TQS
EXECUTIVE
INTELLIGENCE

Europe and the Quantum Horizon

Readiness, Risks & Roadmaps for Europe's Quantum Future

August 2025

Text

THE QUANTUM SPACE

EUROPE AND THE QUANTUM HORIZON

Readiness, Risks & Roadmaps for Europe's Quantum Future

August 2025

TQS Executive Intelligence
Produced & Edited by The Quantum Space
c/o Krowne Communications GmbH, Kufürstendamm 194, 10629 Berlin, Germany

Contents

Forward from The Quantum Space	05
Executive Intelligence Briefing	06
The Strategic Quantum Threat Landscape	08
Europe's Quantum-Safe Roadmaps	10
SECTOR INTELLIGENCE: Government ID Systems	13
SECTOR INTELLIGENCE: Financial Services	16
SECTOR INTELLIGENCE: Industrial & Automation Systems	19
SECTOR INTELLIGENCE: Military & Defense	22
Comparative Roadmap Matrix	25
References	29
About The Quantum Space	31

Forward from The Quantum Space

In the quantum era, time is no longer a neutral factor — it is a compounding risk vector. Every day that Europe's critical systems remain tethered to cryptographic methods vulnerable to quantum attack, adversaries gain opportunities for Harvest Now, Decrypt Later operations. These risks are not speculative; they are advancing on a timeline already visible in research labs and national roadmaps.

The Quantum Space exists to illuminate these converging technological and geopolitical currents. Our mission is to equip Europe's technology leaders — from CTOs steering global infrastructure to compliance officers safeguarding regulated industries — with the strategic clarity and technical precision necessary to act before systemic vulnerabilities crystallise.

This report is built upon an extensive integration of European Commission directives, sector-specific readiness analyses, and global policy trends. It moves beyond the general "quantum threat" narrative to deliver sector intelligence in four domains:

- Government Identity Systems
- Financial Services & Banking
- Industrial & Automation Infrastructure
- Military & Defence Assets

The chapters that follow are designed to be both actionable and anticipatory — blending current readiness assessments with forward-looking risk models and strategic recommendations. Every insight has been filtered through the lens of digital sovereignty, because the ability to own and secure Europe's cryptographic future will define our resilience in the quantum age.

In the years ahead, Europe's competitive edge will hinge on crypto-agility, accelerated adoption of post-quantum standards, and the seamless integration of quantum-safe systems across both civil and defence networks. The leaders who can navigate this transition decisively — without sacrificing interoperability, compliance, or operational performance — will set the standard for resilience in the 21st century.

The quantum clock is ticking. The time to prepare was yesterday. The time to act is now.

Executive Intelligence Briefing

Purpose & Scope

This report provides a strategic readiness assessment of Europe's capacity to secure critical sectors against quantum-enabled cyber threats. It consolidates government policy, sectoral initiatives, and technology developments into a single operational picture designed for Chief Technology Officers (CTOs), Chief Information Security Officers (CISOs), and compliance leaders tasked with safeguarding high-value data and infrastructure.

The scope spans four strategic domains:

1. Government Identity Systems
2. Financial Services
3. Industrial & Automation Infrastructure
4. Military & Defence Assets

Each domain is analysed for readiness level, regulatory drivers, industry positioning, and strategic gaps, with actionable recommendations to inform both short-term mitigation and long-term investment.

Key Findings

1. The Threat Is Accelerating Faster Than Policy Cycles

- The probability of a cryptographically relevant quantum computer (CRQC) emerging by 2035 is between 19–50% depending on the model used.
- This compresses the migration window for post-quantum cryptography (PQC) in sectors with long asset lifecycles, such as government-issued IDs, industrial control systems, and defence platforms.

2. Europe's Readiness Is Uneven Across Sectors

- Financial services: Partial readiness — Tier-1 banks and central banks have pilot PQC/QKD programs, but smaller institutions lag significantly.

- Government ID systems: Moderate readiness — hardware vendors are building crypto-agility into new secure elements, but reissuance cycles create decade-long exposure windows.
- Industrial automation: Low readiness — PQC is not yet embedded in IEC 62443 frameworks, leaving OT/IT convergence points exposed.
- Military & defence: Early-stage quantum integration with strong funding signals, but operational deployment is uneven across Member States.

3. Policy and Investment Alignment Is Improving

- EU-level directives (NIS2, CRA, DORA) now explicitly include or imply quantum-safe mandates.
- Investment vehicles like the EU Chips Act, Quantum Flagship, and Readiness 2030 are unlocking dual-use funding for quantum-safe R&D.

4. Strategic Risks Beyond Encryption

- Quantum sensing and quantum radar could erode current stealth and navigation advantages in military systems.
- Quantum-enhanced optimisation could accelerate adversarial cyber campaigns, disrupting critical infrastructure faster than existing incident response models can handle.

