Routledge
Taylor & Francis Group

Journal of Cyber Policy

ISSN: 2373-8871 (Print) 2373-8898 (Online) Journal homepage: www.tandfonline.com/journals/rcyb20

Q-Day and the international legal order: international law implications of quantum cybersecurity disruption

Jon Truby & Omer Baysal

To cite this article: Jon Truby & Omer Baysal (15 Jul 2026): Q-Day and the international legal order: international law implications of quantum cybersecurity disruption, Journal of Cyber Policy, DOI: 10.1080/23738871.2026.2689321

To link to this article: https://doi.org/10.1080/23738871.2026.2689321

Published online: 15 Jul 2026.

JOURNAL OF CYBER POLICY
https://doi.org/10.1080/23738871.2026.2689321

Routledge
Taylor & Francis Group

Q-Day and the international legal order: international law implications of quantum cybersecurity disruption

Jon Truby[a] and Omer Baysal[b]

[a]Centre for International Law, National University of Singapore, Singapore; [b]Technology & Digital Consulting Services, Forvis Mazars in Qatar, Doha, Qatar

ABSTRACT

Q-Day refers to the point at which a sufficiently powerful quantum computer can break widely used encryption methods, exposing diplomatic, military, financial and personal data to decryption at scale. This article asks whether existing international legal frameworks are adequate for such disruption and argues that they are insufficient. It shows that current regimes, including the Budapest Convention, the Wassenaar Arrangement, the Tallinn Manual 2.0 and international human rights law, provide only partial and indirect coverage of quantum-enabled cyber risks. The article also compares the United States, China and the European Union to show that post-quantum cryptography (PQC) is developing through fragmented national and regional strategies, creating a cybersecurity weakest-link problem in an interconnected digital environment. It argues that the emerging risk of 'PQC sovereignty' may deepen fragmentation unless states coordinate standards and legal responses. Preserving cybersecurity and legal stability in the quantum era therefore requires a coordinated international response combining rapid migration to PQC, interoperable standards, and new legal instruments or agreed norms to address quantum-specific vulnerabilities.

ARTICLE HISTORY
Received 30 May 2025
Revised 14 May 2026
Accepted 3 June 2026

KEYWORDS
Public international law; quantum computing; quantum sovereignty; post-quantum cybersecurity; technology governance

Introduction

Alan Turing's cracking of Nazi Germany's Enigma code was a paradigm-shifting breakthrough in World War II by enabling British intelligence to covertly access encrypted military communications that were considered secure. The computational efforts involved systematic analysis to solve complex mathematical puzzles used to decrypt Enigma. The exploitation of such vulnerabilities in German encryption protocols was ultimately a major factor in the Allied victory since it resulted in the decoding of enemy intelligence in real-time (National Security Agency 2021). Modern encryption methods used in commerce, banking transactions, diplomatic cables and military communications still depend upon complex mathematical problems but have progressed to be currently computationally unsolvable. A sufficiently powerful and fault-tolerant quantum computer could solve certain problems far more efficiently than classical machines because the

CONTACT Jon Truby truby@nus.edu.sg Centre for International Law (CIL), National University of Singapore, Bukit Timah Campus, 469A Bukit Timah Road, Tower Block, #09-01, Singapore 259770

two systems rely on different computational principles (National Institute of Standards and Technology 2024a; Alagic 2022). Recent benchmark demonstrations such as Google's Willow processor suggest rapid progress towards a decryption breakthrough, although such results do not themselves show that deployed encryption can already be broken in practice (Neven 2024). Emerging quantum computing technologies are expected to solve some mathematical problems that underpin widely used public-key encryption once they are sufficiently scalable. Q-Day refers to the point at which this capability becomes operationally significant, an event where Shor's algorithm is deployed to crack all cryptographically dependent passwords. The principal risk is therefore not that all digital security disappears overnight, but that currently deployed schemes become unreliable for protecting sensitive data unless they are replaced by post-quantum alternatives (Baseri, Chouhan, and Hafid 2024).

Recent transformative technological breakthroughs in quantum computing therefore have serious implications for global cybersecurity and, in turn, international law (White House 2024). Indeed, the US Government Accountability Office (GAO) recognizes weaknesses in US federal planning in regard to quantum computing and its threats to critical infrastructure (GAO 2024). A coordinated quantum attack on multiple parts of an electricity grid could cause prolonged regional or national power outages with cascading effects of blackouts on banking, transportation, healthcare and beyond (World Economic Forum 2025). A study by the University of Cambridge and Lloyd's of London modelled a cyber-induced U.S. blackout affecting the American Northeast and estimated economic losses between $243 billion to $1 trillion depending on the severity of the scenario (Lloyd's 2015). A high rate of cyber incidents already target the energy sector, showing that adversaries are actively probing and attacking energy systems (Energy Expert Cyber Security Platform 2017). Quantum computing would give these threat actors a far more potent weapon.

Cryptographic encryption schemes are currently used to safeguard digital communications, financial transactions, personal bank logins and medical records, as well as military communications and state secrets (Heathman 2017). Personal private communications through WhatsApp are secured via encryption, and exposure of such communications would be catastrophic for private citizens' confidential information as well as diplomatic channels which could result in major national security risks (WhatsApp n.d.). Quantum computing may also threaten data integrity if existing digital signature schemes become vulnerable. This could lead to forged records, malicious code, or unauthorised commands becoming harder to detect, thereby undermining trust in digital evidentiary chains and critical systems unless signature systems are migrated to post-quantum alternatives. Q-Day could have severe consequences for military and economic security and could erode trust between states (Kirton 2022). The United Nations (UN, 2024) Secretary-General has warned that quantum's decryption capabilities could 'break down entire systems' by breaching current cybersecurity protections (UN Secretary-General 2024). The GAO further recognises a 'harvest now, decrypt later' strategy by cybercrime groups and intelligence agencies collecting and storing data in the hope of being able to decrypt it once they have access to quantum computing (GAO 2024). There is thus a need to transition global systems to quantum-safe encryption known as Post-Quantum Cryptography (PQC) (Moody's Investors Service 2023). Indeed, states vying for PQC technology see it as a competitive advantage in being able to use

quantum computing not only in cyber defences but also to employ it to intercept other states' data.

From a technical perspective, the rise of quantum computing threatens to dismantle the Rivest–Shamir–Adleman (RSA) and Elliptic-Curve Cryptography (ECC) (Schneier 2015; Vermeer and Peet 2020) encryption standards that secure global digital communications (Brooks 2025; Preskill 2018).[1] In response, PQC, featuring National Institute of Standards and Technology (NIST)-standardized algorithms like Kyber and Dilithium, is being developed to withstand quantum attacks (NIST 2022, 2024a). However, migrating global infrastructure to PQC is a massive undertaking fraught with high costs and technical strain, where failure to update legacy systems poses a critical security risk.

This article asks whether existing public and private international legal frameworks are adequate to address the cybersecurity disruption associated with Q-Day. It argues that they are insufficient. Existing instruments address aspects of cybercrime, export controls, sovereignty, privacy and regulatory compliance, but they do so indirectly and without a coordinated framework for migration to PQC. The article's original contribution is to connect these legal gaps to governance risks including the emergence of 'PQC sovereignty' and a transnational 'weakest-link' problem created by fragmented national transitions. On that basis it advances a *lex ferenda* (a law that ought to be as opposed to a law that is) case for coordinated international standards, migration timelines and legal instruments before large-scale quantum decryption becomes operational.

The article starts by explaining the case selection and compares the post-quantum strategies of the United States, China and the European Union. It finds that, despite their ambitions, the initiatives from these jurisdictions remain siloed within national or regional boundaries and lack global coordination. The article then assesses the adequacy of existing public international law and private international law, concluding that while the former field appears adequately prepared for advances in quantum cybersecurity, the latter is proactively shifting to address quantum risks. However, a risk of inconsistency and security gaps persists without overarching coordination between private and public laws. Finally, the article identifies the principal legal gaps and proposes a coordinated international response centred on interoperable post-quantum standards and legal cooperation.

