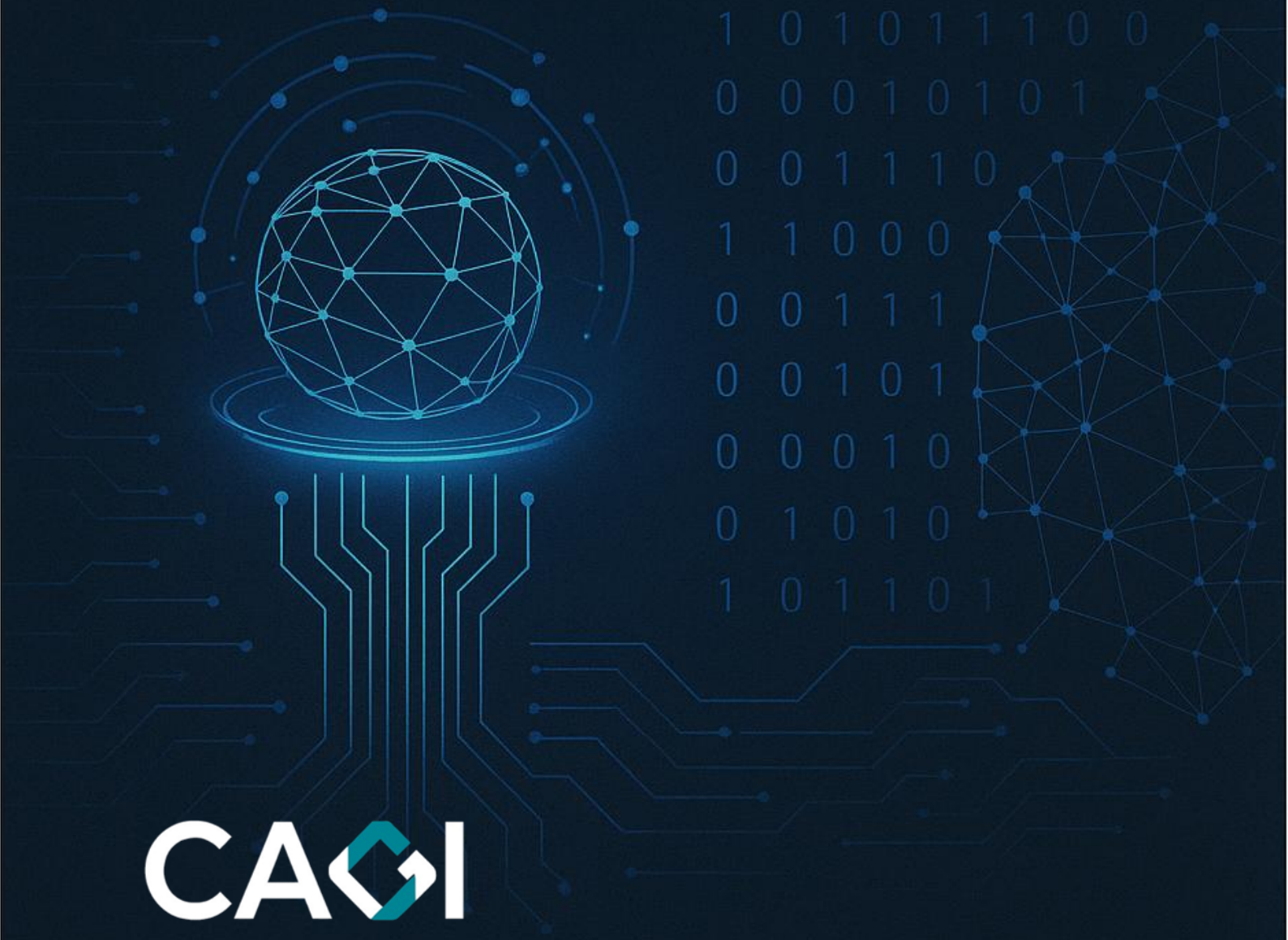
QUANTUM COMPUTING AND CYBERSECURITY

Current State and Future Implications

INDUSTRY INSIGHT



CAGI

Executive Summary

Quantum computing is rapidly advancing as a paradigm-shifting technology with potentially transformative implications for the field of cybersecurity. At its core, it represents a fundamental departure from classical computing. Traditional computers process information using binary bits, strictly zeros and ones, whereas quantum computers operate with qubits, which leverage the principles of quantum mechanics, specifically superposition and entanglement. These quantum characteristics allow qubits to exist in multiple states simultaneously and be intricately correlated with one another, enabling certain types of calculations to be performed exponentially faster than on classical systems.

This unprecedented computational potential holds enormous promise across a wide range of sectors. In fields such as drug discovery, molecular modelling, climate simulation, logistics optimisation, and artificial intelligence, quantum computing could deliver breakthroughs unattainable by current technologies. However, this power also comes with a significant downside- ne that is of particular concern to cybersecurity professionals. The same quantum advantage that enables advances in science and industry could be weaponised to undermine the cryptographic systems that underpin global digital security.

Most of today's public key cryptographic protocols, such as RSA, Diffie-Hellman, and elliptic curve cryptography, derive their security from the assumed difficulty of mathematical problems like integer factorisation and discrete logarithms. These problems are practically insoluble for classical machines at scale. Yet, with the advent of a sufficiently powerful and fault-tolerant quantum computer running Shor's algorithm, these once-unbreakable problems could be solved in polynomial time. The consequences would be dramatic: the encryption systems protecting online banking, secure messaging, government communications, intellectual property, and critical infrastructure could be rendered obsolete virtually overnight.

This looming prospect raises several pressing questions. How close are we to realising a quantum machine with enough stability and scale to break modern encryption? Is this an imminent threat that requires urgent countermeasures, or a theoretical possibility that may remain decades away? More broadly, how prepared are industries, governments, and cybersecurity practitioners to defend against quantum-enabled threats?

This whitepaper aims to answer these questions by providing a comprehensive, evidence-based analysis of quantum computing through the lens of cybersecurity. It evaluates the maturity and trajectory of quantum hardware development, examines the vulnerabilities in current cryptographic systems, and assesses the readiness of different sectors to transition toward quantum-resistant solutions. Importantly, it also considers the dual-use nature of the technology: while quantum computing introduces severe risks, it may also enable new defensive tools such as quantum key distribution (QKD) and truly random number generation.

Adopting a critical and balanced perspective, this paper cuts through the sensationalism often associated with quantum discourse. It avoids both complacency and unjustified alarmism, instead drawing on peer-reviewed research, technical benchmarks, industry roadmaps, and expert surveys. In doing so, it seeks to establish a realistic understanding of where we are today, where we are headed, and what needs to be done to secure the future.

In particular, we explore how quantum computing is likely to impact cybersecurity standards, cryptographic practices, and long-term data protection across a range of industries, including finance, defence, healthcare, telecommunications, and critical infrastructure. As these sectors increasingly rely on digital trust, the urgency of developing a coherent and coordinated post-quantum strategy becomes clear.

The final section of the paper offers actionable recommendations for stakeholders at the national and organisational level. These include accelerating the adoption of post-quantum cryptography (PQC), conducting cryptographic inventories and risk assessments, investing in standards development, and fostering international collaboration. While the exact timeline of the quantum threat remains uncertain, the window for proactive preparation is narrowing. Those who act early will mitigate risk, build resilience, and position themselves ahead of the curve as the quantum era unfolds.

State of Quantum Computing Maturity

Current Capabilities: As of 2025, quantum computing remains in a nascent but rapidly advancing stage. Today's devices are typically labelled "NISQ" (Noisy Intermediate-Scale Quantum) machines- they have tens to a few hundred qubits and are prone to errors due to decoherence and imperfect gate operations. For example, IBM's quantum processors reached 127 qubits in 2021 and 433 qubits in 2022 (IBM Osprey), with a roadmap aiming for over 1,000 qubits by 2023-2024 and beyond. Other major players like Google, IonQ, and Rigetti have likewise expanded qubit counts and qubit quality year-over-year. However, these qubit numbers refer to physical qubits that are *not error-corrected*.

To perform the long, complex computations required to break modern cryptography, a *fault-tolerant* quantum computer with thousands of logical (error-corrected) qubits would be needed. The overhead for error correction is enormous- estimates suggest on the order of 1,000 physical qubits may be required to produce a single high-fidelity logical qubit with the popular surface code. Companies like IBM are exploring more efficient error-correcting codes (e.g. IBM's experimental "bicycle" QLDPC code) to reduce this overhead by an order of magnitude, but fully fault-tolerant quantum computing remains an aspirational goal. IBM, for instance, has outlined a plan for a fault-tolerant machine ("Blue Jay") with ~2,000 logical qubits by 2033- an ambitious timeline that underscores both the progress and the road still ahead.

Quantum Advantage vs. Cryptographic Threat: In 2019, Google captured headlines by claiming "quantum supremacy" - demonstrating that a 53-qubit quantum processor could perform a contrived calculation faster than a supercomputer. Since then, quantum processors have solved certain specialized problems (e.g. simulating quantum systems, basic optimization tasks) beyond the reach of classical brute force. Yet these demonstrations have *not* equated to breaking encryption.

The task of factoring a 2048-bit RSA key or solving the discrete logarithm for elliptic-curve cryptography (ECC) remains astronomically out of reach for current machines. To illustrate, one analysis estimates that hours using Shor's algorithm. Even under ideal conditions, around 4,099 stable logical qubits might factor RSA-2048 in 10 seconds. These numbers far exceed the few hundred *noisy* qubits we have today. As a result, no "cryptographically relevant quantum computer" (CRQC) exists yet. Shor's algorithm has been implemented only for tiny integers (e.g. factoring 21 = 3×7, or factoring RSA-15/RSA-21 on small prototypes)- essentially proofs of concept. The largest integer factored by a quantum device is still trivial compared to real cryptographic keys. This reality tempers the urgency: quantum computing is not a present threat to break encryption in 2025.

