Post-Quantum Cryptography in Europe: Risks, Strategy and Portugal as a National Case Study in the NIS2 Transition

Carlos Lopes, Ivo Rosa*
ISTEC -Instituto Superior de Tecnologias Avançadas, Lisbon, Portugal,
Emails: carlos.lopes@my.istec.pt, ivo.rosa@my.istec.pt
* *Corresponding author*

Abstract: **With Shor's and Grover's algorithms compromising the mathematical core of legacy RSA and ECC, the active threat of 'Harvest Now, Decrypt Later' (HNDL) campaigns is already accelerating the rollout of Post-Quantum Cryptography (PQC). This paper examines the gap between EU compliance mandates, specifically NIS2 Directive and the Cyber Resilience Act, and the actual engineering of quantum-safe systems. We push 'hybrid cryptography' as the immediate standard, layering NIST primitives like ML-KEM and ML-DSA over classical protocols to enforce redundancy in constrained environments. We use the NIST IR 8547 framework to organise migration into discovery, prioritisation, and modernisation. Using Portugal as a national case study, this paper examines how EU-level PQC governance is translated into national implementation through the CNCS, QNRC, and PTQCI frameworks. Ultimately, success depends on building PQC expertise in Portugal while rebuilding cryptographic foundations for the quantum era.**

Keywords: **Digital Sovereignty, Hybrid Cryptography, NIS2 Directive, Post-Quantum Cryptography, Quantum Threat.**

I. INTRODUCTION

The modern digital economy largely rests on the mathematical premise that factoring large integers will remain impossible for classical computers. This difficulty also applies to related problems, such as calculating discrete logarithms. With the advent of quantum computing, these methods are on track to render contemporary public-key cryptography obsolete once scalable machines exist. It bypasses the mathematics we rely on, using pure physics to break security rules that we previously considered inviolable.

The two mathematical algorithms which serve as the base for both RSA and Elliptic Curve Cryptography (ECC) collapse with respect to Shor's Algorithm [1]. Once a CRQC becomes available, the impact on today's public-key encryption schemes will be profound, to the point where they can no longer be treated as reliable options for long-term confidentiality. For symmetric cryptography, Grover's algorithm [2] effectively cuts the security margin in half: a scheme designed for 256-bit resistance offers only about 128-bit resistance against a quantum adversary. It is this dual exposure that explains why static data files are at risk of being subject to future backward decryption [3].

This dynamic is already happening in 'Harvest Now, Decrypt Later' (HNDL) campaigns, where adversaries grab encrypted traffic today with the intention to decrypt it in the future. This isn't just technical; it's a national security problem. At the IT Security Summit Porto 2025, the Coordinator of the National Cybersecurity Centre (CNCS) classified the quantum threat as an active danger. He argued that the potential for decryption already dictates daily risk protocols [4]. Problem is, we lack hard data on intercepted volumes, leaving policymakers blind to calibrated responses [3].

In 2024, the National Institute of Standards and Technology (NIST) officially established the initial Post-Quantum Cryptography (PQC) standards [5-7]. These new methods, which include key-encapsulation (KEM) and digital signatures, will work together with the older methods. The resulting hybrid framework guarantees fallback redundancy by layering unproven post-quantum algorithms over battle-tested classical protocols. Regulatory guidance can't instantly create cryptographic trust. Uncertainties about the long-term mathematical resilience of PQC schemes remain [5-7].

Europe is now mandating quantum-safe crypto, but regional rollout has been patchy. By widening the regulatory perimeter, the NIS2 Directive (EU 2022/2555) places broader critical sectors under severe legal liability [8]. The Portuguese CNCS embeds these exact directives into the National Cybersecurity Framework (QNRC). Private sector PQC roadmaps now function as the actual foundation of the state's cyber-defence strategy [9]. Infrastructure and human capital operate independently to meet these laws: Portuguese Quantum Communications Infrastructure (PTQCI) locks down the physical communications layer, while the C-Academy [10] specifically targets the specialised talent drought. Portugal is examined here not as an isolated jurisdiction, but as a Member State case through which the operational consequences of the European PQC and NIS2 transition can be observed.

It is impossible for a regulation to replace or upgrade a router. Crucially, most security teams struggle to even find the old technical debt hardcoded into their legacy systems [8-10]. For the engineering teams on the ground, PQC migration is simply one of many burdens added to an already overflowing workload. What matters now is how quickly Europe can strengthen its digital sovereignty, before a breakthrough in quantum computing makes all classical encryption obsolete.

Although mathematics is the foundation of cryptographic

theory, modern infrastructure uses it to implement security policies. The speed at which regulatory bodies create new rules surpasses the speed at which governments pass laws. For this reason, these organisations literally define how national defence works in the physical world, using rigorous security embedded in technology.

Scope and contribution: This paper is a structured review combined with an instrumental single-country case study. Its contribution is not a new algorithm or primary benchmark, but an analytical framework that maps the European post-quantum governance stack - the NIS2 Directive, the Cyber Resilience Act, the Cyber Solidarity Act and Commission Recommendation (EU) 2024/1101 - onto the operational migration lifecycle defined in NIST IR 8547 (discovery, prioritisation, modernisation). We apply this framework to Portugal in order to expose where regulatory obligation does, and does not, translate into cryptographic engineering, and we situate Portugal comparatively against larger Member States (Germany, France and Spain). The research question is therefore: how is EU-level PQC governance operationalised at national level under NIS2, and what structural factors determine whether a smaller Member State can meet the 2030 migration horizon?

Method: This review follows a narrative-synthesis protocol. We drew on three classes of source: (i) primary regulatory and standardisation material (EU directives and regulations; NIST FIPS 203-205 and the IR 8413, 8545 and 8547 series; and ENISA, BSI, ANSSI and INCIBE guidance); (ii) peer-reviewed literature on PQC performance and side-channel security indexed in IEEE Xplore, ACM, Springer and the IACR ePrint archive; and (iii) official national documentation from the CNCS and associated Portuguese programmes, published up to December 2025. Sources were selected for authority and relevance to the governance-to-engineering transition; vendor and market material was used only for context. The Portuguese case is treated as an instrumental single case: its institutional artefacts (Decree-Law 125/2025, the QNRC, PTQCI and C-Academy) are read as evidence of how the EU framework is enacted, and are compared against the equivalent instruments of the reference Member States.

II. STATE OF THE ART: FROM CLASSICAL CRYPTOGRAPHY TO THE POST-QUANTUM PARADIGM

Cryptography extends far beyond confidentiality. It provides the hard maths for integrity and authentication, proving data provenance in hostile environments. We are far beyond simple tricks like the Caesar cipher; today, industrial-grade protocols form the backbone of the internet. Encryption migrated from the military sphere into civilian life. It currently secures the protocols behind SWIFT banking and national power grids.

2.1 Technical Foundations of Post-Quantum Cryptography

Current asymmetric encryption depends on the computational intractability of factoring large integers and computing discrete logarithms. Classical hardware cannot complete these workloads in a viable timeframe. This ceiling protected RSA and ECC protocols for decades [11], but the emergence of quantum processing renders these defence layers technically insolvent.

When it comes to the quantum era, Shor's and Grover's algorithms are decisive breaking points for today's encryption standards. Shor's algorithm [1] is a mathematical procedure that facilitates the reduction of factorisation and discrete logs to polynomial-time operations. This computational leap breaks with the main security assumptions of modern public key infrastructure. Grover's algorithm [2] targets symmetric primitives through quadratic acceleration in unstructured searches. Because the algorithm speeds up unstructured searches quadratically, it slices traditional security margins in half. An AES-256 key drops to a mere 128 bits of post-quantum resistance, meaning our long-term data archives aren't nearly as safe as we once thought.