Comparative analysis of national approaches

This comparative section focuses on the United States, China and the European Union, each representing an influential model of post-quantum governance. The US is driving technical standardisation and federal migration policy; China is pursuing a state-led and security-centred strategy; and the European Union offers a supranational regulatory model centred on coordination and market governance. These three cases are especially likely to shape global standards, interoperability and the risk of legal fragmentation.

United States: standardisation, migration and strategic preparedness

Viewing quantum computing as both a national security risk and a technological opportunity, the US has begun preparing for the PQC transition by seeking to develop 'quantum-resistant algorithms'. This idea primarily seeks to develop standards by which

businesses and the public sector can transition their existing digital infrastructure to encryption to resist quantum computing threats. Standardised algorithms are intended to be beneficial in compliance with legal and regulatory obligations and reduce risks and costs involved in implementing new cryptographic measures. Once the standards have been developed the strategy involves migration of federal systems to those new standards, and then preparation against the threats to the private sector and critical infrastructure. Policies, legislation and research initiatives have been initiated to deliver this strategy. At the Federal level, President Biden in 2022 issued a National Security Memorandum, *Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems* (White House 2022), which ordered federal agencies to rapidly inventory and upgrade any vulnerable cryptographic systems to PQC solutions. The Memorandum further aims to continue leadership in quantum information science, demonstrating an intended balance between offensive and defensive interests. The essence of this Memorandum was enshrined in law pursuant to the 2022 *Quantum Computing Cybersecurity Preparedness Act*.

In 2024, NIST released several technical PQC standards designed to withstand cyberattacks from a quantum computer (NIST 2024b). NIST has urged the immediate adoption of these technical norms across industry and government to facilitate quantum-resistant encryption. The Biden Administration's 2023 *National Cybersecurity Strategy* (White House 2023a) also emphasised the accelerated replacement of hardware, software and services that may be vulnerable to quantum attacks. The Strategy encouraged industry to achieve 'cryptographic agility', meaning the ability to quickly replace non-quantum-resistant algorithms with better versions. The *US National Cybersecurity Implementation Plan* further outlined specific objectives to 'Prepare for Our Post-Quantum Future', assigning clear roles and responsibilities to relevant entities accompanied with timelines (White House 2023b). The US National Security Agency (NSA) has itself published guidance for National Security Systems which identifies algorithms to use in the interim until PQC standardisation is complete (National Security Agency 2022). The Cybersecurity and Infrastructure Security Agency (CISA 2024) launched a PQC Initiative to help businesses prepare for migration. Big Tech companies like Google and Amazon are also experimenting with PQC pilot projects and PQC protocols (2024).

The GAO highlighted potential gaps in the plan and consequently recommended the Office of the National Cyber Director take charge of coordination in order to have one single coordinator (GAO 2025). Although challenges remain due to the enormous scale of the upgrades involved, the US, through technical standards, policy, legislation and engagement with industry, is positioning itself to benefit from and protect itself from quantum computing.

China: state-led quantum strategy and standard-setting

China has invested heavily in quantum research and development and regards it as a 'strategic priority' in its pursuit of technological superiority (Kania 2021, 922). China wishes to secure its own data against quantum risks while benefiting from quantum capabilities to upgrade its own cyber and intelligence-gathering capabilities (Radanliev 2024, 28; Hershkovitz 2022). While the US emphasises public standards and private-sector implementation, China's strategy is more centralised and entangled with national security

directives. It is estimated that Beijing has invested several times more funds into quantum technology than any other government (Kim and Monroe 2024) and has demonstrated some of the most advanced quantum computing prototypes (Gao et al. 2025, 09060–2). These investments have produced the world's largest quantum research programs such as *Micius*, the Chinese Quantum Science Satellite, along with the development of national quantum laboratories. China has notably developed its own type of protection against threats from quantum computing through Quantum Key Distribution (QKD) as part of its cybersecurity strategy aiming to protect its military and government communications. China's State Cryptography Administration is also developing Chinese PQC standards to be used in conventional networks in order to have quantum-resistant 'next-generation commercial cryptographic algorithms' (GSMA 2025). The International Standards Organization (ISO) agreed to review a Chinese proposal on quantum-resistant network security protocol related to wireless networks, seen as a victory in the technical standards race (Peng 2024). This suggests that China is not content to simply adopt NIST's PQC algorithms but wishes to advocate for its own standards in international bodies as alternatives to Western cryptographic norms (Sparkes 2025).

Chinese researchers are exploring offensive applications of quantum computing, including how it can already be applied to break or weaken existing encryption. In 2024 Chinese researchers claimed the world's first successful quantum attack on a common encryption algorithm (Chen 2023) as proof-of-concept to demonstrate the risk to even military-grade encryption. As this could be used in cyber offense, it raised concern amongst US intelligence for Chinese espionage operations. China's *2020 Encryption Law* focuses on control and self-reliance in cryptography and classifies encryption into core, common and commercial categories, imposing strict requirements that critical data and state secrets are protected by government-approved encryption algorithms (National People's Congress of China 2020). This law, along with the introduction of export controls, results in a tightly regulated environment where foreign cryptographic products face import restrictions or must undergo security review (Zou et al. 2020). Although China is not a party to the Wassenaar Arrangement, the main multilateral export control regime, it has unilaterally implemented similar controls to prevent adversaries from acquiring its advances in quantum communications. This indicates a desire to prevent adversaries from acquiring Chinese advances in quantum communications (Xu et al. 2020). China's national approach is thus characterised by state-driven innovation, aggressive standard-setting, and securitisation of quantum technology. Through substantial investments in research, developing laws and standards, and integrating quantum into its national strategies such as 'Made in China 2025' and the 14th Five-Year Plan (Creemers et al. 2022), China seeks to benefit from quantum computing as a shield and sword.

European Union: regulatory coordination and quantum resilience

Consistent with its broader approach to digital security, such as the *Digital Operational Resilience Act* to strengthen the financial sector's cybersecurity (European Parliament and Council 2022b), the EU's PQC response has been a coordinated one, including regulations and support for research (European Commission 2023). Mindful that an encryption breakdown risks Europe's digital economy and privacy regime, the EU is coordinating a harmonised transition to quantum-resistant security (European Union Agency for

Cybersecurity 2021). The EU is proactively utilising its policy and regulatory powers to prepare for a quantum future, although it is behind the US in pushing PQC standards and lags behind China in quantum hardware investment.

In 2024, the European Commission issued a landmark *Recommendation on Post-Quantum Cryptography*, urging all EU member states to adopt a unified proactive strategy for transitioning to PQC (European Commission 2024). The Recommendation frames quantum-safe encryption as vital for the security of citizens, the economy and the integrity of the Digital Single Market. The Commission's guidance includes developing an EU-wide PQC transition roadmap by 2026, identifying priority sectors and systems that need early upgrades, and ensuring interoperability of solutions across borders (GSMA 2025). This high-level policy push is backed by the EU Agency for Cybersecurity (ENISA), which recommends steps like incorporating *crypto-agility* into systems design (ENISA 2021). The EU-US Trade and Technology Council and Transatlantic Cyber Dialogues have also included discussions on quantum security, reflecting an EU interest in aligning with allies on standards and timelines (Rodriguez 2025).

While EU PQC-specific legislation is not anticipated in the current Parliament (Keane 2024), it is incorporating quantum resilience into its evolving digital regulatory framework (Balarabe 2025, 749). For instance, the second Network and Information Security Directive (Directive (EU) 2022/2555) requires providers to adopt 'state of the art' cybersecurity measures (European Parliament and Council 2022a). This could be interpreted in the future to include quantum-resistant encryption once standards mature. The EU *2019 Cybersecurity Act* (European Parliament and Council 2019) similarly establishes a framework for EU-wide certification of ICT products. Future updates to certification schemes are likely to include cryptographic requirements that are quantum-safe, designed to ensure that products on the European market gradually become PQC-compliant. The *2016 General Data Protection Regulation* (GDPR) also mandates appropriate security for personal data (European Union 2016). The European Data Protection Board's (EDPB) guidance on international data transfers noted that the strength of encryption and key lengths must take into account the emergence of 'new computing paradigms like quantum computing', suggesting that 'appropriate' encryption means considering the shelf-life of the data's confidentiality in light of quantum threats (EDPB 2021). This forward-looking stance effectively pre-empts regulatory pressure on companies to implement PQC for long-term data privacy compliance, even in the absence of a dedicated PQC law.

