Quantum Computing and Cybersecurity Law: Preparing for the Next Generation of Cyber Threats

Deepak Kallal
Independent Research Scholar, New York, USA, Deepak.kallal0967@gmail.com

Cybersecurity Law and Policy Review
Volume 1, Issue 1 | 2025 | https://clprj.com/journal/index

Abstract

The advent of fault-tolerant quantum computing poses an existential threat to the cryptographic foundations upon which the security of digital communications, financial transactions, governmental systems, and critical infrastructure presently rests. Current public-key cryptographic algorithms — including RSA, elliptic curve cryptography, and Diffie-Hellman key exchange — are mathematically vulnerable to attacks by sufficiently powerful quantum computers running Shor's algorithm, and the widespread deployment of quantum-capable systems within the coming decade or two would render vast archives of encrypted data immediately legible to adversaries who have harvested and stored them. This prospect, known as 'harvest now, decrypt later', represents a present legal and regulatory challenge, not merely a future one. Yet the legal and regulatory frameworks governing cybersecurity have been conspicuously slow to respond to the quantum threat, and the scholarly literature on the legal dimensions of quantum computing remains underdeveloped relative to the technical and policy literature. This article addresses that gap, examining the quantum threat to cybersecurity law from multiple angles: the nature and timeline of the quantum risk; the adequacy of existing legal frameworks to incentivise and mandate the post-quantum cryptography transition.

Keywords: *quantum computing; post-quantum cryptography; cybersecurity law; harvest now decrypt later; NIST PQC standards; quantum-safe migration; cryptographic agility; quantum key distribution; international law; critical infrastructure*

1. INTRODUCTION

In August 2024, the United States National Institute of Standards and Technology (NIST) published the first finalised post-quantum cryptography (PQC) standards, representing the culmination of an eight-year standardisation process and a watershed moment in the global effort to prepare digital systems for the era of quantum computing. The publication of these standards — FIPS 203 (ML-KEM, based on CRYSTALS-Kyber), FIPS 204 (ML-DSA, based on CRYSTALS-Dilithium), and FIPS 205 (SLH-DSA, based on SPHINCS+) — was greeted with cautious relief by the cybersecurity community, which had long identified the transition to quantum-resistant cryptography as one of the most complex and consequential security challenges of the coming decade. Yet the publication of standards is only the beginning of the challenge, not its resolution. The migration of global digital infrastructure from quantum-vulnerable to quantum-resistant cryptographic primitives is a task of

extraordinary technical complexity, financial cost, and organisational difficulty — and one whose urgency is poorly reflected in current legal and regulatory frameworks.

The quantum computing threat to cybersecurity is simultaneously more distant and more immediate than popular discourse often suggests. More distant, because the development of a fault-tolerant quantum computer sufficiently powerful to break current public-key encryption — what researchers call a 'cryptographically relevant quantum computer' (CRQC) — remains a formidable engineering challenge whose timeline is genuinely uncertain, with credible expert estimates ranging from a decade to several decades hence. More immediate, because adversarial state actors are almost certainly already executing 'harvest now, decrypt later' (HNDL) strategies — capturing and storing today's encrypted traffic with the intention of decrypting it once a sufficiently capable quantum computer becomes available. For data that must remain confidential for ten or twenty years — governmental communications, intelligence sources and methods, long-term financial records, medical data, trade secrets — the protection window against HNDL attacks has already narrowed dramatically.

The legal dimensions of the quantum computing challenge have received remarkably little systematic scholarly attention relative to the technical and policy dimensions, a gap that this article seeks to address. Legal frameworks for cybersecurity were designed for a world in which the cryptographic foundations of digital security could be taken as given — a world in which the security of RSA-2048 or AES-256 was a reliable assumption rather than a contingent and time-limited one. The quantum era disrupts this assumption in ways that have profound implications for every domain of cybersecurity law: for the adequacy of existing duty-of-care standards; for the liability of organisations that fail to migrate to quantum-resistant systems; for the regulatory obligations of critical infrastructure operators; for the international law governing quantum-enabled state cyber operations; and for the governance of quantum technologies whose dual-use character poses novel regulatory challenges.

