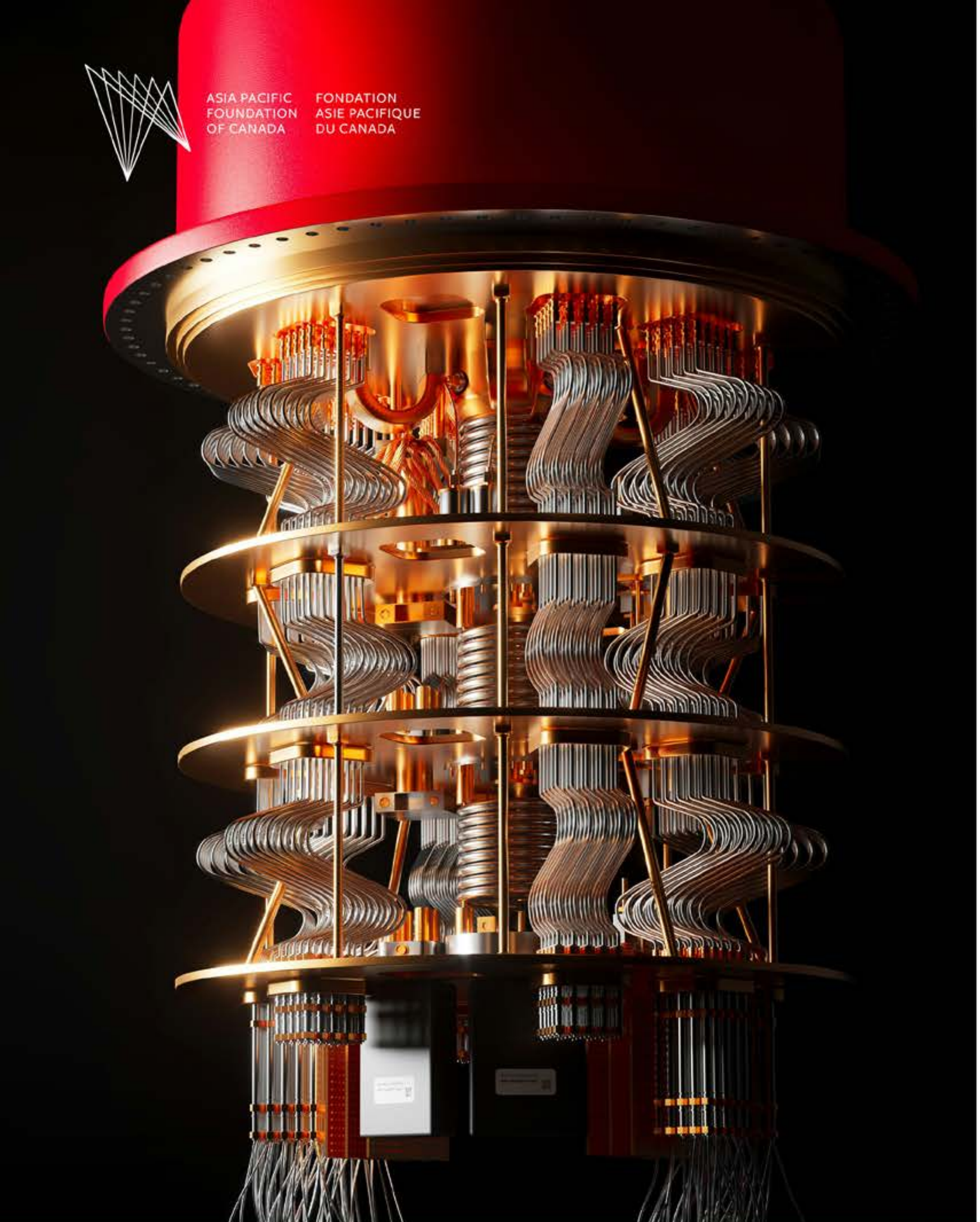
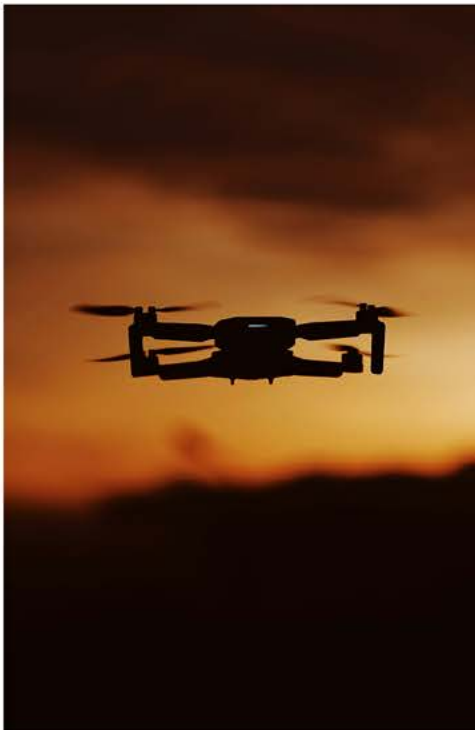




