May 2026

POLICY BRIEF CIRGoM 09

Towards Quantum Diplomacy: Bridging a Global Technological Divide Through Selective Cooperation

By Emma Bolduc

SUMMARY

Quantum technologies are reshaping the foundations of digital security, economic competitiveness, and military balance. The most pressing governance challenge is not any single risk, but the fragmentation that amplifies all of them: as major powers compete for advantage, the international system is drifting toward parallel technological blocs with incompatible standards and severed supply chains. This drift threatens collective cybersecurity, deepens the gap between advanced and developing economies, and forecloses cooperation on shared dangers, most urgently, the looming obsolescence of the encryption that protects banks, hospitals, and public services. This brief argues that selective cooperation, coordination on shared risks even amid strategic rivalry, is the only viable path. It recommends four operational priorities: accelerating the coordinated migration to quantum-resistant encryption, building a plurilateral supply-chain transparency mechanism, agreeing on what counts as an unacceptable use of quantum capabilities against civilian infrastructure, and convening an inclusive group of governmental experts to build a shared vocabulary of quantum risks.

A STRATEGIC INFLECTION POINT FOR GLOBAL GOVERNANCE

Quantum technologies are often framed as a distant frontier, but their implications are already concrete. A sufficiently powerful quantum computer would break the public-key cryptography that underpins virtually every secure transaction online: banking, government communications, electronic health records, and the operational systems of energy and water utilities. Although a fault-tolerant quantum computer — one with error correction robust enough to run such an attack — does not yet exist, adversaries are already collecting encrypted data with the expectation of decrypting it later, an approach known as harvest now, decrypt later. The threat is therefore present, even though the capability is future.

> "Adversaries are already collecting encrypted data with the expectation of decrypting it later."

Quantum sensing and quantum communication, meanwhile, are advancing on a different timeline. Some applications remain experimental, but others are already commercialized and deployed. Quantum magnetometers (including optically pumped and nitrogen-vacancy diamond sensors) are sold today for mineral exploration, medical brain imaging, and increasingly for navigation systems that work where GPS is jammed or unavailable. Atomic clocks based on quantum principles synchronize telecommunications networks, and early quantum key distribution links operate between government and financial

Centre interdisciplinaire de recherche sur la gouvernance mondiale

UNIVERSITÉ LAVAL

sites in several countries. These are not merely scientific advances, they are strategic assets, and states are treating them accordingly.

This asymmetry in levels of maturity and applications creates a policy paradox. Although the timeline for the arrival of a cryptographically relevant quantum computer remains uncertain, the migration to quantum-resistant systems is a multi-year undertaking, one that few governments and even fewer firms have meaningfully begun. Quantum sensing and communication, by contrast, raise governance questions today, as deployments expand in defence, health, and infrastructure. In both cases, existing international frameworks, built for an earlier generation of dual-use technologies, were not designed to manage an innovation cycle that simultaneously affects cybersecurity, trade, and military balance. Without deliberate global coordination, the transition will widen inequalities and destabilize the shared digital infrastructure, the financial, communications, and operational systems that no single state controls but all depend on.

TECHNOLOGICAL RIVALRY AND THE RISK OF A QUANTUM DIVIDE

Quantum development is increasingly shaped by competition among the principal powers (the United States, China, and the European Union) alongside a growing group of mid-sized quantum states including Japan, the United Kingdom, India, Canada, and Australia. Each is investing heavily in research while deploying policies designed to capture advantage. This strategic competition now extends well beyond laboratories. Since 2024, a wave of national export controls has redrawn the boundaries of who can sell what to whom. The U.S. Bureau of Industry and Security introduced worldwide license requirements on quantum computers, components, and related software in September 2024. Comparable measures have been adopted by the United Kingdom, France, the Netherlands, Canada, and Japan, among others, while the European Union added quantum technologies to its dual-use control list in November 2025.

