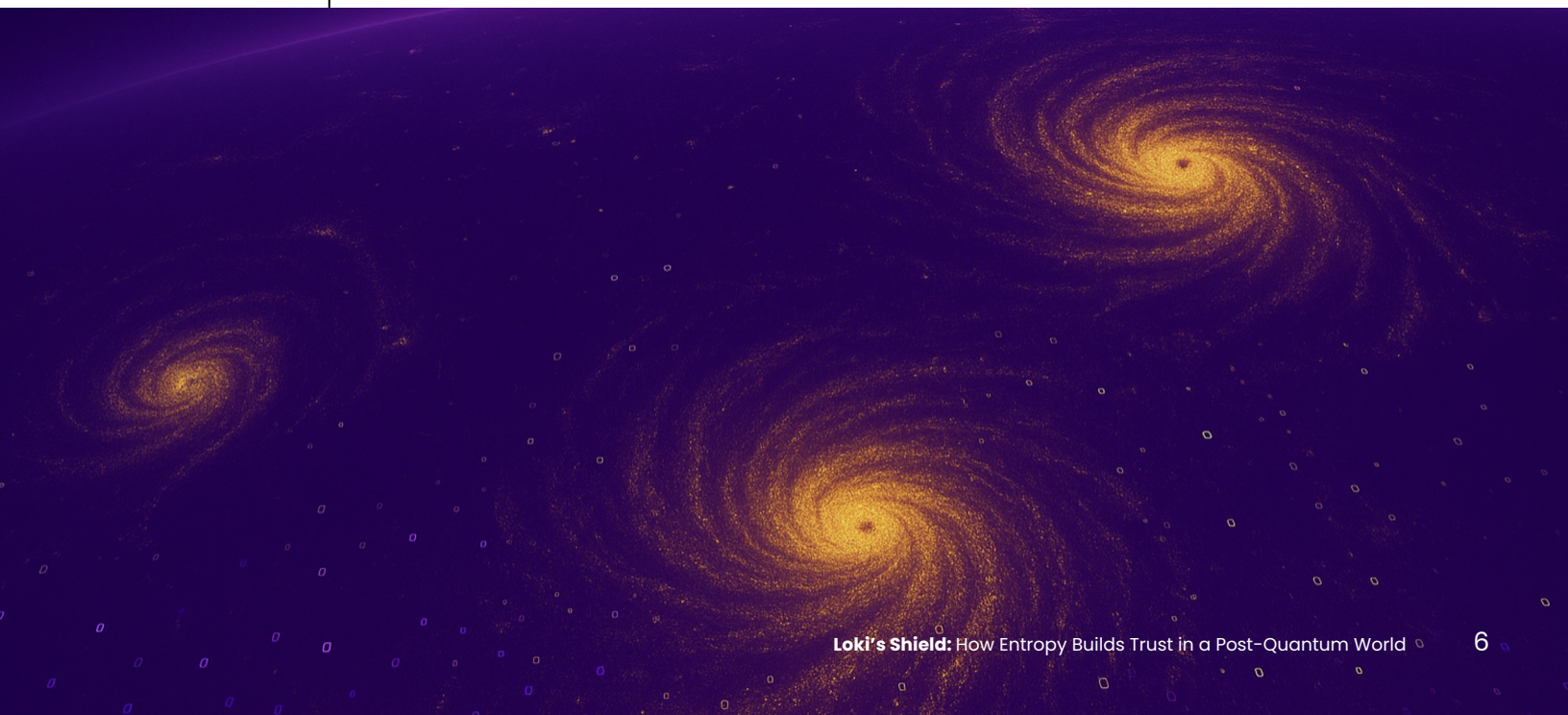
1

The Rising Storm

A convergence of risk

Within a decade, quantum technologies will change the world. In the same way that those who were slow to recognize the power of AI learned to their great expense, the value at stake from quantum is likely to be in the trillions of dollars. Advances in quantum technologies are moving at almost double that of Moore's Law,[5] which observed that the speed and capabilities of integrated circuits had been doubling approximately every two years, unleashing the classical computer revolution ongoing since the 1960s. With transistors in classical computing approaching atomic size, further miniaturization is extremely difficult due to quantum effects like electron leakage. Thus new methods are required to improve performance. Advances in quantum computing, driven by higher processing (doubling of qubits per chip each year) and exponential reduction in error rates (halving each year), is driving this new quantum computing revolution. Dubbed 'Neven's Law' (after Google's Director of Quantum Artificial Intelligence Lab, Hartmut Neven), these developments will revolutionize industries as diverse as drug discovery, weather modelling and cyber security[6].

Recognition of the potential of quantum technologies has never been higher: the 2025 Nobel Prize in Physics was awarded to John Clarke, Michel Devoret and John Martinis who laid the groundwork for modern quantum computing; China's 15th Five-Year Plan announced in October 2025 highlights quantum technologies (alongside advanced artificial intelligence) as a high priority next-generation growth sector; WEF's January 2026 Davos Annual Meeting explicitly flags advances in quantum technologies as a major techno-economical transformation for the upcoming years; and various U.S. policies at the highest levels show quantum's importance to driving the next wave of domestic economic growth. OECD[7] and national agencies in the UK, EU, Canada and other advanced economies have all developed National Quantum Technology Roadmaps for their own domestic economies and to establish leadership in this new frontier technology.



At the same time, the rise of these powerful tools have also driven a commensurately exponential increase in risk. Quantum computing may solve major global challenges if in the hands of good actors. However, if these tools end up under the control of bad actors, they could bring the global economy to a grinding halt within a matter of weeks. This is not just an I.T. issue for many organizations, but one requiring the leadership attention of the C-Suite and board to ensure suitable preparations are taken to avoid an organizational existential crisis from such a cybersecurity breach.

This paper focuses on the nature of this cybersecurity risk, driven by the rise and convergence of exponential technologies, in particular quantum computing, artificial intelligence, and the global connectivity surge. The risk has been given a name: Q-Day, which this paper explores. What is novel is the timelines by which these Q-Day risks may materialize (many experts believe sooner than regulations dictate), and the proposal of a more rapid, less expensive, and easier-to implement solutions than current policies have highlighted.

The evolving threat landscape

Three technological forces are converging to reshape the cybersecurity threat landscape over the next decade:

1. ***Artificial Intelligence (AI)*** autonomous adversaries able to probe defenses at machine speed

2. ***Quantum Computing*** capable within a few years of decoding today's public-key cryptography; and

3. ***A Global Connectivity Surge*** over 40 billion devices by 2030[8], expanding every potential attack surface.

Cybersecurity has evolved from a technical discipline into a top-five board and C-Suite priority, a matter of national and economic security. In its 2024 Global Cybersecurity Outlook,[9] the World Economic Forum (WEF) warned that escalating digital interdependence has made critical infrastructure as exposed as global supply chains were during the pandemic. A single breach in finance, health, or transport now risks cascading losses measured in hundreds of billions of dollars, threatening public safety, macroeconomic health, and political stability alike. The disruption could be of a scale greater than COVID-19 and the 2008 Global Financial Crisis combined, if trust in key institutions (like banking, energy, transportation, communications and healthcare) is not rapidly restored.

Together, they create what can be described[10] as a 'quantum-driven cyber storm.' The most acute moment in that storm is known as Q-Day, the day a fault-tolerant quantum computer can factor RSA-2048 keys in hours instead of centuries, instantly exposing over 99% of today's encrypted data flows. U.S. National Institute of Standards and Technology (NIST), the European Union's Agency for Cybersecurity (ENISA) and national security agencies now treat Q-Day as an inevitable strategic event, not a distant hypothesis. Regulators believe we are 10 years from this point, calling for transitions by 2035[11]. However, a recent survey of over 900 quantum computing academics show that 40% of them believe quantum computing will become a superior technology within five years, much faster than expected, echoing findings from other expert surveys such as by the Global Risk Institute[12].

Yet, amid talk of new algorithms and hardware, the critical weak link remains largely overlooked: the randomness that creates security keys.

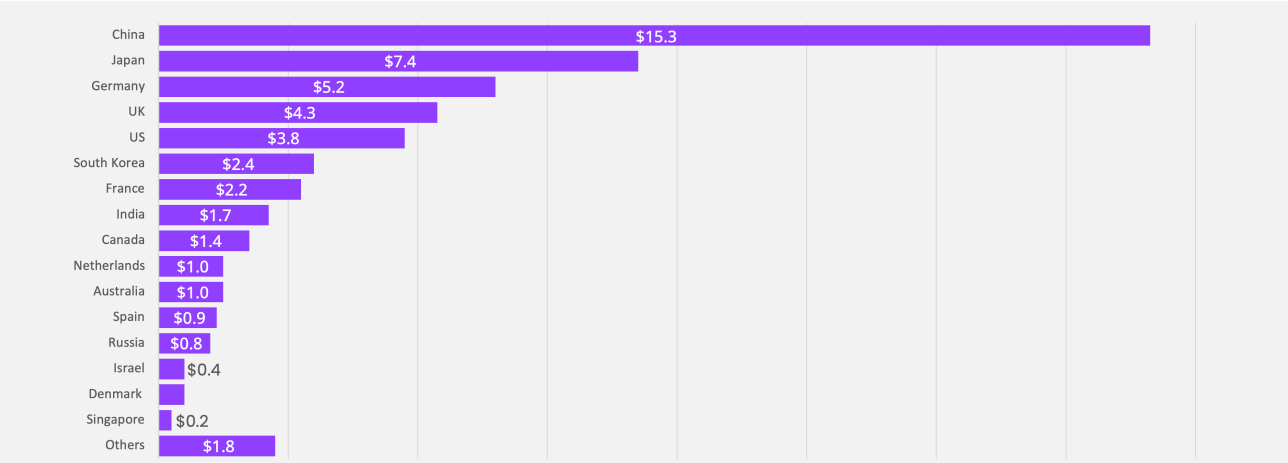
Security keys are the *Achilles Heel* or weak link in an organization's defense against quantum threats. These are the keys protecting a company's most valuable asset: data. If an adversary can model the pattern of your keys, they can model the pattern of your defenses. Randomness itself must become a governed asset.

The greater the randomness of these security keys, the more protected an organization is. Unfortunately today fewer than 1% of public or private organizations today have truly random keys, and are severely exposed to a quantum attack[13].

The first step is recognizing that the storm is already forming on the horizon, and that the time to build Loki's Shield is now.

China is racing ahead with large investments in quantum technologies

Announced Government investments in quantum technologies, $ billions

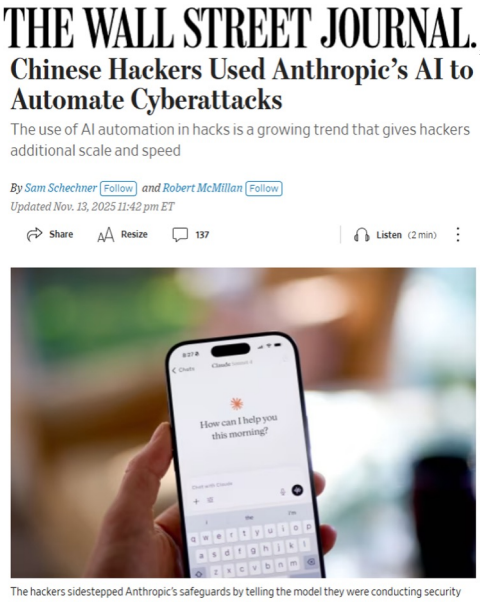


Source: McKinsey Quantum Technology Monitor 2024, 2025, https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/the-year-of-quantum-from-concept-to-reality-in-2025, https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/steady-progress-in-approaching-the-quantum-advantage

'Harvest now/decrypt later': Beijing has stolen data on every British citizen, security experts warn

Dominic Hauschild, Ben Spencer and Dipesh Gadher

THE SUNDAY TIMES



THE WALL STREET JOURNAL.

Chinese Hackers Used Anthropic's AI to Automate Cyberattacks

The use of AI automation in hacks is a growing trend that gives hackers additional scale and speed

By Sam Schechner Follow and Robert McMillan Follow

Updated Nov. 13, 2025 11:42 pm ET

Share Resize 137 Listen (2 min)

The hackers sidestepped Anthropic's safeguards by telling the model they were conducting security audits on behalf of the targets. GABBY JONES/BLOOMBERG NEWS

***Above**: Media coverage reveals that AI-assisted and 'harvest now/decrypt later' cyber attacks are real threats today, and no longer speculation*

2

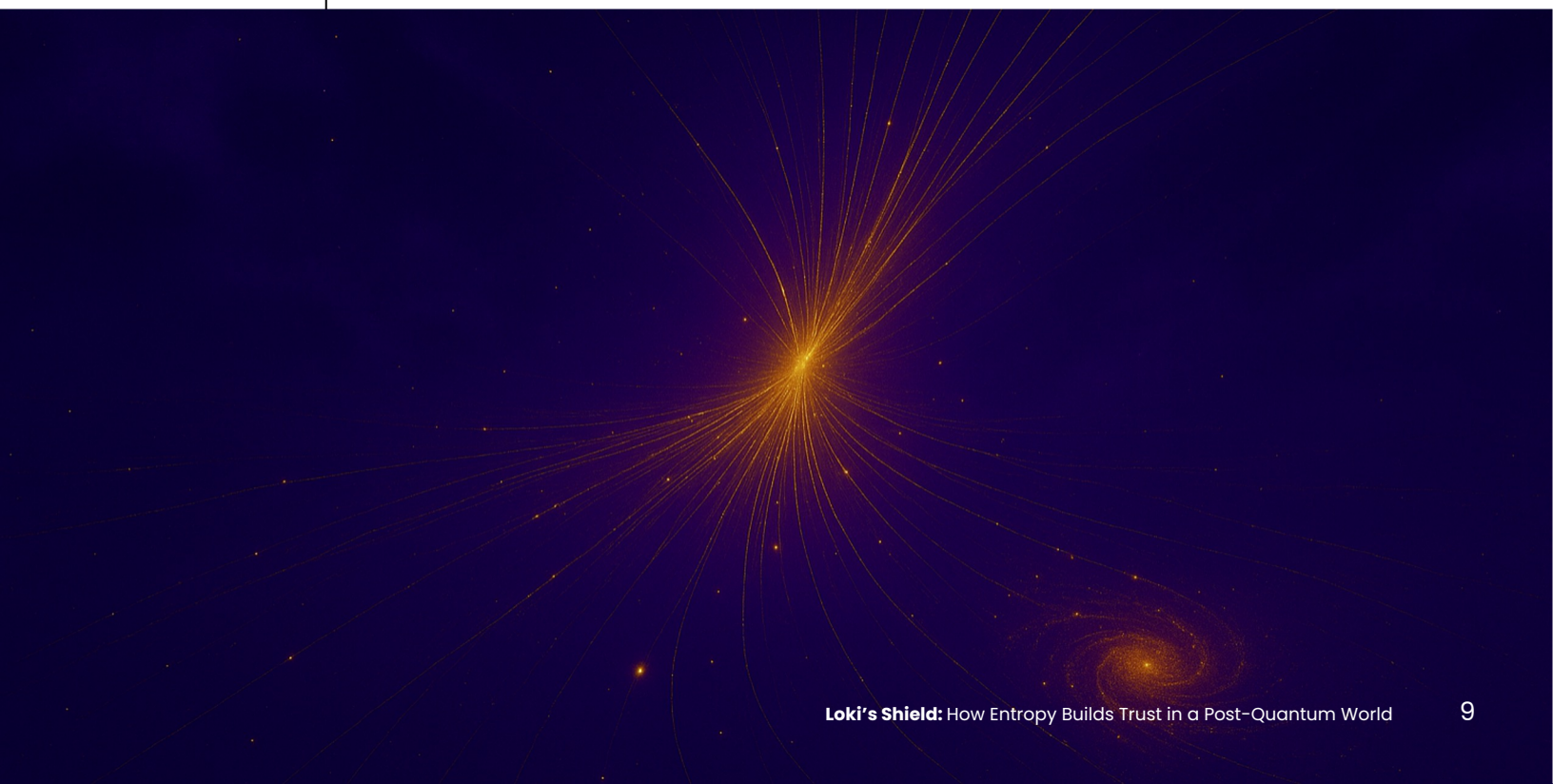
The Q-Day Risk

Precision Surgery vs Chemotherapy

For more than three decades, the backbone of digital trust has rested on a single mathematical assumption; that factoring very large numbers is computationally infeasible. The RSA 2048-bit standard, adopted globally since 2000, underpins online banking, identity verification, e-commerce, cloud encryption, and much of government communication. When that assumption fails, *everything* built upon it collapses.