This article proceeds as follows. Part Two provides an accessible account of the quantum threat to cybersecurity sufficient to ground the legal analysis that follows, including the technical basis of the cryptographic vulnerability, the timeline debate, and the harvest now, decrypt later problem. Part Three examines existing legal and regulatory responses to the quantum threat, assessing their adequacy across key jurisdictions. Part Four identifies the structural legal and regulatory challenges that the quantum threat poses. Part Five develops a normative framework for quantum-ready cybersecurity law. Part Six addresses the international legal dimensions of the quantum threat, including the implications for state behaviour norms and arms control. Part Seven concludes.

2. THE QUANTUM THREAT TO CYBERSECURITY: TECHNICAL FOUNDATIONS

2.1 Quantum Computing and Cryptographic Vulnerability

Classical computers process information in binary bits — each bit representing either a zero or a one at any given moment. Quantum computers exploit the principles of quantum mechanics to process information in quantum bits, or qubits, which can exist in a

superposition of zero and one simultaneously. Combined with the quantum mechanical phenomena of entanglement and interference, this property enables quantum computers to explore vast solution spaces in parallel, conferring exponential speed advantages over classical computers for certain classes of computational problem. The security of the public-key cryptographic algorithms that underpin the vast majority of secure digital communications rests on the computational intractability of specific mathematical problems for classical computers: the factoring of large integers (which underpins RSA), the discrete logarithm problem (which underpins Diffie-Hellman and DSA), and the elliptic curve discrete logarithm problem (which underpins elliptic curve cryptography, or ECC).

In 1994, mathematician Peter Shor demonstrated that a quantum computer could solve both the integer factoring problem and the discrete logarithm problem in polynomial time — an exponential speedup over the best-known classical algorithms. The practical implication of Shor's algorithm is stark: a sufficiently large and error-corrected quantum computer running Shor's algorithm could break RSA-2048 in hours or days rather than the billions of years that would be required by classical computation. A separate quantum algorithm developed by Lov Grover in 1996 provides a quadratic speedup for searching unstructured databases, which effectively halves the security level of symmetric encryption algorithms such as AES — a more modest threat that can be addressed by doubling key lengths (for example, transitioning from AES-128 to AES-256), but a threat nonetheless.

The asymmetric algorithms most fundamentally threatened by Shor's algorithm — RSA, ECC, and Diffie-Hellman — are ubiquitous in digital infrastructure. They secure the TLS/SSL protocols that protect web browsing, email, and the vast majority of internet traffic; the SSH protocols used for remote server administration; code-signing systems that verify the integrity of software; digital certificate infrastructure; virtual private networks; and the cryptographic mechanisms embedded in the hardware and software of critical infrastructure control systems. The scale of the migration challenge is therefore not limited to a specific application or sector but encompasses the entirety of the internet's cryptographic infrastructure.

2.2 The Timeline Debate and Its Legal Significance

The timeline for the development of a cryptographically relevant quantum computer — one capable of running Shor's algorithm against the key sizes currently in use — is the subject of genuine and substantial expert uncertainty. The physical realisation of fault-tolerant quantum computing at the scale required to break RSA-2048 would require millions of physical qubits to realise the hundreds of thousands of logical qubits (accounting for quantum error correction overhead) that the computation demands — a scale several orders of magnitude beyond the largest quantum computers currently available. Governments and private sector organisations including IBM, Google, Microsoft, IonQ, and numerous national quantum programmes are advancing toward this goal, but the engineering challenges of error correction, qubit coherence, and system integration remain formidable.

Published expert assessments of CRQC timelines span a wide range. A 2022 report by the US Homeland Security Advisory Council estimated that a CRQC could emerge within ten to fifteen years; a 2023 RAND Corporation study assessed the risk as more likely to materialise in the 2033–2048 timeframe, with significant probability mass at both tails. The

UK National Cyber Security Centre has publicly stated that it does not expect a CRQC to emerge before 2030 but regards the 2030–2040 window as a period of elevated risk requiring proactive preparation now. Critically, even expert organisations with privileged access to intelligence regarding foreign quantum programmes candidly acknowledge the limits of their knowledge — a classified breakthrough in quantum error correction by a major state adversary could materially shorten the timeline without public warning.