ASIA PACIFIC FOUNDATION OF CANADA
FONDATION ASIE PACIFIQUE DU CANADA

POLICY BRIEF 2: CANADA–SOUTH KOREA TECHNOLOGY SECURITY

Establishing Global Quantum Standards Through Collaboration

BY TAE YEON EOM

Introduction

This series of three policy briefs examines where technology and security meet in the Canada–South Korea relationship. It follows that intersection across three domains: artificial intelligence, quantum technology, and open-source software supply chain security.

The briefs arrive at a pointed moment. On July 6, 2026, Canada selected Germany's ThyssenKrupp Marine Systems as the preferred supplier for its landmark 12-submarine procurement program, moving past South Korea's Hanwha Ocean. The decision opened the next chapter in Seoul's strategy toward the Canadian defence market. Spanning AI, quantum technology, and cybersecurity, the two countries' technology partnership already extends well beyond the Canadian Patrol Submarine Project. It rests on habits of co-operation that no single contract can define or take away.

The first brief defines military AI through the lens of cognitive sovereignty. Control over the software layer dictates battlefield decisions. It proposes concrete mechanisms: a non-U.S. AI chip development alliance, jointly mandated open-architecture standards, a bilateral AI security testing exchange, and an Arctic-Pacific physical AI laboratory. Canadian research strength and South Korean industrial scale combine through these channels into a strategic asset.

The second brief turns to quantum technology. Canada's foundational science and South Korea's commercial deployment capacity form a natural complement. Quantum computing will eventually break today's encryption, exposing defence and financial communications now in transit. The brief charts a path toward a formally recognized Canada–South Korea quantum security standard, anchored in defence industrial benefit obligations. Together, the two countries can become architects of the global quantum standard as the technology matures.

The third and concluding brief confronts the exposed foundations beneath both AI and quantum efforts. Open-source software supply chains form the invisible infrastructure of this entire emerging security architecture. This critical foundation is already under attack. In June 2026, a North Korea-linked group breached 144 code packages in an 88-minute window, highlighting how fast a single point of compromise can cascade through allied systems. The brief calls for a Canada–South Korea federated threat-intelligence bridge, harmonized software bill-of-materials standards, and a joint red-team testbed to close that gap before the next breach outpaces detection.

Together, the three briefs offer a working blueprint for Canada–South Korea technology co-operation. The author is grateful to the officials, researchers, and practitioners across both countries who shared their time and insight. This research was made possible by the Korea Foundation's Policy-Oriented Research Program, with the Asia Pacific Foundation of Canada providing institutional support and serving as the trusted Canadian platform for carrying this co-operation forward.

These pages stand as a lasting intellectual asset, binding the technology security of both nations for years to come.