That failure now has a name: Q-Day. It marks the moment when a sufficiently powerful quantum computer can perform Shor's Algorithm at scale, reducing RSA 2048 (or ECC P-256 encryption) from a task that would take classical supercomputers longer than the age of the universe to one solvable in *hours*. NIST has been explicit: *"All public-key schemes based on factoring and discrete logarithms are vulnerable to quantum attack[14]."*

For years, crossing this threshold was believed to be decades out. Now, with faster than expected advances in quantum technologies, many experts believe the world could be less than 5 years away from Q-Day.



Quantum Technologies are Scaling Faster than Projected

Quantum computing has entered an industrial acceleration phase that is moving faster than even its architects predicted. In 2019, Hartmut Neven, Director of Google's Quantum AI Labs, observed that both qubit counts and reliability were improving together, creating a double-exponential growth curve now known as *Neven's Law*.

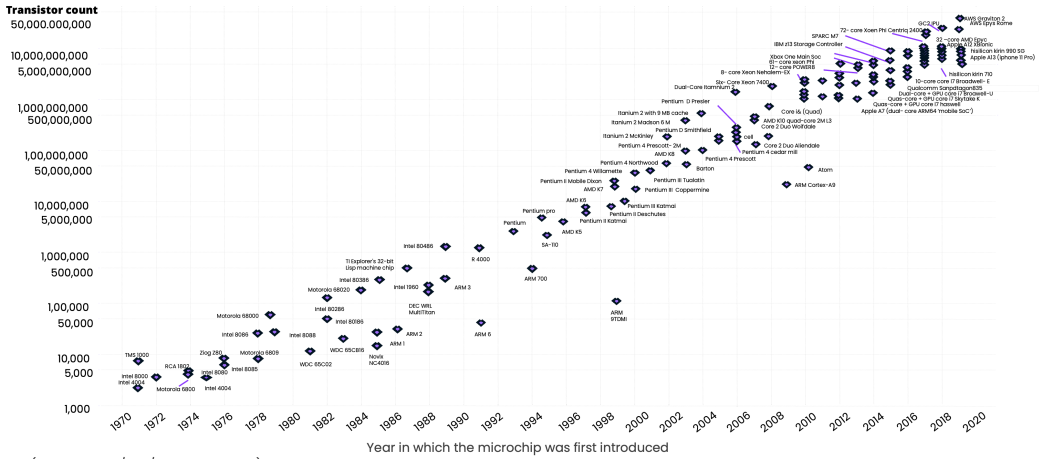
IBM's systems illustrate the curve: from a 5-qubit prototype in 2017 to 127-qubits (Eagle, 2021), 433-qubits (Osprey, 2022), and 1,121-qubits (Condor, 2023), with a 100,000-qubit roadmap before 2030,[15] showing a 20,000X improvement within just a decade. Google's Willow quantum processor (2025) produced a chemistry simulation 13,000X faster[16] than the best classical model, a breakthrough that many 2023 forecasts expected only after 2030. In 2025, IonQ reached 99.99% two-qubit gate fidelity, crossing the "four-nines" threshold required for scalable error correction[17]. Each of these steps doubles usable computing power while halving error, compounding progress far beyond Moore's Law.

Expert forecasts are struggling to keep up. A 2024 survey of 900 quantum experts found 51% believe development is *ahead of schedule*, and 40% now expect quantum advantage by 2029[18], cutting earlier 10-to-15-year roadmaps nearly in half. Predictions of "modest 10-100X speed-ups by 2025[19]" have already been eclipsed by Google's Willow 13,000X breakthrough.

The acceleration is mirrored in investment and deployment. Global quantum revenues will exceed US$1 billion in 2025, up 54% year-on-year[20], driven by commercial access through IBM Q[21], Amazon Braket[22], and Azure Quantum[23] for tasks such as portfolio optimization (Goldman Sachs)[24], catalyst simulation (BASF[25] and Dow[26]), and materials design (Volkswagen[27]). PsiQuantum's $1 billion raise in 2025 with chip manufacturer GlobalFoundries marks the shift from laboratory photonic chips to commercially-viable factory production lines[28]. Operational proof is arriving, too. In April 2025, Australia's Q-CTRL guided an aircraft 500 km without GPS by using a quantum sensor accurate to 150m[29] or roughly 50X better than conventional inertial systems. Such demonstrations confirm that quantum technology is crossing from controlled labs into applied infrastructure.

Moore's Law: in Classical Computing, the number of transistors on microchips doubles every two years

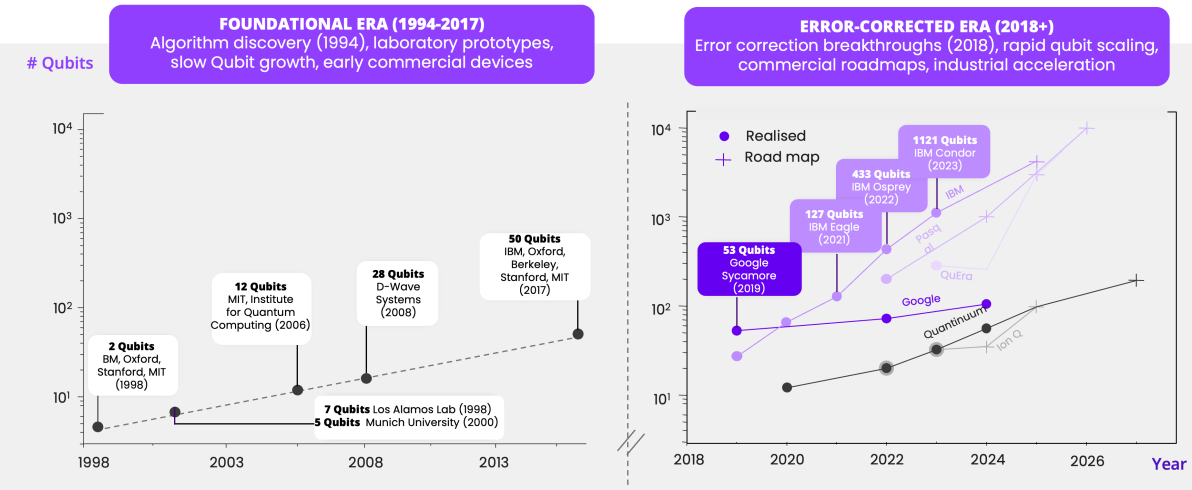
Moore's Law describes how the number of transistors on integrated circuits doubles every two years. This advancement was critical in classical computing for fifty years since the 1970s to improve processing speed or reduce the price of computers.



Source:Wikipedia (wikipedia.org/wiki/Transistor count)

Milestones in Quantum Computing: From Early Discoveries to Exponential Breakthroughs

A decade of technological breakthroughs is now allowing quantum computing to rapidly scale

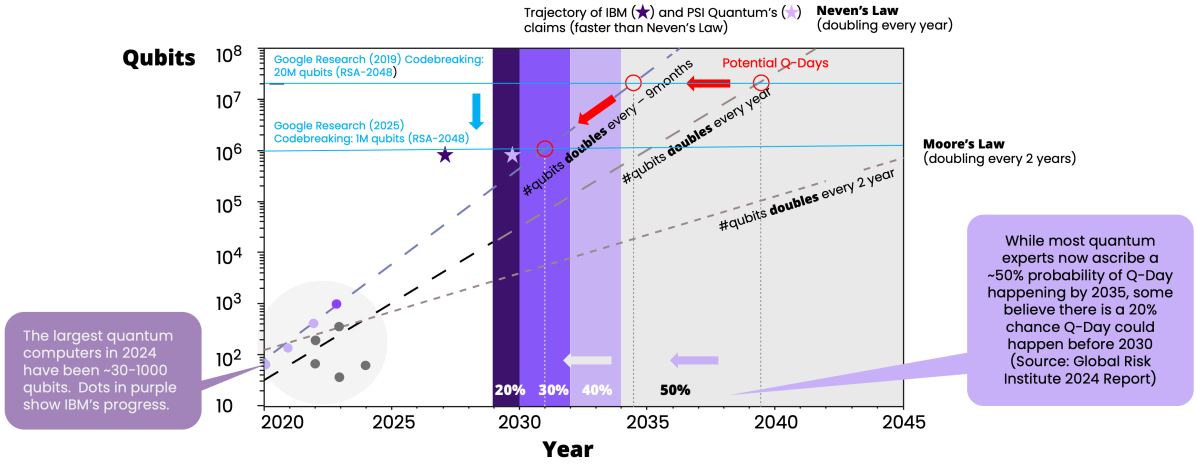


Source: Koen Groenland, Introduction to Quantum Computing for Business (2025)

Above: *Quantum computing has shifted from slow, experimental progress to an era of rapid, error-corrected scaling. Early laboratory prototypes have given way to commercial roadmaps delivering hundreds—and soon thousands—of qubits. This acceleration highlights why cryptographic systems must prepare now for exponential breakthroughs in quantum capability.*

Extrapolating Neven's Law: Long term quantum outlook and a rapidly approaching Q-Day

Extrapolating the current pace of development at more than double Moore's Law reveals a rapidly approaching Q-Day (the moment a quantum computer can break RSA-2048 encryption)

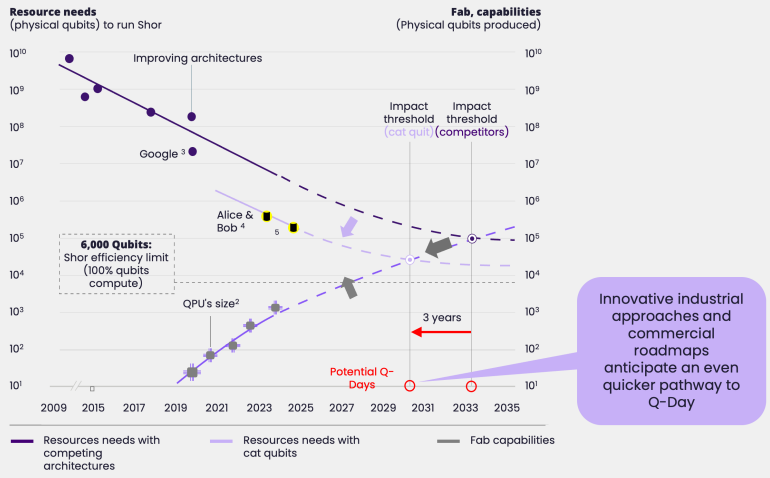


Source: https://thequantuminsider.com/2025/05/24/google-researcher-lowers-quantum-bar-to-crack-rsa-encryption/, Global Risk Institute and EvolutionQ 2024 Report

Above: *Extrapolating Neven's Law shows quantum progress accelerating far beyond Moore's Law, with qubit counts doubling several times per year. Recent Google research suggests RSA-2048 may be breakable with fewer than 20 million physical qubits—far below earlier assumptions. Combined with expert forecasts placing "Q-Day" in the early 2030s, this highlights an increasingly urgent transition window.*

Rapid breakthroughs in quantum are accelerating progress toward Q-Day at an even faster rate

Capital and manufacturing ramp up is leading to stronger forces that accelerating Q-Day at an even faster rate



Source: Alice & Bob, McKinsey Quantum Technology Monitor June 2025

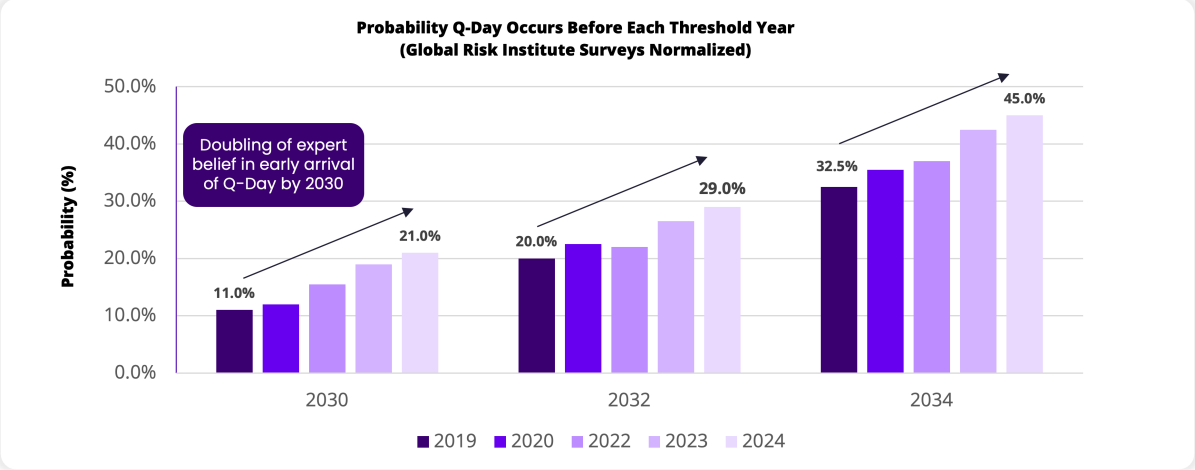
Forces accelerating the path to break RSA-2048 encryption

- Algorithmic optimizations
- Error-correction breakthroughs
- Hardware fidelity gains
- Scaling architectures
- Resource-estimation refinements
- Capital and manufacturing ramp up

Above: *Breakthroughs in algorithms, error correction, and quantum hardware are sharply reducing the resources needed to break RSA-2048. Industrial scaling and manufacturing advances are accelerating physical qubit capacity. Together, these trends point to an increasingly compressed timeline toward Q-Day as quantum systems approach practical cryptanalytic capability far sooner than anticipated.*

Between 2019-2024, experts revisited and brought forward their predictions for the arrival of Q-Day

Each year, more quantum experts believed that Q-Day would occur sooner for the threshold years of 2030, 2032 and 2034

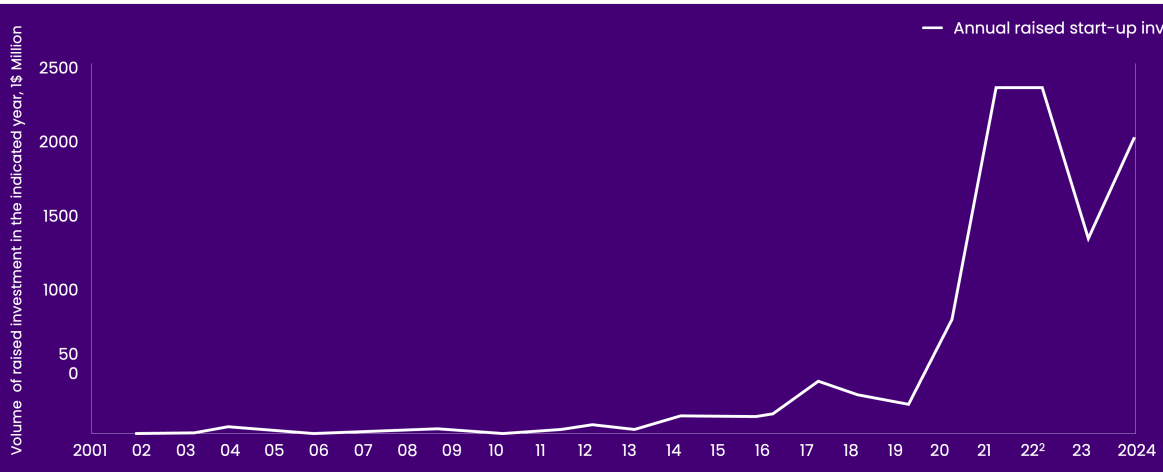


Source: Global Risk Institute and EvolutionQ 2024 Report with normalized survey data of quantum experts

Above: *Expert assessments of Q-Day have shifted markedly over the past five years. Surveys show a doubling of belief that RSA-2048 could be broken by 2030, with rising probabilities across 2032 and 2034 as well. The trend reflects growing confidence in accelerated quantum progress and tightening cryptographic timelines.*

Since 2020, there has been significant VC investments into quantum

Momentum has continued, including with several major, multi-billion dollar quantum manufacturing investments



1. Based on investment data recorded in PitchBook; actual investment likely higher (excludes investments with missing details on investment types); data availability on start-up investment in China is limited.
2. Excludes other uncategorized funding data.

Source: PitchBook

Above: *Quantum investment has surged since 2020, signalling accelerating industrialisation and rising confidence in commercially meaningful quantum breakthroughs.*

Together these milestones show a feedback loop of technology, capital, and commercialization. Under Neven's Law, each advance accelerates the next, while expert expectations continue to be rewritten in real time. Quantum momentum is no longer theoretical, but is unfolding years ahead of schedule.

Most "quantum-readiness" strategies assume ample time, yet hardware roadmaps are showing the opposite. For example, IBM's Condor chip leapt from 433-qubits to 1,121-qubits between 2022 and 2024, and Google's Sycamore 2 demonstrated similar acceleration. If credible 10,000-logical-qubit systems emerge before 2030, the window for safe migration shrinks dramatically.