From a legal and regulatory perspective, the timeline uncertainty has a critical implication: the appropriate response to the quantum threat is not to await greater certainty before acting but to commence the migration to quantum-resistant cryptography immediately, given the length of the transition timeline and the harvest now, decrypt later problem. A large enterprise or government agency typically takes five to ten years to fully migrate its cryptographic infrastructure, accounting for the complexity of discovering all deployments of vulnerable algorithms, updating or replacing legacy systems, testing interoperability, and managing the organisational change involved. For organisations with long data-retention obligations — financial institutions required to retain records for seven years, healthcare providers retaining medical records for decades, government agencies retaining classified materials indefinitely — the protection horizon against HNDL attacks demands action today, not at the point when quantum capabilities are definitively confirmed.

2.3 Harvest Now, Decrypt Later: A Present Legal Problem

The harvest now, decrypt later (HNDL) threat deserves particular emphasis as a legal matter because it transforms the quantum computing risk from a future problem into a present one. HNDL involves the interception and storage of currently encrypted data by adversaries — most plausibly, nation-state intelligence agencies with the technical capability and strategic patience to pursue long-horizon intelligence collection strategies — with the intention of decrypting it once a sufficiently capable quantum computer becomes available. This strategy requires no quantum capability today; it requires only the ability to intercept and store traffic (a capability that major state intelligence agencies demonstrably possess) and the expectation that quantum decryption will become available within the retention period of the stored data.

Intelligence assessments made public by the United States, United Kingdom, and allied governments strongly suggest that major state adversaries — including China and Russia — are actively executing HNDL collection strategies. The systematic targeting of diplomatic communications, intelligence community networks, defence contractor data, and critical infrastructure control systems by state-sponsored cyber actors takes on a new dimension in the light of HNDL: even encrypted data exfiltrated from these systems today may be rendered legible to adversaries within the useful life of the underlying secrets. For categories of data with long-term sensitivity — the identity of intelligence sources, the design parameters of weapons systems, the negotiating positions of governments in ongoing international processes — the harm from future quantum decryption of today's exfiltrated data may be catastrophic.

The legal significance of HNDL is that it makes the quantum cryptographic risk not merely a prospective compliance challenge but an existing data security failure for any organisation that is currently transmitting or storing sensitive data using quantum-vulnerable encryption. A financial institution that encrypts customer data using RSA today,

aware of the HNDL threat, may in a meaningful sense be failing to implement 'reasonable and appropriate' security measures under existing data protection law — not because the encryption is currently breakable but because, given the foreseeable trajectory of quantum computing, it will foreseeably fail to protect the data throughout the period for which the data is required to remain confidential. This analysis, if accepted by courts and regulators, would imply that the duty of care under existing data protection and cybersecurity law already encompasses quantum readiness — a conclusion with substantial regulatory implications that has not yet been definitively addressed by any jurisdiction.

3. EXISTING LEGAL AND REGULATORY RESPONSES TO THE QUANTUM THREAT

3.1 United States Federal Initiatives

The United States has been the most active jurisdiction in developing a legal and regulatory framework for the post-quantum transition, though the framework that has emerged remains predominantly directive- and guidance-based rather than comprehensively mandatory. The Quantum Computing Cybersecurity Preparedness Act, enacted in December 2022, directed the Office of Management and Budget (OMB) to develop guidance for federal agencies on the migration to post-quantum cryptography and required agency heads to prepare inventories of information technology vulnerable to quantum decryption. National Security Memorandum 10 (NSM-10), issued by the Biden Administration in May 2022, established PQC migration as a national security priority and directed the development of a roadmap for transitioning federal government cryptographic systems, with a particular emphasis on national security systems.

The NIST PQC standardisation process, which culminated in the publication of the first finalised standards in August 2024, represents the most substantively significant federal initiative to date. NIST Special Publication 800-208 and the associated migration guidance provide federal agencies with detailed technical direction on the transition, including recommendations for cryptographic agility — the design of systems to support rapid algorithm transitions without wholesale infrastructure replacement. The Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and NIST have jointly published guidance on post-quantum cryptography migration specifically for critical infrastructure operators, though this guidance remains advisory rather than mandatory for private sector entities.