Establishing Global Quantum Standards Through Collaboration

Quantum Technology: An Operational Reality

In late 2026, the Canadian Space Agency will launch the Quantum Encryption and Science Satellite (QEYSSat), Canada's first quantum communications satellite. Built with Honeywell Aerospace, it will exchange quantum-encoded particles of light between a low-earth-orbit microsatellite and ground stations, establishing cryptographic keys that are physically impossible to intercept without detection. Canada and the U.K. have already committed, at the 2025 G7 summit in Kananaskis, to use this capability to build the world's first transatlantic quantum-secured communications link between Five Eyes allies. On the ground, the Business Development Bank of Canada's StrongNorth Fund, announced in May 2026, has invested in Photonic Inc. for distributed quantum computing and Lastwall for quantum-resistant identity security, both already deployed in defence and government operations. Canada's quantum industrial base is generating operational military value in the present tense.

South Korea is generating equivalent value in commercial markets. SK Telecom and Samsung's Galaxy Quantum smartphone series embed a Quantum Random Number Generator (QRNG) chip, producing truly unpredictable numbers from the behaviour of subatomic particles, to protect the financial transactions of millions of daily users. In May 2026, Canadian firm BTQ Technologies was selected as the post-quantum cryptography backbone for South Korea's first bank-led Korean-won stablecoin: a digital currency pegged one-to-one to the won and settled on a blockchain network, now secured with encryption designed to remain unbreakable even after quantum computers arrive. A Canadian firm is already protecting South Korea's regulated bank-led financial infrastructure.

At its core, quantum technology exploits the behaviour of subatomic particles to process an exponential number of possibilities simultaneously, creating machines capable of solving problems that classical computers cannot crack. Beyond defence and cryptography, that same capability is expected to accelerate drug discovery, optimize complex logistics and financial systems, and speed up the training of large AI models.

Taken together, the deployments described above define the threat that makes them necessary. The clearest documented example is the cluster of activity that the Five Eyes jointly attributed to People's Republic of China state-sponsored actors, who maintained long-term, undetected access inside telecommunications and critical infrastructure networks specifically to collect data for future use. That pattern, generalized, is what security researchers call "Harvest-Now-Decrypt-Later" (HNDL): collecting encrypted government, defence, and financial communications today, stockpiling them for decryption once a Cryptographically Relevant Quantum Computer (CRQC) is built, most likely in the 2030s. Cybersecurity experts observe that HNDL campaigns "leave no logs, signatures, or alerts." For Canada and South Korea, whose bilateral data flows span defence research, classified procurement, and financial intelligence, this is an ongoing operation.

Neither country possesses a complete quantum industrial base independently. Canada leads in foundational science, hardware architectures, and cryptographic standards. South Korea leads in manufacturing scale and commercial deployment. The bilateral relationship, elevated to a Comprehensive Strategic Partnership in 2022, has since deepened substantially. South Korean President Lee Jae Myung chose Canada as the destination for his first overseas trip after taking office, attending the G7 summit in Kananaskis in June 2025. Four months later, Canadian Prime Minister Mark Carney travelled to South Korea for the APEC summit in Gyeongju, where the two leaders launched the Canada-ROK Security and Defence Cooperation Partnership (SDCP), Canada's first such security partnership in the Indo-Pacific. The SDCP resolution explicitly names quantum computing, alongside AI and critical minerals, as a pillar of the partnership. In February 2026, a '2+2 Foreign' and Defence Ministerial Meeting in Ottawa signed the Agreement on Protection of Military and Defence Classified Information and confirmed inaugural bilateral cyber policy consultations for March 2026. These developments build directly on the Canada-Korea Joint Science and Technology Cooperation Committee (JSTCC), whose 2024–26 Joint Action Plan separately lists quantum technology, alongside AI and semiconductors, as a named priority area. What they share is scope, not funding: each commits both governments to a shared direction, but none yet attaches a budget line or an implementing agency to quantum technology specifically.