Europe is also contributing to technical solutions on the standardisation front. The German federal cybersecurity agency (Bundesamt für Sicherheit in der Informationstechnik 2021) and France's security agency have each issued recommendations for interim quantum-safe measures and are participating in international cryptographic standardisation efforts (ANSSI 2023). The EU has funded significant research through its Quantum Flagship programme, including a €1 billion investment in quantum technologies (European Commission 2023), alongside Horizon Europe projects focusing on PQC and QKD pilots. EU bodies have also discussed the possibility of identifying European-prioritised PQC algorithms to reduce the risk of dependency on foreign algorithms (European Commission 2024).

The EU's method is one of cooperative engagement and preventive regulation seeking to legislate baseline requirements. The EU's use of soft law such as Commission

recommendations also drives member states to act in concert. The EU's work is relatively transparent and collaborative, such as by sharing studies via ENISA and cooperating with international partners on standards (European Commission 2018). The EU and the North Atlantic Treaty Organization (NATO) have both notably encouraged post-quantum readiness among their members as part of strengthening collective cyber defences (NATO 2024), recognising the need to secure military communications against quantum decryption. The EU as a civilian power complements this by focusing on civilian infrastructure and legal frameworks.

Summary

Each major actor has taken significant domestic steps toward post-quantum cybersecurity. The US has issued National Security Memorandum-10 to jumpstart the federal transition to PQC, China is rapidly building out a national QKD infrastructure and promoting its own quantum cryptography standards, and the EU has adopted a coordinated regulatory roadmap to harmonise its members' shift to quantum-resistant security. Yet, for all their ambition, these initiatives remain siloed within national or regional boundaries and lack global coordination. The transnational nature of digital threats, cryptographic dependencies and critical infrastructure vulnerabilities in an interconnected digital ecosystem means that even the most sophisticated national strategies are inadequate on their own. A single jurisdiction's failure to upgrade an outdated encryption system can serve as the weakest link undermining others' security. The next section therefore turns to public international law and asks whether existing legal frameworks can support the coordination needed to prevent fragmentation from becoming a systemic vulnerability.

Public international law

Quantum computing poses novel challenges to existing international legal frameworks. The difficulty is not that international law is wholly silent. Indeed, current rules were developed for technologically neutral cyber activity and therefore address quantum-related harms only indirectly. Primary international law does not clearly regulate quantum-enabled mass decryption below the thresholds of coercion, use of force or armed attack. International law provides no coordinated framework for migration to PQC across interdependent systems. Finally, it lacks clear mechanisms for interoperability, mutual assistance and accountability when weakest-link failures create transnational harm. The following subsections assess how existing instruments address these issues and where *lex ferenda* development may be needed.

The Budapest convention

The Council of Europe's (Budapest) *2001 Convention on Cybercrime* is the most significant international treaty addressing cyber offences. It facilitates cross-border cooperation on crimes such as illegal access, data interference and digital fraud (Council of Europe 2001a). While the Convention does not explicitly mention encryption or quantum computing, some of its provisions could be indirectly relevant. For instance, Article 6 requires

parties to criminalise the misuse of certain hacking tools. In the future this could arguably cover possession of illicit decryption capabilities, including using a quantum computer to unlawfully decrypt data. The Convention's mechanisms for law enforcement cooperation through mutual legal assistance and data-sharing will be challenged should quantum-driven cyberattacks escalate (Althobaiti and Dohler 2020). The Budapest Convention mostly assumes that strong encryption is a protective measure for responsible state actors, rather than a protection to be routinely broken by attackers (Council of Europe 2001b, 11). It does not address the scenario of a bad actor decrypting vast troves of data, as such decryption was not immediately foreseeable nor feasible when drafted. The Convention's focus on crime and policing may need supplementing as quantum threats emerge. For example, there could be agreements on sharing quantum forensics tools, or on emergency assistance if a quantum-empowered attack occurs (Radanliev 2024, 28). A new UN (Hanoi) *Convention against Cybercrime* has been adopted (UN 2024) but concentrates more on 'traditional' cybercrime without specific mention to quantum computing cybercrime. Overall, the Budapest Convention may therefore remain useful for post-incident cooperation, but it cannot itself organise the coordinated preventive migration to PQC that quantum risk requires.

The Tallinn manual 2.0

The principles of state sovereignty in public international law and the prohibition on unlawful intervention apply to cyberspace. If a state or its proxies were to use quantum computing to conduct massive cyber-espionage or sabotage against another state's critical infrastructure, the question is whether that could be considered a violation of international law (Simmons 2014, 42; Garon 2018, 1; Nguyen 2018, 61). The influential but non-binding Tallinn Manual 2.0 suggests that cyber operations resulting in significant consequences can violate the target state's sovereignty (Schmitt 2017b, 171–175), or even constitute an attack under the law of armed conflict if the result is physical damage or injury (Schmitt 2017a, 126, 156). Should the impact be non-violent but purely data-centric, such as decrypting confidential communications or databases, this would be akin to cyber espionage and Tallinn 2.0 would generally not consider this per se prohibited by international law. This implies that a state using a quantum computer to intercept and decode another state's secret communications might not specifically breach international law, as long as there are no violations of specific commitments (such as treaties on non-interference) or cause effects crossing certain thresholds (Schmitt 2017b, 168–176). This gap is problematic since quantum capabilities could vastly amplify espionage and information theft (Schmitt 2017b, 168) and the international community lacks a consensus on where to draw legal red lines. Some experts argue that if sufficiently invasive, such activity might violate the principle of non-intervention (Buchan 2012, 211). However, that doctrine traditionally requires coercive effect which may be difficult to demonstrate for passive decryption of intelligence.

As a matter of *lex lata* (existing law), the stronger view is that passive quantum-enabled decryption, without coercion, physical effects or breach of a specific treaty obligation, is unlikely at present to qualify as unlawful intervention under existing international law. This article is of a contrary view that existing technology-neutral norms on sovereignty, due diligence, human rights and state responsibility are already capable of addressing

quantum-enabled cyber operations, and that the main problem is political will, attribution and implementation rather than normative deficiency. That position has real force, especially where quantum tools produce effects already captured by existing rules. The difficulty is that many of the most disruptive quantum harms, especially mass decryption, strategic intelligence exploitation and interoperability failures, remain below established legal thresholds or fall between public and private regulatory frameworks (Truby 2026).

If quantum hacking directly enables military operations in armed conflict scenarios like decrypting an enemy's battlefield communications in real-time, then it merely becomes part of cyberwarfare (Nguyen 2013, 1098). This would be governed by existing law of war principles (distinction, proportionality, necessity) as applicable. Though the Tallinn Manual did not specifically contemplate quantum computers, its rules would treat the method of attack as generally irrelevant to legality where what matters are the consequences. Thus using a quantum tool to disable another country's power grid by breaching encrypted controls would likely be seen as a use of force or armed attack, similar to a conventional cyberattack of similar effect (Jensen 2002, 228). In summary, though the Tallinn Manual's influence is limited to academic and policy circles, it does help shape interpretations that could become state practice over time (Duru 2023, 94). States face few legal constraints in developing or amassing quantum attack tools, aside from broad norms of due diligence to prevent internationally wrongful acts from their territory (O'Connell 2012, 190–191).

The Wassenaar arrangement and quantum export controls

One area where an international framework is more directly engaged with quantum cybersecurity is in export controls of dual-use technologies. The *Wassenaar Arrangement* (1996) is a multilateral regime in which 42 participating states (including the US and most EU members, but not China) agree to control exports of certain sensitive technologies. Wassenaar's control lists have more recently included some cryptography items and been updated to cover quantum-related tech. Wassenaar controls now cover 'quantum cryptography' devices (meaning QKD systems) (Groenewegen-Lau and Hmaidi 2024) and proposals have been made and implemented through national rules to control high-performance quantum computing hardware and components (Sparkes 2024). Practically, this means countries like the US, UK and EU states will restrict the sale of advanced quantum computers or quantum-encryption devices to certain countries. The US has added multiple Chinese quantum technology companies to its backlisted 'Entity List' on national security grounds, designed to prevent China's military from gaining advanced quantum capabilities (China's Bureau of Industry and Security 2025). China has meanwhile enacted its own export controls on quantum communication technologies. As China is not part of Wassenaar it is not bound by the same multilateral rules. The Wassenaar Arrangement thus reflects an emerging consensus among Western-aligned states that some quantum technologies should be treated like munitions. This is a notable development in international technology governance.