The federal procurement system represents a potentially powerful but incompletely utilised lever for driving PQC adoption in the private sector. Federal Acquisition Regulation (FAR) and Defence Federal Acquisition Regulation Supplement (DFARS) requirements impose cybersecurity obligations on federal contractors that, if updated to mandate PQC compliance, would affect a significant segment of the economy — including the defence industrial base, federal IT service providers, and critical infrastructure operators with significant government contracting relationships. As of this writing, the inclusion of specific PQC requirements in procurement regulations remains incomplete, representing a significant gap in the federal framework.

3.2 European Union and Member State Approaches

The European Union has approached the quantum cybersecurity challenge through a combination of research investment, standardisation activity, and nascent regulatory engagement. The European Quantum Flagship programme, launched in 2018 with a one-billion-euro budget over ten years, has provided substantial research funding for quantum technologies including quantum key distribution (QKD) and post-quantum cryptography. The European Telecommunications Standards Institute (ETSI) has maintained an active quantum-safe cryptography working group since 2008, producing technical reports and specifications that have fed into the NIST standardisation process and will inform European standardisation activity.

At the regulatory level, the European Union Agency for Cybersecurity (ENISA) has published a series of reports on post-quantum cryptography, including a comprehensive 2022 report on the post-quantum threat landscape and migration recommendations. The NIS2 Directive's requirement that covered entities implement 'state-of-the-art' cryptographic measures has been interpreted by some member state authorities as already encompassing an obligation to assess and plan for the PQC transition, though no definitive authoritative guidance has yet been issued to that effect across the EU. The European Central Bank and European Banking Authority have begun incorporating quantum risk into their assessments of financial sector operational resilience, and the Digital Operational Resilience Act (DORA) framework for the financial sector is expected to be updated to address quantum threats as the timeline clarifies.

Germany's Federal Office for Information Security (BSI) has been among the most proactive European national authorities, having published detailed technical guidelines for post-quantum cryptography migration as early as 2020 and recommending specific algorithms for different use cases. France's national cybersecurity agency (ANSSI) has similarly issued PQC migration guidance. The United Kingdom's National Cyber Security Centre published a PQC migration guidance document in 2023, recommending that all organisations begin migration planning immediately and that organisations managing data with long-term sensitivity treat PQC migration as a matter of urgency. None of these national guidance documents, however, constitute binding regulatory requirements for private sector organisations outside the government contracting and regulated sector contexts.

3.3 Sectoral and International Developments

In the financial sector, the Basel Committee on Banking Supervision has begun examining the implications of quantum computing for financial stability and has indicated that it will issue supervisory guidance on quantum risk management as the threat landscape develops. The Society for Worldwide Interbank Financial Telecommunication (SWIFT) has announced a programme for quantum-safe cryptography migration across its messaging infrastructure, reflecting an appreciation that financial messaging systems must be quantum-resistant well before quantum computers capable of attacking them are deployed. The Payment Card Industry Security Standards Council has similarly announced its intention to update PCI DSS requirements to address quantum risks.

At the international level, the International Telecommunication Union (ITU) and the International Organization for Standardization (ISO) are developing quantum-safe

cryptography standards that will complement the NIST framework and provide a basis for international harmonisation. The ITU's Focus Group on Quantum Information Technology for Networks has produced technical reports addressing quantum-safe cryptography and quantum key distribution. The degree to which these international standardisation activities will be translated into binding legal obligations remains to be determined by national and regional regulatory authorities.

4. STRUCTURAL LEGAL AND REGULATORY CHALLENGES

4.1 The Standard of Care Problem

The most immediately consequential legal challenge posed by the quantum computing threat is the question of what standard of care with respect to cryptography existing law requires of organisations that hold sensitive data or operate critical systems. This question is not merely prospective — it has present legal force, given the HNDL threat and the foreseeable vulnerability of quantum-susceptible cryptographic systems within the plausible lifetime of data currently being protected. Yet the standard of care under data protection, cybersecurity, financial regulation, and common law negligence principles in most jurisdictions has not been authoritatively interpreted with respect to quantum risk, leaving organisations in a state of genuine legal uncertainty regarding their current obligations.

