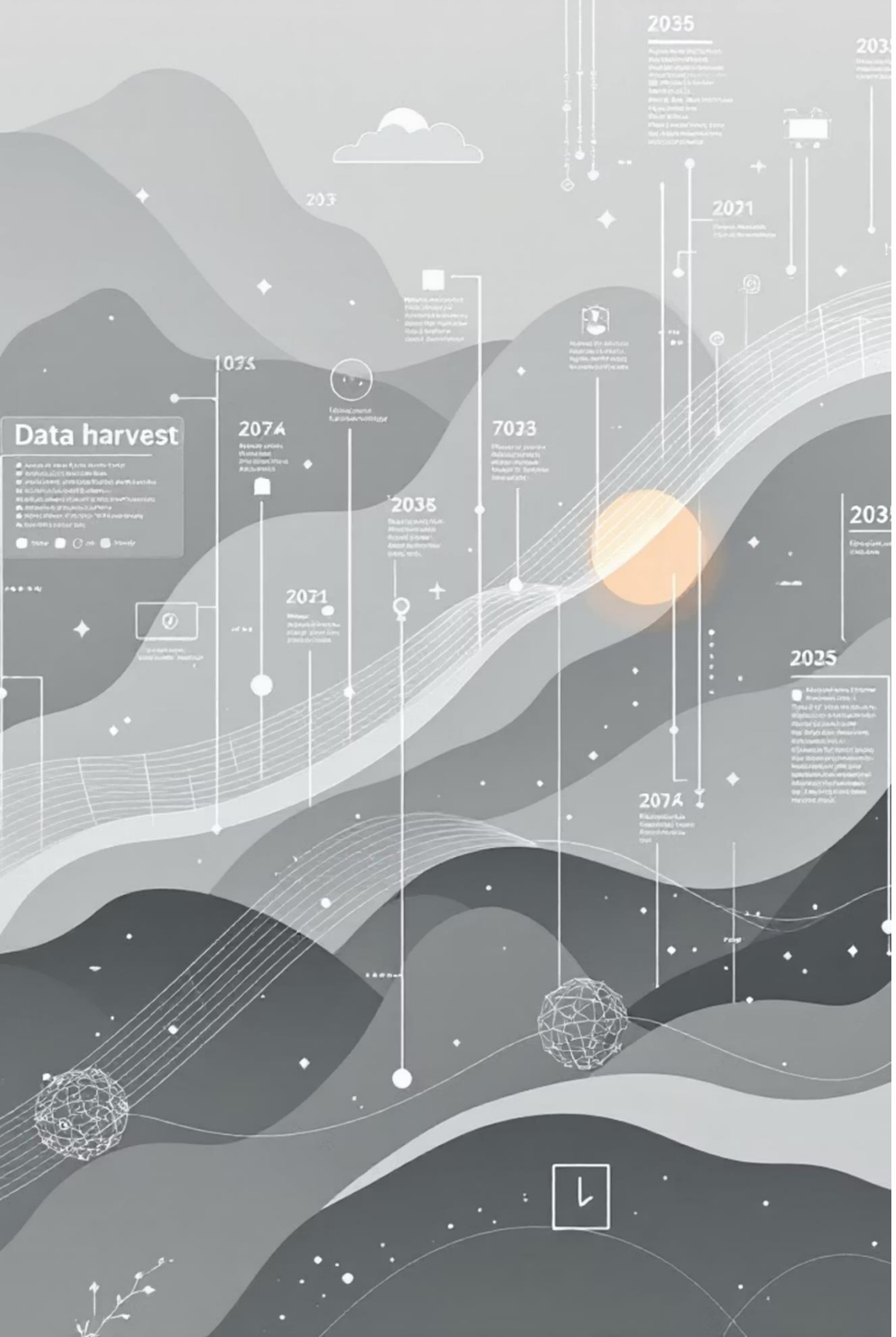
Securing Robot Networks for the Quantum Era

The robots we deploy today will face the quantum computers of tomorrow. Quantum threats are real, and robotics is the next frontier of security.

Nehal Singh, Netskope Inc. USA



Why Quantum Matters Now

Breaking Encryption

Quantum computing can break classical encryption like RSA and ECC using Shor's algorithm.