Timeline Uncertainty: While quantum computers today cannot crack encryption, the field's growth trajectory means the threat is a matter of *when*, not *if*. Predicting that timeline is difficult- expert opinions range from pessimistic (several decades away) to optimistic (within this decade). A 2025 RAND analysis notes that current quantum machines are "nowhere near up to the task" of attacking cryptography and the threat may still be ~15 years away. Some renowned cryptographers like Adi Shamir (the "S" in RSA) have publicly predicted that practical quantum code-breaking won't happen for 30 years.

On the other hand, organizations like the U.S. National Security Agency (NSA) take the threat seriously *now*- NSA has warned that the "adversarial use of a quantum computer could be devastating" to national security systems and has issued requirements to begin transitioning to quantum-resistant cryptography.

In industry, a 2023 survey by KPMG found 60% of Canadian companies and 73% of U.S. companies believe "it's only a matter of time" (and not much time) before cybercriminals harness quantum power to decrypt data. Meanwhile the Monetary Authority of Singapore advised financial institutions that the risk of quantum decryption could materialize in the next 10 years. This disparity underscores the uncertainty - technological breakthroughs or new algorithmic techniques could accelerate the timeline unexpectedly, while persistent engineering challenges could also delay it.

Notably, sporadic claims of "quantum breakthroughs" have emerged: e.g. in late 2024, Chinese researchers using a D-Wave quantum annealer claimed the first *quantum* attack on encryption, allegedly cracking small instances of certain ciphers. However, their experiment was limited to a toy 22-bit key - nowhere near real-world key sizes. Such demonstrations show progress but also highlight how far there is to go. In summary, as of today quantum computing remains an evolving, immature technology with tremendous promise but significant hurdles to overcome before it becomes a practical tool for cryptanalysis.

Nonetheless, given the stakes, the prudential view is to assume that a cryptographically relevant quantum computer *could* arrive within the next decade or two, and to begin preparing well in advance.

The Quantum Threat to Cryptography

Modern cybersecurity relies heavily on cryptographic algorithms that are mathematically infeasible for classical computers to break within meaningful timeframes. Quantum computing threatens to upend this assumption by exploiting algorithms that can solve certain math problems exponentially faster. Two quantum algorithms in particular cast a long shadow over current cryptography:

- **Shor's Algorithm (1994):** Peter Shor's algorithm can factor large integers and compute discrete logarithms in *polynomial time* on a quantum computer. These problems are the backbone of RSA, Diffie–Hellman (DH), elliptic curve cryptography (ECC), and many digital signature schemes. In essence, Shor's algorithm means that a sufficiently powerful quantum computer could derive private keys from public keys, breaking the confidentiality and authenticity provided by all widely used public-key algorithms. RSA with 2048-bit keys, ECDSA with 256-bit keys, and the like - currently secure against classical attacks - would be easily broken by a quantum adversary.

  This is not a gradual degradation of security; it is a near-total collapse of public-key cryptography as we know it. All protocols that rely on RSA/ECC for encryption, digital signatures, or key exchange (from TLS/SSL web browsing, to VPNs, to code-signing and blockchain wallets) would be vulnerable. Digital signatures could be forged (undermining data integrity and authentication) and encrypted communications could be decrypted. The scope of impact is enormous - everything from online banking and e-commerce, to secure email, to critical infrastructure communications would be affected. It bears emphasizing that Shor's algorithm requires a large quantum computer; as discussed, no such machine exists yet. But the mathematics is sound - if, and when, the hardware catches up, today's public-key cryptography will no longer offer security.

  This impending event is sometimes referred to as "Q-Day" - the day a quantum computer breaks commonly used crypto.

- **Grover's Algorithm (1996):** Lov Grover's algorithm provides a quadratic speed-up for unstructured search problems. In cryptographic terms, Grover's algorithm can brute-force search a key space in roughly $\sqrt{N}$ steps instead of N. This affects symmetric cryptography (like AES, 3DES) and hash functions (like SHA-2) by effectively halving their security strength. For example, a 128-bit AES key, which requires 2^128 tries to brute force classically, could be found in ~2^64 quantum operations using Grover's algorithm.

  Fortunately, this threat is manageable: doubling the key length (e.g. using AES-256 instead of AES-128) counteracts Grover's square-root speed-up. Indeed, NSA's post-quantum guidelines (CNSA 2.0 Suite) already recommend AES-256 for highest security to withstand quantum attacks. No quantum algorithm is known that can outright break symmetric ciphers or hash functions faster than Grover's generic attack, and Grover's algorithm itself is not easily parallelizable (e.g. even running many quantum searches in parallel yields limited further speed-up).

  Thus, symmetric crypto is considered *quantum-resistant* with relatively minor adjustments (larger keys/hashes). The primary concern is with asymmetric (public-key) cryptography, which faces total compromise by Shor's algorithm. As a result, when we discuss "post-quantum security," we predominantly mean replacing public-key algorithms; symmetric algorithms just need slight strengthening.

Harvest Now, Decrypt Later- Data Longevity Risks: One particularly insidious aspect of the quantum threat is that the vulnerability is retroactive. Adversaries don't need to wait for Q-Day to exploit it- they can begin harvesting sensitive encrypted data *today*, store it, and decrypt it the moment they obtain quantum capabilities. This strategy is often termed "Harvest Now, Decrypt Later." Even if it takes 10 or 20 years to build a cryptanalytic quantum computer, any encrypted secrets captured now (for example, intercepted communications or stolen encrypted files) could eventually be decrypted.

This puts data with long-term confidentiality requirements in peril *right now*. For instance, think of: military and diplomatic communications, which might need to stay secret for decades; personal data (health records, financial records) that could harm privacy if exposed in the future; intellectual property and trade secrets that could lose value if revealed after many years. An ISACA survey in 2025 found 56% of cybersecurity professionals were concerned about this harvesting threat and the prospect that attackers "start collecting encrypted data now and decrypt it once quantum computing becomes viable".

National security officials likewise warn that foreign adversaries are likely stockpiling encrypted Western data in anticipation of future decryption. In essence, data longevity is a critical factor: if the required secrecy duration of information (X years) plus the time to transition systems to post-quantum cryptography (Y years) exceeds the time until quantum decryption capabilities (Z years), then that information is at risk.

Mosca's Theorem visualized: If the time remaining for quantum computers to mature (Z) is less than the sum of the time you need to keep data secret (X) and the time needed to upgrade systems (Y), then future quantum breaches will compromise today's secrets. This illustrates the urgency of migrating to quantum-resistant cryptography before "Q-Day."

Renowned cryptographer Michele Mosca encapsulates this with the inequality X + Y > Z as a warning sign. In practical terms, organizations must ask: *How long does our sensitive data need to remain secure? How long will it take to switch our cryptosystems to quantum-safe alternatives?* If the sum of those durations could be longer than the quantum timeline, there is cause for immediate action. Many experts argue we are already in that window for certain types of data. For example, if one believes there is even a modest chance that capable quantum computers could arrive in ~10 years, and one's data must remain confidential for 10+ years, then precautions must start *now*. As we will discuss, governments and standards bodies are responding by urging prompt migration to post-quantum cryptography (while acknowledging that this migration itself will be a multi-year endeavour).

The key point is that the quantum threat extends the security horizon: it forces us to think not just about adversaries' abilities today, but what they might do with data they steal in advance of future capabilities.

Cross-Sector Impact Analysis

The fallout from a quantum computing breakthrough in cryptography would not be confined to any single domain- it would reverberate across all sectors that rely on digital security. Here we analyse the potential impacts and readiness in several key sectors: finance, government/defence, healthcare, and critical infrastructure. Each sector has unique vulnerabilities and stakes in the post-quantum transition, yet common themes emerge around the need for urgent preparedness and long-term planning.

Financial Services and Banking

The finance sector underpins the global economy and is highly digitized, making it a prime arena for cybersecurity risks. Banks, stock exchanges, payment networks, and cryptocurrencies all rely heavily on cryptography. The immediate threat of quantum computing to finance lies in breaking the encryption and authentication schemes that protect financial transactions and records. For example, interbank payment systems and secure financial messaging (like SWIFT) typically use RSA/DH or ECC-based protocols for key exchange and digital signatures.

A quantum adversary could potentially decrypt banking transactions, impersonate financial institutions, or forge digital signatures on payment instructions, leading to fraud or massive disruptions in financial markets. KPMG's surveys indicate that financial firms are well aware of this risk- among U.S. companies (many of which in finance), 78% expect quantum computers to be mainstream by 2030, and most executives rank quantum threats to data encryption as a top concern. Yet paradoxically, readiness is lagging: over 80% admitted they need to do a better job evaluating and addressing their quantum-vulnerabilities.

One area of acute vulnerability is cryptocurrencies and blockchain technologies. Blockchain systems (e.g. Bitcoin, Ethereum) rely on digital signatures (usually ECDSA) to secure ownership of assets. If ECC were broken by quantum computing, an attacker could *retroactively derive private keys from public blockchain addresses*, allowing theft of cryptocurrency on a massive scale. In blockchain networks, transactions already recorded on the ledger could be illegitimately authorized by a quantum-capable thief. Additionally, some blockchain hash algorithms could be affected by Grover's algorithm (though using longer hashes can mitigate this). The crypto community is actively researching quantum-resistant blockchain schemes, but most existing cryptocurrencies remain exposed in the long-term. This poses a financial stability risk beyond individual owners- a quantum attack on a major cryptocurrency could erode trust in digital financial systems. Recognizing this, Singapore's central bank explicitly warned banks about quantum threats to blockchain and advised preparations within the decade.