The most plausible analysis under existing data protection frameworks — including the GDPR and its equivalents — is that the obligation to implement 'appropriate technical and organisational measures' to protect personal data, taking into account 'the state of the art' and 'the nature, scope, context and purposes of processing' as well as the risks to data subjects, already encompasses an obligation to assess quantum risk and to implement mitigation measures proportionate to the sensitivity and retention period of the data in question. For data whose long-term confidentiality is material — financial data, health data, data concerning national security matters — the state of the art now clearly encompasses post-quantum migration planning, and regulators operating under a purposive approach to data protection law should be receptive to this interpretation.

However, the formal articulation of this duty has not yet been achieved in most jurisdictions, and the absence of authoritative regulatory guidance creates compliance uncertainty that may paradoxically inhibit rather than accelerate migration. Organisations face a risk calculus in which the costs of early migration are certain and substantial while the legal consequences of delayed migration remain, in the absence of regulatory guidance, uncertain. Regulators should address this uncertainty by issuing formal guidance on the standard of care with respect to quantum risk under existing data protection and cybersecurity frameworks — guidance that clearly establishes the obligation to conduct quantum risk assessments and implement migration plans as a component of currently required reasonable security practices.

4.2 The Legacy Systems Problem and Regulatory Feasibility

The practical challenge of PQC migration is substantially complicated by the prevalence of legacy systems across critical sectors — systems whose cryptographic components are

deeply embedded in hardware, firmware, or software architectures that cannot be readily updated through software patches. Industrial control systems and operational technology deployed in critical infrastructure frequently have operational lifetimes of ten to thirty years and were designed with little or no provision for cryptographic upgrades. Embedded systems in medical devices, transportation control systems, and utility management infrastructure present particularly acute challenges: replacement cycles are long, regulatory approval processes for updated devices are time-consuming, and the operational sensitivity of these systems may limit the testing and maintenance windows available for updates.

The regulatory feasibility of mandatory PQC migration timelines must therefore be calibrated carefully to the technical realities of different sectors and system categories. A one-size-fits-all mandate with a uniform compliance deadline would impose disproportionate burdens on sectors with the longest legacy system replacement cycles and could, if set too aggressively, incentivise compliance theatre — paper compliance without meaningful security improvement — rather than substantive migration. Differentiated regulatory approaches that impose earlier deadlines on sectors with shorter system replacement cycles and greater flexibility for sectors with genuine legacy constraints, combined with requirements for interim risk mitigation measures (such as hybrid classical/post-quantum encryption for data in transit), represent a more proportionate and operationally realistic framework.

The concept of cryptographic agility — the design of systems to support algorithm transitions without fundamental architectural change — has been widely advocated as a key principle for PQC migration and should be embedded in regulatory requirements prospectively. Systems procured or deployed after a defined date should be required to implement cryptographic agility as a design requirement, ensuring that future algorithm transitions can be executed more rapidly and at lower cost than the current migration challenge. This is analogous to the regulatory requirement for future-proofing in other safety-critical domains: just as building codes require structures to meet not merely current but projected future standards, cybersecurity regulations should require systems to be designed for cryptographic adaptability.

4.3 Liability Frameworks and the Quantum Transition

The liability implications of the PQC transition present novel and as-yet unresolved questions across multiple areas of law. For organisations that suffer data breaches in the quantum era as a result of inadequate cryptographic migration, the central question will be whether the failure to migrate constitutes negligence — a departure from the standard of care required of a reasonable organisation in their position — or whether the quantum attack was a force majeure event outside the defendant's reasonable control. The resolution of this question will depend in large part on whether regulatory standards have clearly established the PQC migration obligation and, if so, on the timeline within which compliance was required.