Analysts estimate that if Q-Day arrived prematurely (even five years ahead of projections) the global cost of compromised data could exceed trillions of dollars, rivaling the 2008 Global Financial Crisis and COVID-19 in economic disruption impact[30]. Just two months of heavily disrupted global GDP would cost the world over $20 trillion in lost productivity. The WEF Transitioning to a Quantum-Secure Economy Report (2022) adds that organizations face a dual challenge: '*Harvest Now/Decrypt Later (HNDL) attacks'*, in which adversaries steal and store encrypted data today, and *reactive migration failure*, when institutions wait too long and are forced into chaotic emergency upgrades.

Why current quantum safeguarding approaches fail

Most enterprise approaches to address quantum vulnerabilities fall into three flawed categories:

1. Slow Migration to 2035 Targets

Many enterprises still plan around NIST's PQC standardization horizon of 2035, budgeting algorithmic transition as a slow compliance project. Yet every hardware forecast points to a shorter fuse. Delaying migration turns long-term encryption assets into immediate liabilities: data copied today could be decrypted the moment machines reach scale. Quantum risk is no longer theoretical; it is compounding faster than defensive planning cycles.

2. Hardware-Only Safeguards (QKD and HSM Replacement)

Some organizations respond to the quantum threat by investing in new hardware. Quantum Key Distribution (QKD), which uses entangled photons to exchange encryption keys, offers physics-level security but remains prohibitively expensive and difficult to scale. Each dedicated fiber link costs roughly between $250,000 and 500,000 to deploy and maintain,[31] nearly a 1000X the cost of a conventional encrypted connection, and typically functions only across 100–200 km before requiring trusted repeater nodes or satellites. At enterprise scale this translates into tens of millions of dollars in capital cost, making QKD viable only for sovereign, defense, or inter-bank networks, not for commercial supply chains or global data platforms.

Replacing fleets of Hardware Security Modules (HSMs) presents a different challenge: upgrade cycles run 24–36 months per enterprise, lagging behind quantum hardware progress. Meanwhile, partial quantum accelerators, already integrated into finance and defense workflows, signal that operational quantum capability will arrive years ahead of the 2035 PQC timeline. Hardware can fortify endpoints, but it cannot keep pace with a software-driven threat landscape.

3. Full Data-System Re-engineering

At the other extreme, some firms attempt full-stack redesigns - rewriting databases, identity systems, and APIs around post-quantum algorithms.[32]

Industry analyses show that large-scale, 'big-bang,' cryptographic changeovers are among the leading causes of cloud downtime. For example, Gartner[33] and Venafi/Cyberark report that mis-managed certificate renewals[34] already account for up to 75% of cryptography-related outages[35], and the Uptime Institute[36] finds most major service disruptions stem from configuration errors. NIST and the World Economic Forum[37] both warn that post-quantum transitions amplify these risks. Re-platforming can thus add complexity without strengthening the underlying entropy that defines true cryptographic resilience.

Bridging the Gap

Each path is analogous to broad-spectrum chemotherapy: expensive, painful, and disruptive to healthy systems.

Between slow compliance and disruptive overhauls lies a pragmatic (precision surgery) alternative: a software-layer approach that enhances entropy and key management now, while remaining compatible with future post-quantum algorithms. This method secures today's systems against tomorrow's machines, closing the readiness gap without waiting for 2035.

Why Security Keys Are the Crucial Line of Defense

Cryptographic keys are the invisible credentials that make digital life possible. Every secure email, bank transfer, identity card, or industrial sensor relies on a pair of numbers (a public key that anyone can see and a private key known only to its owner) to prove authenticity and encrypt information. These keys are generated from random numbers, yet they differ from passwords or firewalls: they are machine-to-machine trust itself.

Once a key is copied, guessed, or mathematically reconstructed, the system no longer knows whom to trust. A single leaked private key can silently unlock millions of records or spoof an entire organization's identity. Because keys are routinely cached, backed up, or embedded in code repositories, they spread faster than any other security element. Quantum and AI advances now threaten to predict or decrypt weakly random keys at scale, turning the cornerstone of cybersecurity into its most critical point of failure.

WHAT HAPPENS ON Q-DAY?

FOUR PHASES OF COLLAPSE: FROM TRUST FAILURE TO NATIONAL PARALYSIS

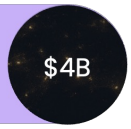
The Trigger

A state-level actor or major technology firm achieves quantum decryption capability- successfully running Shor's algorithm to break RSA and elliptic-curve cryptography (ECC). Decades of intercepted, encrypted data are suddenly readable under the long-anticipated harvest now, decrypt later strategy. Within hours, attackers can forge digital signatures, impersonate institutions, and disrupt authentication across every sector dependent on public-key infrastructure (PKI). The event - termed Q-Day - marks the first real test of digital trust at a national scale.

The First Hour
Loss of Digital Certainty - The Fracture

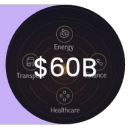
In the opening hour of a quantum decryption breakthrough, confidence in digital infrastructure weakens rapidly. Grid and telecom operators detect authentication errors as digital certificates and keys fail validation. Around 5–10% of substations lose trusted telemetry, prompting grid segmentation to prevent false commands. Internet backbone operators observe 1–3% route instability and increased latency of 100–200 milliseconds due to failed TLS handshakes. In finance, 5–10% of payment APIs return verification errors, forcing short suspensions. Government e-services and logistics management systems begin flagging digital signature anomalies. The aggregate output loss - less than 1% of daily GDP, or roughly $1.7 billion in a U.S.-sized economy - is operationally minor but strategically significant. The event confirms that public-key infrastructure (PKI) and cryptographic trust chains form the most critical vulnerability in national continuity planning.

The First Day
Patchwork Blackouts and Service Pauses



Within 24 hours, local disruptions compound into multi-sector degradation. In energy, authenticated control signals fail in several regional grids, reducing supply 15–25% and triggering limited blackouts. Telecommunications experience 10–20% throughput losses as certificate errors affect routing and DNS services. Financial clearinghouses impose manual review, delaying 20–40% of payments, while major stock exchanges temporarily halt settlement functions. Ports and rail terminals revert to manual operations, cutting throughput 25–30%, and fuel pipelines throttle flow by 30–40%. Healthcare and water utilities shift partial operations to manual oversight, each operating 10–15% below baseline. Government digital services face 20–30% outages due to expired certificates. Cumulative daily GDP declines 3–4%, equivalent to $3.8 billion in lost output. The episode remains geographically uneven, but confidence in remote automation and cloud control systems begins to erode, setting the stage for broader contagion.

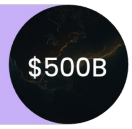
The First Week:
Systemic Contagion and Early Remediation Attempts



By the end of the first week, previously isolated failures evolve into a synchronized crisis. Power generation and transmission drop 30–50%, leading to nationwide rolling blackouts. Financial networks face their most acute stress: 70% of electronic transactions stall as digital certificates expire or are revoked. Telecommunications throughput declines 20–35%, reducing the reliability of command systems and emergency coordination. Ports, airports, and freight rail operate 40–60% below capacity, creating fuel and food distribution shortfalls. Hospitals and water utilities continue at 70–75% capacity, but increasingly rely on manual control.

Efforts to restore trust begin: emergency PKI resets and initial post-quantum cryptographic (PQC) patches are tested in isolated systems. However, supply of certified firmware is limited, and inconsistent vendor standards create new vulnerabilities. Estimated GDP loss reaches $60 billion, roughly 12% of weekly output. The event shifts from a cybersecurity incident to a logistics and trust management emergency.

The First Month
National Paralysis and Chaotic Recovery



After one month, cascading failures solidify into operational paralysis. Grid recovery remains constrained by unverified firmware and missing cryptographic keys, leaving about 60% of U.S. households under rolling outages. Telecom throughput remains 40–60% below normal, and nine out of ten financial transactions are suspended or manually validated. Ports, airports, and rail terminals function at 20–30% capacity, while healthcare and water systems operate at 40–60% of baseline.

The national focus shifts from containment to recovery. Governments and technology providers initiate a global scramble to deploy post-quantum security patches and new PQC-compliant firmware, but the transition is chaotic. Hardware shortages, fragmented standards, and fake patch updates complicate implementation. Systems patched without verification occasionally fail or reintroduce vulnerabilities. The cumulative impact exceeds $500 billion, or around 2% of U.S. annual GDP - the equivalent of a deep recession compressed into four weeks. Recovery requires not only cryptographic modernization but also cross-sector coordination to manage simultaneous trust restoration at scale.

In recognition of this growing fragility, The Certification Authority Browser Forum[38] (made up of internet browser software and certificate issuers like Google, Apple, SSL.com) voted in 2025 to shorten the lifespan of public Transport Layer Security (TLS) certificates (the digital files that authenticates a website's identity or public key and enables encrypted communication between a web server and a browser such as via an encrypted connection like HTTPS) from 398 days today to 47 days by 2029 - forcing global systems to refresh cryptographic trust far more frequently.[39] While intended to tighten operational hygiene, this acceleration also magnifies the risk of renewal failures and automation gaps, with mis-managed certificate rotations now ranking among the leading causes of cloud outages.

Unlike passwords or firewalls, cryptographic keys are the root of digital trust. They unlock everything from payment rails to nuclear-command networks. A single exposed private key can compromise millions of transactions and identities simultaneously. Keys are also copied, cached, and transmitted more widely than any other security element, yet their randomness is rarely verified. When a quantum or AI adversary predicts or reconstructs a key pattern, the entire security architecture collapses regardless of how many other defenses remain intact. That is why strengthening key entropy is not one control among many; it is *the* control on which all others depend.

Where Keys Hide in Your Organization

Cryptographic keys are the digital world's master credentials - mathematical codes proving who can read, write, or move data. Unlike passwords, they underpin every secure transaction, cloud login, and payment rail. If a key is weak, guessed, or stolen, all linked systems fail at once. Quantum and AI tools now threaten to predict keys, making entropy the last true defence.

Keys aren't confined to data centers. They live everywhere: inside cloud access tokens, server certificates, VPN tunnels, and payment APIs. Every connected sensor, laptop, and software update relies on them. Many firms unknowingly hold millions of active keys - some hard-coded into legacy systems or embedded in vendor firmware. When one leaks or is reused, entire supply chains can be compromised.

A more surgical intervention: High-Entropy Security Keys

If Q-Day's immediate vulnerability lies in the *predictability* of security keys, the more effective strategy is precision surgery: strengthen the randomness source that feeds all cryptography. True protection comes from entropy-assured key generation - producing cryptographic material so unpredictable that even quantum systems cannot model its pattern space.

Independent telecom pilots coordinated through the European Telecommunication Standards Institute's (ETSI) Quantum-Safe Cryptography working groups[40] and the GSMA's Quantum-Safe Telecom Readiness White Paper[41] (2024) have shown that *entropy quality* (the true randomness of key material) is a stronger predictor of migration success than the *specific algorithm* chosen. This finding aligns with NIST SP 800-90B[42], which identifies entropy assessment as foundational to cryptographic robustness. The World Economic Forum's Quantum Readiness Toolkit[43] (2023) similarly lists Random Number Generation (RNG) and Entropy Management alongside algorithmic approaches (Post-Quantum Cryptography or PQC) and hardware approaches (Quantum Key Distribution or QKD) as core pillars of a secure transition roadmap.

Entrokey's software-only Entropy Integrity Score (EIS) implements precisely this: hybrid seeding to include hardware Quantum Random Number Generator (QRNG)

plus software algorithmic 'seed' for a Cryptographically Secure Pseudorandom Number Generator (CSPRNG), continuous entropy scoring (over 0.99 min-entropy), and real-time auditing aligned with U.S. Presidential Executive Orders (EO 14144 June 2025 update and OMB M-24-04). Deploying it requires no new hardware and can be achieved through a simple configuration update across existing libraries that implement the SSL and TLS protocols which secures the most internet and e-commerce traffic, such as OpenSSL or BoringSSL used by Google.

This approach converts the migration problem from a decade-long infrastructure overhaul into a software update cycle measured in weeks. It is targeted, reversible, and immediately testable; the medical analogy of a precision operation that removes the tumor before metastasis.

The message for executives is clear: waiting for universal Post-Quantum Cryptography (PQC) rollouts is a gamble; securing entropy is an investment in survivability. In the same way early cancer detection saves lives, early entropy assurance saves organizations.

The Algorithms at Risk: RSA, ECC and Shor's Quantum Breakthrough

RSA-2048 (Rivest, Shamir, Adleman, 1977)

Invented at MIT in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman, RSA is the world's most pervasive encryption system, protecting everything from online banking and email to national defense communications. Its 2048-bit variant (RSA-2048) relies on the infeasibility of factoring two large primes. Billions of devices use RSA through protocols like TLS, HTTPS, and digital signatures, forming the trust backbone of the Internet. A single fault-tolerant quantum computer could break it within hours. The "2048" in RSA-2048 refers to the key length in bits - twice as strong as the earlier RSA-1024 and about half the size of RSA-4096 - representing a 617-digit number with roughly 2^{1024} possible factors, whose sheer magnitude makes classical decryption infeasible.

ECC P-256 (Elliptic-Curve Cryptography 1985-2005)

Proposed by Neal Koblitz and Victor Miller in 1985, elliptic-curve cryptography became the compact, energy-efficient successor to RSA. Adopted widely after NSA Suite B and NIST P-256 approval in the 2000s, ECC powers secure messaging, IoT authentication, and mobile payments. It offers equivalent strength with far shorter keys - critical for constrained devices. It is now embedded in Apple, Google, and government systems worldwide. Yet ECC's mathematical foundation, the discrete-logarithm problem, is also vulnerable to Shor's Algorithm, meaning quantum breakthroughs could simultaneously neutralize both RSA and ECC defenses. The "P-256" in ECC P-256 refers to a 256-bit elliptic-curve system that secures data using geometric mathematics rather than large prime factors, achieving the same protection as RSA-3072 with far smaller keys—ideal for mobile devices, sensors, and government networks.

Shor's Algorithm (1994)

Before 1994, RSA and ECC were considered unbreakable because classical computers could not efficiently factor large numbers or solve elliptic-curve logarithms - tasks requiring trillions of years even on supercomputers. Peter Shor, at Bell Labs, discovered a quantum algorithm that performs both exponentially faster by exploiting quantum parallelism. This breakthrough showed that a sufficiently powerful quantum computer could not only decode RSA and ECC keys but also solve other intractable problems in chemistry, materials science, and optimization. Shor's paper effectively transformed quantum computing from a theoretical pursuit into an existential threat to modern encryption — enabling not only code-breaking, but new modeling advances in chemistry, AI, and logistics.

"Harvest Now, Decrypt Later" Attacks

State-sponsored hackers are quietly copying encrypted data, emails, health, defense records and national security information to decrypt once quantum computers mature. These 'time-bomb' breaches mean secrets stolen today may be exposed years later, making post-quantum security an immediate, not future, priority for governments and corporations alike. Here are six 'Harvest Now Decrypt Later' threats that have been recently exposed:

Salt Typhoon (2025)	The 2025 *Salt Typhoon* campaign, linked to China, reportedly infiltrated the records of 65 million UK citizens held in government databases, as well as U.S. government networks including those used by the U.S. President and Vice-President.
Volt Typhoon (2023 – ongoing)	U.S. and Five Eyes intelligence agencies warned that this state-sponsored group linked to China pre-positioned within U.S. critical-infrastructure networks (energy, telecoms, transport) to *maintain long-term access* for future disruption.
APT 29 'Cozy Bear' (2020 – 2024)	Behind the *SolarWinds* breach and follow-on espionage, it exfiltrated vast troves of encrypted diplomatic and defense emails. Western intelligence agencies later assessed these datasets were being archived by Russia-linked groups for potential post-quantum exploitation.
Chimera Group (2020 – 2022)	This China-linked group targeted telecom operators and universities from the EU and Taiwan, copying credential stores and VPN logs - prime "decrypt-later" material.
APT 40 (2021 – 2023)	This China-linked attack collected encrypted design repositories and ship telemetry within the maritime and defense sectors. The Australian Cyber Security Centre warned that data was being warehoused for future analysis.
Sandworm (2015 – 2022)	Known for Ukraine grid attacks, investigators found encrypted OT/SCADA archives stored on remote servers, suggesting long-term harvest for decryption when feasible from Russia-linked groups.

Sources: CISA/NSA reports, Mandiant Intelligence (2022), Australian Cyber Security Centre (SCSC 2023), ENISA Threat Landscape (2022), NSA, UK NCSC, EU ENISA (2021-24), CISA/FBI Joint Advisory (May 2023), Reuters, The Sunday Times, CISA (2025)

3

Understand the New Threat Vector

Predictability

The speed and sophistication of cyberattacks are no longer limited by human capability. In 2025, the primary threat actors are not lone hackers but autonomous, self-learning systems powered by Artificial Intelligence (AI) and fueled by the explosion of data available across open networks.