Top-Level Recommendations

1. Accelerate Crypto Inventory & Migration Planning
    - Immediate cryptographic asset inventories in all critical sectors, aligned to NIST/EU migration guides.
2. Embed Crypto-Agility in Procurement
    - Mandate modular cryptographic architectures in all new government and regulated-sector contracts.
3. Leverage EU and NATO Funding Streams
    - Engage with projects like EuroQCI, PESCO's "Quest", and DIANA to shape standards and share deployment costs.
4. Institute Sector-Specific Quantum Threat Exercises
    - Integrate "quantum breach" scenarios into red-teaming for financial, industrial, and defence operators.
5. Harmonise Standards
    - Push ETSI/CEN-CENELEC alignment to avoid fragmentation that could delay PQC adoption timelines.

The Strategic Quantum Threat Landscape

Quantum Computing as a Dual-Use Disruption

Quantum computing is not a single technological breakthrough — it is a convergence of hardware engineering, algorithm design, and error-correction science. When these elements mature, they will enable cryptographically relevant quantum computers (CRQCs) capable of breaking today's public-key cryptography.

Two quantum algorithms define the security risk:

- Shor's Algorithm — Efficiently factors large integers and solves discrete logarithms, dismantling RSA, DSA, and ECC, the backbone of global PKI.
- Grover's Algorithm — Provides a quadratic speed-up for brute-force searches, effectively halving the security strength of symmetric encryption like AES.

While full-scale CRQCs are not yet deployed, their arrival is a when, not if scenario. European security planners work on the assumption of a 10–15 year horizon, but outlier scenarios could collapse that to 5–7 years.

Harvest Now, Decrypt Later — A Present Danger

The Harvest Now, Decrypt Later (HNDL) threat model reframes quantum risk as an immediate security problem:

- Adversaries capture and store encrypted traffic today.
- Once CRQCs are operational, this backlog of data is decrypted in bulk.
- High-value targets include diplomatic cables, long-term financial contracts, personal identifiers, and industrial IP.

In sectors with decade-long data confidentiality requirements — such as government ID, defence logistics, and medical archives — this risk is already active.

Europe's Sovereignty Imperative

The quantum threat intersects directly with Europe's digital sovereignty agenda:

- Technology dependency: Over 80% of Europe's digital infrastructure stack depends on non-EU providers for cloud, semiconductors, and cryptographic libraries.
- Investment disparity: The U.S. leads private-sector quantum investment; China leads in state-driven programs. Europe's funding is significant (€1 billion Quantum Flagship; €43 billion Chips Act) but fragmented.
- Standard-setting influence: Without active leadership in ETSI, ITU, and ISO, Europe risks becoming a standards taker rather than a standards maker.

Sectoral Risk Amplifiers

- Finance: Interbank protocols (SWIFT, SEPA) are PKI-dependent; blockchain and DeFi assets could be rendered insecure.
- Government ID: ICAO standards still use vulnerable algorithms; reissuance cycles are slow.
- Industrial Control Systems: IEC 62443 does not yet integrate quantum-safe requirements; legacy OT environments are difficult to retrofit.
- Military/Defence: GPS-denied navigation, encrypted battlefield comms, and stealth systems could be compromised by quantum sensing and cryptanalysis.

Strategic Window for Action

The operational window for secure transition is narrower than it appears:

- Asset lifecycle lag: Large systems in energy, defence, and public administration often remain in service for 15–25 years.
- Migration complexity: Post-quantum cryptography (PQC) requires not just new algorithms but re-architected key management, hardware, and protocols.
- Workforce gap: The EU cybersecurity skills gap stands at ~300,000 professionals; PQC-specific expertise is even scarcer.

Operational Implication

The "future" quantum threat is already embedded in today's threat environment. The strategic calculus for CTOs, CISOs, and compliance officers is not simply when will CRQCs arrive but how much of your data and infrastructure will still be vulnerable when they do.

Europe’s Quantum-Safe Roadmap

Policy Architecture: Laying the Legal and Strategic Foundation

Europe’s approach to quantum-safe security is anchored in a multi-layered policy framework that converges cyber resilience, industrial autonomy, and sovereignty objectives.

Key EU Directives & Recommendations:

- Commission Recommendation (EU) 2024/1101 — Calls for Member States to complete migration to post-quantum cryptography (PQC) in public and critical infrastructure by 2030, with crypto-agility and HNDL mitigation as baseline requirements.
- NIS2 Directive (2022) — Expands cybersecurity obligations for operators of essential services, mandating “state-of-the-art” cryptography — interpreted as including PQC readiness.
- Cyber Resilience Act (CRA) — Requires quantum-safe update capability for connected devices by 2027.
- Digital Operational Resilience Act (DORA) — Financial-sector legislation indirectly mandating PQC as part of ICT risk management frameworks.

National Examples:

- Germany’s BSI: PQC guidelines advocating hybrid deployments for high-value systems.
- UK NCSC: PQC guidance aligned with NIST standards, emphasising implementation security.