This vulnerability is built into widely used public-key systems. Migration efforts stall due to legacy technical debt, strict budgets, and teams that lack PQC skills [12,13]. PQC beats hardware-dependent Quantum Key Distribution (QKD), using Module-Lattices to secure existing digital infrastructure. After eight years of vetting, NIST set its 2024 standards: ML-KEM (FIPS 203) for key encapsulation, ML-DSA (FIPS 204) and SLH-DSA (FIPS 205) for digital signatures [5-7]. Lattices remain the efficiency baseline, yet hash-based signatures like SLH-DSA back up with proven hash math.

Current industrial baselines still assume hybrid deployments rather than standalone PQC. Given that these early PQC algorithms have only recently been introduced, both the German BSI and the French ANSSI recommend a hybrid strategy to address the risks associated with the new algorithms [14,15]. This hybrid approach pairs a trustworthy classical algorithm with a post-quantum algorithm. So, if at least one of the two algorithms remains secure, then overall security will be maintained [16]. Mandates for parallel dual key exchange protocols will force developers to handle the extra bandwidth and added architectural complexity [17].

Algorithmic diversity is a deliberate design goal of the NIST process, documented across two distinct status reports that should not be conflated. NIST IR 8413 [18] closed the third round (September 2022), selecting the first algorithms for standardisation - ML-KEM, ML-DSA, Falcon and SLH-DSA - and advancing four KEM candidates (BIKE, Classic McEliece, HQC and SIKE) to a fourth evaluation round. NIST IR 8545 [19] then concluded that fourth round (March 2025), selecting the code-based KEM HQC to diversify the key-establishment portfolio against a potential future weakness in the lattice family. Maintaining candidates from independent mathematical families is one of the few realistic ways to limit - though not eliminate - the long-term risk of HNDL tactics [2].

2.2 Performance and Algorithmic Trade-offs

The transition disrupts the traditional balance between performance and security [20]. These new standards require more advanced mathematics and longer key lengths than previous ones. Results may vary depending on the hardware, but, as these are chips with limited capabilities, such as the ARM Cortex-M4, they all face more severe bottlenecks [21].

The specification values presented in Table I reveal a complex situation for the FIPS 203, 204, and 205 standards

[5-7]: speed and storage are in constant friction. The ML-KEM-1024 may have 'very high' efficiency, but this speed comes at the cost of a public key of ~1.57 KB, a key almost six times the size required by RSA-2048. The SLH-DSA-128 algorithm reverses the situation, keeping the public key at just 32 bytes, but allowing its signature to reach ~17 KB.

TABLE I. PQC ALGORITHMIC TRADE-OFFS COMPARED TO CLASSICAL STANDARDS

Algorithm	Public Key Size	Signature / Ciphertext Size	Performance	Security Basis
RSA-2048	256 bytes	256 bytes	High (Verification)	Integer Factorization
ML-KEM-1024 (Kyber)	~1.57 KB	~1.57 KB *	Very High	Module-Lattice (ML-WE)
ML-DSA-65 (Dilithium)	~1.95 KB	~3.31 KB	High	Module-Lattice (ML-FIP)
SLH-DSA-128f (SPHINCS+)	32 bytes	~17.09 KB	Very Low	Hash-based (Stateless)
Falcon-512	~0.90 KB	~0.67 KB	High	NTRU Lattice
Classic McEliece	~261 KB	128 bytes*	Moderate	Code-based

*Note: For ML-KEM and Classic McEliece, the value refers to the ciphertext size, not a signature.

Security validation for SLH-DSA from NIST [19], PQShield [22], BSI [14], and ANSSI [15] is unanimous. The operational blocker is signature size. This massive data footprint simply locks the algorithm out of any constrained environments. By bypassing this throughput bottleneck, ML-KEM and ML-DSA have effectively established themselves as the industry defaults for mobile and high-availability systems [23].

Transitioning PQC into production depends on formal mathematical verification. Engineers apply the Jasmin toolchain to compile high-assurance code, specifically preventing side-channel vulnerabilities directly at the assembly level [24]. Currently, both ENISA and the European Cybersecurity Competence Centre (ECCC) are pushing for a hybrid architecture as the standard. Stacking PQC on classical algorithms provides backward compatibility. In practice, this contains the blast radius if early-stage migration efforts fail [12,25].

2.3 Portugal as a Member-State Case Study in European PQC Sovereignty

The PQC strategy established by Europe is a combination of standards, legislation and technological sovereignty [12], [25]. Portugal implements it through the CNCS [27], and with the support of the National Coordination Centre (NCC-PT), translating Brussels logic into local practice. Supported by the QNRC, through the identification of critical assets that need immediate remediation, it leads to real engineering projects such as PTQCI, which is implementing a reinforced quantum layer in Lisbon with a focus on protecting backbone fibre from future interception. For the private and academic sectors, it is not just a network; it is a working, industrial testing ground for architectural stress testing [28,29].

Now NIS2 is law, compliance is no longer optional, requiring more Portuguese entities to adopt rigorous safety standards. The CNCS uses this authority to drive readiness assessment, incorporating post-quantum criteria into its national digital-maturity and risk-evaluation instruments under the QNRC, which help identify lagging sectors and direct support accordingly [9]. Legal pressure is necessary; without it, most organisations would simply wait for a security breach to occur before taking the necessary measures.

III. REGULATORY ARCHITECTURE AND STRATEGIC SOVEREIGNTY IN THE POST-QUANTUM ERA

Technical standards, regulation, and cryptographic autonomy are the core instruments of Europe's PQC governance [12,25]. Phasing out classical encryption triggers a legal conflict that dwarfs any routine update. Member States are trapped: they must lock down data sovereignty without suffocating the industries that build it.

3.1 European Regulatory Architecture

The NIS2 Directive of 2022 (EU) 2022/2555 ended voluntary compliance, imposing stringent risk protocols on all essential and important entities [8], covering government services, transport and the banking sector. These are precisely the sectors that ENISA identifies as the main targets of cyberattacks [25]. Two other laws fill the gaps. First, the Cyber Resilience Act (CRA) obliges hardware and software manufacturers to adopt 'security by design' principles, requiring strong encryption from the production line [31]. Secondly, the Cyber Solidarity Act (CSA) establishes a cross-border shield, providing a reserve of resources to manage large-scale incidents collaboratively [32].

This requirements framework is no longer optional. Organisations must make sure they are using PQC algorithms as part of their regular modernization cycles. Portugal formalised this requirement with Decree-Law No. 125/2025. The legislation's transposition of NIS2 grants the CNCS direct authority for the enforcement of these cryptographic standards across the national critical digital backbone [33].

The divide is total in terms of regulation. In contrast to NIS2 that is aimed at operators the CRA and CSA are targeted at digital products, and the collective defence capacity [31], [32]. The EU's Coordinated Implementation Roadmap defines the exit strategy from classical cryptography [34], enforcing the hard logic of Commission Recommendation (EU) 2024/1101 [35].

As part of the technical architecture of the migration, ENISA has stipulated that each Member State must take three mandatory measures:

- Align national migration plans with NIST FIPS 203-205 standards;
- Implement hybrid encryption now as BSI and ANSSI recommend [14,15];
- Mandate quantum-safe certification under CRA rules [31].