Export controls remain a blunt tool as they may slow proliferation but cannot prevent determined states or non-state actors from developing quantum capabilities alone. Indeed the 2025 DeepSeek disruption demonstrated how export controls can backfire. US export controls on semiconductors designed to limit China's technological growth

in the field of AI drove Chinese technology developers to develop innovative workarounds which helped China not only develop its own competitor to major US generative AI but also helped China reduce dependence on foreign technologies (Zhang 2024, 100098). Export controls only attempt to manage the spread of quantum capabilities and do little to protect against the actual use of such technologies. Competing strategic interests also limit Wassenaar's universal applicability. While regimes like Wassenaar and national export laws have begun to address quantum technologies, they focus narrowly on trade and do not comprehensively tackle the security externalities of quantum computing such as an arms race or stability risks. Export controls may slow proliferation, but they are not a substitute for coordinated international rules on adoption, interoperability and responsibility.

International human rights and data privacy treaties

Another angle is the potential impact of quantum decryption on human rights obligations especially the right to privacy. If cybercriminals or state agencies managed to decrypt personal data at scale, this threatens the privacy of communications currently protected under instruments like the *International Covenant on Civil and Political Rights* (UN 1966). Human rights law requires surveillance or interception to be lawful, necessary and proportionate. While quantum technology does not change those principles, it could render existing encryption-based privacy protections ineffective, putting pressure on states to update laws. One could imagine future arguments that states have a positive obligation to their citizens to maintain adequate cybersecurity including against quantum threats, akin to ensuring safety against foreseeable risks (Gross 2015, 481). Data privacy regimes such as the Council of Europe's Convention 108 or the EU's GDPR are indirectly pushing in this direction by recognising quantum in guidance. The slow development of international human rights law has meant that there has not yet been any explicit norm about 'quantum resilience' as a right. However, as encryption has been deemed crucial for privacy and freedom of expression in the digital age, a quantum-induced erosion of encryption might prompt an international law discussion towards norms against unlawful mass decryption (Van Daalen 2023). Human rights law strengthens the case for quantum-resilient security, but it does not yet supply a concrete international framework for coordinated cryptographic transition.

Soft law norms and confidence building measures

Over the last decade, states have made some progress in articulating voluntary norms of responsible state behaviour in cyberspace. The 2015 report of the UN Group of Governmental Experts (GGE) (UN Secretary-General 2015) set out 11 norms endorsed by the UN General Assembly. These call on states not to attack each other's critical infrastructure in peacetime and to assist other states when asked to mitigate cyber incidents (UN Secretary-General 2015, Articles 11 and 13). Some of these norms may be relevant despite omitting specific mention of encryption or quantum computing. One norm, for instance, urges states to not allow their territory to be used for intentionally wrongful acts using ICTs (UN Secretary-General 2015, Articles 13c). A state orchestrating quantum decryption attacks on another state's critical systems would violate the spirit of this norm (Schmitt

2017a, 87). Another norm encourages exchange of information and best practices (UN Secretary-General 2015). One can envision the extension of this norm to include sharing threat information about quantum vulnerabilities or cooperating on standards. However, these norms are non-binding and have no enforcement mechanism. Ongoing talks in the UN Open-Ended Working Group on ICT (2021–2025) (United Nations Office for Disarmament Affairs, n.d.) similarly have not focused on quantum issues, instead focusing more on general cyber capacity-building and existing norms implementation.

With the international law landscape appearing to be inadequately prepared for advances in quantum cybersecurity, the impact of quantum computing as a potential 'strategic shock' could be akin to the advent of nuclear weapons, thus requiring global cooperation before quantum cyberattacks escalate (Bergeron 2026). There is currently no international treaty or agreement specifically addressing the weaponization of quantum computing or the need for collective action to secure cryptography. Existing instruments like the Budapest Convention cover certain cybercrimes but not state activity. Export control regimes cover hardware but not behaviour and norms cover general responsibilities but not quantum-specific threats. This gap is starting to be noticed. NATO and the G7 have at least 'encouraged' the adoption of PQC as a matter of good practice. The world's ability to maintain cybersecurity and stability in the quantum era will likely depend on developing new norms or even treaties. These soft-law processes could support future quantum governance, but in their present form they are too general to solve the weakest-link problem or to establish binding duties to adopt interoperable post-quantum protections.

Private international law

Private international law does not remove the need for public international coordination. Transnational regulation, contractual compliance and data protection rules are instead likely to drive uneven and market-shaped forms of post-quantum migration, which may accelerate adoption in some sectors while deepening fragmentation in others. This section therefore examines how private law mechanisms may both reduce and reproduce quantum cybersecurity risk across borders.

Corporate cybersecurity standards and liability

Companies operating internationally are increasingly expected by regulators, customers and shareholders to maintain 'state of the art' cybersecurity (Luo 2022, 361), including quantum-resistant encryption where appropriate. The EU's GDPR serves as an example by requiring organisations to implement security measures appropriate to risk (Article 32) or face substantial fines. Meta, for instance, received a record-breaking fine of €1.2 billion from Ireland's Data Protection Commission in May 2023 for data transfer infringements under the GDPR (Irish Data Protection Commission 2023). Should experts warn that certain sensitive personal data like health or financial records will remain confidential for years, then failing to protect that long-term confidentiality against known threats (such as future quantum decryption) could be seen as a compliance lapse (Bruno and Spano 2021, 72). The EDPB has already cautioned data exporters to account for quantum computing in their choice of encryption, warning that current public-key algorithms' protective power will 'decline over time due to … the emergence of new computing paradigms like

quantum computing' (EDPB 2021). It notes that authorities might 'store [encrypted data] until their resources are sufficient for decryption' (meaning harvest-now-decrypt-later) and that supplementary measures should be implemented so that even future decryption would not violate privacy. This guidance effectively puts multinationals on notice to legally safeguard personal data in international transfers plan for PQC. Failure to do so could risk GDPR violations or liability if a breach occurs via a future quantum-enabled attack.

Beyond data protection there are corporate governance and tort law risks to be considered. Board directors have fiduciary duties to manage material risks and cybersecurity is now a board-level risk (Gale, Bongiovanni, and Slapnicar 2022, 102840; Ernst and Young 2024). As awareness of the quantum threat grows, one could foresee shareholders or customers taking legal action if a company negligently ignores the need to transition its security, thus resulting in a breach (Dynkin and Dynkin 2018, 23). A financial institution that continues to use RSA encryption for a long-term sensitive dataset and whose data is decrypted by adversarial quantum computing may face lawsuits for failing to adapt to well-publicised standards. The doctrine of negligence per se could even apply if regulators have by then mandated PQC (Trautman and Ormerod 2017, 1231). Cyber insurers might also start inquiring whether insured entities have migration plans to limit future quantum-related breach claims, much as they ask about ransomware defences today.

The International Organization for Standardization (ISO) and the International Telecommunications Union (ITU) are working on standards for PQC and QKD interoperability, which are likely to become reference points in commercial contracts and procurement. The concept of 'security by design' reinforces this trajectory by encouraging organisations to specify quantum-resistant encryption requirements at the earliest stages of system design, procurement and contracting. Global firms may need to support multiple cryptographic regimes across markets, increasing cost and compliance complexity if international standards diverge. Contracts for cloud services, outsourcing and data processing are therefore likely to include stronger clauses on cryptographic agility and future PQC upgrades (Campagna, Goldsborough, and O'Donnell 2024; Canadian Centre for Cyber Security 2024). Similar to how contracts began mandating compliance with GDPR or with cybersecurity frameworks like ISO 27001, one can now expect to see emerging language about 'quantum-resistant encryption' in long-term outsourcing agreements to ensure future-proofing (Ward 2024). ISO/IEC 4879:2024 now provides vocabulary for quantum computing and standards are expected shortly. A failure to implement PQC in cross-border contracts could even lead to breaches of implied warranties of security or service level agreements (Elvy 2023, 1177).