Another consideration is the longevity of financial data and instruments. Some sensitive financial data (e.g. investment strategies, client portfolios, long-term contracts) might need confidentiality for many years. Moreover, financial regulations (like GDPR or bank secrecy laws) mandate protecting customer data; a quantum breach years down the line could still mean regulatory or reputational fallout. *Personal data handlers* such as banks and insurance firms are legally required to keep data private for extended periods (5, 10, 20+ years), which is directly challenged by the harvest-now/decrypt-later scenario. The finance sector also includes long-lived infrastructure like ATMs, secure payment terminals, and chip-card systems that are deployed for decades. If these devices have cryptographic components that cannot be easily upgraded (many ATMs and point-of-sale systems still run outdated software), they could become weak links in a post-quantum world.

On the positive side, the finance sector has resources and incentives to lead on quantum-safe cryptography. Major banks are already funding research and participating in quantum preparedness forums. Some have experimented with quantum key distribution for ultra-secure links between datacentres or with quantum random number generators to strengthen cryptographic keys. Industry bodies and regulators are increasingly vocal: the World Economic Forum, in collaboration with the UK Financial Conduct Authority, released guidance on Quantum Security for the Financial Sector urging global regulatory approaches. Europol and others have called for a coordinated response to quantum threats in financial services to avoid a patchwork of readiness levels that adversaries could exploit.

In summary, quantum computing presents systemic risks to finance, but also a strong impetus for innovation in cybersecurity. Firms that move early to implement post-quantum solutions (once standards stabilize) can safeguard not just their own assets but contribute to broader financial stability. Conversely, those that lag may find that trust- the bedrock of finance- is easily shattered if their security guarantees suddenly become null and void.

Government and Defense

The defence sector and government intelligence community arguably face the most consequential risks from quantum adversaries. National security communications and classified data have confidentiality requirements stretching into decades- sometimes indefinitely. A breach of military or diplomatic secrets via quantum code-breaking could alter the balance of power. As RAND researchers put it, *"it's hard to overstate the consequences"* if a hostile actor gained the ability to break today's cryptography. Virtually all sensitive government information- from citizens' personal data to state secrets- could become transparent to the adversary that first harnesses a cryptanalytic quantum computer. This is why the NSA warned that quantum attacks could be "devastating" to National Security Systems.

Consider secure military communications: they rely on encryption (often NSA's Suite-B algorithms like AES, ECDH, RSA, etc.). An enemy with quantum capability could potentially decrypt secret troop movements, logistics, or even nuclear command and control messages. The confidentiality, and also integrity, of defence communications is at stake- forged orders or falsified intelligence could wreak havoc. Intelligence agencies are also concerned about archive protection: decades of intercepted but encrypted communications (from both allies and adversaries) could suddenly be deciphered once quantum computing arrives. This is a double-edged sword: while U.S.-allied militaries fear their secrets being read, they also see opportunity in decrypting others' secrets. This dynamic is fuelling what some call a new "cryptographic arms race." Nations that develop quantum computers first (or quantum code-breaking algorithms) will have a significant strategic advantage.

In response, governments are mobilizing. The U.S. government has taken a clear stance: move to post-quantum cryptography (PQC) as the primary defence, rather than physics-based solutions like QKD. In 2022, the White House issued National Security Memorandum 10, which mandates that all federal agencies migrate to quantum-resistant encryption for classified and vital systems by 2035 (or as soon as feasible). This acknowledges the massive effort required- essentially rebuilding or updating every secure system over the next decade. The NSA followed up with detailed guidelines for the Department of Defense and Intelligence Community on prioritizing systems for upgrade. Thanks to years of work by NIST (discussed later), the U.S. has identified candidate PQC algorithms, and the government has earmarked significant funding ($7.1 billion between 2025 and 2035) to implement these upgrades. Allied countries are taking similar steps: for example, Germany's BSI, the UK's NCSC, France's ANSSI, and others have all recommended adoption of PQC for national security purposes. NATO, in a 2022 strategy document, noted that "post-quantum cryptography is an important approach to secure communications against quantum-enabled attacks" and that QKD might contribute in the future, but underscored that PQC is the primary path forward for now.

It's worth noting the debate over Quantum Key Distribution (QKD) in government use. QKD allows two parties to share encryption keys with security guaranteed by quantum physics (typically via fibre optic or satellite links). China has invested heavily in QKD- deploying a 2,000-km fibre network and launching at least two quantum satellites to enable secure communication links between cities and even between Beijing and Vienna. The Chinese government has touted this as enhancing cybersecurity and possibly protecting against future quantum decryption. However, QKD has limitations: it requires special hardware, is distance-limited (for fibre), and crucially, it secures only the link, not the data at rest or in end systems. Moreover, it doesn't protect against man-in-the-middle if the quantum channel's authenticity is not guaranteed. Western agencies like the NSA do not support QKD for national security use, citing its cost and constraints. The U.S. (and allies like the UK and France) explicitly favour software-based PQC over QKD for broad deployment. That said, some governments keep a foot in both camps: e.g., Canada's national quantum strategy includes developing QKD capabilities (even as their policy notes QKD is *"not currently recommended for national security systems"*). This dual approach hedges bets- if QKD technology improves (e.g., satellite QKD covering globe) it might augment security, but PQC is still the more scalable solution for now.

In summary, the defence sector stands at the forefront of quantum cybersecurity risk. Nations are acting now to safeguard military and government data against future quantum foes- essentially re-tooling the foundations of

classified communications. But this effort is uneven globally; it's plausible that some states will reach quantum decryption ability while others remain behind in migration, a scenario with serious geopolitical ramifications. The dual-use nature of quantum tech is on full display here: the same quantum computer can be used to break enemies' codes and protect one's own (if combined with new cryptography and possibly QKD). This intensifies the urgency for governments to not only invest in quantum-resistant security, but also to consider diplomatic and arms-control dimensions - for example, should there be treaties about the use of quantum computing in cyberwarfare, or international cooperation to avoid destabilizing surprises? Those discussions are nascent at best. At a minimum, defence organizations should assume that any adversary communication encrypted with legacy algorithms (RSA/ECC) could be an open book to their opponents within the next decade or two, and plan operations accordingly.

Healthcare Sector

Healthcare has increasingly digitized its operations and records, turning hospitals and clinics into rich targets for cyberattacks. The threat of quantum computing adds another layer of risk to a sector already struggling with cybersecurity. Patient records, genomic data, clinical trial results, and medical IoT devices all have confidentiality and integrity requirements that span many years. Health data is intensely personal and often lifetime-sensitive; a patient's medical history or DNA data may need protection for decades (even beyond the patient's life, considering privacy of descendants and research uses). This long-term sensitivity means healthcare data is a prime candidate for harvest-now/decrypt-later attacks- an adversary might steal encrypted health databases today (via ransomware or breaches) and decrypt them in the future, exposing private medical conditions of individuals or embarrassing information about public figures' health. The repercussions include privacy violations, discrimination, and loss of trust in healthcare providers.

Compounding the risk, healthcare IT tends to lag in security upgrades for reasons such as tight budgets, legacy systems, and the need for 24/7 availability. A 2024 academic review on post-quantum healthcare cybersecurity highlights that the sector faces unique challenges in adopting new cryptography. Integration issues are significant: many medical devices and electronic health record systems use outdated or proprietary protocols; introducing quantum-resistant algorithms (which often have larger key sizes and heavier computational loads) could be difficult without hardware refreshes. Budget constraints are non-trivial- hospitals often operate on thin margins and cybersecurity investments compete with other urgent spending. Implementing post-quantum encryption might require replacing or upgrading a multitude of devices (from MRI machines to infusion pumps) that currently rely on lightweight cryptography, which is a costly proposition. Additionally, there is a skills gap: healthcare IT staff may not be well-versed in cutting-edge cryptography. According to the review, specialized training will be needed to implement post-quantum solutions correctly in healthcare environments.

Despite these hurdles, the healthcare sector cannot afford inaction. As the cited paper concludes, protecting medical data in the quantum era is imperative and a proactive "roadmap for cybersecurity resilience" is needed. This includes deploying quantum-resistant encryption for health data at rest and in transit, ensuring secure communication (e.g. between hospitals, labs, and insurers) that cannot be eavesdropped by future quantum spies. It also means strengthening authentication mechanisms- for instance, moving away from classical RSA-based digital signatures in medical device firmware or health information exchanges, to new PQC digital signatures. Data integrity is another focus: quantum attacks could enable falsification of medical records or test results by forging cryptographic checksums or signatures. Healthcare providers will need robust integrity assurance (potentially using post-quantum secure hashes and digital signatures to verify records).

Moreover, healthcare organizations should establish rigorous key management and access control regimes anticipating a transition (e.g. ensuring they can swap out cryptographic modules in medical devices and software via remote updates as standards evolve).

Encouragingly, the healthcare cybersecurity roadmap suggests an interdisciplinary approach: involving not just IT staff, but also clinicians, device manufacturers, and policymakers. Governments may need to mandate that any new medical devices are "crypto-agile" (able to accept new cryptographic algorithms) and possibly certify devices for quantum-resistant encryption if they handle sensitive data. The FDA in the US, for instance, could include post-quantum considerations in its cybersecurity guidance for medical devices. On the provider side, hospitals can start by

inventorying their systems for use of vulnerable cryptography (much like other industries are doing). Electronic Health Record (EHR) systems and health information exchanges could begin pilot programs using PQC algorithms (once standardized) for high-confidentiality data fields, possibly in a hybrid mode alongside classical encryption until fully vetted. Given the often life-and-death nature of healthcare operations, any cryptographic change must be carefully tested to avoid inadvertently bricking devices or breaking interoperability. This makes the transition timeline critical; the sector will need plenty of time to migrate, which again argues for starting as early as possible.

In summary, the healthcare sector is highly exposed to long-term quantum risks but faces internal challenges to respond. It holds some of the most sensitive personal data and must maintain patient trust. A quantum-compromised healthcare system could mean personal health information splashed on the internet or extortion based on private diagnoses. Therefore, timely adoption of post-quantum strategies is vital for healthcare. By following a clear roadmap - upgrading encryption, securing communications, enhancing authentication, and training personnel - healthcare organizations can bolster the resilience of medical data in the face of coming quantum threats.