Investment Channels: Funding the Transition

Europe's quantum-safe transformation is capital-intensive, with funding distributed across multiple programs:

Program / Fund	Budget	Focus Areas	Horizon
EU Chips Act	€43B	Semiconductor capacity, PQC-ready secure elements	2023–2030
Quantum Technologies Flagship	€1B	Quantum R&D, QKD pilots, PQC algorithm development	2018–2028
EuroQCI	€500M+	Pan-European quantum key distribution network	2021–2030
Horizon Europe	€95.5B* (total)	Defense-grade quantum sensing, PQC in IoT, supply-chain security	2021–2027
Readiness 2030 – SAFE Loan Facility	€150B	Dual-use (civil/military) quantum-secure projects	2025–2035

**Horizon Europe's quantum-security allocations are a subset of the total budget.*

Standardization: Avoiding a Fragmented Ecosystem

Current State:

- NIST PQC Standards (2024) — ML-KEM (Kyber), ML-DSA (Dilithium), SLH-DSA (SPHINCS+).
- ETSI — Developing interoperability standards for QKD and PQC deployment in telecoms and critical infrastructure.
- CEN/CENELEC FGQT — European-focused quantum technology standardisation, including PQC compliance testing.
- ITU — Harmonising QKD standards globally; Europe is a key participant but must scale representation.

Risks:

- Divergent national priorities — e.g., France's heavy QKD emphasis vs. Germany's PQC focus — risk fragmenting implementation.
- Vendor-specific proprietary implementations could undermine interoperability.

Mitigation:

- Push for EU-level procurement mandates requiring standards alignment before funding is released.
- Establish cross-sector conformance labs to test PQC/QKD interoperability in real-world conditions.

Sectoral Integration Timeline

Year	Milestone (per EU Roadmaps)	Priority Sectors
2026	Complete crypto inventories; start high-risk sector migration	Gov ID, Finance, Defense
2030	Full PQC deployment in high-risk sectors; hybrid crypto in others	Industry, Energy, Healthcare
2035	PQC in all medium/low-risk sectors; legacy crypto retired	Long-tail OT environments, SMEs

Strategic Observations

- Europe is one of the few jurisdictions pursuing PQC and QKD in parallel, hedging against performance and scalability challenges.
- Investment is robust, but without strict procurement compliance clauses, funds risk being spent on incompatible systems.
- Policy is ambitious but achievable if Member States accelerate from current “pilot mode” to full implementation between 2026–2030.

Sector Intelligence: Government ID Systems

Strategic Context

Government-issued identity systems — from passports and national ID cards to digital credentials — are foundational to a nation's security posture, economic stability, and citizen trust. Their cryptographic integrity underpins cross-border travel, e-government services, and secure financial transactions.

Today, the majority of these systems depend on public-key cryptography (RSA, ECC) for authenticity, integrity, and confidentiality. The emergence of cryptographically relevant quantum computers (CRQCs) will undermine this foundation.

Primary Vulnerabilities

1. Digital Signature Compromise
    - ePassports and national ID cards rely on RSA/ECC-based digital signatures to validate embedded chip data.
    - A CRQC running Shor's algorithm could forge these signatures, enabling undetectable counterfeit documents.
2. Key Exchange Exploits
    - Diffie-Hellman key exchange in secure chip-to-reader communications is quantum-vulnerable.
    - Attackers could derive private keys and decrypt session data in real-time.
3. Long-Term Data Confidentiality
    - Biometric templates and identity metadata must remain secure for a decade or more.
    - Under an HNDL scenario, adversaries could capture and store ePassport chip data today for future decryption.
4. Global Standards Lag
    - ICAO's current ePassport specifications still permit non-quantum-resistant algorithms.
    - Coordinated global adoption of PQC in ID systems is years away, creating interoperability bottlenecks.

Industry & Government Response

Hardware Sector

- Thales Group — Developing crypto-agile secure elements for ID chips to allow algorithm swaps without hardware replacement.
- Infineon Technologies — Integrating ML-KEM and ML-DSA into secure elements optimised for low-power devices like ePassports.
- NXP Semiconductors — Pursuing hybrid cryptographic models to balance PQC security with performance constraints.

Software & PKI Sector

- Open Quantum Safe (OQS) — Providing open-source PQC libraries for integration into ID verification systems.
- Entrust & DigiCert — Updating certificate authorities to support PQC digital signatures, enabling end-to-end quantum-safe ID issuance.
- Microsoft & IBM — Partnering with governments via the Post-Quantum Cryptography Coalition to modernise identity management platforms.

Policy & Regulatory Drivers

- EU Recommendation (2024/1101) — Mandates PQC integration in public-sector systems by 2030.
- Cyber Resilience Act (CRA) — Imposes update-by-default requirements for secure connected devices, including ID verification terminals.
- NIS2 Directive — Elevates government ID systems into the category of essential services requiring state-of-the-art cryptography.