Two Quantum Industrial Bases, One Strategic Convergence

Both nations arrived at quantum technology through structurally distinct paths, each carrying vulnerabilities the other can remedy. Canada's quantum firms face chronic capital scarcity and exposure to U.S. extraterritorial export controls, creating a compelling rationale for sovereign scale-up partners outside the U.S. regulatory perimeter. On the other hand, South Korea absorbed sharp supply chain lessons when Japan imposed export restrictions on key semiconductor materials in 2019, and it entered the quantum era with a sector workforce of approximately 384 doctoral researchers in 2022, thin for a nation with industrial ambitions at scale.

CANADA: FOUNDATIONAL IP, VALIDATED BY THE PENTAGON'S MOST DEMANDING RESEARCH AGENCY

Canada's National Quantum Strategy (NQS) commits C$360 million over seven years across quantum computing, quantum communications, and post-quantum cryptography, and quantum sensing. The December 2025 Canadian Quantum Champions Programme (CQCP) Phase 1 distributes up to C$92 million to Anyon Systems, Nord Quantique, Photonic Inc., and Xanadu, anchoring intellectual property and talent within Canadian borders.

A quantum state, or qubit, resembles a glass bead shattering at the slightest vibration; quantum error correction wraps thousands of these fragile states in a structural cage, producing something closer to bulletproof glass.

The most authoritative external signal of Canada's hardware readiness came from the Defense Advanced Research Projects Agency (DARPA), the U.S. body whose past inventions include the internet (ARPANET), GPS, and stealth technology. DARPA strictly funds engineered realities and physical validations. Its Quantum Benchmarking Initiative (QBI) is the world's most rigorous public test of whether a fault-tolerant quantum computer can exist by 2033. A quantum state, or qubit, resembles a glass bead shattering at the slightest vibration; quantum error correction wraps thousands of these fragile states in a structural cage, producing something closer to bulletproof glass.

Clearing that bar is what allows a quantum processor to run long enough, and accurately enough, to stay useful for problems like drug discovery, materials design, and complex optimization instead of collapsing into noise after a few computational steps. QBI Stage B verifies that a company's blueprint for that cage is physically plausible. In November 2025, DARPA confirmed that three Canadian firms, Nord Quantique, Photonic Inc., and Xanadu, were among 11 companies globally to clear that bar. For any South Korean manufacturing partner evaluating Canadian quantum firms, the technical due diligence has already been conducted by the U.S. Department of Defense.

SOUTH KOREA: DELIBERATE CATCH-UP AT INDUSTRIAL SCALE

A March 2026 National Bureau of Asian Research analysis characterizes South Korea's approach as "the world's most aggressive transition from a latecomer to a manufacturing hub." Capital has followed conviction: from C$130 million (128.5 billion won) in 2024 to C$185 million (198.4 billion won) in 2025, a 54 per cent increase, with quantum elevated to a strategic priority within a C$5.6-billion (5.9-trillion won) 2026 ministerial portfolio centred on quantum-AI convergence.

South Korea's commercialization machinery engineers speed through structural separation. The Super-Gap Startup Project completely detaches commercialization capital from research budgets, forcing firms strictly to generate market revenues and commercial outcomes. The Unicorn Bridge Project applies further pressure: it admits 50 firms in their first year, then funnels only the strongest performers, the top 20, into a second year of funding, collapsing 60 per cent of entrants out of the programme based purely on market validation. Capital deployment here functions as a mechanism for industrial natural selection. The flagship quantum-classical hybrid hub at KISTI currently connects a U.S.-sourced IonQ Tempo 100-qubit quantum system to the KISTI-6 national supercomputer, meaning South Korea's most important research platform still depends on imported, mostly American, hardware (IBM and Rigetti are the other realistic Western suppliers) while domestic capabilities mature. That dependence is the structural opening that DARPA-validated Canadian technology now addresses: the two-year Xanadu-ETRI collaboration and D-Wave's Yonsei University partnership both point toward South Korea beginning to diversify its hardware sourcing toward Canada. Canadian firm D-Wave Quantum's June 2025 MOU with Yonsei University and Incheon Metropolitan City, supporting joint research and the acquisition of a D-Wave Advantage2 system for Yonsei's Songdo International Campus, confirms that Canadian quantum hardware is already entering South Korea's academic and industrial base through private-sector channels.