The effort will require significant investment and coordination, but the cost of complacency (in privacy violations, legal penalties, and loss of life due to corrupted data) would be far higher.

Critical Infrastructure and Industry

Critical infrastructure - such as energy grids, water systems, transportation networks, and telecommunications - forms the backbone of national well-being. These systems are increasingly "smart" and interconnected, relying on sensors, control systems and communication networks that are secured by cryptography. The quantum threat to critical infrastructure is that an attacker could penetrate these systems by breaking the cryptographic controls that prevent unauthorized access or commands. For example, electric power grids use encrypted communications for telemetry and control (SCADA systems). If those encryption schemes (often RSA/DH based VPNs or proprietary crypto in industrial protocols) were rendered insecure, an adversary could potentially send false control signals - causing blackouts, damaging equipment, or disrupting services.

KPMG notes the "potentially disastrous impact of quantum [attacks] disrupting the operation of a city's power grid" as a vivid example. Likewise, telecommunications providers secure their backbone links and subscriber authentication with algorithms that could be broken, risking eavesdropping or massive telecom fraud. Imagine a scenario where a quantum-capable attacker disables all traffic lights in a city or manipulates rail signalling systems by defeating the cryptographic authentication used in control commands - the results could be dire.

One worry is that much of the critical infrastructure relies on long-life systems. Industrial control systems (ICS) and IoT sensors in utilities are often deployed for decades without major hardware changes. Many run on low-power processors that cannot easily support the computational demands of some post-quantum algorithms. They also often use hard-coded cryptographic keys or algorithms that are not updateable remotely. This "technical debt" means some infrastructure may effectively be stuck with vulnerable crypto unless expensive replacement programs are undertaken. Organizations should begin evaluating which systems will age into vulnerability - for instance, if a sensor network installed in 2020 with RSA/ECC is meant to operate until 2040, that clearly falls into the danger zone of quantum disruption.

Planning for either retrofit (if possible) or earlier replacement will be critical. There is an opportunity now for infrastructure operators to demand crypto-agility in new equipment - ensuring that devices support firmware updates for new cryptographic primitives. Unfortunately, awareness in some industrial sectors is still catching up. The ISACA poll showed that across industries, 44% of professionals had *never heard of* the new NIST post-quantum cryptography standards, and only 5% said their organization treats quantum security as a high-priority issue. This suggests many critical infrastructure entities (utilities, transportation authorities, etc.) may not yet be seriously planning for the quantum transition, which is a gap that needs addressing by sector regulators and government oversight.

Apart from disruption, there is also a national security angle to infrastructure security. Adversaries might target infrastructure not just to cause chaos but to gather intelligence. For example, breaking encryption on a water utility's SCADA system might reveal usage patterns that indicate troop deployments at a military base (through water

consumption changes), or decrypting telecom traffic could expose the conversations of government officials. Thus, securing infrastructure communications against future quantum decoding is part of a nation's broader security resilience.

On the industrial front (manufacturing, supply chain), quantum computing also offers opportunities - for instance, quantum optimization could improve logistics. But our focus here is on cybersecurity. Supply chains could be impacted if quantum breaks the digital signatures used in code signing or product authenticity checks. Many industries rely on PKI (public key infrastructure) to ensure that software updates for equipment are legitimate. If those signatures (often RSA/ECDSA) become forgeable, attackers could install malware via fake updates to factory robots, HVAC systems in data centres, or safety controllers in chemical plants. The integrity of the industrial software supply chain is thus another cross-sector point of vulnerability.

Telecommunications companies are a special category of infrastructure because they carry the communications for all other sectors. Telcos need to consider both upgrading the encryption of backbone links (often done with optical link encryption using algorithms like AES; here the main issue is key exchange procedures that may use RSA/ECC) and the security of subscriber authentication (SIM cards and 5G authentication currently use algorithms that might need to be replaced with post-quantum versions). Some telecom providers in Asia and Europe have experimented with QKD for inter-city links, but those remain pilot projects.

Transportation infrastructure (aviation, maritime, automotive) also uses cryptography extensively: from air traffic control data links to the authentication of messages between autonomous vehicles and traffic management systems. Each sub-domain will need analysis to replace or strengthen those cryptographic protections.

In light of these wide-ranging implications, many governments now classify quantum computing as part of critical technology strategy. The U.S. Department of Homeland Security (DHS) has issued a roadmap for critical infrastructure operators to begin inventorying and assessing their use of vulnerable cryptography, under its Post-Quantum Cryptography Initiative. Similarly, organizations like CISA (Cybersecurity & Infrastructure Security Agency) regularly urge adoption of "crypto-agile" solutions in preparation for PQC.

The Monetary Authority of Singapore released an advisory specifically addressing quantum risks to the financial and critical systems, essentially telling organizations to act now rather than wait. There is a recognition that time is of the essence - "there is little time to lose for organizations to gain a deeper understanding of the risks quantum may pose". Critical infrastructure providers are encouraged to consider the lifetime value of their data and systems: data that would be catastrophic if misused, and systems that will be in service for many years.

In conclusion, critical infrastructure faces a dual challenge: it must mitigate the looming quantum threat to prevent potentially catastrophic disruptions, and it must do so despite having many legacy systems and constrained upgrade cycles. The effort will likely require public-private collaboration, with governments possibly subsidizing upgrades or legislating requirements. It will also require prioritization - not everything can be fixed at once, so identifying the most critical cryptographic vulnerabilities (the ones that protect the grid, transportation safety, etc.) is key.

Encouragingly, being proactive here not only averts quantum risk but can yield near-term security benefits by modernizing aging systems and eliminating known classical vulnerabilities as well. Quantum readiness can thus be folded into broader infrastructure cybersecurity improvements.

Dual-Use Nature of Quantum Computing: Risks

Quantum computing, like many powerful technologies, is inherently dual-use. The same capabilities that adversaries could use to break security can also be harnessed to enhance security (or other beneficial outcomes) if properly applied. In this section, we discuss the two faces of quantum technology- the risks it poses when used with malicious intent, and the opportunities it offers for advancing cybersecurity and communications.

Offensive Risks (Adversarial Use): The offensive implications of quantum computing have been the primary focus of this paper- the ability to undermine encryption, authentication, and essentially all trust in digital systems. To recap the key risks:

- ***Breaking Public-Key Cryptography:*** As detailed, Shor's algorithm on a large quantum computer could instantly break RSA, ECC, Diffie-Hellman, etc., compromising confidentiality (by decrypting communications) and integrity (by forging signatures). This threatens everything from secure websites and VPNs to digital certificates that verify software updates.
- ***Brute-Forcing Symmetric Keys (Grover's algorithm):*** While not as devastating as Shor's, Grover's algorithm would reduce the complexity of brute forcing symmetric keys and hashes, meaning shorter keys/hashes become unsafe. If an organization remained using 128-bit keys or SHA-256 without adaptation, a quantum attacker could potentially succeed with effort. In practice, the fix is to use larger parameters (AES-256, SHA-512, etc.).
- ***Attacking Blockchain and Digital Identities:*** Quantum-enabled attackers could steal cryptocurrency by deriving private keys, or impersonate individuals/organizations by defeating digital signature schemes. This could facilitate fraud, theft, or sabotage in any system that relies on digital signatures (including code signing and secure boot in devices).
- ***Accelerated Cyberattacks:*** Apart from cryptography, quantum algorithms might speed up solving certain hard problems that could be relevant to cyber offense. For instance, a quantum computer could possibly expedite searching for vulnerabilities (through optimization or machine learning), or perform more effective password cracking by modelling it as an unsorted search (though again mitigated by strong hashing). The *emergence of quantum-enabled cyberattacks* means adversaries with quantum access could simply do everything faster and at greater scale- from cracking encrypted passwords to testing large numbers of potential exploits in parallel.
- ***Covert Communications and Detection Evasion:*** A subtle risk is that quantum computing, combined with quantum communications, could enable new forms of stealthy communication or sensing that make detection of malicious activities harder. For example, quantum communication can be theoretically undetectable (quantum steganography), which might aid adversaries in hiding command-and-control channels.

These offensive uses underscore why many view quantum computing as a potential weapon in the cyber realm. There is concern that state-sponsored attackers, cybercriminal syndicates, or even hacktivists could use cloud-based quantum computing services in the future to augment their attacks if access becomes widespread. Indeed, the Global Risk Institute cautions that quantum code-breaking might arise faster than anticipated, implying that organizations should not be complacent.

Defensive Opportunities (Beneficial Use): On the flip side, quantum technologies offer novel ways to strengthen security and privacy:

- ***Quantum-Resilient Cryptography (PQC):*** The foremost defence uses classical algorithms (not quantum computers) but is a response enabled by our understanding of quantum threats. Post-quantum cryptography algorithms (lattice-based, hash-based, code-based, multivariate, etc.) are being standardized to replace RSA/ECC with alternatives believed to withstand quantum attacks. This is not a direct use of quantum tech, but it's a critical opportunity created by foresight of the quantum era- essentially "quantum-proof" math that we can deploy on conventional computers to secure data *before* quantum computers arrive. The opportunity here

is to upgrade digital security across the board, potentially also improving resilience against *classical* attacks (since many PQC schemes are also hard for classical attackers).