Readiness Assessment

Dimension	Current Status	Gaps / Risks	Opportunities for Action
Cryptographic Security	Moderate (PQC pilots underway)	ICAO lag; reissuance cycles create exposure	Push ICAO for accelerated PQC spec adoption
Hardware Capability	Improving via crypto-agile chips	Retrofitting legacy IDs is costly, logistically complex	Require crypto-agility in all new ID chip procurement
Software Ecosystem	PQC-ready PKI pilots in place	Interoperability with legacy protocols	Leverage OQS integration across verification systems
Policy Alignment	Strong EU-level mandates	Inconsistent national rollout pace	Enforce harmonized migration timelines across EU

Strategic Recommendations

1. Mandate Crypto-Agility by Design
    - Specify updatable cryptographic components in all ID system tenders.
2. Synchronise National Reissuance Cycles
    - Coordinate at EU level to avoid staggered vulnerability windows between Member States.
3. ICAO Engagement
    - Lead international working groups to ensure PQC inclusion in global travel document standards.
4. Hybrid Crypto Deployment
    - Combine PQC with classical algorithms during transition to maintain cross-border interoperability.

Sector Intelligence: Financial Services

Strategic Context

The European financial sector operates as both a pillar of economic stability and a prime cyber target. Its daily operations rely on cryptographic primitives — particularly RSA, ECC, and DSA — for transaction authentication, secure messaging, and regulatory compliance.

Quantum computing poses a systemic risk: the compromise of public-key infrastructure (PKI) would undermine everything from SWIFT interbank transfers to blockchain-based asset custody. The consequences extend beyond data theft to the erosion of trust in the financial system itself.

Primary Vulnerabilities

1. Interbank Communications
    - SWIFT and SEPA transaction protocols are PKI-dependent.
    - A CRQC could forge transaction authorisations, enabling large-scale fraud.
2. Client-Facing Services
    - TLS handshakes between banking apps/websites and customers rely on ECC or RSA certificates.
    - Quantum attacks could enable man-in-the-middle interception of sessions.
3. Blockchain & Digital Assets
    - ECDSA signatures securing cryptocurrency wallets and smart contracts are quantum-vulnerable.
    - “Harvest Now, Decrypt Later” (HNDL) risk is acute in high-value, long-term custody scenarios.
4. Data at Rest and in Transit
    - Regulatory retention periods often exceed 10 years, meaning today’s encrypted financial records could be decrypted post-quantum.

Industry & Government Response

Government Initiatives

- EU DORA & NIS2 — Implicitly mandate quantum-safe measures as part of operational resilience.
- ECB & National Regulators — Conducting cryptographic inventories and piloting PQC in digital signatures.
- PQC4MED & PROMETHEUS — EU-funded research projects testing PQC in payment terminals and constrained financial hardware.
- UK NCSC — Guiding hybrid deployments (classical + PQC) in Open Banking APIs.

Industry Actions

- Tier-1 Banks (e.g., JPMorgan, HSBC, BNP Paribas) — Running PQC pilot programs in secure messaging and API endpoints.
- Fintechs & Cloud Providers — Cloudflare integrating hybrid key exchange (X25519 + Kyber) into TLS; AWS KMS and Google Cloud offering PQC-ready key pairs for testing.
- HSM Vendors (Thales, Utimaco, Entrust) — Shipping firmware updates to support ML-KEM/Dilithium hybrid deployments.

Performance & Integration Challenges

- Larger Keys & Slower Operations — PQC introduces computational overhead, especially on mobile banking apps and legacy ATMs.
- Interoperability Risks — Hardcoded cryptographic dependencies in legacy platforms complicate upgrades.
- Regulatory Lag — ISO and PCI DSS have yet to fully harmonise with NIST PQC standards, creating compliance ambiguity.

Readiness Assessment

Dimension	Current Status	Gaps / Risks	Opportunities for Action
Cryptographic Security	Partial — pilots in progress	Slow adoption in mid-tier institutions	Sector-wide crypto inventory & migration plan
Hardware Capability	Upgrading via HSM firmware	ATMs/payment terminals remain vulnerable	Replace/retrofit endpoints during asset cycles
Software Ecosystem	PQC-ready APIs in testing	Legacy banking core software resistance	Use abstraction layers for crypto agility
Policy Alignment	Strong at EU level	Fragmented national enforcement	Link compliance audits to PQC milestones

Strategic Recommendations

1. Treat PQC Migration as a Strategic Initiative
    - Integrate into enterprise risk and capital allocation planning, not as a discrete IT project.
2. Mandate Crypto Agility in Vendor Contracts
    - Require PQC-ready capability in all new fintech, core banking, and HSM procurements.
3. Deploy Hybrid Cryptography in Phases
    - Start with customer-facing TLS and high-value interbank messaging.
4. Engage in Sector-Wide Interoperability Testing
    - Coordinate via ECB or industry consortia to standardise implementation patterns.
5. Incorporate Quantum Threats into Stress Testing
    - Model the systemic impact of a sudden cryptographic break in ECB-led resilience exercises.