Security, Governance, and the Dual-Use Imperative

POST-QUANTUM CRYPTOGRAPHY: MIGRATION AS STRATEGIC CO-ORDINATION

Post-quantum cryptography (PQC) refers to a new generation of encryption algorithms designed to remain secure even against a quantum computer. It is the digital equivalent of changing every lock in a building before anyone has learned how to pick the new design. Canada's PQC migration is co-ordinated between the Canadian Centre for Cyber Security (CCCS) and Treasury Board Secretariat. It requires all federal departments to complete the transition to quantum-safe encryption by 2035, calibrated to the U.S. NIST timeline.

That calibration accelerated sharply in June 2026. The U.S. Department of War released its own PQC strategy, requiring every defence system to support quantum-safe encryption by December 31, 2030. Full, exclusive use follows by December 31, 2031, or the system is phased out. The strategy also draws a critical divergence: it explicitly excludes Quantum Key Distribution (QKD) as an approved confidentiality or authentication measure. South Korea's own PQC deployment, described above, runs partly on QKD.

The exclusion applies to U.S. national security systems specifically. It does not affect QKD's continued commercial viability in consumer and financial applications. But it signals an opening. Canada and South Korea have grounds to build a quantum-safe standard of their own, negotiated bilaterally and owned by both governments. Passive alignment with whichever framework the largest ally happens to certify is the default outcome absent that kind of proactive co-ordination.

A 2026 CIGI governance brief identifies this migration window as a governance tipping point: cryptographic standards embedded in critical infrastructure now will be technically and politically difficult to revise later. South Korea's PQC deployment, running from consumer smartphones to regulated financial infrastructure, provides exactly the production-scale template that Canada's migration strategy needs but currently lacks the manufacturing base to replicate independently.

DEFENCE APPLICATIONS OF QUANTUM TECHNOLOGY: SENSING THE UNSEEN

Quantum sensors offer military capabilities unavailable to any other technology. A quantum gravimeter measures gravitational pull with sub-millimetre precision; a quantum magnetometer detects electromagnetic signatures through hundreds of metres of seawater. Together, they give a submarine crew an accurate positional picture without emitting any signal, and without relying on GPS that does not penetrate ocean depth. Think of it as the ultimate battlefield noise-cancelling instrument: filtering everything except the faint metallic signature of an adversary hull or a seafloor pipeline, in total operational silence. Canada invested over C$161 million in 2026 to advance exactly these capabilities. The Canadian Patrol Submarine Project (CPSP), which in August 2025 shortlisted two suppliers, Hanwha Ocean of South Korea and TKMS of Germany, concluded its competition on July 6, 2026, when Prime Minister Carney named TKMS the preferred supplier. Hanwha Ocean remains the reserve supplier should negotiations with TKMS, expected to run six to eighteen months, prove unsuccessful. The Industrial and Technological Benefits (ITB) framework requires the winning contractor to generate equivalent economic activity in Canada, and that obligation can still be structured to mandate co-development and testing of Canadian quantum sensors within the platform.

Canada and South Korea also stand at the threshold of a multilateral opportunity they can only reach together. The AUKUS Quantum Arrangement (AQuA), the quantum working group under AUKUS Pillar 2, focuses on GPS-denied navigation, undersea quantum sensing, and quantum-secure communications: precisely the capabilities at the centre of Canada-Korea co-operation. South Korea's defence minister raised Pillar 2 participation at the Pentagon in late 2024; U.K. and Australian parliamentary committees have recommended extending Pillar 2 to Canada and South Korea specifically. A demonstrated bilateral track record in undersea quantum sensing and PQC standardization would give both countries the technical credibility that conversation requires.