The ECCC manages funding for collaborative research and capacity building. The groundwork with the private sector is carried out by the European Cybersecurity Organisation (ECSO) to ensure that commercial technologies comply with the legislation.

3.2 National Implementation: The Portuguese Context

The CNCS drives the rollout of Europe's post-quantum roadmap at the national level. The transposition of the NIS2 Directive via Decree-Law No. 125/2025 creates a binding

governance framework for essential and important entities. Public and private entities operate under a binding directive. NIS2 demands strict security governance, fast incident reporting, and thorough supply chain checks [33]. The decree puts into action three key components: the National Cyberspace Security Strategy, the Large-Scale Cyber Crisis Response Plan, and the QNRC [9].

The CNCS operates under a dual mandate: serving as the national cybersecurity authority and the National Coordination Centre (NCC-PT). It channels European funds for technological independence [27] and connects policymakers to R&D hubs like INESC TEC and Porto University. This ensures the shift to quantum resilience is built on hard engineering, not bureaucratic box-ticking. The DISCRETION project exemplifies this, fusing Software Defined Networks (SDN) and Quantum Key Distribution (QKD) to build a sovereign cipher machine for quantum keys [30].

NIS2 locks down the giants, but the supply chain fractures at the Small and Medium Enterprises (SMEs) level. ENISA's NIS Investments 2024 report quantifies this gap. The study surveyed 1,350 organisations across all 27 EU Member States, spanning every NIS2 high-criticality sector plus manufacturing, as a pre-implementation snapshot of the NIS2 transposition. It found that only 4% of surveyed organisations had invested in post-quantum cryptography by the end of 2024, with a further 14% planning to do so, leaving the great majority of the supply chain exposed to HNDL attacks [36]. To stop small firms from acting as open backdoors, the CNCS deployed 'Roteiro NIS2' in November 2025. This initiative provides decentralised training, ensuring the cybersecurity culture reaches the micro-level of the economy [37]. Concurrently, the CNCS is adding post-quantum criteria to digital maturity tools to monitor preparedness.

3.3 Collective Defence and Digital Sovereignty

The governance of the PQC is a priority in Europe's fight for technological self-sufficiency. Dependence on non-EU cryptographic standards creates concerns regarding autonomy and the long-term management of critical digital infrastructure. To mitigate this, the Union encourages cryptographic diversity by supporting both NIST-approved and EU-developed algorithms to break the monopoly. Agencies like France's ANSSI, Germany's BSI, and Spain's INCIBE act as independent evaluators and facilitators for PQC interoperability with European standards. The 2025 Joint Statement [26] and the EU's Coordinated Implementation Roadmap [35], both established under Recommendation (EU) 2024/1101, offer the structure for harmonizing national strategies and establishing a domestic security infrastructure [34].

Portugal contributes to this framework through CNCS participation and national research initiatives linked to European coordination mechanisms. Europe builds sovereignty directly into innovation. Law and tech move together. This stops the clash between rules and progress. The technology underpins digital sovereignty at a time when the margin for delay is shrinking.

IV. TECHNICAL AND IMPLEMENTATION CHALLENGES

Production deployments of PQC must respect tight performance thresholds. Computational overhead must remain flat, and latency spikes are institutional deal-breakers. The deployment baseline is uncompromising: zero downtime for live stacks and zero new vulnerabilities injected into the defence architecture.

4.1 Legacy Systems and Crypto-Agnostic Architectures

To account for heterogeneity of system architecture, especially long-lived ones, crypto-agnostic designs deal with it. Agile deployments use modular wrappers to run parallel classical and post-quantum backends. Running both algorithms side-by-side, lets teams migrate gradually at their own pace without risking downtime or breaking user trust.

Within ENISA, cryptographic agility has ceased to be merely an architectural choice and has become mandatory. With quite clear technical guidelines: integrate modular libraries such as liboqs (OpenQuantumSafe) [38], standardize hybrid key exchanges, and centralize key management. INCIBE follows a similar path, requiring detailed hardware inventories to plan adaptations before implementing any code [39]. In Portugal, the PTQCI programme is putting these ideas into practice [29]. The National Security Office (GNS) coordinates PTQCI as national authority and Deimos Engenharia, with execution by INESC TEC and CNCS oversight via QNRC, these public sector pilot projects serve as real-world testing grounds. While the pilot projects prove that the code works, scaling it is a different challenge. Engineers still face the difficult task of integrating modern cryptography into fragile and legacy systems that simply weren't designed for larger encryption keys.

4.2 Algorithmic Complexity and Performance Trade-offs

Post-quantum algorithms inflict a heavy toll on computational cycles, bandwidth allocation, and architectural complexity [20], [40]. As outlined in earlier benchmarks (Section 2.2), adopting ML-KEM and ML-DSA introduces severe bandwidth penalties that simply do not exist in legacy RSA or ECC architectures. While this resource drain severely complicates deployments in constrained IoT environments and time-sensitive infrastructure [23], [20], these lattice primitives stretch the limits of embedded systems without breaking them. SLH-DSA, by contrast, presents an actual hard limit; its bloated signatures instantly disqualify it from low-power silicon. This is exactly why NIST settled on ML-KEM and ML-DSA. Out of all the options, they alone deliver robust mathematical security without blowing past the memory limits of constrained hardware [20].

Mathematical models rarely survive contact with actual silicon. Figure 1 shows the raw performance telemetry of ML-KEM (Kyber-768) on limited hardware, on constrained silicon against classical RSA-2048 and ECC-P256 standards. Real tests [21] and hardware-level optimisation studies [41], [18] show that ML-KEM decisively outperforms RSA in key generation and decapsulation, matching ECC execution speeds. This confirms that the main issue is now bandwidth, not processing power.

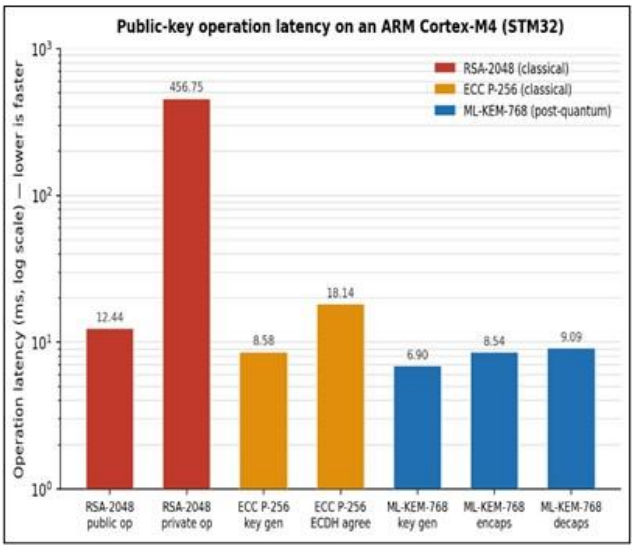

Fig. 1. Public-key operation latency on an ARM Cortex-M4 (STM32), logarithmic scale (lower is faster). ML-KEM-768 (Kyber-768) key generation, encapsulation and decapsulation are compared against RSA-2048 and ECC P-256 (secp256r1) operations measured on the same board. Sources: wolfSSL Cortex-M4 benchmark suite [63]; ML-KEM-768 cycle counts are consistent with the pqm4 reference results [21].

Thanks to this efficiency, ML-KEM is now practical for embedded environments. INESC TEC demonstrated that Jasmin maintains standard hardware speeds without compromising security [24]. When selecting algorithms for critical sectors, bare-metal verification is mandatory; pure theoretical modelling is no longer enough. While post-quantum logic is functionally viable for IoT, the actual optimisation work remains scattered and lacks direction [20].