Technology vendors occupy a particularly complex position in the quantum liability landscape. Vendors of cryptographic software libraries, security products, and connected devices that embed quantum-vulnerable algorithms have a duty — grounded in product liability principles and, in the EU context, the forthcoming Cyber Resilience Act — to provide products that meet the security requirements of their intended deployment context.

A vendor who continues to ship products with RSA or ECC as the sole cryptographic primitive, without post-quantum alternatives, at a point in time when the standard of care clearly requires PQC support, may face product liability exposure for downstream data breaches facilitated by the quantum vulnerability of their product. The allocation of liability between vendors, systems integrators, and end-user organisations will be a significant source of commercial litigation as the quantum threat materialises.

Insurance markets are beginning to grapple with quantum risk, with some cyber insurance policies starting to include quantum-related exclusions or conditions. The interaction between insurance frameworks and regulatory requirements for PQC migration deserves legislative attention: if insurers exclude quantum-related losses from coverage for organisations that have not achieved a defined level of PQC migration, the combination of regulatory mandate and insurance market pressure could create powerful incentives for timely compliance — or, if the requirements are set unrealistically, could leave organisations exposed to uninsured losses for events that regulatory failure to incentivise migration made more likely.

5. A NORMATIVE FRAMEWORK FOR QUANTUM-READY CYBERSECURITY LAW

5.1 Mandating Cryptographic Inventory and Risk Assessment

The foundational element of a quantum-ready legal framework must be a mandatory requirement for all organisations above a defined size threshold, and all operators of critical information infrastructure regardless of size, to conduct comprehensive inventories of their cryptographic deployments and formal quantum risk assessments. These requirements parallel the environmental disclosure obligations imposed by securities regulators — they do not mandate a specific response to the identified risk but require organisations to understand and disclose that risk as a precondition for effective management. A cryptographic inventory that identifies all deployments of quantum-vulnerable public-key algorithms, including in embedded systems, supply chain components, and third-party services, is a prerequisite for any meaningful migration plan and is itself a significant undertaking for complex organisations.

5.2 Sector-Differentiated Migration Mandates

Building upon the foundation of mandatory risk assessments, a quantum-ready legal framework should impose sector-differentiated mandatory migration timelines that reflect the varying sensitivity of different sectors' data, the varying feasibility of migration given legacy system constraints, and the varying public interest in timely migration. The highest-priority category — encompassing national security systems, critical infrastructure control systems, financial market infrastructure, and systems handling data with the longest confidentiality requirements — should be subject to the earliest and most demanding migration timelines, consistent with the HNDL threat analysis developed in Part Two. For these systems, the case for treating migration as an immediate regulatory obligation, rather than a medium-term planning target, is compelling.

A second tier of obligation should apply to operators of regulated industries including financial services, healthcare, telecommunications, and energy, requiring the adoption of quantum-resistant algorithms for all new deployments and the development of binding migration plans for legacy systems, with regulatory review and approval. The NIS2 Directive's framework of security obligations for essential and important entities provides a natural vehicle for EU-level implementation of these requirements, and the forthcoming update to the Cybersecurity Act's certification framework should incorporate PQC compliance as a mandatory element of certification for security-sensitive product categories.

5.3 Standardisation, Certification, and Regulatory Coordination

The legal framework for quantum-ready cybersecurity must be grounded in a robust and internationally coordinated standardisation architecture. The NIST PQC standards provide a crucial technical foundation, and their rapid adoption as the basis for regulatory requirements across jurisdictions is essential to prevent the fragmentation of the global cryptographic landscape. Jurisdictions that develop competing national PQC standards — as China has with its own PQC standardisation process — risk creating interoperability barriers and compliance burdens for multinational organisations that parallel the fragmentation problems already observed in data protection law.

Regulatory authorities across sectors should work toward the development of harmonised PQC compliance frameworks that enable organisations to satisfy the requirements of multiple regulators through a single compliance programme rather than navigating divergent requirements across jurisdictions. The model of the Financial Stability Board's coordination of cybersecurity policy across financial sector regulators globally provides one institutional mechanism through which such harmonisation could be pursued. A dedicated international forum for PQC regulatory coordination — bringing together the relevant standard-setting bodies, national cybersecurity agencies, and sectoral regulatory authorities — would provide the institutional infrastructure for ongoing harmonisation as the technical landscape evolves.

