United Nations University
Centre for Policy Research

Policy Brief

International Inequality and Post-Quantum Cryptography

Michael P. A. Murphy

UNU CPR

GGI Global Governance Innovation

Disclaimer
This brief is an output of the Global Governance Innovation Platform initiative. The views and opinions expressed do not necessarily reflect the official policy or position of the United Nations University.

ISBN: 978-92-808-6672-8

Citation: Michael P. A. Murphy, "International Inequality and Post-Quantum Cryptography", GGI Platform Policy Brief (New York, United Nations University, 2026).

Key Recommendations

- The tendency for quantum cryptographic transitions to be national efforts has led to limited discussion of the role of global governance in supporting transitions in low- and middle-income countries (LMICs). International institutions must recognize the important challenges facing LMICs in developing quantum resilience.
- There is a limited window of time for new global governance frameworks and international initiatives to develop in order to support cryptographic transitions and system maintenance in LMICs before the emergence of threats from cryptographically relevant quantum computers.
    - International institutions with expertise in supporting digital infrastructure development in LMICs should incorporate quantum cryptographic resilience as a strategic objective. Individual countries or minilateral coalitions with capacity for international assistance can also provide funds or offer subsidized education pathways.
    - International assistance should consider targeting funds for quantum risk audits, supporting the training of highly qualified personnel in key fields, and providing financial support for cryptographic transitions.
- Given the necessity of risk auditing for cryptographic transition planning, personnel requirement projections and cost estimates, the first priority for international support must be in the domain of assessing quantum risks.

Challenge

As the development of quantum computing technologies accelerates, many countries around the world are developing plans to ensure cryptographic resilience against the threats that quantum computers will pose to critical systems. Although the cryptographic transition is recognized as important, its costs will be significant. This is especially important because not all countries have the fiscal capacity to absorb additional large-scale expenditures, and the tendency to frame quantum cryptographic transitions as national strategies (or multilateral commitments to be executed by individual countries) means that global coordination to support low- and middle-income countries has been understudied.

Approach

This policy brief provides a background on the need for enhanced cryptographic resilience as the world approaches the launch of cryptographically relevant quantum computers. Rather than focusing on economic opportunities or great power implications, however, the brief highlights the intersection of quantum cryptographic resilience challenges with international inequality. This provides clear analysis of the stakes of quantum cryptographic vulnerability for low- and middle-income countries. The introduction sets the stage for the policy domain and identifies the global governance gap. The second section expands on the "Q-Day" threat. Section three then foregrounds the implications of international inequality on quantum cryptographic resilience and outlines recommendations for global governance solutions.

Section 1

Introduction

As quantum technologies attract greater international attention in national economic and security policy contexts, countries around the world are developing plans to execute a cryptographic transition on an unprecedented scale. Cryptography is the process that keeps data safe from potential adversaries, a mission-critical protection for any system that transmits data over the Internet. For decades, the mathematical foundation of quantum theory has predicted that a sufficiently large quantum computer would be capable of breaking through contemporary cryptographic protocols.[1] In response to the threat of a cryptographically relevant quantum computer (CRQC) acquiring sensitive information, taking control of a system or shutting down critical infrastructure, organizations can choose to upgrade encryption, withdraw from the public Internet or accept complete data vulnerability to the adversary. As discussed below, sufficiently powerful quantum computers do not yet exist, although the "threat period" begins before the successful deployment of such a technology.

Although the choice of upgrading cryptography may seem straightforward, this simplicity masks the practical challenge and high cost associated with such an endeavour. A landmark report released by the White House in July 2024 estimated that the cost of the United States Federal Government transitioning to post-quantum cryptography would be approximately $7.1 billion by 2035.[2] Other levels of government, private sector actors and civil society organizations will all have their own costly migrations over the same period. The total cost of worldwide transitions to post-quantum cryptography will run well into tens or hundreds of billions of dollars. In addition to cost, as countries and corporations migrate their systems, serious strain will be placed on the technical experts capable of executing this work at scale.

Because national cybersecurity organizations have typically been appointed as leaders for quantum-resilient cryptographic transition strategies within borders, insufficient attention has been paid to global governance. This policy brief foregrounds the dangerous intersection of international inequality and the quantum-resilient transition, arguing that low- and middle-income countries (LMICs) face a particularly stark quantum threat, given their limited financial ability to promote quantum resilience. "Q-Day" – the day when a CRQC becomes operational – may mark a rapid reversal of progress made towards universalizing Internet access and the development of digital infrastructures worldwide.

> Because national cybersecurity organizations have typically been appointed as leaders for quantum-resilient cryptographic transition strategies within borders, insufficient attention has been paid to global governance."