The next escalation will be quantum computing, a technology capable of breaking through the computational limits that currently protect digital infrastructure.

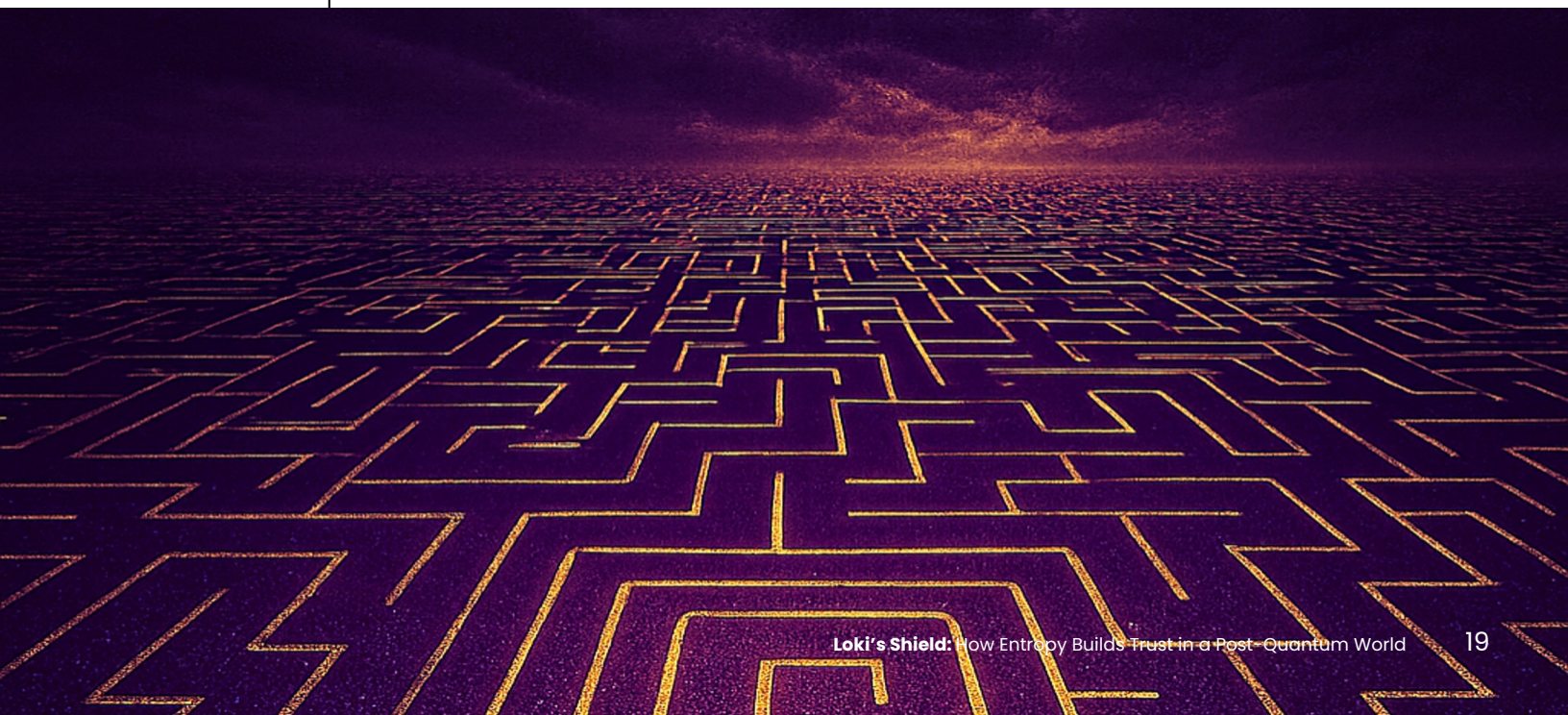
From human hackers to algorithmic adversaries

According to IBM's *2024 Cost of a Data Breach Report*[44], 51% of cyberattacks already exploit some form of AI or automation, reducing detection times from months to hours. These systems learn by recognizing behavioral and network patterns, re-creating digital maps of an organization's operations, users, and defenses faster than human analysts can respond.

In November 2025, AI company Anthropic reported it had disrupted the first AI-orchestrated cyber attack.[45] An internal review of the incident revealed that the attack was likely organized by a Chinese state-sponsored group that manipulated Anthropic's Claude AI Code to attempt to infiltrate 30 global targets (tech companies, financial institutions, chemical manufacturing companies, and government agencies), with some success, and do so with minimal human intervention.

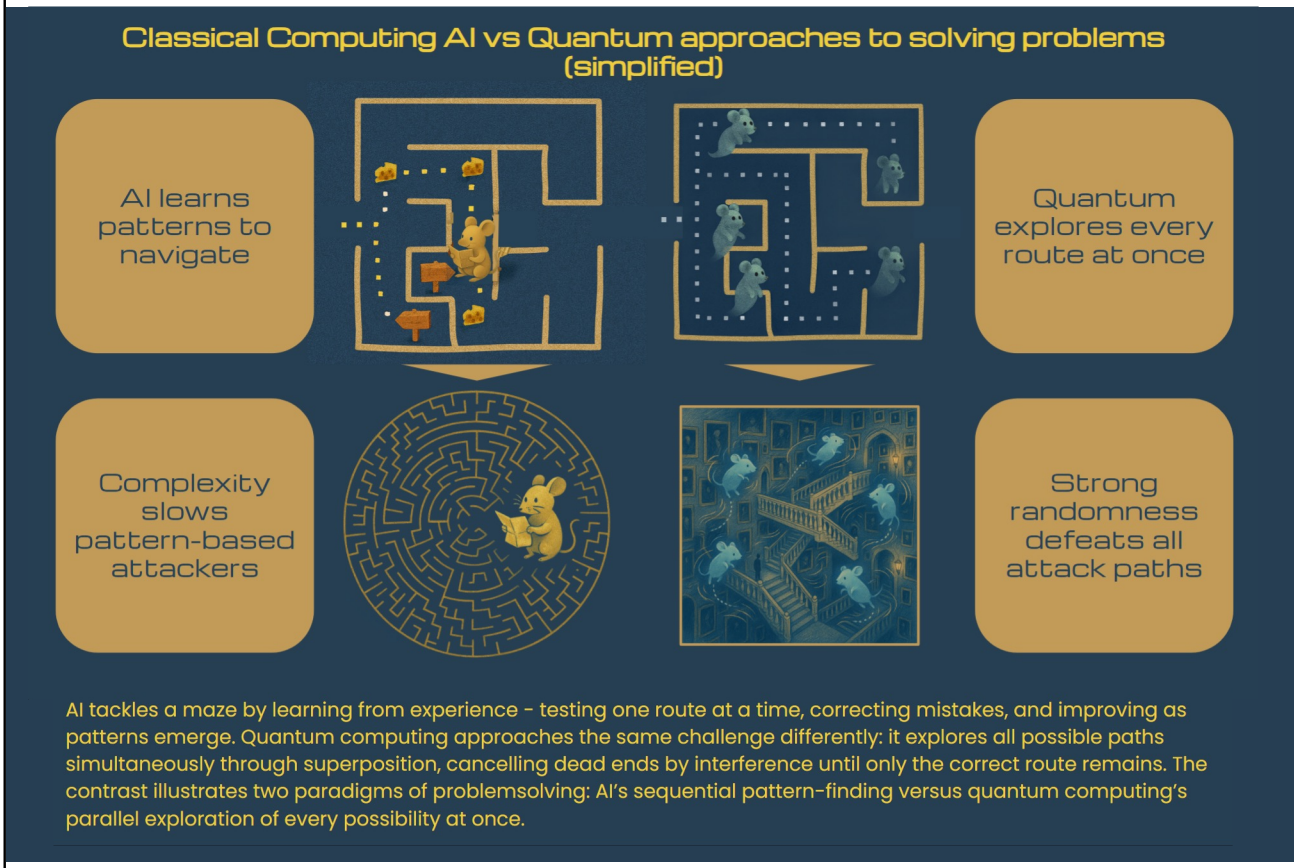
AI adversaries 'don't sleep and don't forget.' They iterate continuously, transforming every prior attack into a training dataset for the next. This 'pattern recognition war' is the heart of the modern cybersecurity arms race. Traditional defenses, such as firewalls, intrusion detection systems, and human analysts, operate sequentially, evaluating one pathway through the maze at a time. AI turns that into parallel exploration: thousands of pathways tested in seconds.

Now imagine Quantum Computing entering that same maze.



As the WEF observed in its *Quantum Readiness Toolkit (2023)*, *"AI learns; quantum solves."* While AI identifies patterns, quantum computers explore *every path at once* through superposition. Rather than sending one mouse through the maze, quantum computing sends a mouse down every corridor simultaneously, collapsing all possibilities into the optimal solution.

When applied to cybersecurity, this means that once a functional, error-corrected quantum computer reaches scale, it could crack today's most common encryption in mere hours.



AI tackles a maze by learning from experience - testing one route at a time, correcting mistakes, and improving as patterns emerge. Quantum computing approaches the same challenge differently: it explores all possible paths simultaneously through superposition, cancelling dead ends by interference until only the correct route remains. The contrast illustrates two paradigms of problemsolving: AI's sequential pattern-finding versus quantum computing's parallel exploration of every possibility at once.

The link between AI, Quantum, and Entropy

What connects both threats (AI pattern attacks and quantum brute-force decryption) is their dependence on *predictability*. The more patterns in a system, the easier it is to map, model, and exploit.

The only true defense is unpredictability, known in cryptography as entropy.

Entropy determines how random your security keys really are. A perfect random number generator (RNG) has a min-entropy value of 1.0; anything below 0.9 introduces measurable predictability.[46]

As several research groups have noted, including work synthesized by Cambridge Frontier Technologies, weak or biased entropy undermines even quantum-resistant algorithms since randomness lies at the root of every cryptographic primitive. Both NIST[47] and ETSI[48] have warned that inadequate entropy sources can compromise post-quantum cryptography, as poorly seeded randomness leaks private keys even in mathematically secure algorithms.

By ensuring that the maze itself constantly re-shuffles, even the most advanced AI or quantum computer loses its advantage.

It's not about making encryption harder; it's about making it impossible to predict the path.

A new class of attack, a new class of defense

The combined rise of AI and quantum computing marks the first time in human history that offense and defense are both powered by machines capable of learning and superposition.

Traditional cybersecurity frameworks built around fixed algorithms and human oversight are outmatched.

As cybersecurity analysts from Cambridge Frontier Technologies Lab observed in their 2025 report,

organizations that treat entropy as a measurable operational asset will transition faster and at one-tenth the cost of those waiting for wholesale PQC adoption.

Entropy becomes the equalizer: the chaos that neutralizes the machines designed to impose order.

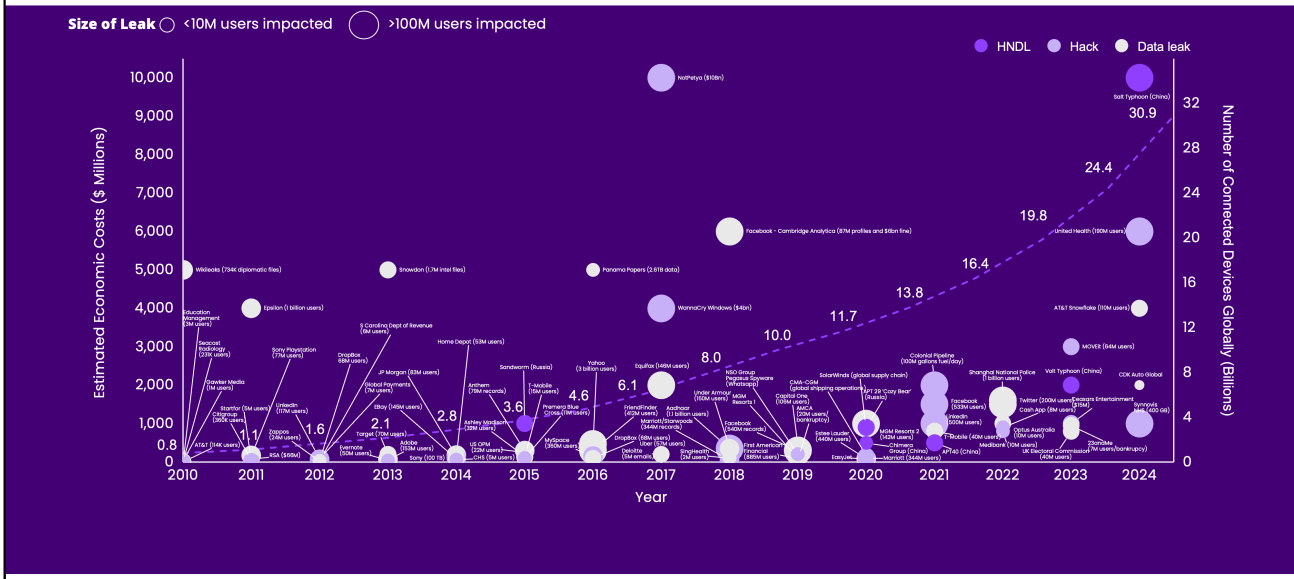
In Norse mythology, Loki, the god of chaos and randomness, could only be defeated when his unpredictability was constrained.

In today's digital mythology, chaos itself is our best defense.

Entropy is Loki's Shield.

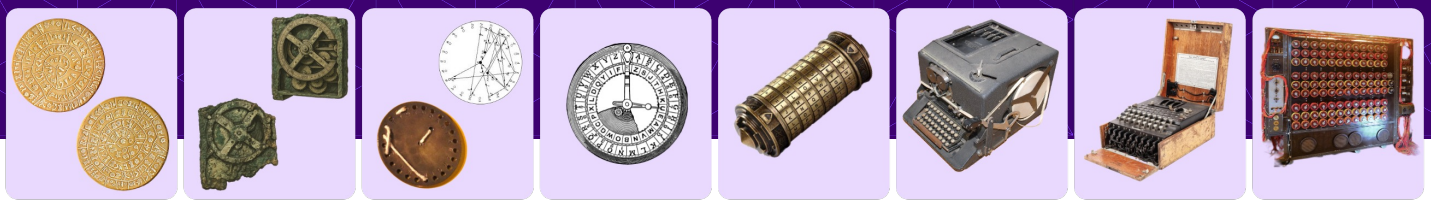
Biggest cyber incidents in history

Escalating Impact of Major Cyber Incidents



Five Eras of Modern Cryptography

Before computers, secrecy lived in gears and ink. Governments and armies relied on mechanical ciphers like Enigma and SIGABA, while human codebreakers - culminating in Britain's Bletchley Park and the Colossus computer - turned cryptanalysis into a science. WWII proved that information could win wars, and the shift from analog rotors to electronic logic marked the birth of modern cryptography.



Mainframe Foundations Era

Postwar research at Bell Labs and MIT produced Claude Shannon's Information Theory (1949), defining secrecy mathematically. As mainframes powered governments and banks, IBM's Data Encryption Standard (DES, 1977) standardized machine security. Encryption became an engineering discipline, woven into magnetic tape, early satellites, and Cold War communications - laying the electronic bedrock for digital trust.

Personal Computing Era

The invention of public-key cryptography by Diffie–Hellman and RSA (Rivest–Shamir–Adleman) solved the "key-exchange paradox," enabling strangers to trade secrets online. This enabled the first secure emails and electronic payments. Encryption moved from classified mainframes to personal computers, protecting everything from NASA's deep-space telemetry to home banking terminals. Mathematics, not secrecy, became the new courier of trust.

Internet Web 1.0 Era

The World Wide Web demanded privacy at scale. SSL/TLS, IPsec, Certificate authorities and PKI turned browsers, servers, routers, email and payment networks into safe channels. Advanced Encryption Standard (AES) replaced DES as the global encryption standard; smartphones and satellites relied on the same math to guard voice, GPS, and data. Cryptography's audience expanded from engineers to everyone with a password—evolving it from a specialist tool into an invisible layer of daily life.

Decentralized and Mobile Era

As cloud computing and AI scaled globally, cryptography followed data into hyperscale data centers. Homomorphic encryption allowed computation on encrypted information; blockchain introduced Merkle trees, proof-of-work, and zero-knowledge proofs for decentralized consensus. Space agencies tested quantum key distribution (QKD) satellites, while industries embraced privacy-enhancing technologies to share data securely. As digital currencies and identity became built upon distributed encryption, cryptography evolved into the architecture of digital trust.

Quantum and AI Resilience Era

Quantum computing's threat to RSA and ECC has triggered the greatest cryptographic transition since the 1970s. NIST's post-quantum standards - Kyber, Dilithium, and Falcon algorithms - are replacing legacy keys across government and industry. Entropy-assurance layers could redefine security as a continuous measurement, not a static lock. AI helps detect entropy drift; DNA and quantum materials promise new data-storage frontiers. Cryptography becomes self-monitoring - an adaptive immune system for the world's digital infrastructure.