5.4 Research Investment, Transition Support, and Equity

The legal framework for the PQC transition must be accompanied by public investment in the research, technical assistance, and financial support necessary to enable organisations — particularly small and medium-sized enterprises and public sector bodies with constrained resources — to achieve timely migration. The PQC transition is not merely a compliance exercise but a fundamental transformation of digital infrastructure whose costs are likely to be substantial and whose benefits are distributed across society in ways that market mechanisms will not reliably internalise. Public goods arguments for government investment in PQC migration support are therefore compelling.

Equity considerations also deserve explicit regulatory attention. Larger organisations with sophisticated security functions and substantial resources will be better positioned to execute timely PQC migration than smaller organisations, managed service providers serving small business clients, or public sector bodies with constrained IT budgets. Regulatory frameworks that impose equivalent obligations on organisations of vastly different capacities, without accompanying support mechanisms, risk producing compliance disparities that leave the most resource-constrained parts of the digital

ecosystem — which may include operators of critical community infrastructure — as the weakest links in the post-quantum security chain. Graduated compliance requirements, technical assistance programmes, and potentially subsidised access to PQC-capable security tools for smaller operators should be considered as essential complements to mandatory standards.

6. INTERNATIONAL LEGAL DIMENSIONS OF THE QUANTUM THREAT

6.1 Quantum-Enabled Cyber Operations and the Jus Ad Bellum

The availability of cryptographically relevant quantum computing to state actors will qualitatively alter the landscape of state-sponsored cyber operations in ways that engage fundamental questions of international law. Quantum decryption would enable state actors to read communications and access systems currently protected by public-key cryptography without any detectable intrusion into the target's systems — a passive intelligence collection capability of extraordinary power. The legal characterisation of such covert quantum decryption under international law depends on whether the activity constitutes a prohibited intervention in the internal affairs of the target state, a violation of the target state's sovereignty, or some other internationally wrongful act — questions to which the existing framework of international cyber law does not provide definitive answers.

More dramatically, a state possessing a CRQC could potentially disable the cryptographic protections securing critical infrastructure control systems, financial networks, and military command and control communications in adversary states without any detectable cyberattack in the conventional sense — simply by decrypting the communications and credentials that protect access to those systems and exploiting the resulting access. Such operations could produce effects equivalent to conventional armed attacks on critical infrastructure while evading the attribution and response frameworks that apply to identifiable cyberattacks. The existing framework of international humanitarian law — which prohibits attacks on civilian infrastructure in armed conflict — would apply to such operations in the context of an ongoing armed conflict, but the peacetime legal framework remains considerably less clear.

The deterrence implications of quantum computing for the stability of the international order in cyberspace are profound. Current cyber deterrence operates partly through the credible threat of attribution and response, and partly through the practical difficulty of achieving decisive strategic effects through cyber operations against hardened, well-defended systems. Quantum computing would substantially alter both dimensions: attribution becomes harder when operations exploit passive decryption rather than active intrusion, and strategic effects become easier to achieve when cryptographic barriers to access are removed. Legal frameworks for cyber norms must anticipate these shifts and develop principles — including, potentially, specific prohibitions on the development or use of quantum capabilities against civilian infrastructure — that preserve the deterrent architecture upon which strategic stability in cyberspace currently partly depends.

6.2 Quantum Technologies and Emerging Arms Control Considerations

The dual-use character of quantum computing technology — its simultaneous applicability to profoundly beneficial civilian purposes (drug discovery, materials science, financial modelling, climate simulation) and to potentially destabilising military and intelligence applications — raises arms control questions that the international community has barely begun to address. There is no existing international legal instrument that regulates the development, deployment, or transfer of quantum computing technology for security purposes, and the prospect of negotiating such an instrument faces the familiar challenges of verification, definitional ambiguity (at what point does a quantum computer become 'cryptographically relevant'?), and the asymmetric strategic interests of major quantum powers.