Data privacy and cross-border data transfers

Immediate private law implications relevant here are the data privacy regulations and the legality of international data transfers given the potential quantum cybersecurity impact. The Schrems II ruling (Court of Justice of the European Union 2020) invalidated the EU-US Privacy Shield in part because of the risk of US surveillance on EU personal data. Encryption was one mitigating factor considered to protect data in transit in the case. It should cover the entire data lifecycle including data at rest, data in transit and data in use. European regulators (EDPB) in their post-Schrems II guidance imply that if data needs to stay

confidential for a sustained period then exporters must consider whether encryption will hold up that long or whether additional measures are needed. Transfers of highly sensitive data to jurisdictions with active quantum computing programs may be deemed non-compliant unless protected by quantum-safe encryption. For example, an EU company sending health data to a processor in a country might be required to encrypt the data with a PQC algorithm (or use QKD-based links if feasible) to satisfy GDPR standards, especially if the country's intelligence agencies are suspected of data collection (Bolatbekkyzy 2024, 286). This would encourage PQC adoption across borders in order to comply with regulations, essentially using privacy law to compensate for the lack of an international security guarantee. Some scholarship suggests going as far as amending the GDPR itself to 'embed post-quantum encryption requirements dynamically' (Bruno and Spano 2021, 72). If the EU were to legislate mandated PQC for certain categories of data or after a certain date, given the GDPR's influence, a 'Brussels effect' may result in global companies and other jurisdictions following suit.

Critical industries, cross-border regulation and conflict of laws

Industry-specific transnational regulatory structures will also be impacted by quantum risks. As illustrated by the Basel/IOSCO cybersecurity guidelines, the banking sector is expected to manage emerging risks to financial stability (Committee on Payments and Market Infrastructures and IOSCO 2016; Basel Committee on Banking Supervision 2018). Banks operate across borders and rely on secure communication such as the SWIFT network for interbank transfers. If one country's banking regulator starts requiring quantum risk assessments and PQC transition plans, multinational banks will have to implement them globally for consistency. Some financial authorities are already moving in this direction. Israel's central bank in 2022 instructed banks to assess quantum vulnerabilities (Bank of Israel 2025) and Switzerland's FINMA (2022) has discussed quantum-readiness as part of operational risk. Companies often comply with evolving laws by meeting the most stringent requirements everywhere they operate, leading to de facto global standards. The SWIFT assessment framework will likely need updating following quantum technology's impact on the SWIFT system (SWIFT 2024).

Differing national timelines for quantum readiness could additionally create a conflict-of-laws issue or trade barriers, similar to a risk of fragmentation should standards between states diverge. A multinational enterprise intending to comply with multiple national standards will need to implement both types of algorithms in its products. Although this can be achieved, it may be an expensive option and may cause security complexities (World Economic Forum 2024). There could also be patent or intellectual property issues. Should a country's PQC algorithm be proprietary then global usage may raise licensing questions. Private law may need to resolve liabilities such as if PQC algorithm is discovered to be flawed. These questions may lead to new contractual clauses and industry agreements to allocate risk (Balarabe 2025, 794).

Supply chain and product liability

Quantum-proofing is a supply chain concern since companies procuring software or devices internationally will place requirements on vendors to provide quantum-safe

security, particularly for products with long lifespans. Should a vendor fail to upgrade and there is a resulting breach then there will likely be issues of product liability or potential warranty claims. Vendors will have to address third-party risks and, since ultimate responsibility stays with the data owner, this will require advanced monitoring to ensure quantum-resistant mechanisms are effective. Regulators may consequently intervene through certification requirements and global manufacturers will have to meet the highest common denominator of crypto requirements to access global markets. Indeed, the US has signalled through the NIST and NSA activities discussed above that devices should implement PQC by the 2030s for government use, and the EU through its certification schemes may introduce similar procurement requirements. Manufacturers will inevitably write these obligations into their contracts with component suppliers which will result in a contractual chain enforcing PQC compliance.

In summary, the private international law landscape is proactively shifting to address quantum risks arguably even faster than public international law. Data protection authorities very much have this on their radars, including in the UK, Germany, Canada and Australia. Industry regulators and standards bodies are also integrating quantum-resilience into their rules and recommendations which in turn drives corporate behaviour. Multinational companies face a significant compliance challenge but there is an opportunity for leaders adopting PQC to assure clients and regulators of quantum-safe security in order to gain a competitive edge. Those who lag may face legal liability, regulatory penalties or exclusion from lucrative markets. One legal implication for critical infrastructure operators and multinationals is the concept of 'reasonable security' as a moving target which means failing to move toward PQC could be deemed unreasonable in hindsight. This puts a premium on monitoring legal developments across jurisdictions. Although the private sector and private law mechanisms may push the world toward quantum-readiness despite slowly formalising public law consensus, without overarching coordination there is a risk of inconsistency and security gaps.

Towards a coordinated international response

The first priority is coordinated migration to PQC. States, regulators and standards bodies should align common timelines, interoperability requirements and risk-based sequencing for critical infrastructure, public administration and long-lived sensitive data. In practice, this means inventories of vulnerable cryptographic systems, phased migration plans, cryptographic agility and hybrid deployment during transition. Legal frameworks in procurement, certification, data protection and sector-specific cybersecurity regulation should be used to support this transition rather than waiting for Q-Day to force reactive compliance. A practical engineering strategy to mitigate quantum decryption risk begins with crypto-agility and hybrid implementation. Organizations should first inventory all cryptographic systems to identify which applications use algorithms vulnerable to quantum attack. They can then deploy a hybrid cryptography approach (Ricci et al. 2024, 23206). Quantum-resistant mechanisms must be implemented across all layers, not just in software but also in hardware, firmware, applications and operating systems. Deployment of PQC thus mandates a re-evaluation of infrastructure capacity (Pote and Bansode 2025, 549; Jung and Oh 2024, 3360). A phased rollout is advisable through prioritising high-value and long-lived data (such as confidential records or critical

infrastructure communications) for early migration to PQC and establishing secure update mechanisms for Internet of Things (IoT) or embedded devices that require firmware updates. By planning for these technical steps, organizations can methodically achieve a quantum-safe encryption posture before Q-Day arrives (Bishwas and Sen 2024).

The second priority is legal coordination. Existing law can address some quantum-enabled harms, but it does not yet provide clear rules on large-scale decryption, duties of notification or cooperation obligations in response to quantum-related incidents. New legal instruments, interpretive guidance or coordinated soft-law norms should therefore clarify state responsibilities, mutual assistance expectations and baseline commitments to protect critical systems and sensitive cross-border data against foreseeable quantum risks. A further challenge is the likely emergence of PQC sovereignty. As states seek trusted control over algorithms, certification and cryptographic supply chains, post-quantum governance may fragment into competing blocs. That development may be strategically understandable, but it risks undermining interoperability and deepening weakest-link vulnerabilities. International coordination is therefore needed not only to improve security but also to prevent geopolitical competition over cryptographic autonomy from destabilising the wider digital order.

Conclusion

This article has argued that existing public and private law frameworks remain relevant but insufficient. They address aspects of cybercrime, export control, sovereignty, privacy and compliance, but they do not yet provide a coherent framework for quantum-enabled mass decryption, coordinated migration to PQC or responsibility for weakest-link failures. The central implication is that legal and technical transition must proceed together. States, regulators, standards bodies and private actors should coordinate interoperable post-quantum standards, shared migration timelines and legal instruments or agreed norms before Q-Day. Without such coordination, the emergence of PQC sovereignty may deepen fragmentation and undermine collective security. With it, the transition to quantum-safe systems can strengthen rather than destabilise the international legal order. Quantum computing does not simply pose a new technical challenge. Rather it exposes a structural weakness in the international legal order, which relies on interdependent cryptographic systems that are currently vulnerable to a strategic shock, comparable in strategic and technological significance to the deployment of nuclear weapons. While preparedness is developing through fragmented national and sectoral responses, we argue that existing public and private law frameworks remain relevant but ultimately insufficient.