[1] Mastercard. "Migration to post-quantum cryptography", Mastercard R&D white paper (n.d.). Available at https://www.mastercard.com/content/dam/mccom/shared/news-and-trends/stories/2025/quantum-explainer-and-white-paper/Migration-to-post-quantum-cryptography-WhitePaper_2025.pdf.

[2] United States of America, Executive Office of the President of the United States, *Report on Post-Quanum Cryptography as required by the Quantum Computing Cybersecurity Preparedness Act, Public Law No: 117-260* (Washington DC, 2024). Available at https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/07/REF_PQC-Report_FINAL_Send.pdf.

Given the rapid progress of quantum computing research, there is an immediate need for the international community to establish an action plan for supporting quantum-resilient cryptographic transitions in LMICs. International institutions, minilateral coalitions and States with the capacity to support international assistance must develop immediate-term funding mechanisms for quantum risk audits and upskilling to support a transition to post-quantum cryptography (PQC). Over the next decade, international funding support for critical system migrations will be necessary to ensure that Internet accessibility and cybersecurity are not driven out of reach for LMICs by the rise of quantum-enabled cyberthreats.

Section 2

Understanding the Threat of Q-Day

Contemporary digital communications are typically secured by public key cryptography, a term covering different algorithmic approaches that provide security for information exchange without requiring specific private network connections between exchangers. Given the computational advantage promised by quantum computers, these public key frameworks will become vulnerable to hacking once sufficiently large quantum computers are available. The specific threats posed by quantum-enabled hackers include the decryption of sensitive information as well as the forging of digital signatures to enable a wide range of fraudulent activities in environments assumed to be secure.[3] Valuing the potential damage of such attacks is proving to be a challenge for risk analysts given the scope and scale of threats. For example, economic modelling of a single one-day quantum-enabled attack on a large US bank's access to the Fedwire Funds Service could cause national annual Gross Domestic Product to fall by 17 per cent.[4]

This is only the tip of the iceberg of potential damage, as "the true economic cost" of quantum-enabled hacking "could ultimately reflect the value of every digital interaction or asset that relies on classical cryptography".[5] The potential scale of impact of a quantum attack on the financial system is significant; while the highest-income countries may be prepared to invest in infrastructural resilience and provide economic stimulus in response to economic shocks, the threat of Q-Day is heightened in countries where there is less fiscal flexibility to fund preparedness and relief.

Although it might seem comforting that the development of a CRQC is still years away by best estimates, this timeline is misleading for three reasons:

- **First**, the increasing capital allocated to research has led to breakthroughs across fields of quantum technology, and there is uncertainty about how much time remains before Q-Day.

[3] Mastercard, "Migration to post-quantum cryptography"; Ria Chakraborty, Kim de Laat and Raymond Laflamme, *Canada's Migration to Post-Quantum Cryptography: Public-Private Roles* (Waterloo, Centre for International Governance Innovation, 2025); Tracey Forrest, Paul Samson, Yash Kalash and Michael P.A. Murphy, *Quantum Technologies and the Geostrategic Landscape: Implications for Finance and Central Banks* (Waterloo, Centre for International Governance Innovation, 2026); Ronit Ghose, Sophia Bantanidis, Prag Sharma, Ronak Shah and Kaiwan Master, *Quantum Threat: The Trillion-Dollar Security Race Is On* (New York, Citi Institute, 2026).

[4] Alexander W. Butler and Arthur Herman, *Prosperity at Risk: The Quantum Computer Threat to the US Financial System* (Washington DC, Hudson Institute, 2023).

[5] Ghose et al., *Quantum Threat*, p. 7.

- **Second**, the cryptographic migration to post-quantum cryptography is a digital project of unprecedented scale, and even the most aggressive migration plans from the world's wealthiest countries recognize that the process will take years to complete.
- **Third**, some data remain sensitive over a long-term horizon, and long-shelf-life data exfiltrated in an encrypted state may be decrypted after Q-Day.

Within communities of quantum cybersecurity, "Mosca's inequality" provides a framework for assessing the threat of quantum computing to sensitive data. In Mosca's inequality, X represents the shelf-life of the data, Y represents the duration of quantum-resilient migration and Z marks the time remaining until vulnerability.[6] The table below breaks down two possible outcomes of the inequality. For purposes of clarity, the examples in the table fall clearly into a category of clear priority/non-priority; the most difficult – and important – work in risk assessment will be identifying the risk level and necessary responses for marginal or unclear cases. The specific assessment will differ between data given the shelf-life, the complexity of the system migration and the unknown time remaining to Q-Day. A critical insight from Mosca's inequality is that we already live in a period of quantum threat, at least for longest-shelf-life data, and more data becomes threatened at present with every passing year.