Sector Intelligence: Industrial & Automation Systems

Strategic Context

Industrial automation — encompassing manufacturing, energy, utilities, and transportation — is the operational backbone of European economic output. These environments are increasingly digitised, with operational technology (OT) and information technology (IT) converging into integrated cyber-physical systems.

The standards governing industrial control system (ICS) security, notably IEC 62443, currently provide comprehensive guidance on access control, network segmentation, and patch management — but do not yet embed quantum-resilient cryptography requirements. This creates a high-exposure gap for long-lifecycle assets that will remain in service well beyond the arrival of cryptographically relevant quantum computers (CRQCs).

Primary Vulnerabilities

1. Long Asset Lifecycles
    - ICS equipment (e.g., PLCs, SCADA systems) often remains operational for 15–25 years, making mid-life cryptographic retrofits costly and technically complex.
2. Legacy Protocol Dependencies
    - Many OT protocols (Modbus, DNP3, Profinet) were never designed for cryptographic security, let alone PQC. Security is often bolted on via VPNs or gateways using RSA/ECC.
3. Supply Chain Risks
    - Industrial vendors often source components from global suppliers. PQC-readiness is uneven, and insecure firmware in third-party components can propagate vulnerabilities across critical sectors.
4. Convergence Threat Surface
    - The integration of ICS with cloud analytics and remote management systems increases exposure to HNDL attacks on encrypted telemetry and control channels.

Industry & Government Response

Regulatory & Standards Initiatives

- NIS2 Directive — Expands coverage to manufacturing and energy operators, obligating “state-of-the-art” cybersecurity.
- CEN/CENELEC Focus Group on Quantum Technologies (FGQT) — Exploring PQC inclusion in European industrial standards.
- EU Chips Act — Funding secure semiconductor design for PQC-ready industrial controllers.

Vendor & Ecosystem Actions

- Siemens & ABB — Early-stage research into crypto-agile industrial controllers capable of upgrading to PQC algorithms without hardware replacement.
- Bosch Connected Industry — Testing hybrid PQC + classical encryption on industrial IoT gateways to maintain interoperability.
- European R&D Consortia — Horizon Europe-funded projects piloting PQC in smart grid communications and energy management systems.

Performance & Integration Challenges

- Resource Constraints — PQC algorithms have larger key sizes and higher computational demands, challenging small embedded devices.
- Interoperability — Upgrading ICS without disrupting time-sensitive control loops requires rigorous validation.
- Vendor Lock-in — Proprietary implementations risk fragmenting the market and slowing standardised adoption.

Readiness Assessment

Dimension	Current Status	Gaps / Risks	Opportunities for Action
Cryptographic Security	Low — PQC largely absent	Legacy OT protocols; long upgrade cycles	Add PQC as a requirement in IEC 62443 updates
Hardware Capability	Mixed — pilots in progress	Incompatibility with low-power devices	Leverage EU Chips Act for secure controller R&D
Software Ecosystem	Limited PQC-ready ICS software	Interoperability with legacy SCADA	Develop crypto-agile middleware for OT networks
Policy Alignment	Moderate — NIS2 coverage	No explicit PQC mandate in industrial standards	Push FGQT to accelerate PQC standardization

Strategic Recommendations

1. Mandate PQC in ICS Standards Updates
    - Work through IEC 62443 committees to define quantum-safe profiles for industrial environments.
2. Embed Crypto-Agility in All New Deployments
    - Ensure controllers and gateways can swap algorithms without full hardware replacement.
3. Synchronise OT/IT PQC Migrations
    - Align ICS upgrades with IT-side cryptographic transitions to avoid interoperability gaps.
4. Use Hybrid Deployment Models
    - Combine PQC with current crypto during migration to balance performance with security.
5. Test in Controlled Environments
    - Establish cross-sector testbeds for PQC-enabled industrial networks under Horizon Europe funding.

Sector Intelligence: Military & Defence

Strategic Context

In the defence domain, quantum technologies are shifting from theoretical potential to operational planning. Quantum-enabled capabilities — from secure communications to advanced sensing — are dual-use by nature, serving both civilian and military needs. For Europe, quantum readiness in defence is not just a matter of national security; it is also a sovereignty safeguard against technological dependency in high-stakes environments.

Primary Vulnerabilities & Opportunities

1. Secure Communications
    - Military command-and-control networks rely on cryptographic authentication and encryption vulnerable to Shor's algorithm.
    - Quantum key distribution (QKD) offers one countermeasure, but deployment across dispersed, mobile forces remains technically challenging.
2. Navigation & Timing
    - GPS-denied navigation is critical in contested environments. Quantum sensing offers precision alternatives — but adversaries could use similar systems to bypass stealth or disrupt positioning.
3. Data Confidentiality in Long Lifecycle Systems
    - Defence platforms often operate for 20–30 years, meaning today's crypto vulnerabilities could persist for decades.
4. Dual-Use Acceleration Risk
    - Civilian R&D breakthroughs in quantum computing and PQC can be rapidly adapted for offensive military cyber operations.