A primary deficiency in *lex lata* (existing law) is that international law does not clearly regulate quantum-enabled mass decryption below the thresholds of coercion, use of force or armed attack. While the Tallinn Manual 2.0 suggests that cyber operations resulting in physical damage violate sovereignty, it generally does not consider passive decryption of confidential communications such as 'harvest now, decrypt later' operations to be prohibited per se. This implies that a state using a quantum computer to decode another state's secret communications might not breach international law under current interpretations, provided no specific treaty obligations are violated. Consequently, the case for treating large-scale quantum decryption as internationally wrongful is largely

lex ferenda, depending on future state practice and the recognition of systemic harms caused by strategically consequential decryption at scale. The reliance on the Wassenaar Arrangement as a primary tool for quantum governance highlights further legal limitations. As a multilateral export control regime, Wassenaar focuses narrowly on the trade of hardware and dual-use technologies, but it cannot prevent determined states from developing indigenous quantum capabilities. Furthermore, major actors like China are not parties to the arrangement, leading to a landscape of unilateral, retaliatory controls that may fuel international tensions and drive technological workarounds. This fragmentation risks the emergence of 'PQC sovereignty', where states seek trusted control over their own algorithms and supply chains, potentially undermining global interoperability and deepening weakest-link vulnerabilities in the interconnected digital ecosystem.

Preserving cybersecurity and legal stability in the quantum era requires a coordinated international response that moves beyond technologically neutral norms. Public international law lacks clear mechanisms for mutual assistance, interoperability and accountability when weakest-link failures create transnational harm. There is a compelling argument that states may eventually be seen as having a positive obligation to maintain adequate quantum resilience to protect the fundamental right to privacy and the integrity of critical infrastructure. Legal and technical transformation must occur in tandem. States and international bodies should prioritize the development of new legal instruments or agreed norms that clarify state responsibilities regarding mass decryption and establish shared timelines for migration to PQC. Without such coordination, the transition to the quantum era will likely destabilize the international legal order. A proactive multilateral framework can positively strengthen collective security against a borderless quantum threat.

Note

1. For current computers, it is easy to multiply two very large prime numbers and reach the result. However, vice-versa (factoring out very large prime integers) is not easy. This is the logic upon which RSA is built. RSA includes not only RSA public-key encryption but also RSA digital signature (where RSA is heavily used).

Acknowledgements

The authors would like to thank Huang Fan, PhD student at National University of Singapore, for research assistance.

Author contributions

CRediT: **Jon Truby:** Conceptualization, Formal analysis, Investigation, Methodology, Project administration, Resources, Supervision, Writing – original draft, Writing – review & editing; **Omer Baysal:** Investigation, Writing – original draft.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Declaration of generative AI and AI-assisted technologies in the writing process

During the preparation of this work the author(s) used ChatGPT to improve the readability and language of the manuscript. After using this tool/service, the authors reviewed and edited the content as needed and take full responsibility for the content of the published article.

References

Agence nationale de la sécurité des systèmes d'information (ANSSI). 2023. "ANSSI Views on the Post-Quantum Cryptography Transition." December 21. https://messervices.cyber.gouv.fr/documents-guides/follow_up_position_paper_on_post_quantum_cryptography.pdf.

Alagic, Gorjan. 2022. "Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process." NISTIR 8413. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8413.

Althobaiti, Ohood Saud, and Mischa Dohler. 2020. "Cybersecurity Challenges Associated With the Internet of Things in a Post-Quantum World." *IEEE Access* 8:157356–157381. https://doi.org/10.1109/ACCESS.2020.3019345.

Balarabe, Kasim. 2025. "Quantum Computing and the Law: Navigating the Legal Implications of a Quantum Leap." *European Journal of Risk Regulation* 16 (2): 794–813. https://doi.org/10.1017/err.2025.8.

Bank of Israel. 2025. "Banking System Preparedness for Cyber Risks Arising from Quantum Computing Capabilities." Letter, January 7. https://www.boi.org.il/en/economic-roles/supervision-and-regulation/letters/letter202501en.

Basel Committee on Banking Supervision (BCBS). 2018. *Cyber Resilience: Range of Practices*. Basel: Bank for International Settlements. https://www.bis.org/bcbs/publ/d454.pdf.a

Baseri, Yaser, Vikas Chouhan, and Abdelhakim Senhaji Hafid. 2024. "Navigating quantum security risks in networked environments: A comprehensive study of quantum-safe network protocols." *Computers & Security* 142:103883. https://doi.org/10.1016/j.cose.2024.103883.

Bergeron, James Henry. 2026. "Emerging Disruptive Technologies: Dilemmas of Deterrence." Geostrategy Programme, GSPE04. London: Council on Geostrategy. https://www.councilongeostrategy.org/explainers/emerging-disruptive-technologies.

Bishwas, Arit Kumar, and Mousumi Sen. 2024. "Strategic Roadmap for Quantum-Resistant Security: A Framework for Preparing Industries for the Quantum Threat." arXiv preprint arXiv:2411.09995. https://doi.org/10.48550/arXiv.2411.09995.

Bolatbekkyzy, Gulbakyt. 2024. "Legal Issues of Cross-Border Data Transfer in the Era of Digital Government." *Journal of Digital Technologies and Law* 2 (2): 286.

Brooks, Chuck. 2025. "Quantum Computing has Arrived. We Need to Prepare for Its Impact." Forbes, February 22. https://www.forbes.com/sites/chuckbrooks/2025/02/22/quantum-computing-has-arrived-we-need-to-prepare-for-its-impact/.

Bruno, Luigi, and Isabella Spano. 2021. "Post-Quantum Encryption and Privacy Regulation: Can the Law Keep Pace with Technology?" *European Journal of Privacy Law and Technologies* 2021 (1): 72–81.

Buchan, Russell. 2012. "Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?" *Journal of Conflict and Security Law* 17 (2): 212–227. https://doi.org/10.1093/jcsl/krs014.

Bundesamt für Sicherheit in der Informationstechnik (BSI). 2021. "Quantum-Safe Cryptography: Fundamentals, Current Developments and Recommendations." October. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.pdf.

Bureau of Industry and Security (BIS). 2025. "Commerce Further Restricts China's Artificial Intelligence and Advanced Computing Capabilities." Press release, March 25. https://www.bis.gov/press-release/commerce-further-restricts-chinas-artificial-intelligence-advanced-computing-capabilities.

Campagna, Matthew, Melanie Goldsborough, and Peter O'Donnell. 2024. "AWS Post-Quantum Cryptography Migration Plan." AWS Security Blog, December 5. https://aws.amazon.com/blogs/security/aws-post-quantum-cryptography-migration-plan/.

Canadian Centre for Cyber Security (CCCS). 2024. "Recommended Cyber Security Contract Clauses for Cloud Services (ITSM.50.104)." October 22. https://www.cyber.gc.ca/en/guidance/recommended-cyber-security-contract-clauses-cloud-services-itsm50104.

Chen, Stephen. 2023. "Chinese Scientists Hack Military-Grade Encryption with Quantum Computer, Paper Says." South China Morning Post, April 6. https://web.archive.org/web/20241125004946/https://www.scmp.com/news/china/science/article/3282051/chinese-scientists-hack-military-grade-encryption-quantum-computer-paper.

Committee on Payments and Market Infrastructures (CPMI) and Board of the International Organization of Securities Commissions (IOSCO). 2016. "Guidance on Cyber Resilience for Financial Market Infrastructures." Basel: Bank for International Settlements. https://www.bis.org/cpmi/publ/d146.pdf.

Council of Europe. 2001a. "Convention on Cybercrime." https://rm.coe.int/1680081561.

Council of Europe. 2001b. "Explanatory Report to the Convention on Cybercrime." https://rm.coe.int/16800cce5b.

Court of Justice of the European Union (CJEU). 2020. "Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems." Case C-311/18.

Creemers, Rogier, Hunter Dorwart, Kevin Neville, Kendra Schaefer, Johanna Costigan, and Graham Webster. 2022. "Translation: 14th Five-Year Plan for National Informatization – Dec. 2021." DigiChina, January 24. https://digichina.stanford.edu/work/translation-14th-five-year-plan-for-national-informatization-dec-2021/.