Notation	Meaning	Examples	Impact
X+Y<Z	The length of time until the quantum threat is expected is longer than the shelf-life of the data plus the time to migration.	• An advance copy of a government's annual budget, which remains sensitive only until the budget's release date. • Trade secrets relating to a patent which expires before the expected Q-Day.	There is sufficient time to protect the data before the threat is expected to materialize.
X+Y>Z	The sum of the data's shelf-life and the time to migration is greater than the time remaining before the quantum threat.	• Sensitive military information that must be protected for the lifecycle of a major asset (e.g. fighter jet). • Personal health information that citizens wish to keep private for their lifetimes.	The information is already vulnerable to a "harvest now, decrypt later" attack.

In order to ensure that systems are resilient before it is too late to safeguard critical data, strategies for PQC migration are developing around the world. In the United States, the National Security Agency's guidance for national security systems and the defence industry recommend that all systems be quantum-resilient by 2035, while the European Union's tiered roadmap with high-priority systems is set to transition in 2030, prior to medium-risk systems by 2035.[7] The Group of 7 (G7) Cyber Expert Group has similarly suggested a layered approach that prioritizes highest-impact systems in the near term before then moving to lower-sensitivity systems.[8] Throughout these high-income countries, where significant resources can be allocated to critical cyber defences, there is a recognition that the scale of the undertaking will take considerable time.

6 Michele Mosca, "Setting the Scene for the ETSI Quantum-safe Cryptography Workshop", e-proceedings of 1st Quantum-SafeCrypto Workshop (Sophia Antipolis, 2013), pp. 26–27; Michele Mosca and John Mulholland. *A Methodology for Quantum Risk Assessment* (Toronto, Global Risk Institute, 2017).

7 National Security Agency, "The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ", December 2024. Available at https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF; NIS Cooperation Group, "A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography", European Union, 11 June 2026. Available at https://ec.europa.eu/newsroom/dae/redirection/document/117507.

8 G7 Cyber Expert Group, "Advancing a Coordinated Roadmap for the Transition to Post-Quantum Cryptography in the Financial Sector", statement, January 2026. Available at https://assets.publishing.service.gov.uk/media/6966149d8d599f4c09e1ffab/G7-CEG-Quantum-Roadmap.pdf.

> In order to ensure that systems are resilient before it is too late to safeguard critical data, strategies for PQC migration are developing around the world."

The urgent need to transition systems towards quantum-resilience has become a point of consensus within cybersecurity circles. Many governments around the world have recognized this necessity, as well as the unprecedented cost of this system upgrade. The still unanswered questions concern the total worldwide cost and how lower-income countries will allocate resources.

Section 3

International Inequality and Quantum Resilience

Since the early 2000s, the widespread adoption of digital technologies has reshaped economies and societies. However, access to technologies and development of the digital infrastructures necessary to connect with these systems has been uneven around the globe. International inequality is a major determinant of a society's ability to access the Internet and associated digital technologies; although improvements can be observed for countries across all income quartiles, countries' wealth is a strong predictor of access.[9] Recognizing the potential for this feedback loop to reinforce inequality, organizations like the United Nations Technology Bank for the Least Developed Countries are seeking to address critical bottlenecks in infrastructure and access before lower-income countries miss out on future economic development opportunities.[10] These issues are about to become even more complicated, as the world prepares for a CRQC.

Although the costs of PQC migration are recognized as significant for the world's highest-income countries, they are likely to be absorbed with minimal societal impact. However, that budgetary flexibility is a luxury. International inequality is high at present, perhaps most directly reflected in the World Bank's recent finding that "among the 22 most highly indebted countries, one out of every two people today cannot afford the minimum daily diet necessary for lasting health".[11] In a world where large debt service obligations, infrastructure gaps and

[9] International Telecommunication Union, *Measuring Digital Development: Facts and Figures 2025* (Geneva, 2025). Available at https://www.itu.int/dms_pub/itu-d/opb/ind/d-ind-ict_mdd-2025-3-pdf-e.pdf.

[10] For example, see Federica Irene Falomi, Marti Serra Figarola and Hyunjee Sung, "Turning Artificial Intelligence into a Development Asset in Least Developed Countries", UN Technology Policy Brief (Gebze, United Nations Technology Bank for Least Developed Countries, 2026). Available at https://www.un.org/technologybank/sites/www.un.org.technologybank/files/policy_brief_ai_15012026.pdf.

[11] The World Bank, *International Debt Report 2025* (Washington, The World Bank, 2025), p. xi.