Two asymmetries in this picture deserve direct comment. First, South Korea has pursued Pillar 2 access more visibly than Canada: Seoul's defence minister raised it personally in Washington, while Ottawa's engagement has so far run mainly through third-party recommendations alone. This is not necessarily a problem. Pillar 2 association is decided collectively by the three AUKUS members, not granted bilaterally, so Korea's advocacy does not crowd Canada out; if anything, a Korea that is already building the evidentiary track record this brief describes gives Canada a ready-made partner once Ottawa engages more assertively.

Second, Canada is simultaneously deepening separate bilateral quantum ties with the U.K. (the QEYSSat transatlantic link) and France (a May 2026 joint statement on quantum research co-operation), raising the question of whether this dilutes Canada's attention to Korea. The more likely effect runs the other way: each additional Canadian bilateral partnership extends the same allied standards architecture that Korea would otherwise have to join from outside, making Canada a more valuable bridge into the European Telecommunications Standards Institute (ETSI), the International Telecommunication Union (ITU), and AQuA. The real risk is dilution of Canada's limited programme budget across an expanding roster of bilateral partners. South Korea's interest is best served by insisting that concrete bilateral deliverables keep pace across all of Canada's quantum partnerships simultaneously, alongside the diplomatic statements that currently lead them.

QUANTUM GOVERNANCE: RESPONSIBLE TECHNOLOGY AS STRATEGIC POSITIONING

Quantum technology is inherently dual-use, and governance failures carry strategic costs. A quantum system that enhances undersea navigation for a Canadian submarine also enhances it for any navy that acquires the same technology. A post-quantum cryptographic standard adopted without allied co-ordination creates interoperability gaps at precisely the moment when interoperability matters most. Responsible quantum development, covering export control co-ordination, technology transfer protocols, and co-ordinated governance frameworks, is therefore a security interest in its own right.

Canada and South Korea are well positioned to lead on quantum governance jointly. The February 2026 Canada-ROK '2+2' Ministerial Meeting explicitly committed both governments to co-operation on cyber, technology, AI, and space security: the precise domains where quantum governance frameworks are most urgently needed. Canada's forthcoming Quantum Communications and Networking Demonstrator programme invites international expressions of interest; South Korean participation would extend the bilateral relationship from hardware and software into the governance and standardization layer.

The strategic value of that governance layer is more than procedural. Bilateral co-ordination on technology transfer protocols creates what functions as a regulatory safe zone, operating on a similar logic to the regulatory sandboxes used in AI governance, where firms test new approaches under temporary, government-defined rules before a full regulatory regime catches up. Here, the zone is a jointly defined protocol space within which Canadian and South Korean firms can co-develop intellectual property without triggering the unpredictable compliance liability that currently deters private-sector engagement. Government leadership in establishing this space is the precondition for private-sector innovation, since no individual firm can absorb cross-border regulatory risk on its own. Joint participation in ETSI and ITU standard-setting processes would then extend this bilateral safe zone into a multilateral architecture, positioning both countries as rule-writers in the global quantum governance order.

The same co-ordination logic extends to privacy regulation. Canada's Office of the Privacy Commissioner has already signalled that PQC standardization should trigger a reassessment of how organizations safeguard personal data, particularly the health, financial, and biometric records most exposed to harvest-now-decrypt-later collection. A bilateral Canada-Korea quantum working group should therefore seat privacy regulators alongside cryptography and export control officials. That composition would keep the technical migration to quantum-safe systems and the legal obligation to protect citizens' personal information moving on the same timeline.

Two Actionable Co-operation Models

MODEL 1 | TALENT AND STANDARDS: THE CANADA–SOUTH KOREA JOINT QUANTUM SECURITY FELLOWSHIP

South Korea's quantum capital injection cannot by itself produce foundational theorists. A KISTI analysis identifies talent development as the highest-priority investment subcategory precisely because foundational research capacity remains thin despite aggressive spending.

In January 2026, Mitacs, Canada's national research networking body, and South Korea's Quantum Information Research Support Center (QCenter) signed a Letter of Intent for researcher mobility exchange. Both governments should formally elevate this agreement into a Canada–South Korea Joint Quantum Security Fellowship, funding doctoral and postdoctoral placements that pair Canadian theoretical physicists with South Korean engineering and commercialization teams, and vice versa.