Industry & Government Response

EU & Member State Initiatives

- Readiness 2030 & SAFE Loan Facility (€150B) — Funds dual-use projects, including quantum-secure communications and sensing.
- EU Quantum Strategy — Roadmap for quantum sensing and defence applications to be issued by 2026.
- PESCO's "Quest" Initiative — Finland-led program targeting PQC, encryption-breaking resilience, and quantum-based navigation systems.

NATO Programs

- DIANA Accelerator — Funding startups like LevelQuantum for deployable QKD solutions in military networks.
- Quantum Skills Academy (planned) — To address the shortage of defence-focused quantum engineers by 2026.

UK Defense Posture

- CyberEM Command (£1B) — Integrated cyber and electromagnetic warfare command including quantum computing and PQC research domains.

Performance & Integration Challenges

- Operational Deployment at Scale — QKD over mobile and tactical networks remains immature.
- Interoperability in Coalitions — Aligning PQC/QKD standards across NATO and EU member states is politically and technically complex.
- Supply Chain Hardening — Ensuring defence contractors integrate PQC into all communications and control systems.

Readiness Assessment

Dimension	Current Status	Gaps / Risks	Opportunities for Action
Cryptographic Security	Early PQC/QKD pilots	Coalition-wide interoperability	Develop NATO/EU PQC standard alignment frameworks
Hardware Capability	R&D funding in place	Mobile/tactical QKD deployment	Leverage EuroQCI for hybrid QKD + PQC solutions
Software Ecosystem	Limited PQC integration in C2 apps	Long lifecycle systems with fixed crypto	Retrofit via crypto-agile modules
Policy Alignment	Strong at EU/NATO level	Divergent member state priorities	Joint procurement clauses for quantum-safe systems

Strategic Recommendations

1. Treat Quantum as Core to Defence Readiness
    - Integrate PQC and quantum sensing into defence capability planning cycles.
2. Push Coalition Interoperability Standards
    - Use NATO and PESCO forums to align cryptographic migration timelines.
3. Deploy Hybrid Security Models
    - Combine PQC for general encryption with QKD for mission-critical command channels.
4. Invest in Quantum Workforce Development
    - Secure early access to Quantum Skills Academy graduates through defence-sector partnerships.
5. Harden Supply Chains
    - Mandate PQC compliance for all defence contractors in communications and control systems.

Comparative Readiness Matrix

The following matrix synthesises sector readiness across Government ID, Financial Services, Industrial & Automation, and Military & Defence. It evaluates each domain against four dimensions: Cryptographic Security, Hardware Capability, Software Ecosystem, and Policy Alignment.

Table: Sector-by-Sector Quantum Readiness Assessment

Sector	Readiness Level	Cryptographic Security	Hardware Capability	Software Ecosystem	Policy Alignment	Key Risks	Strategic Leverage Points
Government ID	Moderate	PQC pilots in progress; hybrid crypto in trials	Crypto-agile chip prototypes in development	PQC-ready PKI pilots; OQS integration underway	Strong EU-level mandates; ICAO lag	Long reissuance cycles; ICAO standard delay	Mandate crypto-agility; accelerate ICAO PQC standards
Financial Services	Partial Readiness	High-value assets piloting PQC/QKD	HSM firmware updates; hybrid crypto support	PQC-ready APIs in testing	Strong at EU level; fragmented enforcement	Legacy systems; mid-tier adoption gap	Sector-wide crypto inventory; ECB-led interoperability
Industrial & Automation	Low	PQC absent in ICS standards	Pilot PQC-enabled controllers; low-power constraints	Minimal PQC software for ICS	NIS2 coverage but no explicit PQC mandate	Long asset cycles; legacy protocol dependencies	Update IEC 62443 with PQC; hybrid crypto for OT/IT sync
Military & Defense	Early-Stage	PQC/QKD pilots in command networks	R&D funding for deployable QKD	Limited PQC integration in defense C2 apps	Strong EU/NATO policy alignment	Coalition interoperability; mobile deployment hurdles	NATO/EU PQC standardization; hybrid QKD+PQC deployments

Strategic Observations

1. Government ID is furthest ahead in hardware readiness, with major vendors embedding crypto-agility into secure elements. The primary obstacle is global standards alignment.
2. Financial Services is running advanced pilots, but suffers from uneven adoption. The gap between Tier-1 banks and smaller institutions will create weak links in sector-wide security unless addressed.

3. Industrial & Automation is the most at risk. Long asset lifecycles and outdated protocols mean that without immediate standards updates, quantum vulnerability will persist deep into the 2030s.
4. Military & Defence has strong political momentum and funding, but operational integration lags. The interoperability challenge across EU and NATO partners will be a key determinant of success.

Visual Summary: Relative Readiness

Readiness Score by Sector (1 = low, 5 = high)

Sector	Score
Government ID	3.5
Financial Services	3
Industrial & Automation	2
Military & Defense	2.5

This scoring reflects current implementation status rather than policy intent — indicating that sectors with strong mandates still face execution challenges.