4.3 Protocol Interoperability and Certificate Chains

Adding post-quantum mechanisms to legacy protocols is architecturally complex and creates considerable friction. Existing RSA and ECC infrastructure must suddenly process quantum-resistant certificates. Breaking the established trust chains is not an option. This integration is usually difficult, so the IETF and ETSI got involved directly with hybrid specifications for TLS 1.3, SSH and IPSec. Running classical and post-quantum algorithms side-by-side provides the technical fix. This preserves forward secrecy and stops legacy architecture from crashing.

4.4 Side-Channel Vulnerabilities

The new quantum-resistant cryptographic algorithms offer strong mathematical defence against quantum attacks; but they remain vulnerable to traditional risks like insecure implementation and side-channel attacks, including timing, electromagnetic, power, and fault injection. Attackers extract secret keys directly from poorly implemented hardware or software. The underlying mathematical difficulty simply ceases to matter [43]. Ultimately, even if the underlying PQC algorithms remain secure for decades, poorly designed implementations can give attackers an advantage.

Falcon is the perfect example of this physical risk. Its reliance on floating-point arithmetic creates inherent timing leaks. Achieving constant-time execution on standard hardware is operationally unstable. Protocols using lattices, such as ML-KEM (Kyber) and ML-DSA (Dilithium), have their own physical vulnerabilities. If engineers fail to implement stringent masking or shuffling, these systems simply leak private key bits during power fluctuations [43], [44]. ANSSI identified this systemic implementation flaw within the European framework [15]. This left the European Commission with little choice. Under the Cyber Resilience Act (CRA), side-channel resistance is no longer optional.

Neutralising side-channel leakage is currently a massive engineering priority; academia and industry are both building countermeasures, though their methods differ. In Portugal, researchers at the University of Porto advance the way of protecting these PQC through a complex mix of masking, constant-time arithmetic, and hardware noise injection to blind side-channel sensors. Conversely, the commercial strategy takes a more pragmatic route for embedded architectures like ARM and RISC-V. To address this, vendors rely on specialised libraries written specifically for constant-time execution. This effectively breaks the link between instruction timing and the actual cryptographic data [22].

4.5 Symmetric Cryptography and Key Dimensioning

Quantum computers focus mainly on asymmetric methods. But symmetric methods, such as AES and SHA, will not remain safe either. Grover’s algorithm accelerates the search, effectively cutting the security strength of current keys in half. There is no instantaneous breach here, but architectural inspection has to start now. Engineers must prove their current cryptographic density can sustain data confidentiality through the next decade.

From a design perspective the solution to this problem is very easy, we only need to double the key size. Since AES-128 is obsolete, AES-256 has become the standard for quantum-resistant architectures. Going a step further, France's ANSSI strictly limits block encryption to AES-256 and raises the baseline for cryptographic hashing to SHA-2-384. This requirement is more stringent than both NIST and BSI currently allow [14]. ANSSI enforces this to shield high-value assets (such as state secrets) and sensitive information (like medical records and industrial blueprints). This data simply must remain confidential well beyond the 2030 quantum threshold [3].

4.6 Cryptographic Lifecycle Management

Integrating post-quantum primitives isn't just a simple drop-in replacement; it requires a complete rebuilt of how we manage the cryptographic lifecycle. With larger keys and signatures comes a heavier toll on storage and bandwidth, ultimately forcing us to redesign existing protocols. Because of this, any Key Management Infrastructure (KMI) needs to handle hybrid environments natively. This means building in automated renewal and auditing features explicitly designed for PQC. NIST IR 8547 sets a strict order of operations here. No infrastructure upgrades should begin until IT teams have completely inventoried their assets and triaged the risks [45].

Portugal's CNCS utilises this exact framework to determine transition readiness. The agency conducts deep technical assessments (such as configurations) and mandatory governance checks. The aim is to ensure robust compliance with NIS2 and the Cyber Resilience Act (CRA). This strategy follows the QNRC’s lead on continuous risk evaluation [9]. Regulatory theory and practice now clash. Regulatory standards currently evolve much faster than any security team can reasonably manage.

V. ETHICAL, ECONOMIC, AND GOVERNANCE CONSIDERATIONS

Migrating to PQC isn't a routine update; it rewrites the entire rulebook for digital governance, upending the long-standing trust models between the state and its citizens. The choice of how to implement will be crucial for the future of trust as well as for the future of Europe's technological self-reliance. It sharpens a long-standing question: who ultimately controls the data?

5.1 Privacy, Surveillance, and Citizen Autonomy

Confidentiality is the stated objective of PQC. The migration itself risks a disproportionate concentration of power over cryptographic baselines. Governments and tech giants could use the transition to push for new rules or backdoors in the tools, using national security as a pretext. This is not a new concern, given the long history of tension between state control and individual privacy [46]. This divide grows as standardisation becomes less clear and more complicated.

In the EU, this debate anchors on ‘standard sovereignty’. The European Parliament Research Service points to a tough decision: Do we just adopt US NIST standards, or do we fund independent European research? Europe’s reliance on foreign cryptography is systemic [47].

The risk is severe. If a foreign agency manages to develop quantum decryption capabilities before any other entity, it will gain unrestricted access to global communications at will. This would be a massive blow to national security and strategic autonomy, especially for smaller states and the privacy of their citizens [48]. For this reason, many agree that transparency and open scrutiny are the baseline for acceptance. Organisations must implement specific strategies to neutralize retroactive decryption and unequal access [49]. Without real oversight from different stakeholders, democratic accountability in cryptography will be impossible to maintain.

5.2 Economic Implications and Industrial Readiness

Many industries will have to replace parts of their base hardware. The current labour market shows a marked shortage of relevant skills, making execution incredibly difficult. This pressure fractures budgets at every level, from government agencies to the small suppliers that keep them running. For most organisations, this is not a stopgap solution, but a complete transformation, forcing security investments that will consume budgets intended for immediate digital priorities.

SMEs operate on minimal margins. Now, they are absorbing a double shock. They face the additional burden of NIS2 requirements, as noted in the ECSO White Paper [50]. Legal compliance on one side and post-quantum migration on the other. To address this specific deficit, Digital Europe and Horizon Europe fund projects such as QARC and FOCAL [51,53]. With the main objective of taking quantum computing-resistant technology out of academic papers and installing it directly into real corporate networks.

Portugal is under significant pressure from the transition timetable. The CNCS, through the National Coordination Centre (NCC-PT), channels EU capital directly to national entities [27]. This converts subsidies on paper into industrial power. Wealthy economies like Germany and France have the fiscal strength to build their own defences. Smaller nations are, in practice, left waiting for Brussels. The risk here is resilience at multi-speed. In practice, geography risks becoming a stronger determinant of security than formal policy.

5.3 Governance and International Cooperation

Managing this transition presents a considerable challenge in terms of governance and deep international cooperation, as well as requiring new strategies at national level. With the aim of preventing total digital fragmentation within the EU, the bloc is introducing regulations designed to reduce its heavy reliance on foreign certifications. The strategic alignment between Germany's BSI, France's ANSSI and Spain's INCIBE creates a united front. The agency actively influences policies within the framework of ECSO, PQC4EU, and ECCC, never acting as a passive observer. Portugal integrates into this framework through the CNCS.