- ***Quantum Key Distribution (QKD):*** As discussed, QKD uses quantum physics (typically sending photons with random polarization states) to establish encryption keys between two parties with provable security - any eavesdropping on the quantum channel will disturb the quantum states and be detected. QKD offers a way to exchange secret keys with information-theoretic security, independent of computational assumptions. The opportunity is a future global network of quantum-secured communication links, as China is pioneering. QKD is already enabling quantum-secure communication for specialized use cases (e.g., inter-bank communication in Switzerland, secure voting transmission in some countries). While it won't replace public-key crypto for all situations (due to needing direct links or trusted relays), it can add an extra layer of security for the most sensitive links (e.g., between government facilities). NATO and others envision that improvements in QKD could complement PQC for secure communications. It's a classic dual-use story: the same quantum principles that threaten RSA can be used to create encryption keys that even quantum computers cannot break (because the keys are truly random and one-time pads can be achieved if keys are as long as the message).
- ***Quantum Random Number Generators (QRNGs):*** High-quality randomness is the bedrock of secure cryptographic keys. Traditional pseudo-random generators can be flawed or seeded poorly, sometimes leading to catastrophic breaches (e.g., predictable RNGs causing crypto wallet thefts). Quantum random number generators leverage inherent quantum indeterminacy (e.g., decay of particles, photon detection) to produce truly random numbers. These can strengthen security by ensuring keys and nonces have maximal entropy. Already, QRNG devices are on the market and being integrated into hardware security modules and even smartphones. As we move to post-quantum algorithms (some of which require longer random seeds), having robust entropy sources is valuable.
- ***Quantum Computing for Good in Security:*** Researchers are also investigating how quantum computing might solve certain hard security problems. For example, quantum algorithms could potentially help in searching large state spaces for vulnerabilities or performing faster simulations of physical processes to test system defences. Quantum machine learning might one day improve anomaly detection by handling complex pattern recognition in network traffic. These applications are speculative and in early stages, but they hint that defenders will also harness quantum computing to bolster cybersecurity (just as today both attackers and defenders use classical supercomputing and AI).
- ***Secure Multi-Party Computation and Zero-Knowledge:*** Quantum techniques might enable new cryptographic protocols as well. There is theoretical work on quantum-enhanced zero-knowledge proofs and other primitives that could make verification processes more secure or efficient. Additionally, quantum computers can potentially facilitate complex tasks like large integer sampling or lattice problems that, interestingly, might even assist in parameter selection for post-quantum cryptosystems (like identifying hard instances).
- ***Privacy and Noise:*** An interesting nuance - the "noise" in current quantum devices, normally seen as an obstacle, can itself be a resource for security. Some proposals suggest using quantum noise to mask communications or to generate one-time pads on the fly.

Quantum computing is not purely a cybersecurity threat. In fact, its emergence has pushed the industry to strengthen cryptographic defences. The development of post-quantum cryptography (PQC) is a direct response, and it may ultimately enhance resilience against both quantum and classical attacks. As Dr. Michele Mosca noted, this is "a blessing in disguise," encouraging the creation of more robust foundations for the digital economy. If the transition to quantum-safe encryption succeeds, we will leave behind protocols that remain secure even in a post-quantum world. Additionally, tools like quantum key distribution (QKD) and quantum random number generation (QRNG) offer new options to augment classical defences.

However, taking advantage of these benefits requires targeted investment and a realistic strategy. Overhyping quantum solutions can be risky. For instance, QKD is not a catch-all solution, and even NIST-approved algorithms like CRYSTALS-Kyber have shown implementation-specific vulnerabilities. These are not failures of the underlying math, but they serve as reminders that no system is immune to flaws. A balanced approach will apply quantum tools where they add real value and focus on robust PQC implementation to ensure broad, sustainable protection.

Current Readiness and the Challenge of Transition

A critical question remains: Are organizations and markets prepared for the coming quantum cybersecurity challenge? Several recent surveys and studies suggest that while awareness has grown, actionable preparedness is lagging across both private and public sectors. There is a gap between recognition of the threat and concrete planning- a gap that must be closed before the technology matures.

Industry Awareness vs Action: The ISACA 2025 Global Poll of over 2,600 IT security professionals revealed striking statistics: 62% of respondents believe quantum computing will break current encryption standards, yet only 5% said their organization considers it a high-priority issue in the near term. Equally, only 5% reported having a defined strategy to address quantum threats. In fact, 40% were not even aware of any company plans, and 41% said their company has *no plan at all* to tackle quantum risks at this time. This indicates a widespread *"wait and see" approach or even complacency*. Part of the issue is likely the timeline uncertainty- with many IT leaders assuming quantum is a distant or speculative threat, it falls to the bottom of budget and strategy priorities. However, this runs counter to the fact that 25% of these professionals believed the "transformative potential" of quantum (including its risks) will be realized in their industry within 5 years, and 39% believed it within 6–10 years. In other words, many acknowledge that within a decade quantum computing could upend cybersecurity, yet a majority are not actively preparing. This is a classic example of a looming risk that suffers from the tragedy of the horizon- it's beyond the immediate quarter or budget cycle, so it's deferred.

Another telling sign is knowledge of solutions: despite NIST working on post-quantum cryptography standards for years, only 7% of the ISACA respondents said they have a strong understanding of these new standards, and a full 44% admitted they have *never heard* of them. This is alarming- it's akin to being worried about a coming storm but not paying attention to the design of the levees that will protect you. It suggests a need for broad education and outreach so that IT professionals even know what tools will be available.

The KPMG surveys similarly show a readiness gap. In Germany, 95% of organizations (in a BSI/KPMG study) rated quantum's impact on cryptographic security as high, and 65% said the risk to their own data was high, yet only 25% have incorporated the quantum threat into their risk management strategy. In North America, while over 70% express extreme concern about quantum threats, over 80% admit they need to do more to shore up their defences. There's also a silver lining: these numbers indicate that top executives are at least *concerned*- that's the first step to getting resources allocated. Quantum risk was cited as a top-three challenge in the next 3-5 years by many C-suite respondents. We may be near a turning point where planning moves from the back burner to active development.

Market Readiness: From a market perspective, the ecosystem for post-quantum solutions is still maturing. As of 2024, NIST has only just released draft standards for the first bunch of PQC algorithms. Vendors are starting to offer implementations (IBM, for instance, had a hand in developing some of the algorithms and is actively pushing "quantum-safe" encryption services). But organizations are hesitant to deploy non-standardized or evolving tech at scale- understandably, they don't want to back the wrong horse or incur costs twice. Many are likely waiting for final standards (expected around 2024 for three algorithms, and 2025 for another, per NIST's timeline) before jumping in. This waiting game can be dangerous if everyone waits until the last minute.

Another aspect of market readiness is the availability of expertise and tooling. Implementing PQC isn't trivial; the new algorithms have different key sizes, performance profiles, and even usage semantics (for example, using a KEM- Key Encapsulation Mechanism- in places where you used Diffie-Hellman requires some protocol redesign). There's a need for updated cryptographic libraries, hardware support (accelerators for lattice operations perhaps), and testing/validation frameworks (e.g., FIPS 140 modules that incorporate PQC). Governments are starting to push this- the U.S. for instance requires agencies to test PQC in systems now and some procurement is mandating crypto-agility (the ability to swap out cryptography without major overhaul). Cloud providers and tech giants are also experimenting: e.g., Google and Cloudflare have run trial implementations of PQC algorithms in TLS to gauge performance and compatibility. These trials have generally shown that while PQC algorithms often have larger overhead (e.g., Kyber key exchange adds some kilobytes of data and some milliseconds of CPU time), they are *feasible* to implement in today's

infrastructure for many use cases. But challenges remain in constrained environments like IoT- some PQC public keys or signatures (hundreds of bytes to a few kilobytes) might strain extremely low-bandwidth or low-memory devices.

Risks of Immature Adoption: An important point is that rushing to deploy immature tech can introduce new vulnerabilities. For example, early implementations of PQC algorithms have already seen issues- a side-channel attack on a specific implementation of Crystals-Kyber was discovered, reminding that things like constant-time implementation and resistance to physical attacks are as important as ever. If organizations implement quantum-resistant encryption poorly, they might unknowingly create backdoors even before quantum computers exist. Similarly, QKD systems, if not properly integrated (e.g., the classical post-processing and authentication of the quantum channel), could be misconfigured to yield a false sense of security. Thus, testing and standards are crucial. We need conformance tests, interoperability tests, and certified hardware supporting PQC to smooth the transition.

The coming years (mid-2020s) will likely see a proliferation of these efforts- which require coordination by standard bodies (ISO, IETF, IEEE, etc., in addition to NIST).

Regulatory Pressure and Incentives: One way to accelerate readiness is through regulations and laws. Governments have begun to act: the U.S. passed the Quantum Computing Cybersecurity Preparedness Act (2022), which essentially mandates the federal government to prioritize transitioning to PQC and to inventory all cryptographic usages in agencies. It also suggests that the private sector will be encouraged (or required via contracts) to follow. National Security Memorandum-10 (mentioned earlier) provides a roadmap with milestones (inventory by 2023, testing by 2025, etc.). In Singapore, the MAS advisory (2024) not only warned banks but *provided guidelines* on how to address quantum risk in their cyber risk assessments. The European Union is considering how to incorporate PQC into its eIDAS framework for digital signatures and into banking regulations.

These policy moves send a strong signal: if you handle critical data or are part of critical infrastructure, you will be expected to demonstrate quantum resilience in the near future. Organizations that start now will find themselves ahead of compliance requirements and better positioned competitively (they can assure clients their data will remain safe for decades).

International and Cross-Sector Collaboration: Preparing for quantum is not something any single entity can fully do in isolation. It requires a whole ecosystem upgrade- from browsers (to support new TLS cipher suites), to certificate authorities (to issue PQC-based certificates), to hardware manufacturers (to embed new algorithms in secure chips), etc. Collaboration is happening through venues like the Internet Engineering Task Force (IETF), which has working groups on post-quantum cryptography integration into internet protocols; through industry consortia like the Global Semiconductor Alliance's cybersecurity forums; and cross-sector initiatives like the Quantum-Safe Alliance. Europol's 2021 "Quantum Safe Financial" forum advocated a common approach so that, for example, banks don't each pick different non-interoperable solutions. The Global Risk Institute's annual Quantum Threat Timeline reports, which gather input from experts worldwide, aim to keep a pulse on the expected development and thus help organizations align their mitigation timelines.