In a world where large debt service obligations, infrastructure gaps and inflation caused by global instability apply extreme pressure to government budgets, the additional burden of a costly cybersecurity transition would place significant strain on core State operations."

inflation caused by global instability apply extreme pressure to government budgets, the additional burden of a costly cybersecurity transition would place significant strain on core State operations. This appears to be a no-win scenario, which leaves LMICs with three options:

1. Accept vulnerability to quantum-enabled attacks
2. Withdraw critical systems from Internet access
3. Reduce State capacity to prioritize a PQC transition.

All of these options reinforce international inequality and increase lived insecurity for citizens living in LMICs, with self-reinforcing effects that can compound societal impacts over time. This forces an impossible choice between necessary functions and a critical risk onto actors whose resources are already under strain.

The alternative to this bleak menu of options is for international cooperation to support PQC transitions through three key stages: funding risk assessments,[12] training highly-qualified personnel to migrate and maintain systems, and financial support to undertake the migration. Mishra and Nair argued that the United States Agency for International Development (USAID) should support quantum readiness in LMICs through the development of quantum risk auditing frameworks that could be implemented by and for LMICs, the development of a global taskforce to support PQC transitions, technical capacity-building efforts, and promotion of public awareness of quantum cyber threats.[13]

Although proposals for country-led international assistance programmes may be promising in terms of rapid deployment of capabilities based on existing frameworks or country-to-country relationships,[14] such programmes are also vulnerable to domestic priorities shifting away from international assistance. In order to avoid the radical reversal of international connectivity, international institutions and minilateral coalitions have a window of opportunity to support quantum risk assessments, international training programmes to build PQC capacity in LMICs, and financial mechanisms to support transitions.

The alternative to this bleak menu of options is for international cooperation to support PQC transitions through three key stages: funding risk assessments, training highly-qualified personnel to migrate and maintain systems, and financial support to undertake the migration."

[12] Risk assessments must be recognized as the most urgent step, as this process is necessary for any further work.

[13] Abhilash Mishra and Bhasi Nair, *Quantum Futures: Making Quantum Computing Work for International Development* (Washington DC, USAID Research Technical Assistance Center, 2023).

[14] For example Mishra and Nair, *Quantum Futures*; Michael P. A. Murphy, "Canada as a Norm Entrepreneur in Quantum Science and Technology", Digital Policy Hub Working Papers (Waterloo, Centre for International Governance Innovation, 2025).

Section 4

Conclusion

The stakes are high. Without immediate-term international support to facilitate quantum readiness, including risk audits and the development of sufficient highly-qualified personnel to lead national PQC migrations, there is a critical risk to the possibility of secure data exchange worldwide. The end of cybersecurity in lower-income countries will rapidly reinforce international inequality and put at risk the economic opportunities created through increased Internet access. However, this is a discrete issue area that can be addressed through international cooperation and the maintenance of a focused scope of mission.

Further cause for optimism can be found in the existing efforts of the Africa Quantum Consortium. The Consortium's white paper provides not only a direct coordination framework for upskilling on the continent through quantum-focused educational programmes but also a model for regional-led development of a quantum agenda.[15] International institutions, minilateral coalitions and region-led initiatives can seek opportunities for synergy in promoting global quantum resilience.

In the immediate term – during the year of quantum security 2026 – international institutions, minilateral coalitions and countries able to support international assistance must support quantum risk audits for all countries that have not yet analysed the security of their critical systems. International training and upskilling of highly-qualified personnel in post-quantum cryptography and risk analysis is also critical to ensure that countries can develop sustainable quantum resilience. Over the next decade, international assistance to fund or finance PQC migrations in LMICs will be necessary to avoid the critical tradeoffs described in section three. What is critical at this juncture is a recognition of the necessity of immediate-term action.

[15] Africa Quantum Consortium, *Africa's Quantum Horizon: A Unified Strategy for Sovereignty and Sustainable Development* (Africa Quantum Consortium, 2025). Available at https://africaquantum.org/whitepaper.html.

United Nations University
Centre for Policy Research

About GGI

The Global Governance Innovation Platform helps UN Member States design new multilateral institutions and reform existing ones. Through interactive mapping and data visualization, we identify and showcase innovative governance models and mechanisms that can be adapted to address urgent global challenges and collective action problems.

About UNU-CPR

The United Nations University Centre for Policy Research is a think tank within the United Nations that carries out policy-focused research and capacity-building on issues of strategic interest and importance to the UN and its Member States. The Centre prioritizes urgent policy needs requiring innovative, practical solutions oriented toward immediate implementation and sustainability over the long term.