The ‘risk window’ first opened in 2024, and long-term data protection was no longer optional [3]. The rules of the EU and the reality of quantum mechanics are in conflict, the Member States must resolve this major problem immediately. From 2026, the focus will be on adopting and certifying hybrids, with a small window before the CRQC deadline of 2030. As Table II shows, the EU’s Roadmap and Portugal’s initiatives (particularly the 2026 mandate for public procurement) as critical countermeasures to a timeline that is shrinking. Updating trust anchors before the 2035 standardisation deadline is mandatory. Implementing the discovery and prioritisation workflows from NIST IR 8547 [45] is essential to secure the Union's networks before legacy encryption becomes obsolete

TABLE II. PQC STRATEGIC TIMELINE: ALIGNMENT OF THREAT AND COMPLIANCE MILESTONES

Year	Quantum Threat Phase (GRI) [3]	Regulation and Governance (EU)	National Action (Portugal)
2024	**Start of risk window**: protection of long-term data is critical.	NIS2 and CRA in force, defining mandatory PQC-related risk management.	NIS2 transposition; application of QNRC for PQC readiness.
2025	**Critical technical decisions**: shift to hybrid as the de facto standard.	Hybrid mandate consolidated; publication of the EU Coordinated Implementation Roadmap for PQC under Recommendation (EU) 2024/1101.	PTQCI implementation; acceleration of C-Academy training.
2026	**Large-scale hybrid adoption**: focus on testing and deployment of PQC solutions.	Initial PQC certifications; PQC libraries start to gain official approval.	PQC mandate in public procurement and national compliance requirements.
2030	**CRQC threshold**: risk window reaches its highest probability point.	End of isolated classical cryptography; standards bodies cease recommending non-hybrid classical schemes.	Complete migration of critical-infrastructure trust anchors.
2035	**Point of no return**: PQC becomes the baseline requirement.	PQC ubiquity: PQC is the new global standard.	Consolidation of Portugal’s quantum security architecture.

2024	**Start of risk window**: protection of long-term data is critical.	NIS2 and CRA in force, defining mandatory PQC-related risk management.	NIS2 transposition; application of QNRC for PQC readiness.
2025	**Critical technical decisions**: shift to hybrid as the de facto standard.	Hybrid mandate consolidated; publication of the EU Coordinated Implementation Roadmap for PQC under Recommendation (EU) 2024/1101.	PTQCI implementation; acceleration of C-Academy training.

To position Portugal analytically rather than descriptively, Table III compares its post-quantum posture against three larger Member States that the literature treats as European reference points: Germany, France and Spain. The comparison is structured along four governance dimensions - the status of NIS2 transposition, the lead national authority, the official stance on hybrid PQC, and the flagship national initiative - drawn from the agencies' own published guidance and legal instruments.

TABLE III. COMPARATIVE POST-QUANTUM GOVERNANCE POSTURE OF SELECTED EU MEMBER STATES

Member State	NIS2 transposition status	Lead national authority	Official stance on hybrid PQC	Flagship national PQC / quantum initiative
Portugal	Transposed via Decree-Law 125/2025 [33]	CNCS (also NCC-PT)	Aligned with the EU hybrid-first approach	PTQCI quantum-communications infrastructure; C-Academy training (PRR-funded)
Germany	Transposition underway (national law in progress)	BSI	Hybrid mandatory (TR-02102-1) [14]	Strong national standardisation and HSM/industry base
France	Transposition underway (national law in progress)	ANSSI	Hybrid mandatory; stricter AES-256 / SHA-2-384 floor [15]	High-assurance sovereign cryptography guidance
Spain	Transposition underway (national law in progress)	INCIBE	Hybrid recommended; hardware-inventory-first [39]	Supercomputing and quantum-security programmes

Two structural contrasts emerge. First, Portugal's smaller institutional scale concentrates authority in a single coordinating body (the CNCS, which also acts as NCC-PT), shortening the chain between EU obligation and national execution relative to the more distributed German and French ecosystems; this is the coordination advantage noted in Section VII.2. Second, that same scale is a fiscal disadvantage: Germany and France can fund sovereign cryptographic capacity directly, whereas Portugal depends more heavily on channelled EU funding (PRR, Digital Europe), exposing it to the 'multi-speed resilience' risk discussed in Section V.2. The comparison therefore treats Portugal not as an isolated description but as a test of whether a smaller Member State can convert regulatory alignment into engineering capacity within the 2030 horizon.

5.4 Ethical Responsibility and the Future of Trust

The implementation of the PQC requires a rigorous review of cryptographic governance; encryption must remain a tool for absolute digital freedom. It must not become a hidden backdoor for state or corporate control. It is necessary to demand a rigorous examination of both the design principles and the origins of the technology.

The objectives of the 'Digital Decade' on the EU agenda stipulate that digital developments must safeguard the fundamental rights to privacy, security and transparency [54]. PQC cannot allow for exceptions. The creation of the 'Trustworthy PQC Ecosystems' envisaged by ENISA requires an end to unknown and hidden development cycles. Trust must be derived from open-source libraries with reproducible evidence and certification processes that verify their integrity.

When implemented correctly, quantum security goes beyond the role of a mere defensive mechanism; it will strengthen the social contract that binds all citizens, states, and the private sector itself. It is much more than a simple software update; proper implementation is the only way to keep Europe's core networks operational and fully independent.

VI. MITIGATION STRATEGIES AND CAPACITY BUILDING

The move to quantum-secure communications will require a big change in existing practices. Theory must become reality in engineering. Policy definition is no longer the primary strategic focus; the absolute priority is the aggressive acquisition of human capital capable of sustaining these systems.

6.1 Cryptographic Inventory and Risk Classification

A comprehensive inventory of information and cryptographic assets forms the absolute prerequisite for any large-scale transition. The NIS2 implementing regulations explicitly mandate strict asset inventory, cryptography policy, and key management [8]. Technical guidance from ENISA actively operationalises these exact rules [13]. Building a baseline inventory involves mapping all active cryptographic mechanisms, specifically identifying algorithms and their associated key lengths. Analysts are responsible for mapping dependent network protocols, including TLS, IPsec, and SSH. The audit catalogues Key Management Systems and certificate chains to ensure infrastructure integrity.

As a next step after listing, it is necessary to classify the data according to risk. The risk assessment should distinguish between active transactional data and short-lived data, with a 'cryptographic lifespan' of several decades, such as health records or industrial intellectual property. Naturally, these long-term assets are the prime targets for HNDL attacks.

These categories guide the risk stratification necessary for NCR. This is an iterative process that depends on continuous auditing of algorithmic maturity to ensure that the defence mechanisms remain effective. Only with a robust lifecycle management strategy can organisations comply with the technical standards set by ENISA [13].

6.2 Hybrid Cryptography: Bridging the Transition

The hybridisation response is a robust approach, given the fast-evolving nature of PQC standards. By fusing the NIST primitives (Section 2.1) with classical algorithms, this

architecture creates a cryptographic safety net. This provides a certain level of robustness; but it comes at a price, this robustness comes at the cost of greater complexity. Certificate Authorities (CA) and Public Key Infrastructure (PKI) may need revisions to handle composite keys and signatures [55]. To ensure interoperability with other systems, sticking to standards such as ETSI TS 103 744 [17] is non-negotiable [17].

The Cloud Security Alliance (CSA) provides a risk assessment framework to identify vulnerabilities in data protection. This methodology establishes a structured defence against attack vectors such as SNDL (Store Now, Decrypt Later) [56], a taxonomy synonymous with the HNDL threat profile.