In summary, current readiness is uneven and generally insufficient if quantum arrived sooner than expected. The world is in a race: will we migrate our cryptography in time or will a surprise quantum breakthrough catch us off-guard? The good news is, the tools to defend (PQC) are emerging at roughly the same pace as the threat. The bad news is, human factors- awareness, budget, organizational inertia- could delay deployment until it's too late. Bridging this gap will require strong leadership and possibly some "sparks"- for instance, if a smaller quantum demo breaks a RSA-1024 key in a lab experiment, that might jolt action. One might compare the situation to Y2K (Year 2000 problem), which likewise required proactive fixes before a firm deadline.

Some call the coming dilemma "Y2Q" (Years to Quantum). The difference is we don't know the exact deadline, making it psychologically harder to prioritize. But the consensus of experts is forming that the wise course is to act now in a phased manner: prioritize sensitive systems first, build crypto-agility, and keep monitoring the evolution of quantum capabilities.

Post-Quantum Cryptography Standards and Migration

A cornerstone of the global response to the quantum threat is the development of Post-Quantum Cryptography (PQC) - new cryptographic algorithms designed to be secure against both classical and quantum attacks. Unlike quantum key distribution, PQC algorithms run on conventional computers and networks, making them practical to deploy widely. After years of international collaboration and competition, the field has converged on several promising families of algorithms, and standards bodies are formalizing these into the next generation of cryptographic standards.

NIST PQC Competition: In 2016, the U.S. National Institute of Standards and Technology (NIST) launched an open competition to evaluate quantum-resistant public-key algorithms. Over three rounds (2017–2022), experts assessed global submissions. By July 2022, NIST named four finalists: CRYSTALS-Kyber (Key Encapsulation Mechanism), CRYSTALS-Dilithium (digital signature), FALCON (another signature scheme), and SPHINCS+ (hash-based signature). Kyber, a lattice-based algorithm, was chosen to replace RSA/ECC for public-key encryption and key exchange. Dilithium and FALCON (lattice-based) were selected for signatures, with SPHINCS+ retained as a non-lattice alternative in case of future breakthroughs against lattice cryptography.

By mid-2024, NIST had released draft FIPS standards for three algorithms: Kyber (as ML-KEM), Dilithium (ML-DSA), and SPHINCS+ (SLH-DSA). The draft for FALCON is expected by late 2024, with final standards anticipated in 2025. These developments mark a significant step toward deploying quantum-resistant cryptographic standards across industries. Recognizing the importance of cryptographic agility, NIST is also evaluating alternatives. A “Round 4” process is underway for other code-based KEMs, including BIKE, HQC, and Classic McEliece. SIKE (isogeny-based) was eliminated after being broken by classical cryptanalysis. NIST will likely select one or two code-based options to complement Kyber. In parallel, a 2023 call for non-lattice digital signature algorithms attracted numerous submissions, now under review, due to limitations of current finalists (e.g., SPHINCS+ has large signatures).

The aim is a diversified post-quantum toolbox using different hard problems - lattices, codes, hashes, multivariate equations - ensuring that no single cryptanalytic advance undermines all defences. While current candidates are believed to be quantum-safe, there are no formal proofs. Crypto-agility and fallback readiness are essential in managing this uncertainty.

Global Standards and Adoption: NIST’s choices carry global weight, but they aren’t the only game in town. European standards bodies and others (ISO/IEC) are also working on aligning or adopting similar standards. The U.S. NSA has updated its suite for National Security Systems to “CNSA 2.0”, which essentially recommends using the forthcoming NIST PQC algorithms (once standardized) for TOP SECRET communications and the like. Many other national cyber agencies (Germany’s BSI, UK’s NCSC, etc.) have indicated they will follow a similar path, focusing on PQC rather than quantum optics (QKD) for general use. One notable effort is in the financial industry via the World Economic Forum and partners, which in 2023 released a paper guiding financial institutions on how to transition to PQC and calling for regulators to incorporate quantum-safe readiness into their frameworks.

Technical Challenges in Migration: Replacing cryptography across systems is not straightforward. Post-quantum algorithms often have much larger key and signature sizes, which can affect existing protocols and storage formats. For example, Kyber public keys are around 800 bytes, compared to 32 bytes for ECC. Dilithium signatures are about 2.7KB, while ECDSA uses just 64 bytes. These increases may break system assumptions.

Although PQC algorithms may demand more computation, many like Kyber and Dilithium remain efficient, performing similarly to RSA-3072 in software. A key challenge is protocol design. During transition periods, hybrid modes are recommended, combining classical and PQC key exchanges. TLS 1.3 is being updated to support this, and certificate authorities plan to issue hybrid certificates with both types of keys and signatures until PQC maturity is proven.

Compatibility issues will also arise. If one device upgrades and another has not, they may not communicate. Early PQC integration, even if unused at first, helps mitigate this.

Industries are adopting phased plans: make systems crypto-agile, introduce PQC in parallel with existing algorithms, then retire older cryptography once new standards are stable.

Cryptographic Agility: This concept has come up repeatedly; it refers to designing systems such that cryptographic components can be swapped out with minimal disruption. Historically, systems that baked in one algorithm (like all those IoT devices hardcoded with RSA/ECC) are now problematic. Going forward, both government directives and industry best practices are emphasizing agility. NIST's framework updates, for example, stress governance processes for updating crypto and testing interoperability of new algorithms. Some organizations are creating internal crypto-agility teams specifically to tackle the quantum transition- an acknowledgment that this is a significant project akin to a major IT migration.

Data Encryption and Key Management in Transition: One tricky area is data already encrypted with classical algorithms - e.g., long-term archival encrypted data or encrypted backups. Organizations should assess whether those need re-encryption with PQC. For very long-term secrets, it might be prudent to re-encrypt now (or soon) with a quantum-resistant scheme rather than relying on RSA. But doing so requires having confidence in a PQC algorithm and available tools. One strategy is to use a hybrid encryption: re-encrypt data with a combination of classical and post-quantum keys such that an attacker would need to break both (which buys time and arguably is safer than each alone). However, complexity arises in maintaining accessibility of that data.

Near-Term Milestones: By 2025, we expect:

- Final NIST standards for the first 3-4 algorithms (Kyber, Dilithium, FALCON, SPHINCS+).
- Early implementations in products: for instance, web browsers might include support for PQC cipher suites (Google already did experiments; U.S. government sites might start requiring PQC cipher support by a certain date).
- Government agencies identifying critical systems that must be migrated by set deadlines (the U.S. has some preliminary deadlines in NSM-10 requiring agencies to submit inventories and plans).
- Possibly the first commercial VPNs or secure communication products boasting "quantum-safe encryption." In fact, companies like Thales, IBM, and various startups (e.g., PQShield, Quantum Xchange) have already begun marketing solutions and urging clients to start trials.

We must remain aware that PQC algorithms, though designed to be secure, will face intense scrutiny. The cryptographic community will actively attempt to break them, as is standard practice. It is possible—though hopefully unlikely—that an unforeseen vulnerability could emerge in a standardized algorithm within a few years. That is why contingency plans are critical. NIST's pipeline of additional candidates and emphasis on cryptographic agility reflect this reality. Historically, we have phased out algorithms like SHA-1 and increased RSA key lengths in response to emerging weaknesses. The difference now is that we are proactively switching algorithms before a quantum attack becomes viable, marking a unique and strategic shift.

In closing, post-quantum cryptography represents our best path forward. Standards are close to finalization, and organizations should begin preparing for adoption now. This includes testing candidate algorithms, tracking standard developments, and planning infrastructure upgrades in a timely, structured way. The groundwork laid by cryptographers is maturing- lattice-based and other PQC solutions are poised to replace RSA and ECC.

However, this transition must be globally coordinated to ensure seamless continuity. If managed well, the shift may go unnoticed by end-users, much like the transition from RSA to ECC in the 2010s. But behind the scenes, it will rank among the most significant transformations in the history of cybersecurity.

Strategic and Policy Recommendations

Facing the quantum cybersecurity threat requires action at multiple levels: governments must steer national efforts and international coordination; enterprises need to upgrade and adapt their security practices; and standardization bodies must ensure robust and usable frameworks for the transition. Here we outline strategic recommendations for each of these stakeholders, aiming to foster a smooth and secure shift to the post-quantum world.