Strategic Recommendations

1. Accelerate Cryptographic Inventory & Risk Mapping

- Action: Conduct a full inventory of cryptographic assets, including embedded systems, third-party dependencies, and data stores with long-term confidentiality needs.
- Rationale: Without precise mapping, PQC migration plans risk missing hidden vulnerabilities.
- TQS Note: Use Cryptographic Bill of Materials (CBOM) methodology to ensure asset visibility across both IT and OT networks.

2. Mandate Crypto-Agility in All New Procurement

- Action: Embed clauses requiring modular, updatable cryptographic components in hardware, software, and managed services contracts.
- Rationale: Reduces future migration costs and accelerates response to newly standardised algorithms.
- TQS Note: For government ID, crypto-agility should be a non-negotiable tender criterion from 2025 onwards.

3. Deploy Hybrid Cryptography During Migration

- Action: Implement PQC alongside classical algorithms in critical systems to maintain interoperability during phased rollouts.
- Rationale: Avoids system downtime and compatibility issues while standards mature globally.
- TQS Note: This is essential for international-facing sectors such as finance and travel.

4. Establish Sector-Wide Interoperability Testbeds

- Action: Create cross-industry labs under EU funding to validate PQC and QKD performance across vendor ecosystems.
- Rationale: Reduces risk of fragmented deployments and ensures compliance with evolving ETSI and NIST standards.
- TQS Note: Defence and industrial automation sectors particularly benefit from shared validation infrastructure.

5. Integrate Quantum Threat Scenarios into Resilience Exercises

- Action: Incorporate quantum breach simulations into red-team and crisis-management exercises.
- Rationale: Builds operational familiarity with PQC-enabled incident response under real-world conditions.
- TQS Note: ECB-led stress testing for financial services should include “cryptographic break” scenarios from 2026.

6. Align National & EU-Level Migration Timelines

- Action: Synchronise national migration deadlines with EU targets (e.g., 2030 for high-risk sectors).
- Rationale: Prevents staggered adoption that can create exploitable gaps between jurisdictions.
- TQS Note: Critical for defence coalition partners where interoperability is mission-essential.

7. Leverage Funding Instruments for Dual-Use Solutions

- Action: Tap into Readiness 2030, EuroQCI, and Horizon Europe funding streams to co-finance PQC upgrades that benefit both civil and military systems.
- Rationale: Accelerates deployment and distributes cost across multiple use cases.
- TQS Note: Priority for industrial vendors supplying both public infrastructure and defence.

8. Build the Quantum-Safe Workforce Pipeline

- Action: Develop internal training programs in PQC and quantum network security; partner with universities and EU Skills Academy initiatives.
- Rationale: Technical scarcity is already slowing migration projects.
- TQS Note: Workforce readiness will determine whether the EU meets its 2030 PQC milestones.

9. Harden Supply Chains Against Quantum Vulnerabilities

- Action: Require upstream vendors to certify PQC readiness for all cryptographic components.
- Rationale: Prevents “weakest link” exploitation through subcontractor systems.
- TQS Note: This should be a binding requirement in all defence and industrial contracts from 2025.

10. Maintain Strategic Flexibility Beyond PQC

- Action: Track advances in quantum-resistant protocols, quantum-safe networking, and alternative security paradigms.
- Rationale: PQC is a step forward, not the endpoint; future-proofing requires ongoing adaptability.
- TQS Note: Establish a dedicated threat intelligence function to monitor and evaluate new cryptographic candidates.