4

The Science of Randomness

Entropy as a new frontier

Loki's Lesson: Harnessing Chaos

In Norse mythology, Loki was the god of chaos: unpredictable, mischievous, and impossible to contain. For millennia, civilizations feared chaos; in the digital age, we must embrace it. Randomness, or entropy, is now the ultimate defense.

The Science of Randomness

At its core, every cryptographic system relies on randomness. The numbers used to generate encryption keys, digital certificates, and authentication tokens must be truly unpredictable. If a machine, or an attacker, can anticipate the next number, the system is already compromised.

This unpredictability is measured through entropy, quantified on a scale where 1.0 represents perfect randomness. Anything lower introduces bias. NIST Special Publication 800-90B defines entropy as *"a measure of uncertainty associated with a random variable; the higher the entropy, the greater the unpredictability."*

As quantum computing and artificial intelligence advance, that unpredictability becomes the single most valuable, and fragile, commodity in cybersecurity.

How Machines Create Randomness

Random-number generation (RNG) underpins everything from the padlock icon in a web browser to the timing of a stock-exchange order. Over time, five main classes of Random Number Generation approaches have emerged - each with their own strengths, weaknesses and use cases:

Five classes of Random Number Generators (RNGs)

01 PRNG

Pseudo-Random Number Generators (PRNGs)

Mathematical formulas that simulate randomness. Fast, scalable for non-security tasks (e.g., gaming). But if the seed is known, all future outputs can be predicted.

02 CSPRNG

Cryptographically Secure PRNGs (CSPRNGs or Deterministic Random Bit Generator DRBG)

These mix in unpredictable system data – keyboard timings, network noise, disk latency – to keep output from repeating. Every encrypted web session and mobile-banking app relies on them (used widely in website cryptographic libraries such as OpenSSL and Google's BoringSSL). Yet cloud servers cloned from the same image can draw from identical entropy pools, producing similar keys. Entropy drift has caused real-world breaches (e.g., Debian OpenSSL 2008 impacted millions of systems as private keys were limited to fewer than 33,000 variations).

03 TRNG

Classical True RNGs (TRNGs)

Hardware devices harvesting natural physical noise - electrical noise, radioactive decay, avalanche diodes. Genuine physical randomness but susceptible to drift and environmental degradation without continuous monitoring.

05 Hybrid

Hybrid RNGs (TRNG/QRNG sources + CSPRNG Processing + continuous entropy validation)

Modern systems that blend TRNG/QRNG sources with CSPRNG post-processing and continuous entropy validation. Modern cloud and telecom systems blend both digital and physical sources - combining TRNG/QRNG sensor data sources with CSPRNG output. They improve quality but currently lack a consistent way to measure entropy once blended.

04 QRNG

Quantum RNGs (QRNGs)

Hardware deriving randomness from quantum phenomena - photon shot noise, beam splitters, vacuum fluctuations. Rooted in quantum physics to generate truly unpredictable bits. Used by Central Banks and Defense Networks but are costly and distance limited.

Why the Seed Matters

The seed is the *first domino*. If it's truly random, everything that follows is unpredictable; if it's copied or reused, every sequence falls the same way. Entropy integrity means checking constantly that this first domino remains trustworthy and refreshing it when it weakens.

Why This Randomness (or Entropy) Matters

Weak randomness has caused real-world breaches: cloned virtual machines producing identical keys, IoT devices reusing predictable tokens, and blockchain wallets compromised by poor seeding. The math was sound; it was the randomness behind it that failed. That silent erosion of entropy is precisely what the Entropy Integrity Score (EIS) was built to detect and correct.

Demonstrating Continuous Entropy Assurance

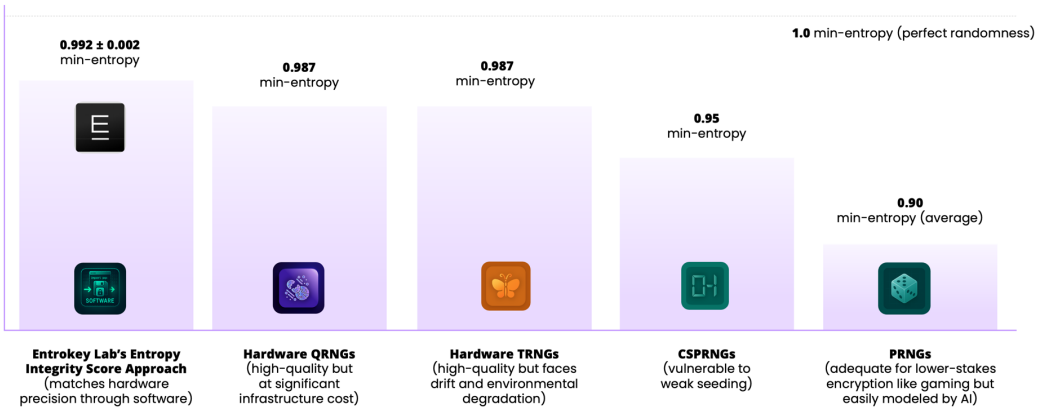
The central question behind the Entropy Integrity Score (EIS) is simple: *can software alone sustain quantum-grade randomness at enterprise scale continuously, affordably, and without new hardware?*

Entrokey Labs tested EIS across 500 cloud instances and 10 edge devices, comparing it to traditional PRNG, CSPRNG, and QRNG systems. Over four days and 100 million random samples, entropy quality was assessed using the U.S. Government's NIST Statistical Test Suite (STS), the global benchmark for detecting patterns in random sequences. It passed every test while also adding continuous, AI-resistant monitoring capable of spotting the subtle entropy drift that static tests can't see.

The results were striking. "The layer meets and exceeds the statistical rigor of NIST SP 800-22, identifying subtle non-linear patterns that the existing suite cannot detect." It also supports and augments NIST SP 800-90B entropy-source validation requirements, reinforcing FIPS 140-3 certified cryptographic modules that depend on high-quality entropy inputs.

Entropy software can sustain quantum-grade randomness at enterprise scale

Entrokey lab test using nist statistical test suite and 100 million samples on 500 cloud instances and 10 edge devices, compared to PRNG, CSPRNG, QRNG systems



Source: Cambridge Frontier Technology Labs (2025)

When deliberate bias was introduced, EIS detected and corrected drift within five minutes, automatically reseeding the entropy pool. Performance overhead remained under 1% CPU and 20MB RAM per node, with full enterprise deployment completed in less than two weeks, 10X faster than hardware retrofits that typically span 24–48 months.

Economically, EIS achieved over 90% cost reduction relative to quantum hardware deployments (~$1–2M vs ~$100–300M). These findings reveal that entropy assurance can now be delivered as a software capability rather than a capital project.

Evidence from the Field

Independent research supports these findings. Cambridge Frontier Technologies' 2025 program[49] has initiated the first large-scale entropy assessment of public Bitcoin keys, designed to analyze roughly ten percent of the ledger using both NIST-standard and AI-enhanced entropy models. Early stage analyses across synthetic and system-generated sources already show a consistent pattern: when entropy is weak or structured, cryptographic material becomes partially predictable even though the underlying algorithms remain mathematically sound.

This underscores a hard truth: encryption often fails not because the math is broken, but because the randomness seeding it quietly degrades. EIS addresses that gap directly by continuously monitoring entropy in real time and preventing the subtle drift that has contributed to past wallet vulnerabilities and multi-billion dollar losses across the broader blockchain ecosystem.

Cambridge's Predictive Indexing experiments further demonstrate why this matters. In controlled lab tests, NIST SP 800-22 repeatedly passed a deeply patterned generator as "healthy," while AI-based entropy models detected structure invisible to classical statistical tests. Small but measurable predictability far below human perception can remove dozens of bits of effective entropy, collapsing a problem believed to require astronomical brute force effort into one within reach of future large scale compute. In Entrokey's evaluation, EIS-generated sequences remained statistically indistinguishable from true randomness across NIST, compression, and ECC-bias metrics, offering no exploitable structure to AI inference models.

Together, these findings validate a new principle: entropy must be treated as a governed resource, not a background process.

Entropy Integrity as Infrastructure

For decades, high-assurance randomness depended on physical devices and certification cycles. EIS replaces that model with a living software layer that continuously measures and synchronizes entropy across systems. In doing so, it transforms randomness from a hidden engineering function into an auditable performance metric, a new category of operational integrity.

The implications extend far beyond cybersecurity: in finance, it safeguards long-term confidentiality of stored data; in energy and transportation networks, it protects control signals from predictive interference; in AI governance, it ensures that model training, token issuance, and digital identity systems cannot be gamed by entropy manipulation.

Entropy assurance is becoming the connective tissue of digital trust across critical sectors.

Policy and Economic Impact

Continuous entropy assurance also redefines the economics of quantum readiness.

Cambridge Frontier Technologies Lab (2025) Report[50] estimates that entropy-assured architectures can cut migration costs by 80% and risk exposure windows by half. Because EIS integrates into existing cryptographic libraries, it converts quantum readiness from a multi-year infrastructure upgrade into a routine software update. This is the "quantum-security dividend": faster resilience at lower cost and greater transparency.

Entropy as "Clean Energy" for the Digital Economy

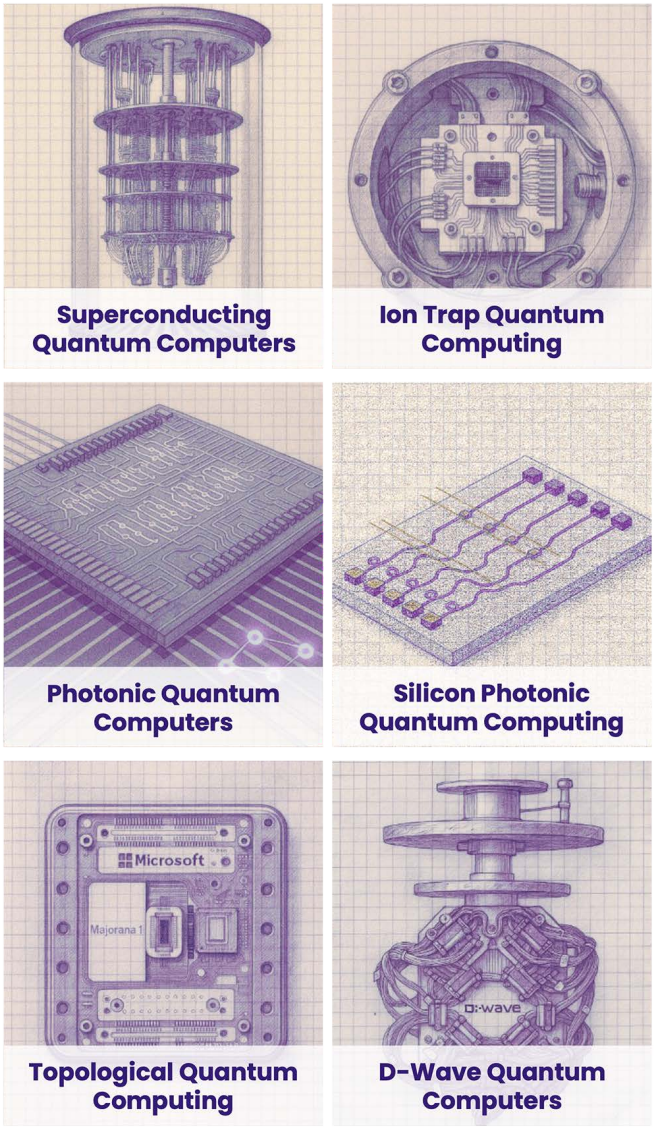
Entropy is to cybersecurity what clean energy is to the environment: the invisible foundation of sustainability.

It fuels every transaction, certificate, and digital identity without being seen. When measured, regulated, and refreshed continuously, it provides the stability to withstand even quantum-scale shocks. As the Cambridge Frontier Technologies Lab Report (2025) observed, *"entropy is the clean energy of computation - the resource that turns mathematical hardness into real-world resilience."* Like renewable power grids, entropy assurance requires constant monitoring and transparent governance.

Entropy is not chaos. It is structured unpredictability, the scientific expression of resilience. And like Loki's shield, it transforms chaos into protection.

When harnessed correctly, randomness becomes order's strongest ally.

The Technological Race for Quantum Supremacy



Source: Michio Kaku (2025) Quantum Supremacy

5

Why Entropy determines the Post Quantum Cryptography Pathway

The Cryptographic Trust Stack

A central requirement in post-quantum transitions is **crypto-agility**: the ability to update algorithms, keys, and cryptographic modules at software speed without re-architecting infrastructure.

Modern cryptography rests on a three-layer trust stack:

- At the base is **entropy**, the randomness that seeds encryption keys and session secrets.
- Above it sits the **algorithm layer,** the familiar machinery of RSA, ECC, AES and the new post-quantum algorithms such as Kyber, Dilithium and Falcon.
- At the top lies the **infrastructure and governance layer**: certificate lifecycles, key-management systems, HSMs, identity frameworks, and compliance controls.

Weakness propagates upward from an unstable base. If entropy at Layer 1 becomes predictable, even the strongest post-quantum algorithms at Layer 2 fail, and the operational systems at Layer 3 inherit systemic fragility. Most enterprises today lack crypto agility. Their cryptographic modules, HSMs, and certificate systems are tightly coupled to specific entropy sources and algorithms, creating brittle upgrade paths that significantly slow PQC migration.

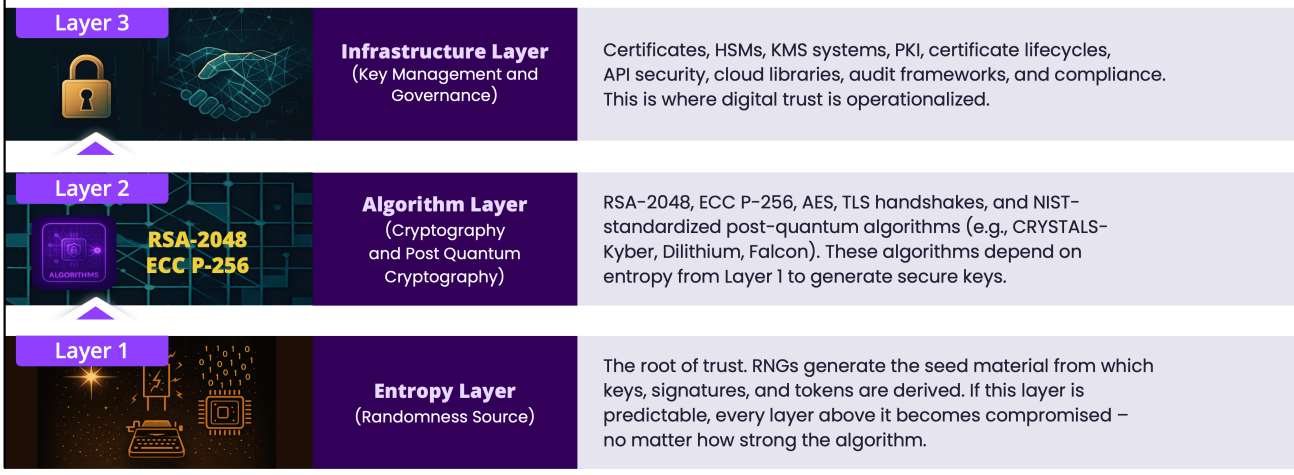
This is why the choice of random-number generator determines an organization's post-quantum transition roadmap. Each RNG class carries different strengths, deployment models and path dependencies.

PRNGs: These funnel organizations into a high-risk path that requires an expensive and comprehensive algorithmic overhaul, i.e., replacing RSA-2048 and ECC P-128 across all keys in an organization with NIST-approved algorithms. This is a lengthy and costly exercise.

CSPRNGs: The statistical backbone of modern operating systems, these generate strong randomness only when seeded with sufficiently high entropy. They therefore require one of two additional steps: seed-hardening hardware (such as TPM chips or TRNG modules) or a software entropy-assurance layer that continuously validates entropy quality.

TRNGs: Based on physical noise, these reduce algorithmic dependency but introduce new operational risks: drift, bias, environmental variation and device failure. They necessitate a hybrid hardware–software pathway, where the TRNG feeds entropy upward but a software layer detects anomalies.

The Cryptographic Trust Stack



QRNGs: These generate extremely high-quality entropy but are hardware-locked: they require optical components, certified modules and specialist deployment models, which force organizations onto the QKD or quantum-HSM pathway.

Hybrid RNGs: Blending TRNG, QRNG, and CSPRNG outputs with continuous entropy scoring, these can move cleanly into a software-defined PQC transition path with no hardware lock-in and just software-based continuous entropy integrity monitoring.