1. **Develop and Implement a National Quantum-Safe Strategy:** Governments should create clear roadmaps for migrating public sector and critical infrastructure systems to post-quantum cryptography. This includes setting target timelines (as the U.S. has done with an objective of 2035 for broad PQC deployment in federal systems) and intermediate milestones (inventory of vulnerable systems, pilot implementations, etc.). A national strategy helps coordinate resources and signals urgency to industry and academia.
2. **Lead by Example- Upgrade Government Systems:** Public sector agencies, especially those handling sensitive data (defence, intelligence, healthcare, citizen data registries), should be early adopters of PQC. Allocating budget for crypto-modernization is crucial. The U.S. has committed $7.1 billion through 2035 for its migration - other governments may need comparable investments proportionate to their infrastructure. By updating government websites, secure email systems, and internal platforms to support PQC, governments also drive vendors to incorporate those algorithms into products (since enterprise software often serves government clients).
3. **Mandate Crypto-Agility and PQC Readiness in Critical Sectors:** Through regulations or incentives, governments should ensure sectors like banking, energy, telecommunications, and transportation take quantum threats seriously. This could take the form of requiring critical infrastructure operators to report on their quantum readiness or include PQC in their cybersecurity frameworks. For instance, banking regulators might require banks to have a post-quantum transition plan as part of their IT risk management. Some regulators are already moving this way (e.g., Singapore's MAS advisory in 2024 explicitly guides banks on quantum risk). Sector-specific guidelines can be developed, ideally harmonized internationally to avoid confusion.
4. **Update Standards and Compliance Requirements:** Government standards (like NIST guidelines, FIPS requirements, or equivalent standards by BSI, etc.) should be updated to include approved post-quantum algorithms as they become available. Compliance regimes such as FIPS-140 (for cryptographic modules) need to test against PQC implementations. Governments can issue updated algorithm profiles for protocols (e.g., an updated TLS configuration baseline that includes PQC cipher suites). This provides clarity to industry on what is expected.
5. **Encourage Research and Workforce Development:** Policy makers should fund research in both quantum computing and post-quantum cryptography. This means supporting universities and public-private research labs to work on next-generation algorithms, quantum-resistant network protocols, and tools for smooth migration. Simultaneously, invest in training cryptographers and security professionals. The lack of awareness (only 7% of professionals strongly familiar with PQC per ISACA) is a bottleneck- so government-backed training programs, cyber range exercises focusing on PQC, and inclusion of quantum security in professional certifications will help build capacity.
6. **International Collaboration and Treaties:** Quantum threats are global; governments should collaborate to share timelines and best practices. Forums like the IEEE, ISO, and the ITU can help coordinate standardization worldwide. Additionally, consider diplomatic dialogues on "quantum arms control." While it's unrealistic to expect a halt to quantum computing research, world powers might agree on norms such as not attacking each other's critical infrastructure with quantum tools or sharing information on quantum cryptanalysis if it threatens global financial stability, etc. Early conversations via the UN or bilateral channels could lay groundwork for responsible use of quantum capabilities. NATO's inclusion of quantum in its defence strategy and WEF's convening of financial sector talks are examples to build on.
7. **Avoid Over-Reliance on Proprietary or Unproven Solutions:** Governments should be wary of quick-fix offers like proprietary "quantum encryption" schemes that lack public vetting. The preference should be for open, standardized approaches (PQC, and standardized QKD if used). NSA's stance against QKD for national security

systems, for example, is rooted in concerns about practicality and reliability. Governments must base decisions on technical merit and strategic need, not hype. That said, they can support multiple approaches (e.g., fund both PQC and QKD research) but should have a primary plan (most have converged on PQC as that plan for now).

8. **Protect Current Data Now:** Governments should assess what critical encrypted data (state secrets, personal data held by the state) might be at risk of being harvested. For extremely sensitive long-term secrets (e.g., intelligence archives, cryptographic keys that protect data at rest), consider re-encrypting with interim quantum-resistant schemes (even if not standardized yet, one could use robust combinations like AES-256 with very large symmetric keys, or layering a NIST finalist PQC algorithm in hybrid mode). Also, ensure all new classified data uses quantum-resistant protection going forward, if possible, to limit the window of vulnerability.
9. **Public Awareness and Industry Engagement:** Governments can play a role in disseminating information about quantum threats and defences to a broader audience, including small businesses who might not have on-staff cryptographers. Publishing easy-to-follow migration frameworks or hosting public-private workshops demystifies the issue. The UK, for instance, might leverage the NCSC's public advice channels to provide guidance on quantum-safe practices for enterprises.

Recommendations for Enterprises and Critical Infrastructure Operators

1. **Assess and Inventory Cryptographic Usage (Know Your Crypto):** Organizations should immediately start a comprehensive inventory of where and how cryptography is used in their systems- akin to a "crypto baseline." This includes identifying all applications, protocols, and devices that rely on RSA, ECC, Diffie-Hellman, or other quantum-vulnerable algorithms. Many organizations have thousands of such instances (from VPN appliances to SSL/TLS on servers, to code signing, to partner data exchange formats). Knowing what you have is the first step; the U.S. federal agencies had a directive to do this by 2023, and private companies should do likewise. This inventory should also estimate data sensitivity and required longevity for each use case.
2. **Develop a Quantum Transition Plan:** Using the inventory, prioritize which systems need to be upgraded first. Not all data is equal- focus on systems protecting data with long confidentiality needs or high sensitivity. For example, an enterprise might prioritize securing its VPN and database encryption (protecting years' worth of customer PII) over, say, short-lived session encryption that isn't recorded. The plan should outline funding, resources, and timelines. Importantly, it should be integrated into the enterprise risk management process, so that leadership is aware and supportive. Given that surveys show only 25% of firms currently address quantum in risk management, adding it explicitly to the risk register is key.
3. **Implement Crypto-Agility in Design:** Enterprises should adopt architectures and products that allow easy swapping of cryptographic algorithms. When developing or procuring software, require that cryptographic components are modular (using standard libraries that can be updated) rather than hard-coded. If you have a custom protocol, consider redesigning it to be flexible with respect to algorithms. Embrace standards like TLS 1.3, which has extension points for new cipher suites, or JOSE (JSON Object Signing and Encryption) which can be extended with new alg identifiers, etc. Where possible, deploy hybrid solutions in the interim- for instance, some organizations experimenting with PQC in TLS do so by performing both classical and PQC handshakes and combining keys. This ensures security even if one or the other is later found weak.
4. **Begin Testing Post-Quantum Algorithms Now:** Don't wait for an emergency to try out PQC. Enterprises can set up a test environment (or pilot project) where a PQC algorithm like Kyber or Dilithium is implemented in a controlled setting- e.g., a test website using a PQC TLS cipher, or a test VPN link using a PQC key exchange. Several organizations (Microsoft, Cloudflare, Google) have already done such pilots in the real world, even partnering to see how different browsers/servers handle it. Enterprises should leverage open-source implementations (many are available from the NIST competition) to gauge the performance and integration issues.

   This hands-on experience will be invaluable for planning production rollout. It also signals to vendors that you are serious- for instance if you use a third-party VPN product, ask the vendor how they plan to integrate PQC

and if you can beta test it. KPMG observed that 62% of firms acknowledge they need to better evaluate their current capabilities for quantum security- testing is a concrete way to do that evaluation.

5. **Strengthen Symmetric Crypto and Hashes:** As a quick win, ensure that the organization's use of symmetric algorithms is already aligned with quantum-resistant best practices. This means using AES-256 instead of AES-128 (or 3DES, which should be retired entirely). Use SHA-384 or SHA-512 for digital signatures (since those outputs would need quantum Grover attacks 2^192 or 2^256 operations, respectively, which is infeasible). These changes can often be done by configuration tweaks and have minimal downside (AES-256 might be slightly slower, but on modern hardware that's negligible in most cases). Many organizations have already moved to these for classical security reasons, but if not, do so now. It "future proofs" symmetric cryptography cheaply.
6. **Secure Long-Term Data Today:** If your enterprise holds data that absolutely must remain confidential for, say, 10+ years (think: healthcare records, intellectual property like designs or formulas, sensitive legal documents, etc.), consider re-encrypting or adding an extra layer of encryption with a quantum-safe algorithm **now**. For instance, one could encrypt a data archive with a hybrid approach (encrypt with classical AES, then encrypt the AES key with a lattice-based KEM like Kyber and store that alongside). Even if PQC algorithms are not yet standardized, using a well-regarded finalist in addition to existing encryption can hedge against the worst-case scenario. Some organizations are doing "crypto overlay," where they wrap data with an additional encryption layer that can be peeled off once PQC is finalized, but would defeat an attacker who breaks the outer layer. This kind of defence-in-depth may be warranted for particularly critical data (the "crown jewels").
7. **Monitoring and Threat Intelligence:** Stay informed about developments in quantum computing. Assign someone (or a team) the responsibility for tracking progress in quantum technology and cryptanalysis. Subscribe to updates from NIST, academic conferences, and industry groups. The situation is dynamic- a major breakthrough (or conversely, a significant delay) in quantum computing R&D could change risk calculations. Being plugged into the latest reports (like the Global Risk Institute's annual threat timeline) will enable course corrections in your plan. Also monitor your industry peers- if big players in your sector begin migrating (or if regulators issue guidance), adjust accordingly.
8. **Collaborate and Share Knowledge:** Enterprises should not tackle this alone. Join industry consortia or working groups focused on PQC transition. For example, there are user groups forming for testing PQC in specific contexts (like the U.S. electrical sector could form a task force under NERC, or global banks under the Institute of International Finance). Share experiences from pilots- what performance impacts did you see, how did customers react, etc. Collaborating can reduce duplication of effort and ensure interoperability.

   This also extends to the supply chain: if you rely on vendors (IT providers, cloud services, etc.), engage them now about their quantum-safe roadmap. Perhaps include language in procurement RFPs requiring quantum-resistant options or at least a commitment to upgrade when standards are ready.
9. **Educate and Train Staff:** As with any major tech shift, your people need to be prepared. Conduct workshops or training for developers and engineers on the basics of PQC algorithms and how to implement them properly. Ensure that security architects understand the differences (for instance, that some PQC algorithms have larger keys that might not fit into legacy protocol message fields, etc.). Incorporate quantum-safety into secure coding guidelines and design reviews. By raising internal awareness, you reduce the risk of mistakes during migration. Given the low familiarity reported (less than 10% feel strongly knowledgeable about PQC), internal education is an urgent need.
10. **Plan for Flexibility and Multiple Scenarios:** The future is uncertain- maybe quantum comes in 5 years, maybe 20. Enterprises should adopt a scenario-based planning: what will we do if a big quantum leap is announced in 2027? Are we ready to accelerate our timelines? Conversely, what if progress stalls- do we still invest steadily or slow down?

    Having contingency plans and triggers (e.g., "If a nation-state announces a 1,000-qubit stable quantum computer, we expedite phase 2 of our migration plan") can be wise. Also plan for the possibility that a chosen PQC algorithm might later be found weak- build the transition such that switching to an alternate algorithm (say from Kyber to a code-based KEM) is not as painful as this first swap from RSA. That may mean avoiding overly custom tweaks and sticking to standard implementations that can be replaced.