Cybersecurity and Infrastructure Security Agency (CISA). 2024. "Preparing Critical Infrastructure for Post-Quantum Cryptography." https://www.cisa.gov/quantum.

Data Protection Commission (DPC). 2023. "Data Protection Commission Announces Decision Against Meta Platforms Ireland Limited." Press release, May 22. https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-against-meta-platforms-ireland-limited.

Duru, Omer. 2023. "From Tallinn Manual 'Law-Talking' to Law Making: How Expert-Written Manuals Inform the Development of State Practice on Cyber Due Diligence Obligations." *Naval Law Review* 69:94–115.

Dynkin, Barry, and Benjamin Dynkin. 2018. "Derivative Liability in the Wake of a Cyber Attack." *Albany Law Journal of Science & Technology* 28 (3): 23–44.

Elvy, Stacy-Ann. 2023. "Commercial Law as a Source of Privacy and Cybersecurity Protection." *Harvard Journal of Law & Technology* 37 (3): 1177–1200.

Energy Expert Cyber Security Platform. 2017. "Cyber Security in the Energy Sector: Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector." European Commission. https://energy.ec.europa.eu/system/files/2017-03/eecsp_report_final_0.pdf.

Ernst and Young. 2024. "The CRO Cyber Risk Agenda: What Boards Should Be Asking." Board Matters. https://www.ey.com/en_us/board-matters/cyber-risk-questions-for-boards.

European Commission. 2018. "Rolling Plan for ICT standardisation: Quantum Technologies (RP2023)." February 19. https://interoperable-europe.ec.europa.eu/collection/rolling-plan-ict-standardisation/quantum-technologies-rp2023.

European Commission. 2023. "Quantum Technologies Flagship." December 19. https://digital-strategy.ec.europa.eu/en/policies/quantum-technologies-flagship.

European Commission. 2024. "Commission Recommendation of 11 April 2024 on a Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography." European Commission/2393 final.

European Data Protection Board (EDPB). 2021. "Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data." Ver. 2.0/1.

European Parliament and Council of the European Union. 2016. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)." OJ L119.

European Parliament and Council of the European Union. 2019. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and ICT Cybersecurity Certification (Cybersecurity Act). OJ L151/15.

European Parliament and Council of the European Union. 2022a. "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity Across the Union (NIS2 Directive)." OJ L333/80.

European Parliament and Council of the European Union. 2022b. "Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on Digital Operational Resilience for the Financial Sector (Digital Operational Resilience Act, DORA)." OJ L333/1.

European Union Agency for Cybersecurity (ENISA). 2021. "Post-Quantum Cryptography: Current State and Quantum Mitigation." May 3. https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation.

Gale, Megan, Ivano Bongiovanni, and Sergeja Slapnicar. 2022. "Governing Cybersecurity from the Boardroom: Challenges, Drivers, and Ways Ahead." *Computers & Security* 121:102840. https://doi.org/10.1016/j.cose.2022.102840.

Gao, Dongxin, Daojin Fan, Chen Zha, Jiahao Bei, Guoqing Cai, Jianbin Cai, Sirui Cao, Fusheng Chen, Jiang Chen, et al. 2025. "Establishing a New Benchmark in Quantum Computational Advantage with 105-qubit Zuchongzhi 3.0 Processor." *Physical Review Letters* 134 (9): 090601. https://doi.org/10.1103/PhysRevLett.134.090601.

Garon, Jon M. 2018. "Cyber-World War III: Origins." *Journal of Law and Cyber Warfare* 7 (1): 1–20.

Government Accountability Office (GAO). 2024. "Future of Cybersecurity: Leadership Needed to Fully Define Quantum Threat Mitigation Strategy." GAO-25-107703, November. https://www.gao.gov/assets/gao-25-107703.pdf.

Government Accountability Office (GAO). 2025. "Quantum Computing: Leadership Needed to Coordinate Cyber Threat Mitigation Strategy. Testimony before the Subcommittee on Cybersecurity, Information Technology, and Government Innovation, Committee on Oversight and Government Reform, US House of Representatives, June 24. GAO-25-108590." https://www.gao.gov/assets/gao-25-108590.pdf.

Groenewegen-Lau, Jeroen, and Antonia Hmaidi. 2024. "China's Long View on Quantum Tech Has the US and EU Playing Catch-Up." MERICS, February 22. https://merics.org/en/report/chinas-long-view-quantum-tech-has-us-and-eu-playing-catch.

Gross, Oren. 2015. "Cyber Responsibility to Protect: Legal Obligations of States Directly Affected by Cyber-Incidents." *Cornell International Law Journal* 48 (3): 481–539.

GSMA. 2025. "Post-Quantum Government Initiatives by Country and Region." March 2. https://www.gsma.com/newsroom/wp-content/uploads/Post-Quantum-Government-Initiatives-by-Country-and-Region-02-Mar-2025.pdf.

Heathman, Amelia. 2017. "Quantum Computing: The Most Exciting Thing in Computing Is Also the Most Terrifying." Verdict, July 21. https://www.verdict.co.uk/quantum-computing-the-most-exciting-thing-in-computing-is-also-the-most-terrifying/.

Hershkovitz, Shay. 2022. *The Future of National Intelligence: How Emerging Technologies Reshape Intelligence Communities*. Lanham: Rowman & Littlefield.

ISO/IEC. 2024. "Information Technology – Quantum Computing – Vocabulary. ISO/IEC 4879:2024." Geneva: International Organization for Standardization. https://www.iso.org/standard/80432.html.

Jensen, Eric Talbot. 2002. "Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense." *Stanford Journal of International Law* 38:207–228.

Jung, Heonhui, and Hyunyoung Oh. 2024. "Designing a Scalable and Area-Efficient Hardware Accelerator Supporting Multiple PQC Schemes." *Electronics* 13 (17): 3360. https://doi.org/10.3390/electronics13173360.

Kania, Elsa B. 2021. "China's Quest for Quantum Advantage—Strategic and Defense Innovation at a New Frontier" *Journal of Strategic Studies* 44 (6): 922–952. https://doi.org/10.1080/01402390.2021.1973658.

Keane, Jonathan. 2024. "Is Quantum Computing the Next Technology on the EU's Regulation Agenda?". EuroNews, January 30. https://www.euronews.com/next/2024/01/30/is-quantum-computing-the-next-technology-on-the-eus-regulation-agenda.

Kim, Jungsang, and Christopher Monroe. 2024. "America Is the Undisputed World Leader in Quantum Computing Even Though China Spends 8x More on the Technology—But an Own Goal Could Soon Erode US Dominance." Fortune, April 12. https://fortune.com/2024/04/12/america-undisputed-world-leader-quantum-computing-even-though-china-spends-technology-us-dominance/.

Kirton, David. 2022. "The Quantum Hack: Inside the Race to Lock Down the Internet Before China Can Hack It." Reuters, November 23. https://www.reuters.com/investigates/special-report/us-china-tech-quantum/.

Lloyd's and University of Cambridge Centre for Risk Studies. 2015. "Business Blackout: The Insurance Implications of a Cyber Attack on the US Power Grid." https://www.lloyds.com/about-lloyds/media-centre/press-releases/lloyds-study-highlights-wide-ranging-implications-of-cyber-attacks.

Luo, Yadong. 2022. "A General Framework of Digitization Risks in International Business." *Journal of International Business Studies* 53 (2): 344–361. https://doi.org/10.1057/s41267-021-00448-9.

Moody's Investors Service. 2023. "Cyber Risk – Global: Transition to Post-Quantum Data Encryption Will Be Complex, Costly and Prolonged." August 10. https://www.moodys.com/research/Cyber-Risk-Global-Transition-to-post-quantum-data-encryption-will-be-Sector-In-Depth–PBC_1417045.

National Institute of Standards and Technology (NIST). 2022. "First Four Quantum-Resistant Cryptographic Algorithms." NIST News, July 5. https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms.

National Institute of Standards and Technology (NIST). 2024a. "What Is Post-Quantum Cryptography?". https://www.nist.gov/cybersecurity/what-post-quantum-cryptography.

National Institute of Standards and Technology (NIST). 2024b. "NIST Releases First 3 Finalized Post-Quantum Encryption Standards." August 13. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards.

National People's Congress of China. 2019. "Cryptography Law of the People's Republic of China".