This list can be summarized in the table below:

PQC Transition Pathways

RNG-Type	Hardware	Algorithms	Software		Real-world deployment share (estimate across enterprises)
PRNG	✕	Requires expensive algorithm upgrades for keys (post RSA-2048)	✕	✕	~20% (legacy, weak, disappearing fast)
CSPRNG	✕	✕	Requires Entropy Integrity layer software	Also requires stronger entropy seed (hardware)	~60% (dominant in modern systems)
TRNG	✕	✕	✕	Software tracks for environmental drift and Hardware for seed	~10% (hardware-limited deployments)
QRNG	Just hardware needed due to high quality quantum entropy	✕	✕	✕	~2% (high-end telecom, defense, research)
Hybrid RNG	✕	✕	Requires continuous Entropy Integrity monitoring software	✕	Growing fastest ~8% now but on track for 20–30%

Although just two of the five RNG classes, **CSPRNG** and **Hybrid RNGs,** support the software PQC pathway, these two will soon account for over 80% of all entropy used in enterprise systems worldwide (e.g., finance, health, cloud, telecom, energy, aviation). This is the largest and fastest-growing share of the market.

CSPRNGs are embedded in every major cryptographic library (OpenSSL, BoringSSL, WolfSSL), every operating system kernel (Linux, Windows, macOS), every smartphone and browser, and every cloud platform (AWS KMS, Azure Key Vault, Google Cloud KMS). They underpin billions of daily TLS handshakes and secure API sessions.

Hybrid RNGs are rapidly growing across cloud-native stacks, secure enclaves, AI accelerators, crypto wallets and regulated workloads requiring reliability. When combined, these two RNG classes govern the entire software-defined entropy landscape, and thus create the only pathway with global-scale reach.

By contrast, **TRNGs** are deployed primarily in embedded systems, IoT devices, hardware tokens, and specialized modules; important but collectively a small, slow-moving market. QRNGs, though cryptographically pristine, are deployed in *microscopic* volumes: telecom carriers' QKD pilots, national labs and niche defense networks. These hardware pathways cannot support global PQC deployment at speed or scale.

The software-defined entropy-integrity pathway overlays the existing software-first infrastructure of five to ten million enterprise servers, billions of mobile and browser endpoints, every cloud provider, and the core financial, healthcare, energy and aviation systems that constitute the backbone of the digital economy. It offers the lowest cost, fastest adoption curve, and minimal path dependency, making it the only PQC transition path capable of operating at planetary scale.

6

AI and Post-Quantum Cryptographic Transition Pathways

Mapping the four strategic routes toward quantum-safe resilience

As quantum technologies advance from research to deployment, every organization faces a pivotal choice in how it transitions its cryptographic infrastructure. The journey to quantum-safe security is not a single path but a spectrum of Cryptographic Transition Pathways, each reflecting different balances of cost, complexity, and readiness.

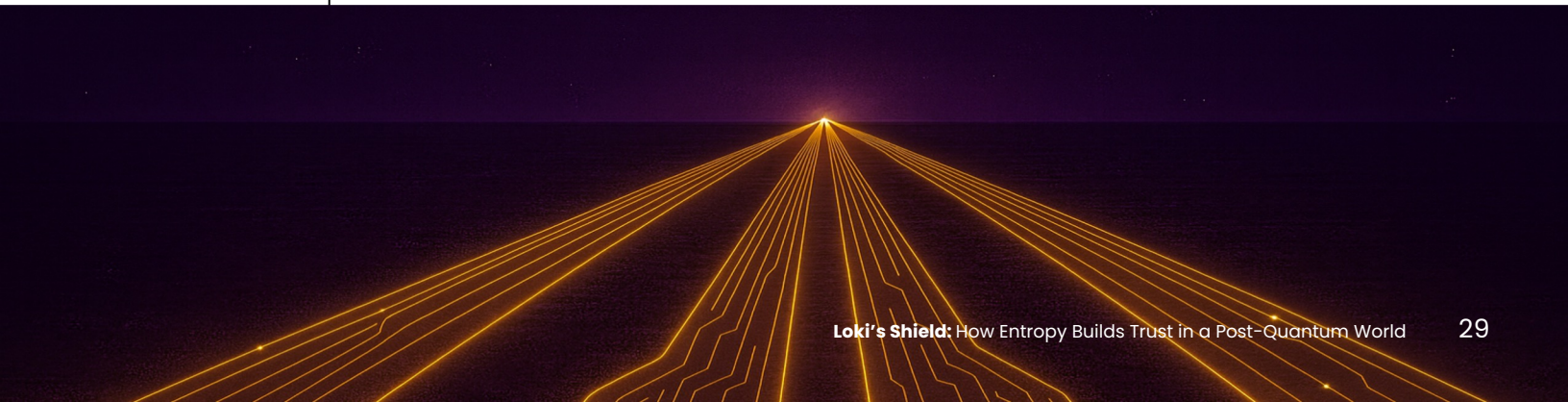
These pathways reflect the dominant approaches used by the major cloud service providers, Hardware Security Module vendors, and large enterprise-security platforms. While aligned with NIST-recommended migration frameworks, they share a core limitation: none directly address entropy quality, even though weak randomness is a root cause of systemic cryptographic fragility.

The four principal pathways emerging across industry and government are:

- **Hardware Quantum Distribution (QKD / Quantum HSMs[51]):** Employing physics-based or dedicated hardware systems for key generation and exchange.
- **Algorithmic Migration (PQC[52]):** PQC algorithms such as Kyber and Dilithium were standardized by NIST in 2024 for government use. This pathway would update existing RSA-2048 encryption standards to NIST-approved post-quantum algorithms.
- **Hybrid Hardware and PQC Systems:** Integrating new algorithms with certified entropy modules for incremental improvement.
- **Software-Defined Entropy Integrity (EIS):** Deploying continuous, software-based entropy scoring and synchronization across existing cryptographic stacks.

Each pathway represents a legitimate route toward quantum resilience, shaped by different governance and infrastructure realities. The purpose of this framework is not to compare products or vendors but to clarify strategic options for decision-makers confronting the same systemic risk: the erosion of digital trust as quantum capabilities mature.

Together, these pathways form the Post-Quantum Cryptographic Transition Map - a visual guide to help leaders assess where they are on the journey from classical encryption to governed, entropy-assured security.



Post-Quantum Cryptographic Transition Pathways

Four strategic approaches - from algorithmic to software-defined entropy assurance - positioned by deployment speed and implementation complexity:

Hardware Quantum Chips (QKD/HSM)

What: Quantum Key Distribution (QKD)/Hardware Security Modules (HSM) like tamper-resistant chips. These are hardware-based security systems that use physical principles to secure cryptographic keys.
How: Quantum Key Distribution (QKD) sends photons whose quantum states reveal any interception; Quantum HSMs generate and store keys in tamper-proof modules with quantum random sources.
Examples: ID Quantique QKD networks; Toshiba QKD pilot (UK–Japan); Thales Luna Quantum HSM
Cost: Very High (≈ $100–300 M enterprise rollout)
Timeline: 2–4 years
Complexity: Extremely high—new fibre or satellite infrastructure.

Algorithmic Migration (PQC)

What: This replaces all existing RSA and ECC encryption with new PQC algorithms. Most common enterprise plan right now and promoted by NIST, CISA and WEF. Challenge is updating millions of keys, certificates and vendor integrations without downtime.
How: Replaces vulnerable math with lattice- or hash-based equations (e.g., CRYSTALS-Kyber for key exchange, Dilithium for signatures). Runs on current hardware but requires re-keying and software rewrites across systems.
Examples: Google & Cloudflare's hybrid TLS (Kyber + RSA); Microsoft Azure VPN pilots; IBM Quantum-Safe Roadmap; NSA's CNSA 2.0 mandate.
Cost: High (≈ $15–25 M per enterprise) Timeline: 18–36 months
Complexity: Major re-engineering effort.

Hybrid Hardware and PQC Systems

What: Combining new PQC (Post-Quantum Cryptography) algorithms with hardware entropy chips (TPM 2.0, QRNG cards) to boost key randomness and shorten migration risk.
How: PQC handles the math; embedded hardware ensures high-entropy key generation. Offers stronger defense but depends on certified device supply chains.
Examples: Intel TPM-based PQC pilots; IBM Quantum Safe and Thales HSM integrations; government telecom trials mixing Kyber with QRNG modules.
Analogy: Lock and vault combo—balanced protection, but limited by hardware rollout.
Cost: Moderate (≈ $5–10 M)
Timeline: 1–2 years
Complexity: Medium—hardware calibration and certification cycles.

Software-Only Entropy Assurance

What: A lightweight software layer that continuously measures and refreshes randomness across existing encryption systems—no new hardware required.
How: Integrates into OpenSSL/BoringSSL libraries, combining quantum and cryptographic random sources, verifying entropy ≥ 0.99 min-entropy in real time.
Examples: Entrokey EIS deployments; alignment with U.S. Executive Order 14144 and OMB M-24-04; cloud and edge implementations across finance and energy sectors.
Analogy: A continuous lock-calibration system—keeps every key unpredictable at software speed and minimal cost.
Cost: Low (≈ $0.5–2 M enterprise licence) Timeline: < 2 weeks
Complexity: Low—simple software update.

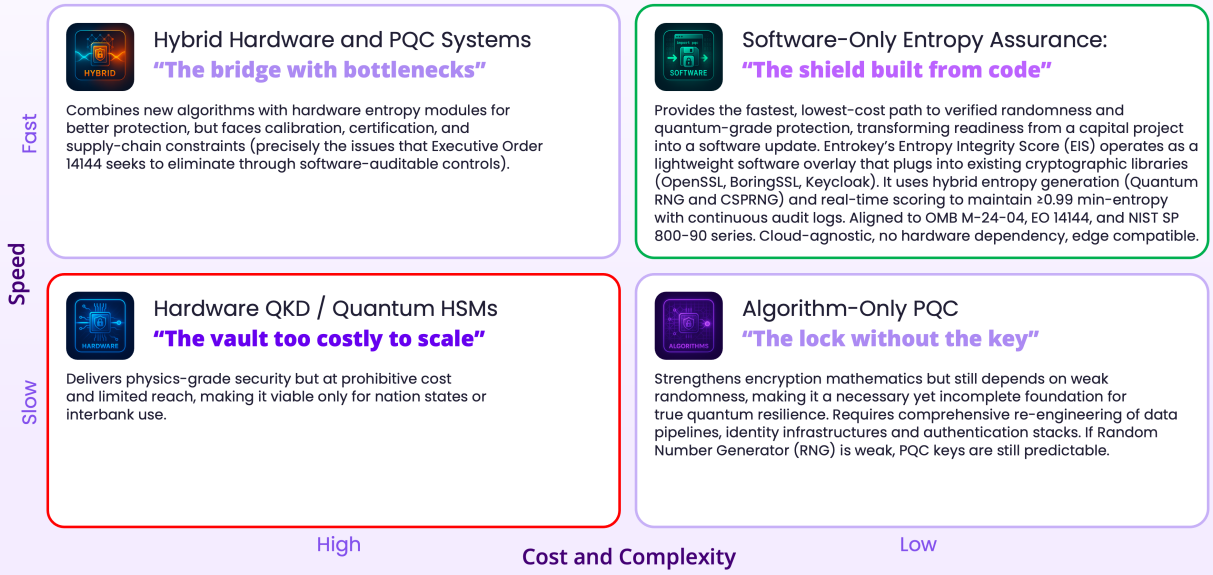
Takeaways on Transition Pathways

"In practice, most organizations operate dozens of heterogeneous and often undocumented cryptographic module across cloud services, Continuous Integration/Delivery pipelines, IoT systems, legacy infrastructure, and shadow IT. This fragmentation makes coordinated PQC migration far harder and increases the probability that weak or unverified entropy sources persist undetected.

Entrokey achieves the best performance-to-cost ratio in the field, 10X faster deployment and over 90% lower cost than hardware-based alternatives. It converts quantum readiness from a capital project into a software update cycle.

As physical quantum systems scale, a purely software entropy layer provides the missing complement: it protects against the very breakthroughs, such as IonQ's and IBM's manufacturing advances, that render older encryption obsolete.

Four Post-Quantum Cryptographic Transition Pathways



Strategic Implications for Leaders

The lesson from the four quadrants is clear: speed, entropy, and governance now define resilience. Algorithmic and hardware-first defenses offer mathematical strength but demand years of re-engineering and heavy capital outlay. Hybrid solutions strike a balance but still carry supply-chain and certification risk.

By contrast, software-based entropy assurance achieves quantum readiness through code, not construction. It enhances any PQC stack, scales instantly across clouds and devices, and aligns with OMB M-24-04 and Executive Order 14144 June 2025 update on cryptographic resilience. As the WEF concluded in its 2024 *Quantum Security for the Financial Sector* report, *"The most cost-effective and scalable defenses will be software defined."*

For business and government leaders, the message is simple:

- **Speed is security.** Each month of delay feeds the "harvest-now, decrypt-later" archive.
- **Entropy is leverage.** Strengthening randomness multiplies the lifespan of every encryption layer.
- **Software is sovereignty.** The nations and organizations that can upgrade at software speed will control the standards of post-quantum trust.

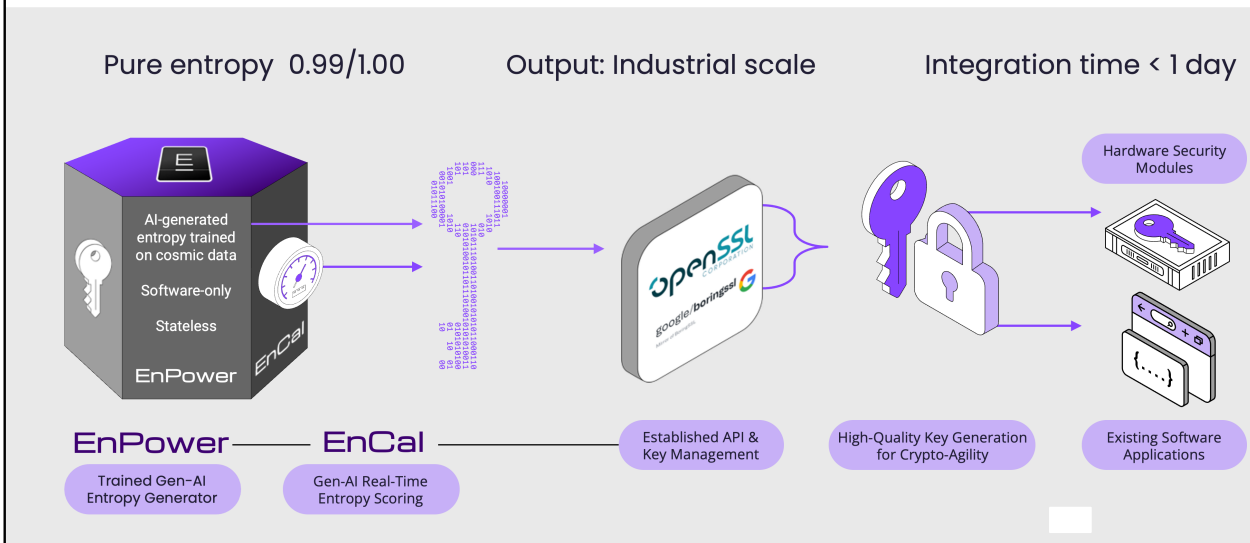
In short, quantum readiness is no longer a capital project; it is a leadership decision.

Entrokey Lab's Unique Entropy Software Proposition

High-quality entropy enables true crypto-agility, allowing systems to rotate keys, shift algorithms, and evolve cryptographic stacks without hardware replacement. Entrokey Labs is uniquely positioned to deliver a highly-secure, low-cost solution that aligns with key U.S. regulations (OMB M-24-04 and Executive Order 14144 June 2025 update). It's novel technology of near-perfect Random Number Generation (approaching 0.99 min-entropy under continuous scoring) through a proprietary AI model trained on high-volume astrophysical and natural stochastic data sources for entropy generation (EnPower™) combined with Generative-AI Real-Time Entropy Scoring (EnCal™), means that it can generate over 1 Gb/second within established API and Key Management libraries (e.g., OpenSSL, BoringSSL), High Quality Key Generation for Crypto-Agility that can result in integration into both Hardware Security Modules and Existing Software Applications within a day. This is at a fraction of the cost and over 99% faster than other Post-Quantum Cryptography solutions on the market.