Recommendations for Standardization Bodies and Consortia

1. Finalize and Publish PQC Standards Promptly: Standardization bodies such as NIST, ISO, IEC, ETSI, and IETF must continue to prioritise post-quantum cryptography (PQC). NIST's schedule to finalise core algorithms by 2024 and additional selections by 2025 is appropriate. Any delay could obstruct broader adoption. Once complete, the standards must be published accessibly, including reference code and test vectors, to allow confident implementation. ISO and IEC working groups should accelerate adoption to ensure international alignment.
2. Develop Migration Guidelines and Reference Architectures: Beyond algorithms alone, detailed guidance on real-world application is essential. Standards bodies or industry alliances should publish templates and blueprints for implementing PQC, such as quantum-safe VPNs, hybrid X.509 certificates, and transitional models. NIST's December 2023 "Quantum Readiness" guidance is a useful example, outlining potential pitfalls and practical solutions. Clear reference materials will reduce friction and duplication during implementation.
3. Ensure Algorithm Diversity and Ongoing Evaluation: Approving a first wave of algorithms is only the start. Continued review of alternative approaches, such as code-based or multivariate cryptography, remains necessary. Standards bodies should prepare for additional standardisation phases and establish continuous monitoring of emerging cryptanalysis. This mirrors how NIST oversees ongoing validation of AES and hash functions. Flexibility to revise, retire, or supplement algorithms is vital.
4. Support Interoperability and Benchmarking: To promote reliable deployment, organisations like the IETF should host interoperability testing events. These will help ensure, for instance, that different vendors' implementations of Kyber or Dilithium function together correctly. Publication of performance benchmarks across systems, from smartphones to IoT devices, will also be important. Public challenges focused on optimisation can encourage innovation and drive more efficient use of resources.
5. Standardise Quantum-Enhanced Technologies (QKD, QRNG): While PQC remains the main priority, it is also time to prepare standards for quantum-enhanced tools such as QKD and QRNG. ETSI and the ITU are already working on QKD integration frameworks. These standards must include key handoff processes, reconciliation mechanisms, and hybrid usage models with classical encryption. For QRNG, it will be important to define entropy testing, integration protocols, and randomness validation to ensure quality and consistency.
6. Update Security Certification and Compliance Criteria: Compliance regimes such as FIPS 140-3 and Common Criteria should incorporate PQC requirements. Hardware Security Modules and similar devices should support generation and protection of Kyber and Dilithium keys. Testing labs and standards bodies must create new validation profiles and establish guidance for hybrid modes to support auditors and technical teams with clear compliance pathways.
7. Enhance Communication and Outreach: Raising awareness of PQC readiness will be vital. When standards are finalised, organisations like NIST should lead public engagement efforts, including technical briefings, explainer documents, and workshops. As ISACA's survey revealed, understanding across the industry remains limited. A structured education campaign will ensure organisations are prepared to take action.
8. Clarify Patent and Licensing Issues: Intellectual property concerns are a potential barrier, particularly for smaller firms or open-source projects. Standards bodies should ensure that approved algorithms are available under royalty-free terms or provide clear alternatives. Most leading PQC designers have committed to open access, but any remaining legal uncertainty should be addressed quickly to prevent delays.
9. Promote Global Harmonisation: Alignment between jurisdictions is critical. Algorithm identifiers, key formats, and certificates should be consistent worldwide to support secure interoperability. While most international standards bodies appear to be following NIST's lead, continuous collaboration is necessary. In regions where different algorithms are preferred, systems should still allow multiple signatures or keys within a single certificate to maintain trust and compatibility across borders.

Conclusion

Quantum computing is no longer a distant theoretical concept; it is a fast-evolving reality that demands foresight in cybersecurity. While a cryptography-breaking quantum computer is not yet here, the window for proactive action is finite and closing. Our analysis shows that *current encryption and cybersecurity practices - if left unchanged - are on borrowed time*.

The maturity of quantum hardware is advancing, and whether the pivotal breakthrough comes in 5, 10, or 20 years, the consensus is clear that it will come within the lifespan of many of our security systems and the data they protect.

From a critical, balanced perspective, we conclude that quantum computing represents a real but manageable threat to cybersecurity. It is not a cause for panic or fatalistic surrender- indeed, labelling it a doomsday that will "break the internet" overnight is overhyped. On the contrary, it is a challenge that we have the tools and knowledge to address, provided we act with urgency and diligence. The threat is *speculative only in timing*, not in nature. Every major public-key algorithm in use today rests on mathematical problems that quantum algorithms target effectively. Thus, unless current schemes are supplanted, a sufficiently powerful quantum computer will compromise them. The prudent stance is to assume that adversaries are racing on their side- whether we see it or not- to achieve that capability.

We have also highlighted the dual-use nature of quantum technologies. Quantum computing is not solely a threat; it brings opportunities to revolutionize security (e.g. quantum-proof encryption, QKD, improved randomization). It reminds us that the cybersecurity field is dynamic- threats beget new defences, and the cycle continues. The advent of quantum computing is in some ways a catalyst forcing overdue upgrades to our cryptographic infrastructure (some algorithms like RSA have clung on since the 1970s; a refresh would be wise even absent quantum, given incremental classical advances in cryptanalysis and the benefits of modern cryptographic design). In preparing for quantum threats, we may actually bolster security against a range of other threats, achieving a net gain in robustness. However, the transition will not be trivial. Challenges span technical, organizational, and policy domains. Technically, deploying post-quantum cryptography requires careful integration and potentially impacts performance and protocols. Organizations will need to surmount inertia and allocate resources to a problem that has been easy to postpone. The "risk–action gap" evidenced by surveys- many are worried, few are acting- is a gap that must be closed by leadership and perhaps nudged by regulation. Policy and standards bodies have a guiding role to play, and encouragingly, they have moved faster in this area than in some past cryptography transitions. For instance, the collaborative global effort to produce PQC standards by mid-decade is on track, reflecting an understanding of urgency.

We offer strategic recommendations that can serve as a roadmap for various stakeholders. In summary:

- Governments should coordinate national responses, enforce preparedness in critical sectors, invest in research and talent, and lead in deploying quantum-safe technologies in government systems. International cooperation is needed to manage the broader strategic implications.
- Enterprises (especially those in finance, healthcare, defence contracting, and infrastructure) should not wait to be mandated- they should begin inventorying and upgrading their cryptography now, test new solutions, and cultivate crypto-agility. This not only mitigates future quantum risk but often improves overall cyber hygiene.
- Standardization bodies have delivered new tools (PQC algorithms) and must continue to support implementation with clear standards, interoperability guidance, and agility to adapt if any algorithm falters. Ensuring that global standards remain aligned will make the transition smoother worldwide.

Ultimately, preparing for quantum computing is about preserving the trust that underlies our digital society. Trust that our communications are private, that transactions are authentic, that systems will function securely- all this would be undermined if we allowed known vulnerabilities to persist until an exploit exists. By acting decisively on the knowledge we have today, we can ensure that the quantum revolution, when it arrives, will be remembered not for chaos and crises, but for how we harnessed it safely and innovatively. The tone of our times should not be one of vague optimism

that “everything will somehow be fine,” but rather one of determined pragmatism: *we know the task at hand, and we will get it done*.

In the words of one cybersecurity leader, *“At first glance quantum appears to be a curse to security… but this challenge is a blessing in disguise”.* It is a once-in-a-generation opportunity to upgrade and future-proof the digital foundations across all sectors. The cost of action, while not negligible, is far less than the cost of inaction in the face of a threat that grows more concrete every year. With vigilance, cooperation, and strategic investment, we can meet the quantum challenge and emerge with a stronger, more secure cyber landscape that stands the test of time- and of technology.

Sources:

- NIST/IETF- Shor’s algorithm threat and qubit estimates for RSA-2048.
- ISACA (2025)- Survey of professionals on quantum risk, low prioritization, harvest-now decrypt-later concerns.
- KPMG (2023)- Executive surveys on quantum threat perception vs. action in US, Canada, Germany.
- RAND (2025)- NSA’s view of quantum threat as “devastating” to national security systems.
- The Register (2024)- Adi Shamir’s estimate of 30-year timeline vs. others warning of 10-year risk.
- KPMG- Impact on critical infrastructure (power grid disruption example).
- SaberiKamarposhti et al., Heliyon (2024)- Post-quantum healthcare challenges (integration, budget, training).
- SaberiKamarposhti et al.- Need for quantum-resistant encryption, secure comms, robust auth in healthcare.
- Palo Alto Networks - Overview of risks: breaking asymmetric crypto, forging signatures, blockchain vulnerabilities, IoT exposure.
- IETF Draft (2023)- Grover’s algorithm effect and mitigation by doubling key lengths; no practical threat to symmetric crypto.
- Quantum Computing Report (2024)- NIST finalized 3 PQC algorithms (Kyber, Dilithium, SPHINCS+), urging transition and US Gov $7.1B plan (2025–2035) for adoption.
- Quantum Computing Report- Need for multiple PQC algorithms (diverse math approaches) and NIST Round 4 for additional KEMs (HQC, BIKE, McEliece) after some (SIKE) broken.
- KPMG- Quote by Dr. Michele Mosca on quantum’s impact as impetus for stronger security.
- The Register- Chinese experiment with D-Wave annealer attacking 22-bit key cipher, claimed “first quantum threat” to encryption (but on small scale).
- ISACA- Only 7% have strong understanding of NIST PQC, 44% never heard of them (skills gap).
- Global Risk Institute (2024)- Expert assessment that threat “may be closer than previously thought,” urging proactive mitigation.

About CAGI

The Cybersecurity & Artificial Intelligence Governance Initiative (CAGI) is an independent, international institute focused on closing the gap between rapidly evolving technologies and effective governance.

CAGI brings together industry leaders, practitioners, academics, and public-sector stakeholders to translate foresight into actionable governance. The institute operates as a neutral platform, providing evidence-based guidance rather than advocacy or compliance checklists.

Get involved: CAGI welcomes participation from individual professionals, corporate members, and sponsors who wish to contribute to the development of credible, future-ready governance and to help shape how AI and cybersecurity are governed in practice.

www.thecagi.com