This shift matters for global governance. The traditional multilateral mechanism for coordinating dual-use controls, the Wassenaar Arrangement, maintains lists of technologies that its 42 member states agree to monitor at export. The Arrangement has been largely paralyzed since 2022, when Russia began using its veto to block additions to those lists, including emerging quantum capabilities. In response, like-minded countries have moved toward a plurilateral approach, coordinating export controls through bilateral arrangements and informal alignments outside the Wassenaar framework, with smaller, more aligned groups of partners. This is more agile, but it also risks institutionalizing the splitting of the global technology system into parallel ecosystems.

Within the quantum sector, the most concentrated points of vulnerability sit at the upstream end of the supply chain. Cryogenic refrigeration units (Finland, United Kingdom), ultra-low-noise amplifiers (Sweden), isotopically pure materials (Russia, Germany), and specialized photonics (Canada, United States, several European countries) are produced by a small number of firms in a small number of countries. This concentration is what makes upstream components particularly exposed to geopolitical pressure: they are governed more restrictively than downstream services and applications, and once treated as strategic instruments, they create powerful incentives for states to localize production. The result raises costs, reduces interoperability, and locks in technological divergence that is difficult to reverse.

Beyond these upstream pressures, the consequences extend further. Incompatible standards would impede cross-border data flows and joint security responses. Unequal access would deepen what UNESCO has begun calling the "quantum divide" between the Global North and the Global South. Private actors (universities, startups, and research consortia) would face compounding regulatory uncertainty as they navigate competing rules. None of this is the result of malice; it is the cumulative effect of unilateral choices made in the absence of governance.

GLOBAL GOVERNANCE GAPS IN THE QUANTUM ERA

Despite mounting stakes, no comprehensive international framework currently addresses the full range of security, ethical, and economic implications of quantum innovation. There are partial successes. The NIST Post-Quantum Cryptography Standardization Process, running from 2016 to 2024, drew submissions from 25 countries and selected three quantum-resistant encryption algorithms now being adopted globally, a genuine instance of de facto international coordination, albeit under U.S. leadership rather than through a multilateral body. Other standard-setting efforts are emerging at the International Telecommunication Union and the International Organization for Standardization, but they remain fragmented. Beyond cryptographic standards, there is no agreed taxonomy of quantum risks, no shared lexicon of confidence-building measures, and nobody with authority to convene rivals at the table.

Three structural obstacles explain the gap. First, the dual-use character of quantum technology makes transparency itself a strategic risk: even sharing civilian research can reveal capabilities with military significance, so states default to opacity. Second, the pace of innovation outstrips traditional consensus-building. Multilateral standard-setting takes years; quantum hardware milestones now arrive in months. Third, no shared normative framework exists. Unlike nuclear weapons, where decades of doctrine produced concepts such as deterrence and non-proliferation, quantum has no equivalent vocabulary. This absence increases the likelihood of misperception during a crisis: a state may read a technical demonstration as a threat the demonstrating state does not intend.

> "The dual-use character of quantum technology makes transparency itself a strategic risk."

Beyond technical standards, there are early political signs. The United Nations General Assembly proclaimed 2025 the International Year of Quantum Science and Technology through Resolution A/RES/78/287, coordinated by UNESCO, which has explicitly recognized the quantum divide and emphasized capacity building in the Global South. But a year of awareness, however valuable, is not a governance regime. The institutional architecture that would translate political acknowledgment into operational coordination remains to be built.

WHY SELECTIVE COOPERATION REMAINS POSSIBLE

> "Even modest forms of cooperation can generate disproportionate gains."

Even amid intensifying competition, the case for cooperation is not naive. Quantum research depends on international talent, peer-reviewed publication, and supply chains that no single country controls; even as recent restrictions narrow that openness, these dependencies remain transnational. Rival states also share an interest in a stable digital environment: the financial system, government services, and health infrastructure they all rely on can be undermined by quantum-enabled attacks regardless of who launches them.

Selective cooperation is the pragmatic alternative to either uncritical openness or full decoupling. What makes it particularly relevant for quantum is the asymmetry between defensive and offensive uses of the same technology: defensive measures, like the migration to post-quantum cryptography, create mutual gains and demand cooperation now; offensive capabilities, like cryptanalytic tools, remain domains of strategic competition where states will not share. Selective cooperation accepts this asymmetry, concentrating governance effort where defensive cooperation can defuse offensive risks, and where the technical timeline permits action.