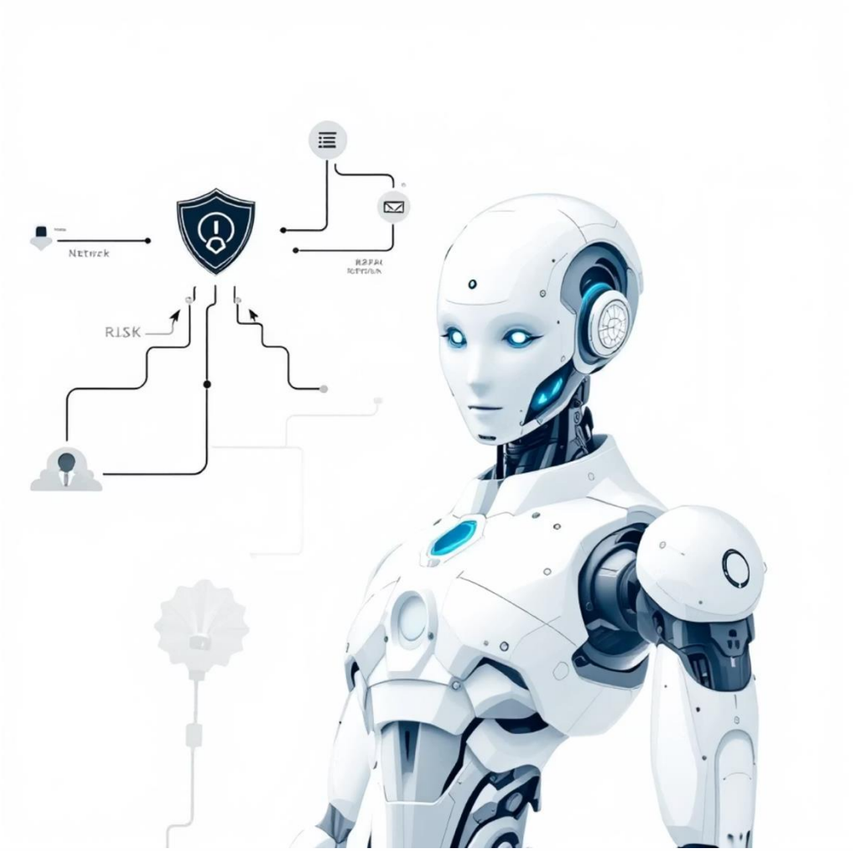
Harvest-Now, Decrypt-Later

Attackers are already collecting encrypted data to decrypt once quantum computers arrive.

Long-Lived Robot Data

Robots store sensitive operational data, firmware, and telemetry for years—making them prime targets.

The Robotic Network Attack Surface



Critical Exposure Points

- Control & telemetry channels
- Firmware & OTA updates
- Inter-robot communication
- Cloud integration endpoints
- Sensor data and command authentication

Each layer introduces potential compromise points with physical-world consequences.

The Quantum-Safe Toolkit

Post-Quantum Cryptography (PQC) provides algorithms resistant to quantum attacks. NIST-standard picks include Kyber for key encapsulation and Dilithium for digital signatures.

Kyber (KEM)

Lattice-based key encapsulation mechanism for secure key exchange.

Dilithium (Signatures)

Digital signature algorithm for authentication and integrity verification.

Ready Today

PQC libraries exist and are testable for implementation now.

Bridging the Gap with Hybrid Models

Classical Crypto

Existing RSA/ECC systems maintain compatibility.

Combined Layer

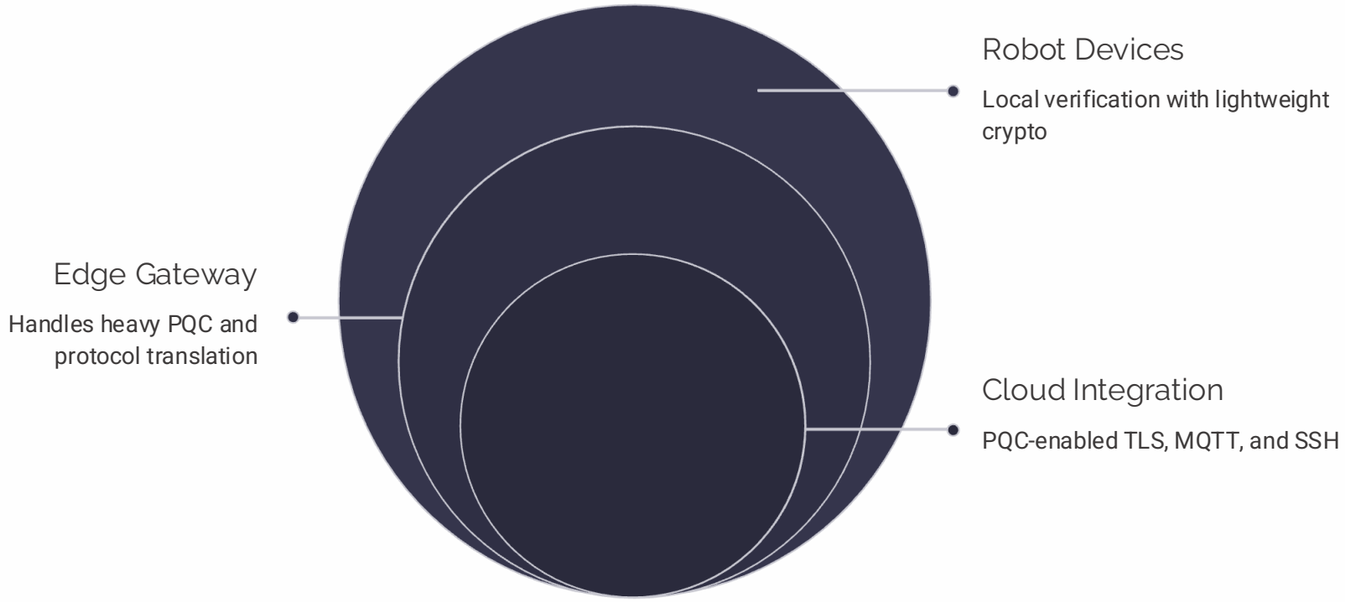
Hybrid approach runs both algorithms in parallel.