How it works

Generator, Scoring & Integration



7

Safeguarding Your Organization

Immediate Actions

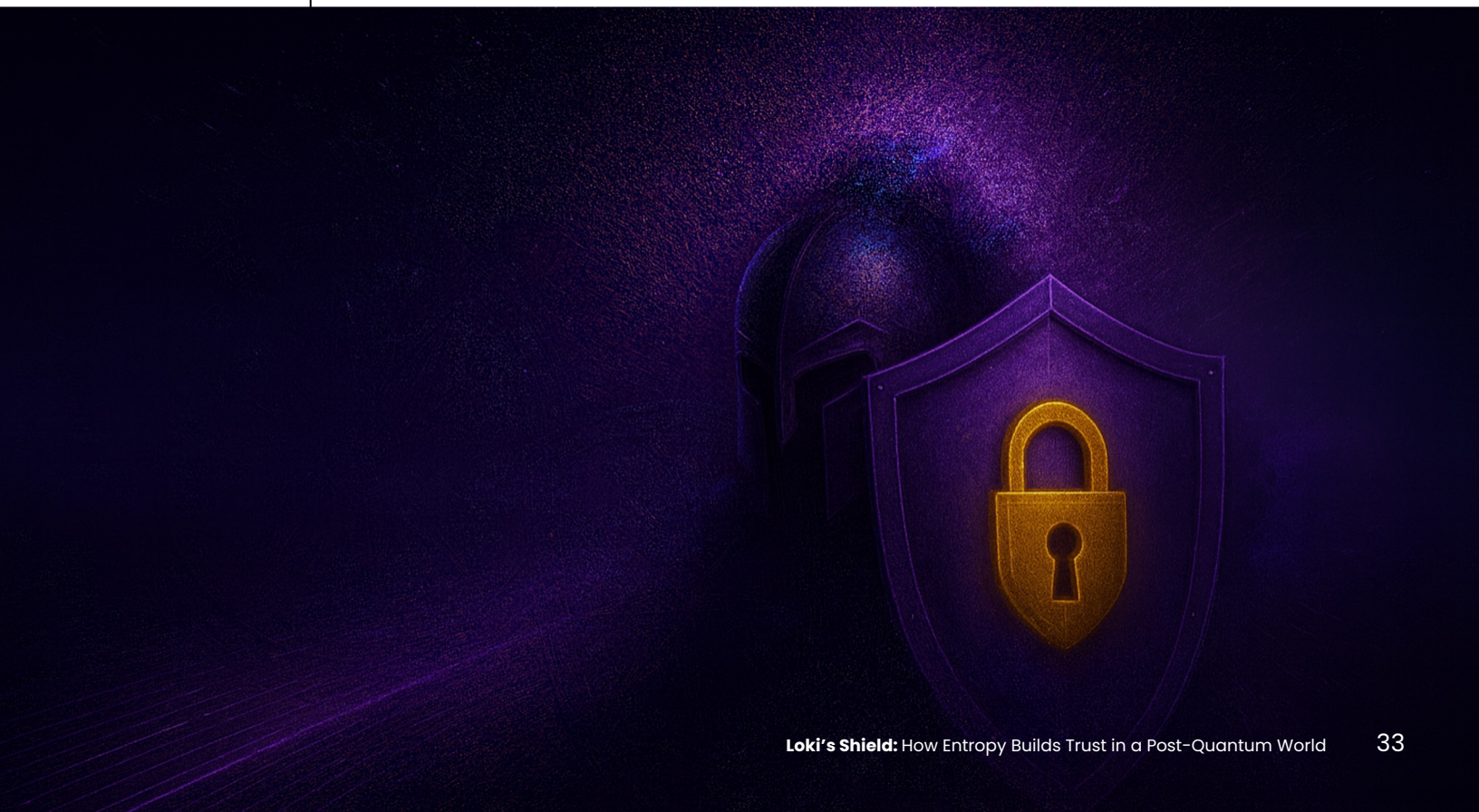
No chief executive or public official wants to wake up to the message that their organization's systems have been breached or its data sold on the dark web. By then, it is already too late: the damage to trust, reputation, and national security cannot easily be undone. Yet the window for prevention remains open.

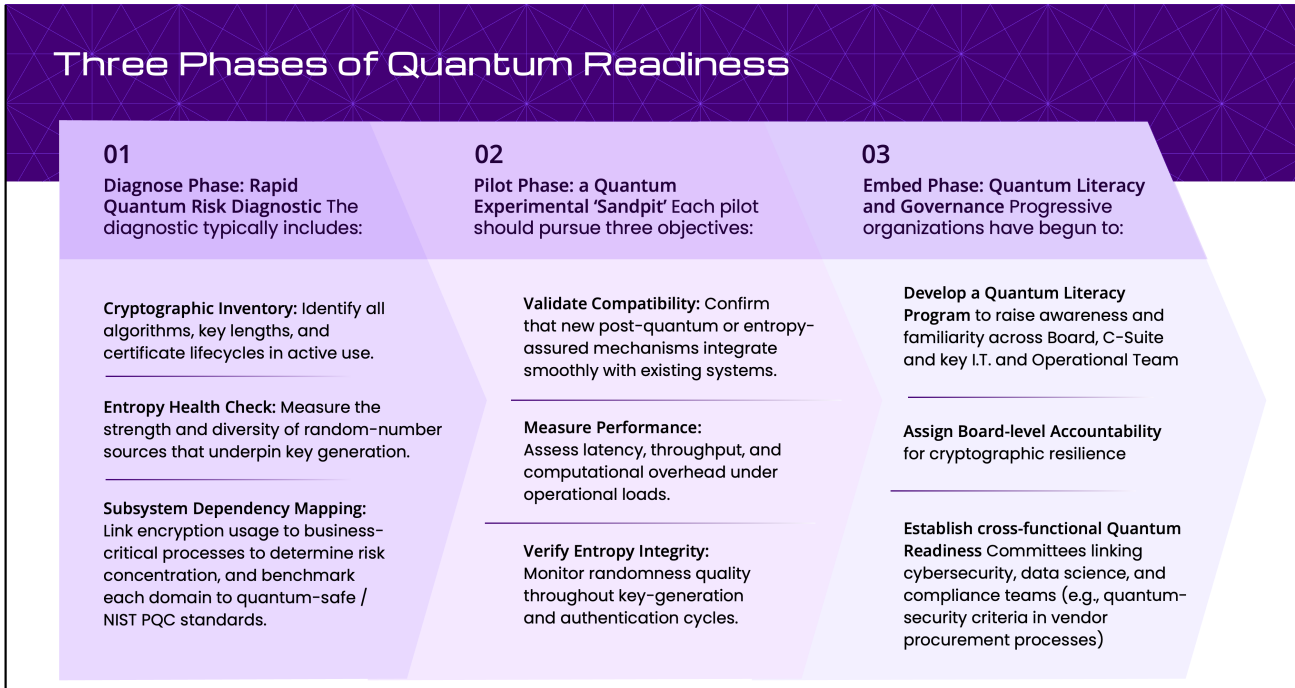
Three Phases of Quantum Readiness

The shift to post-quantum security marks one of the most significant transformations in the history of digital trust. For decades, cryptography has operated behind the scenes, rarely questioned, rarely measured. Today, advances in quantum computing have turned it into a board-level risk.

Yet, unlike traditional cyber threats, the challenge is both predictable and preventable. Preparing for the post-quantum era is no longer a theoretical exercise. It is a leadership imperative, and it has already begun as the *Harvest-Now Decrypt Later* or AI-Anthropic agent cyberattacks have shown. The next wave of cyber disruption will not reward organizations that wait for standards to settle, but those that act with agility and foresight. Organizations that act early can preserve continuity, protect data longevity, and strengthen public confidence long before Q-day arrives.

Across sectors, three steps consistently deliver early advantage: conduct a Quantum Risk Diagnostic, launch targeted pilot programs, and embed quantum literacy and governance accountability at the board level. Together, these actions shift quantum readiness from concept to measurable practice.





1. Rapid Quantum Risk Diagnostic (Diagnose Phase)

The first step in any transformation is visibility. A rapid Quantum Risk Diagnostic helps organizations map where quantum vulnerability actually resides within key management systems, authentication stacks, or data-in-transit channels.

Conducted over five to ten days, the diagnostic inventories encryption dependencies, entropy sources, and certificate lifecycles to create a clear baseline of exposure. The findings typically reveal that 60–80 % of subsystems use cryptography inherited from legacy deployments, often with weak or unverified randomness. This may expose future vulnerabilities across critical subsystems such as key management, authentication services, APIs, databases, and communication channels. This data-driven and factual baseline enables leaders to prioritize interventions where they deliver the greatest resilience return, whether through algorithmic migration, hardware reinforcement, or adoption of software-defined entropy assurance layers.

Entropy sources may be unverified, and authentication tokens may reuse deterministic seeds—problems invisible in daily operations but critical under quantum conditions. By quantifying exposure, the diagnostic converts abstract threats into actionable data. With the risk landscape visible, organizations can then move quickly to test countermeasures in controlled environments before scaling systemwide.

2. Launch Targeted Pilot Programs (Pilot Phase)

Pilot programs are the bridge between awareness and institutional change. Following the diagnostic, select two to three high-value domains, such as secure communications, identity management, or data storage, and deploy limited-scope pilots that integrate post-quantum algorithms or entropy assurance mechanisms.

Many early adopters may combine NIST-approved algorithms such as Kyber or Dilithium with continuous entropy-scoring software to monitor randomness quality in real time. Others could explore hybrid models where classical and post-quantum keys coexist within the same handshake protocols.

These limited-scope implementations reduce risk and cost. They produce empirical data that can inform procurement, vendor selection, and compliance reporting. Equally important, they build institutional confidence, transforming quantum readiness from a theoretical discussion into a measurable engineering practice.

Pilot results can be shared across industry consortiums or regulatory sandboxes, accelerating sector-wide learning. As the WEF's *Quantum Readiness Toolkit* notes, organizations that "experiment early and iterate quickly" achieve readiness maturity nearly twice as fast as those that wait for standards to finalize.

3. Build Literacy, Governance, and Continuous Oversight (Embed Phase)

Technology alone cannot secure the quantum future; leadership and culture must complete the equation. Embedding quantum literacy and governance accountability ensures that readiness is sustained beyond the lifespan of any single algorithm. Building quantum literacy within leadership and technical teams ensures that decisions made today remain valid as standards evolve. Board members should understand how entropy, algorithmic hardness, and key management interact to determine true security.

Modern governance frameworks increasingly require boards to treat cryptography as a living control function, not a static asset.

Quantum literacy and education remains central. Executives should understand the difference between algorithmic hardness and entropy integrity, and why both are required for trustworthy encryption. Operational teams must learn how post-quantum algorithms, hardware security modules, and entropy-assurance software interlock to maintain unpredictability at scale. By institutionalizing this literacy, quantum security becomes a durable organizational capability rather than a one-off transition project.

Embedding governance also aligns with international policy trajectories. The U.S. Executive Order 14144 June 2025 update and OMB M-24-04 both call for "measurable assurance" of cryptographic health that complies with or exceeds NIST SP 800-90B and SP 800-22 randomness test requirements. The European Union's upcoming *Cyber Resilience Act* is expected to require similar transparency. Integrating continuous entropy assurance and key-lifecycle visibility into existing compliance programs therefore future-proofs the enterprise against evolving regulation.

By conducting a rapid diagnostic, piloting emerging solutions, and embedding literacy at the leadership level, organizations establish a living system of cryptographic resilience. Those that act now will enter the post-quantum era not as observers, but as architects of the new trust infrastructure.

"Begin small, learn fast, and go early - because in quantum security, waiting is the only unrecoverable error."
- WEF Quantum Security Network

8

Epilogue: Entropy as Trust

Loki's Rescue

Every technological revolution eventually forces leaders to confront a single question: *What sustains trust when the rules of power change?*

Steam reshaped industry. Electricity redefined speed. The Internet connected everyone, but also exposed everyone. Now, as Artificial Intelligence and quantum computing converge, the foundation of digital trust itself is being rewritten.

Cambridge Frontier Technologies' market simulations estimate that transitioning global infrastructure to quantum-safe standards via hardware-centric QKD would exceed $1.4 trillion in capital costs. Entrokey's software-defined entropy upgrade achieves equivalent resilience with a 90% Total Cost of Ownership reduction and full deployment in under 30 days.

In its August 2025 joint advisory, CISA, NSA, and FBI warned that Salt Typhoon and affiliated state actors are already pre-positioning within all sixteen U.S. critical-infrastructure sectors, leveraging router and edge-device weaknesses to prepare for mass decryption operations. These findings validate the immediate need for software-first entropy reinforcement, the only approach fast enough to meet the 2035 mandate from the National Security Memorandum on Quantum Computing[53] (NSM-10) and to mitigate 'Harvest Now / Decrypt Later' exploitation already underway.

Quantum Security as National and Economic Security

Cybersecurity has become a core determinant of sovereignty. The World Economic Forum's *Global Cybersecurity Outlook 2024* warns that a large-scale quantum decryption event could erase trillions of dollars in global economic value within days, disrupting financial markets, transport grids, and government services[54]. The U.S. National Cyber Director and the EU's ENISA both classify quantum readiness as a Tier-1 national-security priority.

The U.S. government now treats quantum manufacturing capacity as a national-security asset on par with semiconductor fabrication.

IonQ's quantum computer factory[55], IBM's next generation quantum-computing platform (System Two plant[56]), and Finland's cryogenic modules[57] mark the start of an industrial base that will define sovereign control over quantum supply chains.

History shows that technological preparedness defines national competitiveness. In the 20th century, energy independence decided wars and industrial leadership. In the 21st, entropy independence, the ability to generate and verify true randomness, will determine digital sovereignty. Nations that can guarantee the unpredictability of their cryptographic systems will anchor global supply chains, finance, and defense alliances.

The Economic Opportunity of Quantum Readiness

The migration to quantum-secure systems is not merely a compliance cost; it is an industrial catalyst. McKinsey (2024) projects that quantum-safe infrastructure will create new markets worth over $2 trillion a year across cybersecurity, cloud, manufacturing and financial services within a decade[58].

The WEF (2023) further emphasizes that the same technologies that protect data, high-grade randomness, verified entropy, and AI-driven assurance, can also power new innovations in privacy-preserving AI, verifiable digital identity, and secure data marketplaces.

Organizations that treat entropy as a measurable, auditable resource are effectively building the trust layer of the global digital economy, a capability as fundamental as bandwidth or energy. Those who delay risk being locked out of future trade, data-sharing frameworks, and critical-infrastructure contracts that will soon require quantum-resilience certification.

A *War on the Rocks* analysis projects that America's early investment in quantum manufacturing could equally unlock $2 trillion in value across navigation, sensing, and secure communications,[59] proof that building quantum infrastructure and entropy assurance together is both defensive and a growth strategy.

Entropy as Trust Infrastructure

Entropy is no longer an abstract mathematical concept. It is the invisible substrate of confidence in every transaction, authentication, and digital handshake. Just as electricity powers factories silently in the background, entropy powers trust: unseen yet indispensable.

Entrokey's Entropy Integrity Score (EIS) operationalizes this vision: software that turns chaos into control, aligning perfectly with Executive Order 14144 June 2025 update on trustworthy AI and the OMB M-24-04 mandate for cryptographic resilience. It is a pragmatic, deploy-anywhere framework that translates national policy into operational readiness; a trust upgrade delivered as code, not hardware.

The Leadership Moment

For boards and government officials, the question is no longer if quantum disruption will happen, but who will lead the transition. As the World Economic Forum notes across its quantum security reports (2022–2024), organizations that act early in the quantum transition will both protect value and help shape the standards that others must follow.

This is the inflection point: the emergence of Entropy as a Service, the creation of trust grids that interlink secure AI, finance, and communications, and the birth of a new global industry built on measured randomness. The nations and companies that master it will own the backbone of the post-quantum world.

Entropy is Loki's Shield.

Chaos, once feared, becomes our strongest defense. In embracing randomness, we rediscover control.

The storm is coming, but with entropy as our infrastructure of trust, humanity can sail straight through it.

