WHITE PAPER

The Post-Quantum AI Telecom Operator

A new category of telecommunications provider, designed to be quantum-safe from the start, intelligent by design, and delivered as a programmable platform rather than a legacy network.

PUBLISHED
November 2026 · Version 1.8

CATEGORY
Secure Telecom Infrastructure

AUTHOR
Q-M Networks Inc.

CONTACT
bgrisdale@qmnetworks.ca

EXECUTIVE SUMMARY

Telecom's security foundation is being rewritten.

Many operators will find it difficult to move fast enough.

Mobile networks have become critical national infrastructure. They carry the authentication, payments, health, energy, and government traffic that modern economies depend on, and they are protected by public-key cryptography that a sufficiently capable quantum computer is expected to break.

The threat does not wait for that machine to arrive. Encrypted traffic can be intercepted and stored today to be decrypted later, an attack pattern security agencies call “harvest now, decrypt later”. Data that must remain confidential for a decade deserves protection now.

Standards bodies and governments have responded. In August 2024 the U.S. National Institute of Standards and Technology (NIST) finalized its first post-quantum encryption standards. Its October 2026 transition report (NIST IR 8547) sets 2030 and 2035 as the dates after which today's quantum-vulnerable public-key schemes are deprecated and then disallowed. Canada has published a federal migration roadmap with deadlines running to 2035.

The challenge is structural. Established carriers run large, long-lived core and billing systems that were not designed for rapid cryptographic change, and migrating them is expected to be a multi-year program layered on top of live networks.

Q-M Networks is taking a different path. We are building a cloud-native mobile operator without a legacy core to migrate, designed to combine quantum-safe security, AI-driven network intelligence, and platform-based service delivery from the outset. Q-M Networks is pre-commercial; this paper describes our architecture and market thesis.

It sets out the category we are building, the four capabilities that define it, the deployment model, and why Canada is a natural first market.

2024

First NIST post-quantum encryption standards finalized

2030 → 2035

NIST deprecates, then disallows, today's quantum-vulnerable public-key schemes (NIST IR 8547, Oct 2026)

2031 → 2035

Canada's federal migration milestones for high-priority, then remaining, systems

By design

Security built into the architecture rather than added later

> **Credibility comes from assurance, not slogans: moving quickly while keeping auditability and governance discipline.**

01 · A NEW CATEGORY

Not another MVNO. A secure digital infrastructure platform.

Traditional mobile operators compete on coverage, price, and handsets. Q-M Networks is designed to compete on a different axis: a network that is built for the quantum era, intelligent about its own data, and programmable like software.

We call this category the Post-Quantum AI Telecom Operator, defined by four capabilities engineered together from the outset rather than added over time. Each exists individually in the market; integrated into a single operator, they are intended to compound into a differentiated architecture.

01

Cloud-native telecom core

A software-defined mobile core and voice stack designed to launch services in a fraction of the time and cost of hardware-heavy infrastructure. No towers, no spectrum lock-in.

02

Quantum-safe security

Post-quantum protection designed for the layers Q-M Networks operates and controls: subscriber authentication, call and messaging signalling, data sessions, and back-office operations. Scope and limits are set out in Section 03.

03

AI-driven network intelligence

Operational and behavioural data treated as a live asset: predictive analytics, automated revenue optimization, and personalized services.

04

Platform-based delivery

Modern service orchestration (billing, provisioning, activation, partner ecosystems) that lets organizations deploy telecom the way they deploy software.

The reframing that matters. This moves the MVNO from reseller of someone else's network to Telecom Platform Provider. The unit of value is no longer a SIM sold at a margin; it is a secure, programmable network that enterprises, governments, and industries can deploy and operate as a service. Q-M Networks goes to market as a full MVNO that runs its own core network on a host operator's radio access. The core is designed to operator grade, so the same architecture can extend to operators that want to run it themselves.

02 · WHY THE INDUSTRY IS READY

Three structural shifts have arrived at once.