References

[1] European Commission, Recommendation (EU) 2024/1101 of 11 April 2024 on the coordinated transition to post-quantum cryptography, Apr. 2024. [Online]. Available: https://eur-lex.europa.eu/eli/reco/2024/1101/oj
[2] European Union, Directive (EU) 2022/2555 (NIS2 Directive) on measures for a high common level of cybersecurity across the Union, Dec. 2022.
[3] European Commission, Cyber Resilience Act, Sep. 2022.
[4] European Parliament, Digital Operational Resilience Act (DORA), Dec. 2022.
[5] European Commission, EU Chips Act, 2023.
[6] European Commission, Quantum Technologies Flagship, 2018–2028.
[7] European Commission, European Quantum Communication Infrastructure (EuroQCI), 2021–2030.
[8] European Commission, Horizon Europe Work Programme 2021–2027.
[9] PESCO, Quest – Quantum Secure Communication and Navigation Systems, 2025.
[10] National Institute of Standards and Technology (NIST), Post-Quantum Cryptography Standards: ML-KEM, ML-DSA, SLH-DSA, Aug. 2024.
[11] European Telecommunications Standards Institute (ETSI), Quantum Key Distribution (QKD) and Post-Quantum Cryptography Standards, 2024.
[12] CEN/CENELEC Focus Group on Quantum Technologies (FGQT), Quantum Technology Standardisation Activities, 2024.
[13] International Telecommunication Union (ITU), QKD Interoperability Standards, 2024.
[14] International Civil Aviation Organization (ICAO), Machine Readable Travel Document (MRTD) Standards, 2023.
[15] Thales Group, Crypto-Agile Secure Elements for Government ID, 2024.
[16] Infineon Technologies, Post-Quantum Secure Elements for ePassports, 2024.
[17] NXP Semiconductors, Hybrid Cryptography Solutions for Secure ID, 2024.
[18] Open Quantum Safe Project, liboqs and PQC Integration in PKI Systems, 2024.
[19] Entrust Datacard, PQC-Ready Certificate Authority Solutions, 2024.
[20] DigiCert, PQC Integration in Digital Certificates, 2024.
[21] Microsoft, Post-Quantum Cryptography Coalition Contributions, 2024.
[22] IBM, Quantum-Safe Technology Program, 2024.
[23] Gartner, Crypto-Agility Best Practices, 2023.
[24] European Central Bank (ECB), Digital Signature PQC Pilot Programs, 2024.
[25] PQC4MED Project, Post-Quantum Cryptography for Medical and Payment Devices, 2023.
[26] PROMETHEUS Project, Post-Quantum Cryptographic Mechanisms for Constrained Financial Hardware, 2021.
[27] UK National Cyber Security Centre (NCSC), Guidance on Hybrid Cryptography, 2024.

[28] JPMorgan Chase & Co., Quantum Key Distribution Trials with Toshiba and Ciena, 2021.
[29] Cloudflare, Experimenting with Post-Quantum Cryptography, 2021.
[30] Amazon Web Services (AWS), PQC-Ready Key Management Service, 2024.
[31] Google Cloud, PQC Key Management Testing, 2024.
[32] Thales, HSM Firmware PQC Support, 2024.
[33] Utimaco, PQC Integration in Hardware Security Modules, 2024.
[34] Siemens, Crypto-Agile Industrial Controllers R&D, 2024.
[35] ABB, Quantum-Safe Industrial Automation Research, 2024.
[36] Bosch Connected Industry, Hybrid PQC for Industrial IoT Gateways, 2024.
[37] Horizon Europe, Smart Grid PQC Pilots, 2024.
[38] International Electrotechnical Commission (IEC), IEC 62443 Industrial Cybersecurity Standards, 2024.
[39] EU Council, Readiness 2030 SAFE Loan Facility, 2025.
[40] NATO DIANA Accelerator, QKD Defence Network Startups, 2024.
[41] NATO, Quantum Skills Academy, 2024.
[42] UK Ministry of Defence, CyberEM Command: Quantum Integration, 2024.
[43] BSI, Status of Quantum Computer Development, 2024.
[44] Global Risk Institute, Quantum Threat Timeline Report, 2023, 2024.
[45] NIST, The PQC Migration Handbook, 2024.
[46] P. W. Shor, “Algorithms for quantum computation: discrete logarithms and factoring,” Proc. 35th Annual Symposium on Foundations of Computer Science, IEEE, 1994.
[47] L. Chen et al., “Report on Post-Quantum Cryptography,” NISTIR 8105, National Institute of Standards and Technology, 2016.
[48] National Security Agency (NSA), Quantum Computing and Post-Quantum Cryptography: FAQ, 2022.
[49] White House, National Security Memorandum 10: Promoting United States Leadership in Quantum Computing, May 2022.

About The Quantum Space

The Quantum Space (TQS) is an independent research and intelligence platform dedicated to quantum computing, post-quantum cryptography, cybersecurity, and digital sovereignty. Our mission is to equip Europe's decision-makers with actionable, evidence-based insights to anticipate and adapt to the quantum era.

We specialise in sector-specific strategic analysis that bridges the gap between technical depth and boardroom priorities — supporting leaders in technology, defence, finance, and infrastructure with intelligence that is:

- Technically rigorous — grounded in verifiable data, technical standards, and leading-edge research.
- Strategically relevant — framed in the context of sovereignty, resilience, and competitive advantage.
- Forward-looking — identifying not just immediate threats, but the emerging opportunities of quantum technologies.

Our research methodology integrates:

1. Primary source analysis — EU directives, national strategies, and industry technical publications.
2. Sector engagement — consultation with vendors, regulators, and operators across critical industries.
3. Comparative intelligence — mapping Europe's positioning against global competitors in quantum readiness.

TQS operates as an independent voice, committed to transparency and neutrality in its assessments. We work with public-sector agencies seeking to set resilient quantum migration policies and private-sector leaders integrating quantum-safe technologies into mission-critical systems. We also work with industry consortia shaping international standards and collaborative innovation.

Contact & Collaboration

Website: www.thequantumspace.org
Email: steve.atkins@thequantumspace.org
LinkedIn: The Quantum Space

The Quantum Space — Strategic Intelligence for the Quantum Age.


THE
QUANTUM
SPACE
thequantumspace.org