National Security Agency. 2021. "World War 2: Enigma." https://www.nsa.gov/History/National-Cryptologic-Museum/Exhibits-Artifacts/Exhibit-View/Article/2719176/world-war-2-enigma/.

National Security Agency. 2022. "Announcing the Commercial National Security Algorithm Suite 2.0." https://media.defense.gov/2025/May/30/2003728741/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.PDF.

Neven, Hartmut. 2024. "Meet Willow, Our State-of-the-Art Quantum Chip." The Keyword, December 9. https://blog.google/innovation-and-ai/technology/research/google-willow-quantum-chip/.

Nguyen, Reese. 2013. "Navigating Jus Ad Bellum in the Age of Cyber Warfare." *California Law Review* 101:1079–1098.

Nguyen, Fiona Q. 2018. "The Standard for Biometric Data Protection." *Journal of Law and Cyber Warfare* 7 (1): 61–80.

North Atlantic Treaty Organization (NATO). 2024. "Summary of NATO's Quantum Technologies Strategy." January 16. https://www.nato.int/cps/cn/natohq/official_texts_221777.htm.

O'Connell, Mary Ellen. 2012. "Cyber Security without Cyber War." *Journal of Conflict and Security Law* 17:187–209. https://doi.org/10.1093/jcsl/krs017.

Peng, Dannie. 2024. "China 'Poised to Lead' Creation of Quantum-Proof Telecoms Security Protocol." South China Morning Post, October 30. https://www.scmp.com/news/china/science/article/3284381/china-poised-lead-creation-quantum-proof-telecoms-security-protocol.

Pote, Prajakta, and Rajesh Bansode. 2025. "Performance Evaluation of Post-Quantum Cryptography: A Comprehensive Framework for Experimental Analysis." *Journal of Information Systems Engineering and Management* 10 (9): 548–556. https://doi.org/10.52783/jisem.v10i9s.1253.

Preskill, John. 2018. "Quantum Computing in the NISQ Era and Beyond." *Quantum* 2:79. https://doi.org/10.22331/q-2018-08-06-79.

Radanliev, Petar. 2024. "Cyber Diplomacy: Defining the Opportunities for Cybersecurity and Risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing." *Journal of Cyber Security Technology* 9 (1): 28–78. https://doi.org/10.1080/23742917.2024.2312671.

Ricci, Sara, Patrik Dobias, Lukas Malina, Jan Hajny, and Petr Jedlicka. 2024. "Hybrid Keys in Practice: Combining Classical, Quantum and Post-Quantum Cryptography." *IEEE Access* 12:23206–23219. https://doi.org/10.1109/ACCESS.2024.3364520.

Rodriguez, Andrea G. 2025. "A Quantum Cybersecurity Agenda for Europe II." European Policy Center, January 17. https://www.epc.eu/content/Cybersecurity_2.pdf.

Schmitt, Michael N. 2017a. "Law of International Responsibility." In *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, edited by Michael N. Schmitt, 79–167. Cambridge: Cambridge University Press.

Schmitt, Michael N. 2017b. "Cyber Operations Not Per Se Regulated by International Law." In *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, edited by Michael N. Schmitt, 168–176. Cambridge: Cambridge University Press.

Schneier, Bruce. 2015. "NSA Plans for a Post-Quantum World." Lawfare, August 21. https://www.lawfaremedia.org/article/nsa-plans-post-quantum-world.

Simmons, Noah. 2014. "A Brave New World: Applying International Law of War to Cyber-Attacks." *Journal of Law and Cyber Warfare* 4 (1): 42–68.

Sparkes, Matthew. 2024. "Multiple Nations Enact Mysterious Export Controls on Quantum Computers." New Scientist, July 3. https://www.newscientist.com/article/2436023-multiple-nations-enact-mysterious-export-controls-on-quantum-computers/.

Sparkes, Matthew. 2025. "China Launches Hunt for Ways to Protect Data from Quantum Computers." New Scientist, February 17. https://www.newscientist.com/article/2467574-china-launches-hunt-for-ways-to-protect-data-from-quantum-computers/.

SWIFT. 2024. "Customer Security Controls Framework." https://www.swift.com/myswift/customer-security-programme-csp/security-controls.

Swiss Financial Market Supervisory Authority (FINMA). 2022. "Operational Risks and Resilience – Banks." Circular 2023/1, December 7. https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2023-01-20221207.pdf.

Trautman, Lawrence J., and Peter C. Ormerod. 2017. "Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Data Breach." *American University Law Review* 66 (5): 1231–1291.

Truby, Jon. 2026. "From Paris to New Delhi, India's AI Governance Is Being Written in Hospitals and Banks." MENA, January 20. https://www.menaexecutivetraining.com/post/from-paris-to-new-delhi-india-s-ai-governance-is-being-written-in-hospitals-and-banks.

UN General Assembly. 1966. "International Covenant on Civil and Political Rights." December 16. United Nations Treaty Series, vol. 999: 171.

UN Group of Governmental Experts (UN GGE). 2015. "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note / by the Secretary-General." A/70/174. https://digitallibrary.un.org/record/799853.

UN Office for Disarmament Affairs (UNODA). n.d. "Open-Ended Working Group on Information and Communication Technologies." https://meetings.unoda.org/open-ended-working-group-on-information-and-communication-technologies-2021.

UN Secretary-General. 2024. "Remarks at the Security Council's High-Level Debate on 'Maintenance of International Peace and Security: Addressing Evolving Threats in Cyberspace'." Global Security, June 20. https://www.globalsecurity.org/security/library/news/2024/06/sec-240620-unsg01.htm.

United Nations. 2024. "Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes." UN Doc A/RES/78/198.

Van Daalen, Ot L. 2023. "The Right to Encryption: Privacy as Preventing Unlawful Access." *Computer Law & Security Review* 49:105804. doi:doi:10.1016j.clsr.2023.105804.

Vermeer, Michael J. D., and Evan D. Peet. 2020. "Securing Communications in the Quantum Computing Age." Rep. RR-3102. RAND Corporation. https://www.rand.org/pubs/research_reports/RR3102.html.

Ward, Isabella. 2024. "US Government Urges Federal Contractors to Strengthen Encryption." Bloomberg, March 21. https://news.bloomberglaw.com/federal-contracting/us-government-urges-federal-contractors-to-strengthen-encryption.

WhatsApp. n.d. "About End-to-End Encryption." https://faq.whatsapp.com/820124435853543.

White House. 2022. "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems." May 4. https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/.

White House. 2023a. "National Cybersecurity Strategy."

White House. 2023b. "National Cybersecurity Implementation Plan." July. https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf.

White House. 2024. "National Cybersecurity Strategy Implementation Plan (Version 2)." May. https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/05/NCSIP-Version-2-FINAL-May-2024.pdf.

World Economic Forum. 2024. "Quantum Security for the Financial Sector: Informing Global Regulatory Approaches." Geneva: World Economic Forum. https://www.weforum.org/publications/quantum-security-for-the-financial-sector-informing-global-regulatory-approaches/.

World Economic Forum. 2025. "Global Cybersecurity Outlook 2025." January 13. https://www.weforum.org/publications/global-cybersecurity-outlook-2025/.

Xu, Rachel, Kelly Ann Shaw, Ajay Kuntamukkala, Ben Kostrzewa, and Roy Zou. 2020. "Final Version of China's Export Control Law Will Take Effect in Less Than Two Months." Hogan Lovells, October 23. https://www.hoganlovells.com/en/publications/final-version-of-chinas-export-control-law-will-take-effect-in-less-than-two-months_1.

Zhang, Kevin Honglin. 2024. "Geoeconomics of US-China Tech Rivalry and Industrial Policy." *Asia and the Global Economy* 4 (2): 100098. https://doi.org/10.1016/j.aglobe.2024.100098.

Zou, Roy, Jessie Xie, Lan Zu, and Carol Shao. 2020. "Chinese Regulators Set Import Licence or Export Control Requirement for Certain Commercial Encryption Products." Hogan Lovells, December 24. https://www.hoganlovells.com/en/publications/chinese-regulators-set-import-license-or-export-control-requirement-for-certain-commercial-encryption-products_1_1.