1 · Security has become a sovereignty question. Telecom networks are treated as critical national infrastructure. Governments and enterprises increasingly expect communications that resist today's cyber attacks and future quantum decryption. With “harvest now, decrypt later” in play, the clock has already started, and quantum-safe protection is becoming a procurement expectation.

2 · Data has become the core telecom asset. Operators hold enormous volumes of behavioural and operational data, much of it underused. Treating the network as a data-intelligence system, not just a pipe, supports predictive customer analytics, revenue optimization, personalized services, and sharper operational insight.

3 · Infrastructure has become software. Telecom is moving decisively toward cloud-native architectures. A software-defined core allows new services to be stood up rapidly, without the capital intensity and integration cycles of traditional hardware.

The policy context. Canada's federal post-quantum roadmap frames the threat as immediate, assigns lead authorities, and sets migration deadlines. The question has shifted from “whether to move” to “how to move quickly while keeping governance discipline.” The same urgency is visible in the United States, where NIST's October 2026 report supports accelerated federal deadlines of December 31, 2030 for post-quantum key establishment and December 31, 2031 for post-quantum signatures on the most sensitive systems.

Recent policy momentum

DEVELOPMENT	SOURCE
Critical Cyber Systems Protection Act receives Royal Assent (June 2026, Bill C-8), covering finance, telecommunications, energy and transportation	Public Safety Canada
Canada joins the G7 Cybersecurity Working Group call to action on preparing for the post-quantum era	Cyber Centre
Quantum Safe Technologies Initiative for critical sectors including defence, finance, telecommunications, health and transportation, 2026 to 2028	National Research Council
Policy direction on migrating Government of Canada systems to post-quantum cryptography in effect Oct 9, 2025; departmental migration plans due April 1, 2026, with post-quantum clauses in new contracts that have a digital component	Treasury Board Secretariat
NIST IR 8547, Transition to Post-Quantum Cryptography Standards (October 2026): quantum-vulnerable public-key schemes deprecated after 2030 and disallowed after 2035; names “harvest now, decrypt later” as the reason key establishment is urgent	NIST

Reference: NIST finalized FIPS 203 (ML-KEM), FIPS 204, and FIPS 205 in August 2024. NIST IR 8547 (October 2026) supports U.S. Executive Order 14412 and OMB Memorandum M-26-15 and states that NIST's existing symmetric-key standards are significantly less vulnerable to known quantum attacks than public-key cryptography. Canada's migration roadmap (Canadian Centre for Cyber Security, ITSM.40.001) sets departmental planning in 2026, high-priority system migration by 2031, and remaining non-classified systems by 2035.

03 · THE PLATFORM ARCHITECTURE

A programmable telecom stack, layer by layer.

The platform is organized as a layered stack. Each layer is designed to be independently sound and standards-aligned; combined, they form a programmable, quantum-safe telecom network.

LAYER 6

Application & Services

Enterprise mobile networks, private MVNOs, IoT connectivity, secure government communications, digital identity.

LAYER 5

Data Intelligence

AI analytics turning network and subscriber data into predictive, revenue, and operational insight.

LAYER 4

Service Orchestration

Modern OSS/BSS: billing, provisioning, activation, and partner ecosystem management.

LAYER 3

Quantum-Safe Security

Post-quantum protection designed to span the Q-M Networks-operated layers above and below it (Layers 2 to 6).

LAYER 2

Telecom Core

Cloud-native voice, messaging, and subscriber services, designed for standards-compliant interconnection.

LAYER 1

Network Access

Wholesale radio access from host mobile network operators under regulated MVNO access regimes.

Because security is designed into the stack rather than retrofitted onto it, the architecture is intended to protect subscriber authentication, call and messaging signalling, data sessions, and back-office operations alike, with no legacy core to migrate.

How protection works across networks. Q-M Networks runs its own core network, so protection does not depend on the transport beneath it. A device registered to a Q-M Networks core is protected end to end when it communicates with any other registered device on any connected core, whether those cores belong to different companies, sectors, or countries. The cellular network, spectrum, and towers of a host operator, or any other transport, carry that traffic without being part of its security. Where traffic leaves the Q-M Networks federation to a device that is not registered, protection ends at that boundary. Within the federation it remains encrypted all the way to the registered end device. Host operators may still observe network-level information such as attachment events.