Recent mandates from ANSSI and BSI have officially elevated hybridization from a recommended 'best practice' to a mandatory requirement [14,15]. In Portugal, the PTQCI consortium orchestrates the initiative, bringing together academic, government, and industry experts [28]. They are using pilot networks to test open-source cryptographic stacks, such as liboqs (OpenQuantumSafe). This enables the detection of integration errors in a test environment before they cause failures in the production system [40].

6.3 Workforce Training and Technical Certification

A talent vacuum in low-level systems engineering limits the PQC transition. The industry faces a critical shortage of professionals capable of bridging high-level cryptography with low-level infrastructure operations [47,50]. To overcome this severe talent shortage, there is an urgent need to expand specialised training programmes.

The C-Academy actively confronts this deficit. Operated by the CNCS and funded by the Recovery and Resilience Plan (PRR), the programme upskills public administration and essential service teams to execute the transition.

At the European level, the CyberSecPro Initiative restructures cybersecurity education [57]. Funded by the Digital Europe Programme, the project eradicates the gap between the way that cybersecurity is taught in the classroom (using academic models), and what employers expect of new employees. The effort to standardize skills within the Digital Single Market ensures that specialization in PQC ceases to be a elite specialization and becomes a fundamental and operational requirement for the entire Union.

6.4 Government and Critical Sector Incentives

Driving the quantum-safe transition demands a combination of regulatory pressure and modernisation grants for the smart manufacturing sector. The Digital Europe Programme underwrites this process by funding sovereign cybersecurity efforts across Member States [57]. These funds are then used by national coordination centres to encourage local industries to drive quantum-resistant innovation.

Portugal has made a significant change to its legal landscape with the enactment of Decree-Law No. 125/2025. By transposing the NIS2 Directive with this law, cryptography is elevated to a central legal pillar in risk management, under the terms of Article 21 [33]. This removes any sense that cryptographic upgrades are optional: adherence to NIST standards becomes a prerequisite. For operators of essential services, this is no longer merely a recommended practice; it is an obligatory requirement.

In addition to regulatory requirements, market dynamics are accelerating PQC implementation. Cyber insurance providers are increasing the eligibility of coverage for ties to advance migration, establishing it as a standard risk management metric. At the same time, governments are using their buying power to force change. Public procurement contracts now often depend on meeting the supply chain security rules defined by NIS2. This is in line with the World Economic Forum's goal of a 'safe quantum economy'. For organisations targeting regulated markets, implementing PQC functions is a strict condition for commercial viability in relation to simple operational costs [58].

VII. FUTURE PERSPECTIVES

We are no longer at the ‘proof-of-concept’ stage. The real fight now is making sure that basic systems can deal with the mix of new math and strict legal requirements. This requires deploying lattice-based algorithms and hybrid key encapsulation mechanisms (KEMs) to secure legacy networks against future quantum decryption.

7.1 Global Technology Evolution

The rate of PQC implementation currently corresponds to the level of hardware development. PQC-ready silicon and secure elements are entering production, HSMs execute lattice-based schemes natively. Native execution makes it possible to eliminate the performance overhead as discussed in Section IV.2. These hardware advancements support NIST's 'PQC 2.0' initiative prioritizing algorithms designed for constrained environments [19].

The mobile messaging sector has emerged as the primary frontline for PQC deployment. Applications such as Signal and Apple's iMessage currently use hybrid cryptographic protocols, integrating classical and post-quantum primitives, to ensure data confidentiality [59,60]. Despite these advances, implementation is not yet the industry standard. Until PQC libraries become standard in the main development tools, the market will not change.

In high-security environments, such as defence and diplomacy, hybrid cryptographic architectures are increasingly required. Organizations are combining PQC mathematics with the physical security of Quantum Key Distribution (QKD). The overlay of the BB84 optical protocol with PQC [61] mitigates the intrinsic vulnerabilities of relying on either technology in isolation [16,28,62].

Blockchain networks are currently undergoing similar structural changes. Current decentralized identity projects substitute legacy signatures with Dilithium and Merkle tree constructions. This technical transition is necessary to meet EU regulations for long-term verifiable records [44].

7.2 Portugal’s Strategic Opportunity

From an operational perspective, Portugal's demographic scale presents a distinct benefit. Coordinating national authorities and research institutions (such as INESC TEC and IPN Coimbra) naturally requires fewer intermediary steps in a smaller economy. In this context, it suggests that Portugal may be able to implement security structures more quickly than larger Member States, which typically have to deal with much more complex administrative layers.

Practical deployment is currently underway through the PTQCI framework, which utilizes quantum-secure network segments to measure protocol overhead and latency impacts. Concurrently, updating infrastructure for eIDAS 2.0 compliance provides a direct pathway to test PQC within national digital identity systems. This parallel work ensures citizen certificates will meet upcoming cryptographic regulations without operational delays.

By focusing on the intensive training of professionals across the country, the C-Academy directly mitigates the cybersecurity skills deficit identified in Section V.2. If it is carried out well, it could change Portugal's role from a predominantly technology consumer towards a more active contributor, and could, over time, provide a useful reference for similar projects in the Union.

VIII. LIMITATIONS

This study has several limitations that bound its conclusions. First, it relies exclusively on secondary and documentary sources - regulatory texts, standards, agency guidance, peer-reviewed literature and official programme documentation - and does not generate primary benchmark data or field measurements; the performance figures discussed are drawn from the cited implementations rather than re-measured here. Second, the case study is single-country and instrumental: it is designed to illustrate the governance-to-engineering transition in one smaller Member State, not to provide a statistically representative sample of the EU, so its findings transfer analytically rather than statistically. Third, quantitative indicators of national-programme effectiveness - for example, the number of professionals trained through C-Academy or the measured latency overhead of PTQCI segments - are not yet publicly reported in a verifiable form; where such figures are unavailable we have refrained from estimating them, and we flag their collection as future work. Fourth, the comparative dimension is based on publicly documented national positions and may not capture non-public operational progress. Finally, the field is evolving rapidly: standardisation (such as the HQC selection and the additional-signatures on-ramp), national transpositions and the EU roadmap continue to change, so specific figures and milestones reflect the state of knowledge as of December 2025 and should be read as a snapshot.

IX. CONCLUSION

PQC has moved from theoretical research to practical implementation in critical infrastructures. With the enforcement of NIS2 and the Cyber Resilience Act, the period of observation is over. For the operators of our essential backbones, treating cryptographic agility as a mere best practice is simply no longer an option under the current legal frameworks.

Portugal is responding to this pressure through the QNRC and with pilot projects such as the PTQCI; but, as expected, implementation itself is proving difficult. We are dealing with technical debt, budgetary constraints and a severe skills shortage, which C-Academy is seeking to address. This is more than a routine update; it is a major overhaul of systems that must remain online. The Portuguese case illustrates the broader European challenge: translating NIS2 and CRA obligations into cryptographic engineering while keeping critical services operational.

The real test for these new standards is whether cryptography remains a tool that supports democratic freedoms instead of an opaque control mechanism. Success here depends entirely on maintaining the social trust that characterises the European digital space.