Endnotes

1. World Economic Forum, *Global Risks Report 2024* (Geneva: WEF, 2024), Figure 1.5, "Top 10 Long-Term Global Risks," p. 15.
2. Cambridge Frontier Technologies (2025): Quantum Key Distribution Market Analysis: Disrupting Hardware GKD with Software-Only Solutions
3. https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/steady-progress-in-approaching-the-quantum-advantage#/
4. The term "Entropy Integrity Score (EIS)" was first introduced in the white paper Loki's Shield: Entropy as the Foundation of Quantum Trust (The Entropy Institute, 2025).
5. https://newsroom.intel.com/press-kit/moores-law
6. https://www.bcg.com/publications/2024/long-term-forecast-for-quantum-computing-still-looks-bright
7. https://www.oecd.org/en/publications/a-quantum-technologies-policy-primer_fd1153c3-en.html
8. https://iot-analytics.com/number-connected-iot-devices/
9. https://www.weforum.org/publications/global-cybersecurity-outlook-2024/
10. https://www.weforum.org/stories/2024/08/us-tools-encryption-breaking-quantum-computing-nist/
11. Several roadmaps (e.g., NSA CNSA 2.0, NIST/OMB memos, EU guidance) work with 2030–2035 timelines for completing PQC migration
12. https://globalriskinstitute.org/publication/2023-quantum-threat-timeline-report/
13. https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final228.pdf
14. NIST Post-Quantum Encryption Standards https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
15. https://newsroom.ibm.com/2022-11-09-IBM-Unveils-400-Qubit-Plus-Quantum-Processor-and-Next-Generation-IBM-Quantum-System-Two?utm_source=chatgpt.com
16. https://thequantuminsider.com/2025/10/22/google-quantum-ai-shows-13000x-speedup-over-worlds-fastest-supercomputer-in-physics-simulation/
17. https://investors.ionq.com/news/news-details/2025/IonQ-Achieves-Landmark-Result-Setting-New-World-Record-in-Quantum-Computing-Performance/default.aspx
18. https://www.quera.com/press-releases/research-reveals-quantum-computing-development-is-faster-than-expected-set-to-become-superior-technology-within-five-years
19. https://www.quantum.gov/
20. https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/the-year-of-quantum-from-concept-to-reality-in-2025
21. https://www.ibm.com/quantum
22. https://aws.amazon.com/braket/
23. https://azure.microsoft.com/en-us/solutions/quantum-computing
24. https://aws.amazon.com/blogs/quantum-computing/a-detailed-end-to-end-assessment-of-a-quantum-algorithm-for-portfolio-optimization-released-by-goldman-sachs-and-aws/
25. https://www.iotworldtoday.com/industry/basf-explores-quantum-for-industrial-catalyst-discovery
26. https://www.sandboxaq.com/post/optimizing-industrial-catalyst-discovery-with-ai-quantum-computing-and-a-little-magic
27. https://www.vwpress.co.uk/releases/3351
28. https://gf.com/dresden-press-release/psiquantum-and-globalfoundries-build-worlds-first-full-scale-quantum-computer/
29. https://q-ctrl.com/blog/q-ctrl-overcomes-gps-denial-with-quantum-sensing-achieves-quantum-advantage
30. https://www.secureworks.com/blog/predicting-q-day-and-impact-of-breaking-rsa2048
31. ESI QSC (2024) https://www.etsi.org/events/2284-10th-etsi-iqc-quantum-safe-cryptography-event
32. https://www.apmdigest.com/clock-ticking-how-47-day-certificates-and-quantum-threats-are-reshaping-cybersecurity
33. Effectively Manage Your Organization's Certificates, Gartner (2024); accessible here: https://www.tec-bite.ch/wp-content/uploads/2024/05/Effectively_Manage_Y_804504.pdf
34. https://www.cyberark.com/resources/ebooks/the-impact-of-machine-identities-on-the-state-of-cloud-native-security-in-2024
35. https://www.gartner.com/en/articles/post-quantum-cryptography
36. https://uptimeinstitute.com/resources/research-and-reports/annual-outage-analysis-2024
37. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf
38. https://cabforum.org/about/
39. https://www.infosecurity-magazine.com/news/digital-certificate-lifespans-fall/
40. ETSI QSC Report GR QSC 015 (2024): *Quantum-Safe Telecom Readiness Assessment*. https://www.etsi.org/technologies/quantum-safe-cryptography
41. https://www.gsma.com/solutions-and-impact/technologies/security/gsma_resources/starting-the-journey-to-quantum-safe/
42. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-90b.pdf
43. https://www.weforum.org/publications/quantum-readiness-toolkit-building-a-quantum-secure-economy/
44. https://www.ibm.com/reports/data-breach
45. https://www.anthropic.com/news/disrupting-AI-espionage
46. https://csrc.nist.gov/projects/entropy-source-validation
47. NIST SP 800-90B (2018) https://csrc.nist.gov/pubs/sp/800/90/b/final
48. ETSI GR QSC 015 (2024) https://www.etsi.org/events/2284-10th-etsi-iqc-quantum-safe-cryptography-event
49. Cambridge Frontier Technologies (2025), *A Software-Define Paradigm for Quantum-Resistant Security*
50. Cambridge Frontier Technologies (2025), Cryptographic Resilience in the AI Quantum Age: A Predictive Indexing Approach to Entropy Assessment
51. PQC = Post-Quantum Cryptography
52. QKD = Quantum Key Distribution and HSM = Hardware Security Modules
53. National Security Memorandum on Promoting United State Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems (2022). https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/
54. https://www.iankhan.com/the-quantum-security-revolution-why-every-business-must-prepare-now/
55. https://www.geekwire.com/2024/ionq-new-quantum-computer-factory/
56. https://newsroom.ibm.com/2025-10-14-the-basque-government-and-ibm-inaugurate-europes-first-ibm-quantum-system-two-in-donostia-san-sebastian
57. https://www.dailyfinland.fi/business/45744/Cryogenic-chip-tech-from-Finland-wins-European-innovation-award
58. https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/steady-progress-in-approaching-the-quantum-advantage#/
59. https://warontherocks.com/2025/10/americas-quantum-manufacturing-moment/

Glossary of Key Quantum and Cryptographic Terms

RNG — Random Number Generator: A mechanism that produces random values used to create cryptographic keys. Security depends on the unpredictability of the output.

PRNG — Pseudorandom Number Generator: Algorithmic generator that produces deterministic sequences from an initial seed. Fast and scalable but not inherently secure unless cryptographically strengthened.

CSPRNG — Cryptographically Secure PRNG: A PRNG designed so that outputs cannot be predicted even with partial knowledge of the internal state. Required for secure key generation in classical and PQC systems.

TRNG — True Random Number Generator: Generates randomness from physical processes (thermal noise, photons, etc.). Higher quality entropy but often slower and hardware-dependent.

QRNG — Quantum Random Number Generator: A TRNG that uses quantum-mechanical phenomena (e.g., photon arrival, vacuum fluctuations) to produce provably unpredictable randomness.

Hybrid RNG: Combines physical entropy sources with cryptographic conditioning algorithms. Increasingly recommended for resilience against hardware, supply-chain, or environmental failures.

RSA-2048
A widely used public-key encryption scheme based on the difficulty of factoring large integers. Secure against classical computers but vulnerable to quantum attacks using Shor's Algorithm.

ECC P-256 (Elliptic Curve Cryptography)
An elliptic-curve-based public-key scheme offering strong security with smaller keys. Also vulnerable to quantum factoring and discrete log attacks.

Shor's Algorithm
A quantum algorithm (1994) that can factor large integers and solve discrete logarithms exponentially faster than classical methods—breaking RSA, ECC, and all similar public-key systems.

Shannon's Law (Shannon Limit)
Describes the maximum information that can be transmitted over a noisy channel with zero error. Often referenced in discussions of entropy, noise, and cryptographic information capacity.

CQRC — Cryptographically-Relevant Quantum Computer
A quantum system powerful enough (in qubits, gate fidelity, and depth) to break RSA-2048 or ECC P-256 using Shor's Algorithm. Sometimes referred to as a "Q-Day-capable machine."

Q-Day
The moment a CQRC becomes operational and can decrypt today's Internet-scale encryption. A systemic national-security, financial-system, and critical-infrastructure risk.

PQC — Post-Quantum Cryptography
Advanced cryptographic algorithms designed to remain secure against quantum attacks. NIST is standardizing PQC for global adoption (e.g., Kyber, Dilithium, Falcon).

Physical Qubits
The actual hardware qubits inside a quantum processor. Large numbers of imperfect physical qubits are required to create one high-fidelity *logical qubit* for computation.

Error Correction (Quantum Error Correction)
Techniques that encode logical qubits across many physical qubits to protect against noise, decoherence, and gate faults. Determines how quickly a CQRC could emerge.

Entropy (Cryptographic Entropy)
A measure of unpredictability in a random source. Low entropy compromises key generation—even in PQC—making entropy assurance foundational to cryptographic trust stacks.

NIST — National Institute of Standards and Technology
The U.S. standards body leading the global transition to PQC, including RNG standards (SP 800-90B), statistical test suites, and PQC algorithm selection.

NIST STS — NIST Statistical Test Suite
A battery of statistical assessments for evaluating randomness quality. Used to validate entropy sources during certification processes.

ENISA — European Union Agency for Cybersecurity
The EU body publishing quantum-readiness guidance, cryptographic transition frameworks, and risk assessments for critical infrastructure.

OMB — Office of Management and Budget (U.S.)
Issued binding directives (e.g., M-23-02) requiring all federal agencies to inventory cryptographic assets and plan for PQC transitions.

EO — Executive Order
U.S. Presidential directives shaping cybersecurity and quantum policy. Relevant examples: EO 14028 (Improving the Nation's Cybersecurity) and EO 14144 (Safe, Secure AI) including June 2025 update on strengthened resilience.

Authors

Nishan Degnarain

Nishan Degnarain is a Harvard-educated Development Economist focussed on exponential technologies. He is currently Co-founder and Managing Partner of The Exponential Academy, a leading Silicon Valley technology and economic advisory firm.

He has given keynote addresses to governments, United Nations agencies, the IUCN, World Bank, and IMF, and has worked with some of the biggest technology companies on breakthrough innovations. Since 2013, Nishan has chaired the World Economic Forum's Global Agenda Council on the Ocean, a group of leading ocean experts from around the world that meet at Davos each year. He sits on several boards and was previously on the Monetary Policy Committee of the Central Bank of Mauritius.

Prior to this, Nishan worked at McKinsey and Company, the World Bank, the UK Prime Minister's Strategy Unit under Tony Blair, and as a broadcast journalist for the BBC. Nishan holds an undergraduate degree from the University of Cambridge and a postgraduate degree from Harvard University's Kennedy School of Government in International Economic Development.

He is the author of three books: *Soul of the Sea in the Age of the Algorithm* (2017), on how exponential technologies can heal our oceans, *Zero Point Four* (2024) on how U.S. leadership in maritime will secure America's future, and *The Exponential Ministry* (2025) on how governments can achieve 10X more with 10X less. Nishan has received several international awards, such as being recognized as a Young Global Leader by the World Economic Forum and winning the Economist's Ocean Economy Innovation Prize.

Zenia Tata

Zenia Tata is an innovation strategist and futurist dedicated to leveraging human potential and disruptive technologies to tackle global challenges. She is currently Head of The Entrokey Institute and SVP of Strategic Ventures at Entrokey Labs, a U.S.-based quantum and AI-resistant cybersecurity pioneering company.

Previously, as Chief Impact Officer at XPRIZE, Zenia spearheaded the design of over 25 moonshot innovation competitions targeting breakthroughs in hydrogen energy, carbon dioxide removal, alternative proteins, desalination, and longevity. Notably, Zenia designed the groundbreaking $100 million Carbon Removal XPRIZE funded by Elon Musk.

Before XPRIZE, she served as Executive Director at International Development Enterprises (iDE) USA, driving market-based strategies that lifted 24 million farming families out of poverty across 20 countries.

An acclaimed public speaker, Zenia merges moonshot thinking, biomimicry, and exponential technologies in her unique methodology for creating audacious impact. Frequently cited by Wired and BBC as a breakthrough thinker, Zenia brings 25 years of global innovation experience to her work on achieving Audacious Impact, solidifying her reputation as a visionary leader in disruptive technology.

In collaboration with

The Entrokey Institute

The Entrokey Institute is the research and innovation arm of Entrokey Labs, dedicated to exploring entropy as the organizing principle for secure, energy-efficient, and ethically aligned technologies. Operating at the intersection of cryptography, physics, mathematics, quantum science, and AI, the Institute leads research and incubation efforts that help humanity transition safely into a post-quantum, AI-driven world.

The Entrokey Institute aims to become a US-led, global nucleus for entropy-driven innovation, bridging science, security, and sustainability. By blending rigorous academic validation with ethical acceleration, it ensures that the technologies shaping our quantum and AI future remain trustworthy, energy-efficient, and human-aligned.

Cambridge Frontier Technologies Lab

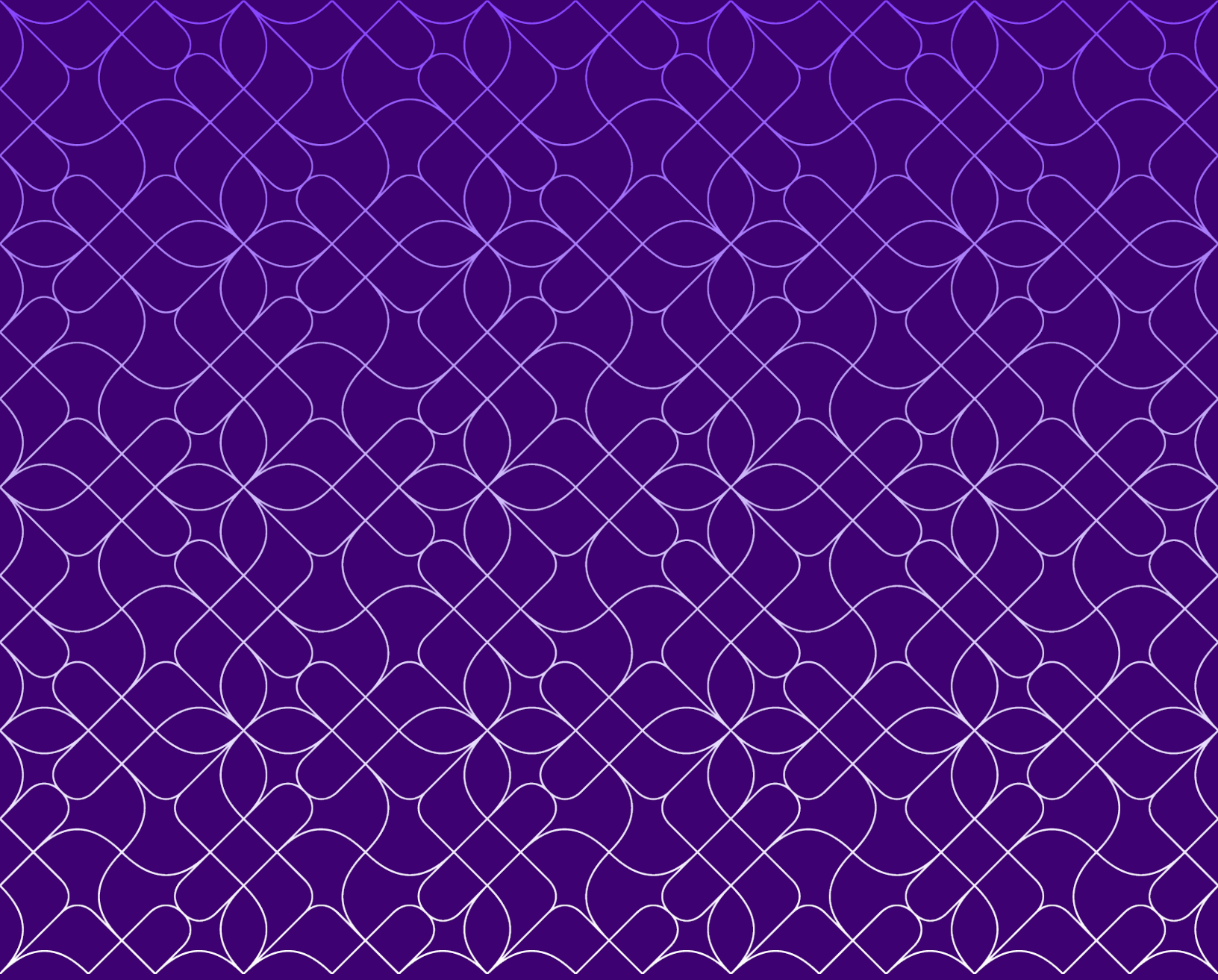
The Frontier Technologies Laboratory at the University of Cambridge (UK) is an ecosystem of Cambridge-based academics and societies experimenting with novel technologies, alongside its academic and industry partners. FTL is collaborating with members from the University of Oxford, Harvard and MIT to develop an 'Open Innovation Ecosystem'.

For the advancement of science and working at the intersection of academia and industry, FTL is an interdisciplinary and collaborative research environment which fosters innovation and impact. It enables those who wish to explore advanced technologies and their impact on society. FTL researches, provides evidence-based clarity, teaches, mentors, consults and builds.

The Exponential Academy

The Exponential Academy is dedicated to empowering businesses with thought leadership and a proven methodology to utilize exponential technologies, driving innovation and transformation to ensure sustainable growth with a competitive advantage.

The Academy supports organizations industry-wide, enabling senior leadership to understand and respond to the emergence of exponential technologies.



EntrokeyLabs.com

zenia.tata@entrokeylabs.com

ENTROKEY INSTITUTE™