Why end to end matters. Many solutions protect data only as far as the enterprise or service perimeter. Beyond it, content is decrypted on platforms run by third parties, often foreign, which can place the content of government communications such as calls, recordings, and transcripts within reach of those providers. Q-M Networks is designed to keep protection in place from device to device, so that the content, not just the network it travels over, remains under customer and Canadian control.

Cryptographic approach (design intent). The architecture is designed around quantum-safe key agreement and symmetric-key protection, with crypto-agility so that methods can be updated as standards evolve. NIST's October 2026 report states that its existing symmetric-key standards are significantly less vulnerable to known quantum attacks than public-key cryptography and that it does not expect to need to transition away from them (at 128-bit security and above; NIST will disallow the few 112-bit standards in 2030). Detailed specifications are available under NDA.

Telecom as a Service. The same stack, delivered as a service, lets an organization deploy a network the way it deploys an application: choose capabilities, provision, and go live, with security, intelligence, and orchestration included by design. This is the mechanism that turns “an operator” into “a platform.”

04 · THE DEPLOYMENT MODEL

From a consumer network to sovereign federations.

One platform, five tiers of deployment, each designed to extend the secure perimeter outward, from a public mobile network to encrypted communication across organizations and nations.

1

Public MVNO Core

Quantum-safe-by-design mobile communications over the public network, extending protection to the network edge for consumers and small businesses.

2

Private Node

Enterprises and governments deploy a private node intended to cover the IP-addressed devices in their environment (servers, containers, gateways, and VPN appliances), not just handsets.

3

Container / Subnode Federation

Departments, contractors, and subsidiaries are segmented into subnodes for granular access control within a single organization.

4

Cross-Organization Sovereign Federation

Independent organizations form a federation designed to support end-to-end encrypted communication across organizational boundaries.

5

International Platform Licensing

The platform architecture is intended to be licensed to operators, governments, and allied and government networks, extending sovereign, quantum-safe communication across borders.

The same core capability, quantum-safe key management applied to a cloud-native network, is designed to scale from a single subscriber to an international federation without rebuilding the architecture. That scalability is what makes the model a platform rather than a product.

05 · MARKET OPPORTUNITY

Compliance-driven demand that is only beginning to be served.

Near-term markets are being created by regulation and risk. Any organization with data that must stay confidential for a decade, and any buyer facing a post-quantum compliance obligation, is a potential customer for a network designed to be quantum-safe.

Enterprise MVNO platforms

Logistics, transportation, retail, and industrial firms seeking direct control of secure mobile connectivity.

Government secure communications

Emergency services, public-sector networks, and digital sovereignty programs.

Industrial & private networks

Energy, mining, utilities, transportation, and manufacturing deploying private connectivity for operational technology.

IoT connectivity platforms

Large device fleets needing secure connectivity, lifecycle management, and analytics-driven services.

Architectural posture: purpose-built versus retrofit

DIMENSION	RETROFIT OF AN ESTABLISHED NETWORK	PURPOSE-BUILT PLATFORM (Q-M NETWORKS DESIGN INTENT)
Security architecture	Cryptographic change layered onto live systems	Quantum-safe protection designed in from the start
Migration effort	Multi-year program expected	No legacy core to migrate, by architecture
Operations & billing security	Addressed system by system	Designed as part of one orchestration layer
Compliance enablement	Dependent on program completion	Designed to support customer assurance requirements

Illustrative comparison of design approach, not a statement about any specific carrier. Q-M Networks is pre-commercial and capabilities described are design objectives.

06 · STRATEGIC VALUE & SOVEREIGNTY

Why Canada is a natural first market.

Canada has treated quantum safety as a matter of timely execution, which creates room for operators that can contribute now.