REFERENCES

[1] P. W. Shor, “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer,” *SIAM J. Comput.*, vol. 26, no. 5, pp. 1484-1509, Oct. 1997, arXiv:quant-ph/9508027

[2] L. K. Grover, “A fast quantum mechanical algorithm for database search,” in *Proc. 28th Annu. ACM Symp. Theory Computing. (STOC ‘96),* Philadelphia, PA, USA, May 1996, pp. 212-219, arXiv:quant-ph/9605043

[3] M. Mosca and M. Piani, “*Quantum Threat Timeline Report 2024*,” Toronto, Canada, Dec. 2024. [Online]. Available: https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/

[4] I. G. Martins, "Centro Nacional de Cibersegurança: 'Não falta muito tempo para termos computadores quânticos capazes de quebrar os mecanismos de cifra'," *IT Security*, May 22, 2025. [Online]. Available: https://www.itsecurity.pt/news/its-conference/centro-nacional-de-ciberseguranca-nao-falta-muito-tempo-para-termos-computadores-quanticos-capazes-de-quebrar-os-mecanismos-de-cifra-com-video-

[5] National Institute of Standards and Technology, “Module-Lattice-based Key-Encapsulation Mechanism Standard,” *Federal Information Processing Standards (FIPS) Publication 203*, Gaithersburg, MD 20899-8900, USA, Aug. 2024, DOI: 10.6028/NIST.FIPS.203

[6] National Institute of Standards and Technology, "Module-Lattice-Based Digital Signature Standard," *Federal Information Processing Standards (FIPS) Publication 204*, Gaithersburg, MD 20899-8900, USA, Aug. 2024, DOI: 10.6028/NIST.FIPS.204

[7] National Institute of Standards and Technology, "Stateless Hash-Based Digital Signature Standard," *Federal Information Processing Standards (FIPS) Publication 205*, Gaithersburg, MD 20899-8900, USA, Aug. 2024, DOI: 10.6028/NIST.FIPS.205

[8] European Parliament and Council of the European Union, “Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union,” *Official Journal of the European Union*, vol. L 333, pp. 80-152, Dec. 27, 2022, ELI: https://data.europa.eu/eli/dir/2022/2555/oj

[9] Portuguese National Cybersecurity Centre (CNCS), *National Cybersecurity Framework (NCF-PT/QNRC)*, ver. 1.0. Lisbon, Portugal: CNCS, Apr. 2020. [Online]. Available: https://www.cncs.gov.pt/docs/qnrcs-web-eng.pdf

[10] Portuguese National Cybersecurity Centre (CNCS), “*C-Academy*,” 2024. [Online]. Available: https://www.cncs.gov.pt/en/c-academy

[11] C. Paar and J. Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners*. Berlin, Heidelberg: Springer, 2010, DOI: 10.1007/978-3-642-04101-3

[12] European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape 2023, *Publications Office of the European Union*, Luxembourg, Oct. 2023, DOI: 10.2824/782573

[13] European Union Agency for Cybersecurity (ENISA), Technical Implementation Guidance on Cybersecurity Risk Management Measures, *Publications Office of the European Union*, Luxembourg, Tech. Rep. Version 1.0, Jun. 2025, DOI: 10.2824/270254

[14] BSI, “Cryptographic Mechanisms: Recommendations and Key Lengths (BSI TR-02102-1),” *Federal Office for Information Security, Bonn*, 2025. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?__blob=publicationFile&v=9

[15] ANSSI, "Avis de l’ANSSI sur la migration vers la cryptographie post-quantique (suivi 2023)", Agence nationale de la sécurité des systèmes d’information, Paris, France, *Technical Report ANSSI-PA-098 v1.0*, Dec. 2023. [Online]. Available: https://messervices.cyber.gouv.fr/documents-guides/anssi-avis-migration-vers-la-cryptographie-post-quantique.pdf

[16] S. Ricci, P. Dobias, L. Malina, J. Hajny, and P. Jedlicka, "Hybrid Keys in Practice: Combining Classical, Quantum and Post-Quantum

Cryptography," *IEEE Access*, vol. 12, pp. 28835-28849, Feb. 2024, DOI: 10.1109/ACCESS.2024.3364520

[17] European Telecommunications Standards Institute (ETSI), "Quantum-safe Hybrid Key Establishment," ETSI, Sophia Antipolis, France, *Technical Specification TS 103 744 V1.2.1*, Mar. 2025. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/103700_103799/103744/01.02.01_60/ts_103744v010201p.pdf

[18] National Institute of Standards and Technology (NIST), "Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process," *NIST Interagency/Internal Report (NISTIR) 8413*, Gaithersburg, MD, USA, Sep. 2022, DOI: 10.6028/NIST.IR.8413-upd1

[19] National Institute of Standards and Technology (NIST), "Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process," *NIST Interagency/Internal Report (NIST IR) 8545*, Gaithersburg, MD, USA, Mar. 2025, DOI: 10.6028/NIST.IR.8545

[20] T. Liu, G. S. Ramachandran, and R. Jurdak, "Post-Quantum Cryptography for Internet of Things: A Survey on Performance and Optimization," Jan. 2024, arXiv:2401.17538

[21] M. J. Kannwischer, J. Rijneveld, P. Schwabe, and K. Stoffelen, "pqm4: Testing and benchmarking NIST PQC on ARM Cortex-M4," *IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES)*, vol. 2019, no. 4, pp. 295-321, 2019, DOI: 10.13154/tches.v2019.i4.295-321

[22] PQShield, "PQCryptoLib-Embedded and the Quantum Threat," *PQShield Product Insights*, Nov. 04, 2024. [Online]. Available: https://pqshield.com/pqcryptolib-embedded-and-the-quantum-threat/

[23] A. Astarloa, J. Lázaro, and J. I. Gorate, "CRYSTALS-Dilithium post-quantum cyber-secure SoC for wired communications in critical systems," *Internet of Things*, vol. 33, Art. no. 101656, 2025, DOI: 10.1016/j.iot.2025.101656

[24] J. B. Almeida et al., "Jasmin: High-Assurance and High-Speed Cryptography," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS)*, Dallas, USA, 2017, pp. 1807-1823, DOI: 10.1145/3133956.3134078

[25] European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape 2025, *Publications Office of the European Union*, Luxembourg, Oct. 2025, DOI: 10.2824/1946374

[26] German Federal Office for Information Security (BSI), "Joint Statement on Post-Quantum Cryptography Transition," 2025. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement-2025.pdf?__blob=publicationFile&v=3

[27] Portuguese National Cybersecurity Centre (CNCS), Portugal, "NCC-PT - National Coordination Centre in Portugal," 2024. [Online]. Available: https://www.cncs.gov.pt/en/ncc-pt-centro-nacional-de-coordenacao/

[28] Portuguese Quantum Communications Infrastructure (PTQCI), "*Official Website/Project Documentation*," 2025. [Online]. Available: https://www.ptqci.pt/

[29] Instituto de Telecomunicações, "*PTQCI - Portuguese Quantum Communications Infrastructure*," Project No. 4845. [Online]. Available: https://www.it.pt/Projects/Index/4845

[30] INESC TEC, "Estudo sobre a Comunidade de Competências em Cibersegurança: Relatório Julho 2023," *Centro Nacional de Cibersegurança (CNCS)*, Lisboa, Portugal, Jul. 2023. [Online]. Available: https://www.cncs.gov.pt/docs/comcompciber-obcibercncs.pdf

[31] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 9 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 1025/2012 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), *Official Journal of the European Union*, L 2024/2846, 23 Oct. 2024, ELI: https://data.europa.eu/eli/reg/2024/2847/oj

[32] Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen the Union's solidarity and capabilities to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act), *Official Journal of the European Union*, L 2025/38, 15 January 2025, ELI: https://data.europa.eu/eli/reg/2025/38/oj

[33] Portugal, Decreto-Lei n.º 125/2025, de 4 de dezembro, Aprova o regime jurídico da cibersegurança, transpondo a Diretiva (UE) 2022/2555, *Diário da República*, 1.ª série, n.º 234, pp. 1-65, 4 Dec. 2025, ELI: https://data.dre.pt/eli/dec-lei/125/2025/12/04/p/dre/pt/html