The fellowship should also mandate development of a joint SME adoption toolkit for PQC migration: a 2025 CIGI analysis identifies smaller organizations lacking internal cybersecurity capacity as the cohort most likely to fall behind without structured transition support. No market actor is positioned to provide that support at scale without government backing. The budget mechanism is in place; the required action is a decision to upgrade its scope and link it explicitly to the bilateral PQC standardization agenda.

The export control friction here operates as a licensing bottleneck. Under the U.S. Commerce Department's 2024 interim rule on quantum export controls, sharing controlled quantum technical data with a non-U.S. researcher, even informally, even inside a shared lab, counts as a 'deemed export' and can require a government licence before the conversation is legally permitted to happen. For a Canadian and a Korean physicist working together, this can turn a project that should take weeks to start into one that takes months, with civil or criminal liability if the paperwork is wrong. The Mitacs-QCenter fellowship mechanism reduces this risk because it operates through academic research channels that qualify for general licence exclusions under the rule, and personnel and educational exchanges between Five Eyes and treaty ally institutions sit at the centre of what those allied carve-outs are designed to facilitate. Formalizing the fellowship through the existing SDCP and JSTCC frameworks further anchors it within sanctioned allied co-operation.

MODEL 2 | INDUSTRY: SCALING THE QUANTUM KOREA 2026 ROUNDTABLE INTO STANDING INDUSTRIAL CO-OPERATION

On July 1, 2026, the day before Quantum Korea 2026 opened in Seoul, South Korea's K-Quantum International Cooperation Office convened a bilateral government dialogue and roundtable. The event brought together roughly forty officials, researchers, and industry representatives, including a Canadian delegation organized by Global Affairs Canada under the National Quantum Strategy.

The two sides reviewed existing co-operative efforts, including basic research funding through South Korea's National Research Foundation and Canada's Natural Sciences and Engineering Research Council. They also evaluated mission-oriented R&D via Canada's National Research Council and the Mitacs-QCenter talent exchange discussed in Model 1. Building on this foundation, participants agreed to expand toward corporate-level industrial co-operation. This expansion will leverage South Korea's Grand Manufacturing Challenge alongside the Eureka and Eurostars joint R&D frameworks to increase firm and industry-association involvement.

The immediate task is to institutionalize this preliminary agreement into a funded, recurring mechanism. Concretely, Canada and South Korea should establish an annual Canada-Korea Quantum Industrial Cooperation Track, co-chaired by ISED and MSIT. This track requires two standing features. First, a matching fund will allow Canadian quantum SMEs to bid into South Korea's Grand Manufacturing Challenge upon its 2027 launch. Second, a reciprocal channel will enable South Korean quantum manufacturers to access Eureka and Eurostars-eligible Canadian projects.

BTQ Technologies' participation in the July 1 roundtable illustrates the pattern already at work. One day later, BTQ's French subsidiary-in-acquisition, QPerfect, launched its quantum emulator as a paid commercial service inside QuREKA, the hybrid quantum cloud platform operated by South Korean firm SDT, giving South Korean research institutions and enterprises direct cloud access to Canadian-owned quantum software. Individual companies are already using these government-convened venues to close bilateral deals; the missing piece is a standing institutional channel that does not depend on either government re-convening a roundtable each time a new opportunity arises.

The Standard-Setter Thesis

Canada and South Korea enter the quantum decade as standard-takers. Both are close U.S. allies whose quantum budgets trail Washington and Beijing by an order of magnitude. Both remain outside the core of AUKUS, the most consequential allied technology partnership of this era. Both absorb cryptographic norms, hardware architectures, and governance frameworks that larger players negotiate among themselves.