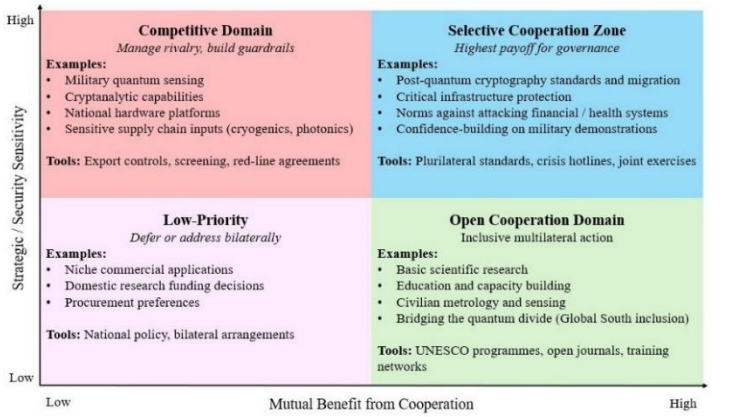

Figure 1. A framework mapping quantum policy issues by strategic sensitivity and mutual benefit from cooperation. The upper-right quadrant (where stakes are high but interests align) is where governance investment should concentrate. Author's framework.

Figure 1 maps this logic. The upper-right quadrant, where strategic stakes and mutual benefit are both high, is where governance investment yields the largest returns, and where this brief's recommendations concentrate. Framed in this way, selective cooperation aligns with broader principles of responsible innovation: anticipating risks before they materialize, including affected communities in governance, and remaining reflexive about which trade-offs are acceptable. The quantum field is still young enough that these principles can shape it, rather than being applied retroactively.

The barriers to selective cooperation are real, but they are not insurmountable. Trust between major powers is limited, and domestic politics often penalize leaders who appear to constrain national autonomy. Yet the cost of inaction is higher. A fragmented quantum landscape would produce systemic vulnerabilities that no single state could fix, weaken cybersecurity for everyone, and concentrate the benefits of quantum progress in the hands of a few advanced economies. Even modest forms of cooperation (technical, informational, and procedural) can generate disproportionate gains.

RECOMMENDATIONS

The current trajectory of quantum governance carries several risks: accumulating export controls that are hard to coordinate, plurilateral arrangements hardening into closed blocs, and the urgency of the cryptographic threat pushing states toward unilateral action. Yet opportunities are also emerging. These can be articulated through four recommendations.

1. Governments must accelerate the global migration to post-quantum cryptography.

In August 2024, the U.S. National Institute of Standards and Technology finalized the first three post-quantum encryption standards (FIPS 203, 204, and 205), with additional algorithms in the pipeline. These standards, the result of an open international process, provide the technical foundation for global adoption. The challenge now is no longer technical but coordinated implementation.

Migration in critical infrastructure (finance, energy, government communications) has been slow and progresses unevenly across countries. Governments should set binding migration deadlines for systemically important sectors, fund migration support for small and medium-sized enterprises, and coordinate with partners on three specific dimensions: synchronizing migration timelines across interdependent sectors (financial systems cannot migrate alone), ensuring interoperability between national implementations to avoid new fragmentation, and providing technical assistance to developing economies that lack the in-house expertise to migrate in time.

The global migration from DES to AES encryption in the 2000s showed that large-scale cryptographic transitions are feasible, but it unfolded over nearly a decade, a luxury current conditions do not allow. Delay is not neutral: every month of inaction extends the window for harvest-now-decrypt-later attacks, and coordination delays compound this risk for every state that cannot migrate alone.

2. States must build a plurilateral quantum supply-chain transparency mechanism.

Rather than racing toward full decoupling, which is costly, destabilizing, and probably impossible, states should build on the constellation of partners that has coordinated quantum export controls since 2024: the United States, the European Union, the United Kingdom, Japan, Canada, Australia, and the Netherlands. These states already share aligned threat assessments and compatible national controls.