[34] European Commission, "Commission Recommendation (EU) 2024/1101 of 11 April 2024 on a coordinated implementation roadmap for the transition to post-quantum cryptography," *Official Journal of the European Union*, L 2024/1101, 2024, ELI: https://data.europa.eu/eli/reco/2024/1101/oj

[35] European Commission, "A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography," *NIS Cooperation Group*, Tech. Rep. Part 1, Version 1.1, Jun. 2025. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

[36] ENISA, "NIS Investments 2024: Cybersecurity Policy Assessment," *European Union Agency for Cybersecurity*, Report, Nov. 2024. [Online]. Available: https://www.enisa.europa.eu/publications/nis-investments-2024

[37] CNCS, "*Portal C-Academy - Roteiro NIS 2," Centro Nacional de Cibersegurança*, 2025. [Online]. Available: https://www.c-scademy.pt/CNCS/web/roteiro/

[38] Open Quantum Safe Project, *liboqs - C Library for Post-Quantum Cryptography*, 2025. [Online]. Available: https://openquantumsafe.org/liboqs/

[39] INCIBE, "*Cibersecurity in supercomputing and quantic computing*," Madrid, Sep. 18, 2025. [Online]. Available: https://www.incibe.es/en/incibe-cert/blog/cibersecurity-supercomputing-and-quantic-computing

[40] J. Hekkala, M. Muurman, K. Halunen, and V. Vallivaara, "Implementing Post-quantum Cryptography for Developers," *SN Computer Science*, vol. 4, no. 365, 2023, DOI: 10.1007/s42979-023-01724-1

[41] O. Alnaseri, Y. Himeur, S. Atalla, and W. Mansoor, "Complexity of Post-Quantum Cryptography in Embedded Systems and Its Optimization Strategies," in *2025 International Wireless Communications and Mobile Computing (IWCMC)*, Dubrovnik, Croatia, May 2025, pp. 776-781, DOI: 10.1109/IWCMC65282.2025.11059522

[42] A. A. Fall, "SoK: Systematizing Hybrid Strategies for the Transition to Post-Quantum Cryptography," *IACR Eprint*, 2025. [Online]. Available: https://eprint.iacr.org/2025/2052.pdf

[43] P. V. Ravi, S. S. Roy, A. Chattopadhyay, and S. Bhasin, "Generic Side-Channel Attacks on CCA-Secure Lattice-Based PKE and KEMs," *IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES)*, vol. 2020, no. 3, pp. 307-335, Aug. 2020. DOI: 10.13154/tches.v2020.i3.307-335

[44] Y. Wang and E. S. Ismail, "A Review on the Advances, Applications, and Future Prospects of Post-Quantum Cryptography in Blockchain and IoT," *IEEE Access*, vol. 13, pp. 1-25, 2025, DOI: 10.1109/ACCESS.2025.3584473

[45] National Institute of Standards and Technology (NIST), *NIST IR 8547 ipd (Initial Public Draft): Transition to Post-Quantum Cryptography Standards*, Nov. 2024, DOI: 10.6028/NIST.IR.8547.ipd

[46] M. Wimmer and T. G. Moraes, "Quantum Computing, Digital Constitutionalism, and the Right to Encryption: Perspectives from Brazil," *Digital Society*, Springer, 2022, DOI: 10.1007/s44206-022-00012-4

[47] S. De Luca and T. Marcelin, "Cryptographic security: Critical to Europe's digital sovereignty," *European Parliamentary Research Service (EPRS)*, Briefing PE 766.237, Brussels, Belgium, Nov. 2024. [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/766237/EPRS_BRI(2024)766237_EN.pdf

[48] A. Ganz et al., "Submarine Cables and the Risks to Digital Sovereignty," *Minds and Machines*, Springer, 2024, DOI:10.2139/ssrn.4693206

[49] R. Coates, D. Douglas, and M. Per, "AI and quantum computing ethics: Same but different? Towards a new sub-field of computing ethics," *Quantum Science and Technology*, vol. 10, no. 3, Art. no. 035030, May 2025, DOI: 10.1088/2058-9565/add9c2

[50] European Cyber Security Organisation (ECSO), "NIS2 Implementation: Challenges and Priorities," Brussels, *Belgium, White Paper*, Jan. 2025. [Online]. Available: https://ecs-org.eu/ecso-uploads/2025/01/ECSO-NIS2-White-Paper.pdf

[51] European Commission, "The Digital Europe Programme", *Publications Office of the European Union*, Luxembourg, 2025. [Online]. Available: https://digital-strategy.ec.europa.eu/en/activities/digital-programme

[52] European Commission, "*Quantum-Resistant Cryptography in Practice (QARC)*," CORDIS Project 101225691, Jun. 2025, DOI: 10.3030/101225691

[53] European Commission, "*Functional cOmposition of post quantum Cryptosystems At Large (FOCAL)*," CORDIS - Projects ID 101225859, Jul. 2025, DOI: 10.3030/101225859

[54] European Commission, European Declaration on Digital Rights and Principles for the Digital Decade, 2023/C 23/01, *Off. J. Eur. Union*, Jan. 23, 2023, CELEX: 32023C0123(01)

[55] C. Paquin, D. Stebila, and G. Tamrakar, "Benchmarking Post-Quantum Cryptography in TLS," *IACR Cryptology ePrint Archive*, Report 2019/1447, 2019. [Online]. Available: https://eprint.iacr.org/2019/1447

[56] Cloud Security Alliance (CSA), "A Practitioner's Guide to Post-Quantum Cryptography," *Quantum-Safe Security Working Group*, Publication, Jan. 2025. [Online]. Available: https://cloudsecurityalliance.org/artifacts/a-practitioners-guide-to-post-quantum-cryptography/

[57] European Commission, "Project CyberSecPro: Living-Lab for Cybersecurity Professional Training," *Digital Europe Programme (DIGITAL)*, Grant Agreement No. 101083594, Fact Sheet, 2025. [Online]. Available: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/43152860/101083594/DIGITAL

[58] World Economic Forum, "Transitioning to a Quantum-Secure Economy," *White Paper*, Geneva, Switzerland, Sep. 2024. [Online]. Available: https://www.weforum.org/publications/transitioning-to-a-quantum-secure-economy/

[59] Signal Messenger LLC, "*Signal Protocol and Post-Quantum Ratchets*," Signal, 2025. [Online]. Available: https://signal.org/blog/spqr/

[60] Apple Inc., "iMessage with PQ3: The new state of the art in quantum-secure messaging at scale," *Apple Security Research*, 2024. [Online]. Available: https://security.apple.com/blog/imessage-pq3

[61] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, Dec. 1984, pp. 175-179. [Reprinted in *Theor. Comput. Sci.*, vol. 560, pp. 7-11, 2014, DOI: 10.1016/j.tcs.2014.05.025]

[62] A. K. Fedorov et al., "Deploying hybrid quantum-secured infrastructure for applications: When quantum and postquantum can work together," *Front. Quantum Sci. Technol*, Apr. 2023, DOI: 10.3389/frqst.2023.1164428

[63] wolfSSL Inc., "Post-quantum Kyber benchmarks on ARM Cortex-M4 (STM32)," *wolfSSL Benchmarks*, 2024. [Online]. Available: https://www.wolfssl.com/post-quantum-kyber-benchmarks-arm-cortex-m4/