> **Such countries dictate terms; such countries shape the architecture.**

Bilateral quantum co-operation functions as the precise mechanism through which two capable democracies construct the evidentiary base for geopolitical centrality. Concretely, that means three things: a bilaterally developed PQC standard formally adopted by ETSI or the ITU; a Canadian-built sensor validated and fielded on an allied naval platform; and demonstrated participation in AQuA. These are the markers that separate a standard-setter from a standard-follower, and they are achievable on the timelines this brief has set out. Countries that arrive at multilateral technology negotiations holding these kinds of active bilateral deployments, joint governance standards, and validated defence applications carry a fundamentally different weight than countries arriving with only ambitions and a funding announcement. Such countries dictate terms; such countries shape the architecture.

Consider the Canada–South Korea bilateral relationship in 2030 if the two models proposed here are implemented. Canadian quantum error correction operates as the reference architecture for allied post-quantum systems. A quantum magnetometer, validated on a Korean-designed submarine hull under Canadian ITB obligations, commands evaluation by AQuA member states. The Mitacs-QCenter fellowship routinely produces researchers holding DARPA-validated engineering intuitions and Korean-scale commercialization experience simultaneously. The joint SME adoption toolkit has helped hundreds of Canadian and Korean firms complete their PQC transitions without regulatory exposure. Neither country can produce this reality alone.

Whether formal AUKUS Pillar 2 association follows will also depend on political decisions in Washington, London, and Canberra. But Canada and South Korea, having done the work, would bring a concrete portfolio of deliverables to that conversation: a fielded sensor, a jointly adopted cryptographic standard, and a functioning researcher exchange. The regulatory safe zone that bilateral governance co-operation creates will have lowered the barriers that currently prevent private firms from engaging fully, accelerating the commercial and defence deployments that make the diplomatic case self-evident. Quantum Korea 2026 in Seoul, which closed on July 4 with a dedicated Canadian national pavilion and a formal bilateral roundtable already on the record, has already supplied the opening move this brief called for. What it has not yet supplied is the standing institutional follow-through: a commercialization fund, a PQC working group with privacy regulators at the table, and an industrial co-operation track that survives past the week the conference tents come down.

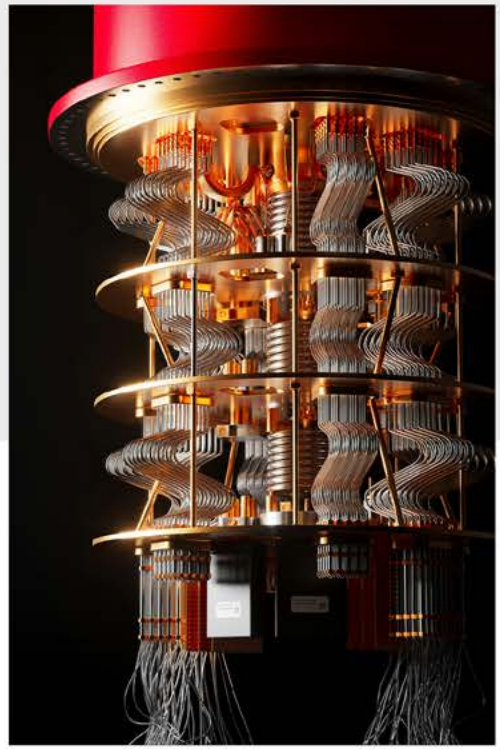
Ottawa and Seoul spent that week demonstrating intent. The remainder of 2026 will show whether either government is prepared to fund it.

Ottawa and Seoul spent that week demonstrating intent. The remainder of 2026 will show whether either government is prepared to fund it.

ACKNOWLEDGMENTS

The author is grateful to the many practitioners, officials, researchers, and industry leaders across Canada and South Korea who generously gave their time and candour over the course of this research. Most requested anonymity; their perspectives and insights are present throughout these pages, even if their names are not. The analysis, conclusions, judgments, and any errors that remain are entirely those of the author.

This brief is in a series produced with the support of funding from the Korea Foundation.



ASIA PACIFIC
FOUNDATION
OF CANADA

FONDATION
ASIE PACIFIQUE
DU CANADA