The mechanism should extend this coordination in three ways: reciprocal information-sharing on chokepoint components (cryogenic systems, specialty photonics, isotopically pure materials), replacing unilateral announcements with structured exchange; shared early-warning on supply disruptions; and common licensing standards to lower compliance costs for firms operating across jurisdictions.

The mechanism should be designed from the outset to admit new participants who meet substantive criteria like

alignment on export-control implementation, adequate security clearances for shared information, and acceptance of common licensing principles. States likely to join over time include South Korea, Singapore and India, depending on their willingness to harmonize national practices. Without built-in openness, the mechanism risks reproducing the very fragmentation it aims to prevent. As the paralysis of the Wassenaar Arrangement shows, such a mechanism must be designed for evolution, not entrenchment.

3. States should establish, through a UN General Assembly process, a shared political understanding of what constitutes an unacceptable use of quantum capabilities against civilian infrastructure.

International humanitarian law already governs all means and methods of warfare. What is missing is not law but interpretation. States have not agreed on whether, for example, the pre-positioning of quantum decryption capabilities against the financial or health systems of another state constitutes a hostile act, an act of espionage, or routine intelligence collection. This ambiguity is itself destabilizing. In a crisis, one state's intelligence-gathering may be read as another's preparation for attack.

A political declaration should therefore do two concrete things: define a baseline category of civilian systems (hospitals, payment infrastructure, power grids) that states commit not to target with quantum-enabled disruption; and establish that the deliberate harvesting of encrypted civilian data for future decryption, while difficult to prohibit, will be treated as a hostile act when directed at these systems.

4. States should establish a UN Group of Governmental Experts on quantum risk terminology and confidence-building measures.

The most basic gap in quantum governance is not institutional but conceptual: rival states have no shared vocabulary for describing quantum risks. There is no agreed definition of what counts as a destabilizing capability, a hostile demonstration, or a defensive measure. This absence is dangerous because, in a crisis, states interpret ambiguous actions through worst-case assumptions.

A UN Group of Governmental Experts is the appropriate instrument precisely because it is modest. It does not require states to constrain their behavior, only to talk. The cyber experience is instructive: between 2004 and 2021, successive groups of governmental experts brought rival powers — including the United States, China, and Russia — to the same table and produced a shared baseline vocabulary, even as those states competed fiercely in cyberspace. The output was imperfect and non-binding, but it created reference points that later negotiations could invoke. A quantum equivalent is feasible because it asks little: a General Assembly resolution to convene it, and the willingness of states to define terms. It is the lowest-cost, highest-leverage entry point for quantum diplomacy, and it should include emerging economies from the outset, so that the vocabulary of quantum governance is not written solely by those who already hold the technology.

REFERENCES

Csenkey, K., & Bindel, N. (2023). Post-quantum cryptographic assemblages and the governance of the quantum threat. *Journal of Cybersecurity, 9*(1), tyad001.

Krelina, M. (2021). Quantum technology for military applications. *EPJ Quantum Technology, 8*, 24.

OECD. (2025). *A quantum technologies policy primer* (OECD Digital Economy Papers No. 371). OECD Publishing. https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/01/a-quantum-technologies-policy-primer_bdac5544/fd1153c3-en.pdf

Vaynman, J., & Volpe, T. A. (2023). Dual use deception: How technology shapes cooperation in international relations. *International Organization, 77*(3), 599–632.

World Economic Forum. (2024). *Quantum economy blueprint*. https://www3.weforum.org/docs/WEF_Quantum_Economy_Blueprint_2024.pdf

CENTRE INTERDISCIPLINAIRE
DE RECHERCHE SUR LA GOUVERNANCE
MONDIALE (CIRGoM)

Pavillon Charles-De Koninck
1030, avenue des Sciences humaines, local 2472B
Université Laval
Québec (Québec) G1V 0A6
cirgom@ulaval.ca

www.cirgom.ulaval.ca