Canada's approach has been to name the risk, coordinate centrally, set timelines, and invest in the industrial base. Federal departments face concrete migration deadlines, and public investment in the quantum ecosystem is scaling.

A regulated wholesale MVNO access regime is in place, giving new operators a defined path to network access. The structural prerequisite for a new entrant exists; the differentiator is what that entrant brings.

Mandated migration timelines, an established access regime, and a sector that is only beginning to adopt quantum-safe network infrastructure make for a timely opening. Launching here can help make Canada the home of a next-generation telecom platform, strengthening digital sovereignty, cybersecurity capability, and exportable technology.

The same logic extends to allied and government partners. European priorities in cybersecurity, digital infrastructure, AI, and telecom modernization align with the platform, opening collaboration and technology-export pathways.

Sovereignty goes beyond the network. Keeping protection in place from device to device is designed to keep the content of government communications under Canadian control, including where it passes through third-party platforms.

The defensible posture. Where urgency can lead vendors to overstate “quantum safe”, credibility comes from assurance. Q-M Networks aims to help customers and governments move quickly without pretending the governance problem is already solved, with auditability, standards alignment, and assurance built in.

07 · THE LONG-TERM VISION

The software platform that powers telecom networks.

The long-term objective is not to own towers or spectrum. It is to become the secure, intelligent software platform on which others build and operate their own telecom networks.

Just as cloud platforms turned computing infrastructure into a programmable service, Q-M Networks aims to turn telecommunications infrastructure into a programmable, quantum-safe service layer. In that model, telecom operators become platform partners, enterprises become network operators, and infrastructure becomes software-defined, with security and intelligence provided by design rather than assembled by each customer.

> **A next-generation operator at the intersection of telecom infrastructure, cybersecurity, artificial intelligence, and digital platforms.**

08 · WHERE WE ARE TODAY

An early-stage company with the foundations in place.

Q-M Networks is pre-commercial. This page sets out where the company stands so that readers can judge the thesis against the work done to date.

AREA	STATUS
Company	Federally incorporated (CBCA) in March 2026 and based in Alberta.
Stage	Pre-commercial. Capabilities described in this paper are design objectives.
Licence	ISED non-competitive local licence as a Radiocommunication Service Provider.
Go-to-market	Enters the market as a full MVNO running its own core network on a host operator's radio access. The core is designed to operator grade.
Intellectual property	Patent-pending portfolio covering the core inventions, assigned to the company.
Funding & ecosystem	ElevateIP Alberta participant (2026), supporting prosecution of the patent portfolio as conversion begins. Corporate member of Quantum City at the University of Calgary.
Network build	Core network partner in place. Target: a running core at Mobile World Congress, Barcelona, in March 2027. This is a target, not a commitment.
First deployment	A first community deployment in Alberta is in development.
Federal engagement	Technical discussions with the Canadian Centre for Cyber Security, and participation in federal post-quantum industry events.

Topics we would value a funding adviser's view on. Protecting and prosecuting our intellectual property internationally; funding the build of the first running core network and the first community deployment; fit with research and development tax and innovation programs; and fit with federal and defence challenge-based programs for sovereign technology.

Organization: Q-M Networks Inc. (CBCA, incorporated March 2026)
Document: White Paper · November 2026 · Version 1.8
Contact: Brent Grisdale, Founder & CEO · bgrisdale@qmnetworks.ca · 587-896-4312 · qmnetworks.ca

This white paper is a strategic overview provided for informational purposes. It describes an architectural approach and market thesis and does not constitute an offer of securities, a technical specification, or a guarantee of future performance. Q-M Networks Inc. is pre-commercial; capabilities described are design objectives. Standards and regulatory references reflect publicly available information as of the publication date. “Quantum-safe” describes an architecture designed to resist anticipated quantum-computing threats using post-quantum and symmetric-key cryptographic methods; no cryptographic system should be represented as unconditionally unbreakable. References to NIST publications describe NIST's published positions and do not imply NIST review or endorsement of Q-M Networks. Q-M Networks Inc. holds an ISED non-competitive local licence as a Radiocommunication Service Provider.