7. CONCLUSION

The quantum computing challenge to cybersecurity law is at once technical, legal, institutional, and geopolitical in its dimensions, and demands a response that is commensurate with its complexity and urgency. This article has argued that the quantum threat is not a future problem to be addressed once the technology matures but a present legal and regulatory challenge — manifested most acutely in the harvest now, decrypt later threat — that demands immediate action from legislators, regulators, and the organisations they govern.

The normative framework advanced here — mandatory cryptographic inventories and risk assessments, sector-differentiated migration mandates grounded in the NIST PQC standards, harmonised international standardisation, procurement-driven market incentives, and public investment in transition support for resource-constrained organisations — is ambitious but not unprecedented. It draws upon the approaches developed in analogous domains: environmental disclosure regulation, critical infrastructure security mandates, and safety-critical product standards. The common thread is the recognition that where markets systematically under-provide socially essential security investments because costs are concentrated while benefits are diffuse, law must step in to rebalance the incentive structure.

The international legal dimensions of the quantum threat are less tractable in the near term but no less important. The implications of quantum computing for the jus ad bellum, international humanitarian law, and strategic stability in cyberspace require urgent attention from the international law community, and the development of quantum-specific norms and confidence-building measures deserves a place on the agenda of international cybersecurity diplomacy. The window for proactive norm development — before the deployment of CRQCs transforms these from theoretical to acute strategic challenges — is finite and may be narrower than current public discourse suggests.

REFERENCES

Bernstein, D.J. and Lange, T., 'Post-Quantum Cryptography' (2017) 549 Nature 188.

British Standards Institution, 'PAS 1093:2023 — Quantum-Safe Cryptography: Guidance for Organisations' (BSI, 2023).

Bundesamt für Sicherheit in der Informationstechnik (BSI), 'Migration to Post-Quantum Cryptography' (BSI, 2020).

Chen, L. et al., 'Report on Post-Quantum Cryptography', NISTIR 8105 (NIST, 2016).

Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA) and NIST, 'Quantum-Readiness: Migration to Post-Quantum Cryptography' (CISA, 2023).

Digital Operational Resilience Act (DORA), Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022.

European Union Agency for Cybersecurity (ENISA), 'Post-Quantum Cryptography: Current State and Quantum Mitigation' (ENISA, 2022).

Federal Information Processing Standards (FIPS) 205, 'Stateless Hash-Based Digital Signature Standard' (NIST, 2024).

Grover, L.K., 'A Fast Quantum Mechanical Algorithm for Database Search', Proceedings of the 28th Annual ACM Symposium on Theory of Computing (1996) 212.

Homeland Security Advisory Council, 'Final Report of the Quantum Computing Subcommittee' (US Department of Homeland Security, 2022).

Kaye, P., Laflamme, R. and Mosca, M., 'An Introduction to Quantum Computing' (Oxford University Press, 2007).

Mavroeidis, V. et al., 'The Impact of Quantum Computing on Present Cryptography' (2018) 9(3) International Journal of Advanced Computer Science and Applications 405.

Mosca, M., 'Cybersecurity in an Era with Quantum Computers: Will We Be Ready?' (2018) 15(2) IEEE Security & Privacy 38.

National Cyber Security Centre (NCSC), 'Post-Quantum Cryptography: PQC Migration Guidance' (NCSC, UK, 2023).

National Security Memorandum 10 (NSM-10), 'Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems' (4 May 2022).

NIST Special Publication 800-208, 'Recommendation for Stateful Hash-Based Signature Schemes' (NIST, 2020).

Perlner, R.A. and Cooper, D.A., 'Quantum Resistant Public Key Cryptography: A Survey', Proceedings of the 8th Symposium on Identity and Trust on the Internet (2009) 85.

Schmitt, M.N. (ed.), 'Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations' (2nd ed., Cambridge University Press, 2017).

Shor, P.W., 'Algorithms for Quantum Computation: Discrete Logarithms and Factoring', Proceedings of the 35th Annual Symposium on Foundations of Computer Science (1994) 124.

United States, 'National Cybersecurity Strategy' (The White House, March 2023).

United States, 'National Quantum Initiative Act', Pub. L. No. 115-368 (21 December 2018).

Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (1996, as amended).