PQC Protection

Quantum-safe algorithms provide future resilience.

Hybrid cryptography enables smooth migration without breaking existing systems. Start with hybrid TLS/SSH for robotic communications to reduce risk while maintaining backwards compatibility.

Architecting Quantum-Safe Robot Networks



01

Robot Layer

Local verification with lightweight crypto operations.

02

Edge Gateway

Handles heavy PQC cryptography and protocol translation.

03

Cloud Integration

PQC-enabled TLS, MQTT, and SSH ensure end-to-end encryption.

04

OTA Updates

Secure firmware signing with Dilithium-based certificates.

Zero-Trust Meets PQC

Zero-Trust Principles

Never trust, always verify. Every access request is authenticated, authorized, and encrypted regardless of location.

- Continuous device authentication
- Least privilege access control
- Behavioral telemetry monitoring
- Policy-based trust decisions

PQC Strengthens Identity

Post-quantum cryptography reinforces the identity layer with quantum-resistant authentication.

Operational Roadmap

Cryptographic Inventory

Audit all encryption points across your robotic systems.

Prioritize Risk

Protect firmware and command channels first.

Pilot Hybrid TLS

Test gateway-cloud communications with hybrid cryptography.

Hardware Readiness

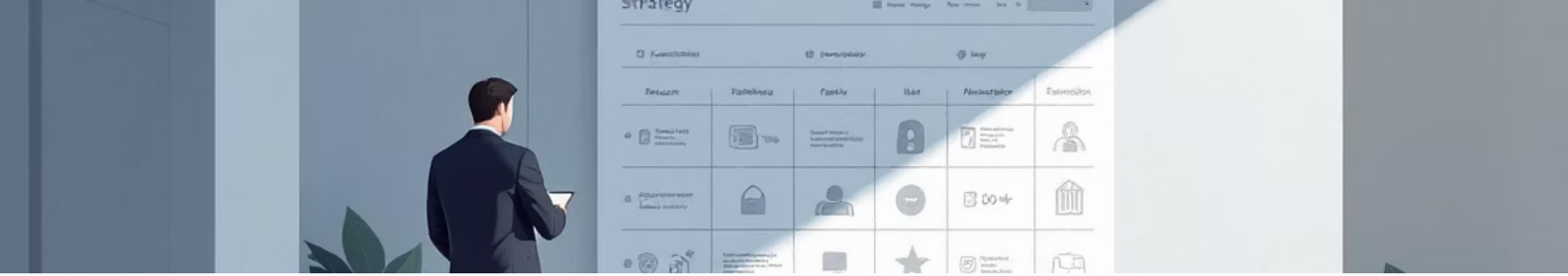
Verify HSM/TPM firmware compatibility and performance.

Measure Performance

Track latency, handshake success, and system impact.

Document Governance

Establish incident handling and compliance procedures.



Risk Mitigation & Lessons Learned

Algorithm Substitution

Enforce fixed PQC policy to prevent downgrade attacks and unauthorized crypto changes.

Legacy Crypto

Wrap or sandbox legacy systems before full replacement to maintain security during transition.

Vendor Dependency

Choose PQC-ready toolchains and maintain crypto agility with modular APIs.

Implementation Errors

Third-party validation is essential—independent audits catch critical vulnerabilities.

Quantum Resilience Starts Today

1 Inventory

Conduct a complete cryptographic audit of your robotic systems.

2 Pilot

Test hybrid PQC implementations in controlled environments.

3 Policy

Establish governance frameworks and incident response procedures.

> *"The best time to secure your robots was yesterday—the next best is today."*

Join open-source PQC and robotics security communities to stay ahead of quantum threats.