247 ENERGY

Quantum Technology and Energy Infrastructure:

Preparing for the Post-Quantum Era

What every energy storage operator and investor needs to understand.

James Troch
Chief Executive Officer
247 Energy NV
First published: 2023 | Updated: March 2026

FOREWORD

Why I Write About This Now

When I first wrote about quantum technology and its implications for energy infrastructure in 2023, the response from peers in our industry ranged from polite scepticism to genuine alarm. The concept of a quantum computer powerful enough to break the cryptographic foundations of modern communications seemed, to many, like science fiction with a horizon so distant that it barely warranted attention alongside more pressing operational concerns. I have always disagreed with that view, and the intervening years have confirmed why.

Energy infrastructure is not like a consumer application that can be patched overnight. The battery management systems, grid communication protocols, and control interfaces that underpin utility-scale energy storage facilities are designed to operate for decades. When we make architectural decisions today, those decisions carry consequences well into the 2030s and beyond. The question of whether to invest in quantum-safe security posture is therefore not a question about a future threat: it is a question about whether the systems we commission today will still be trustworthy when quantum computers reach operational maturity.

The March 2026 update to this paper reflects a landscape that has shifted considerably. The U.S. National Institute of Standards and Technology finalized its first suite of post-quantum cryptographic standards in 2024. The European Union has embedded quantum resilience requirements within its broader cybersecurity framework. Governments and regulators across the world have moved from awareness to mandate. The window for proactive transition is still open, but it is narrowing, and organizations that have not yet begun their cryptographic inventory will find themselves under growing pressure to accelerate.

At 247 Energy we have made a deliberate choice to keep security architecture at the centre of how we design and operate our battery energy storage parks. That commitment extends to quantum readiness. This paper sets out the context, the risk, and a practical path forward. I hope it serves as a useful reference for investors, operators, and policymakers who share our conviction that critical energy infrastructure deserves the most rigorous protection available.

James Troch,

Chief Executive Officer,

247 Energy

Why Energy Infrastructure Cannot Wait

A Threat That Is Already Active

Energy infrastructure occupies a unique position in the landscape of cybersecurity risk. Unlike financial services or telecommunications, where the assets under protection are primarily data and transactions, energy infrastructure couples digital systems to physical consequences. A compromised battery management system does not merely result in a data breach: it can trigger cascading failures in storage facilities, alter the behaviour of grid-connected assets, or expose sensitive operational data to adversaries who may use it to time future attacks. The stakes are, by any measure, higher than those faced by most other sectors.

Quantum computing introduces a specific and well-defined class of threat to these systems. The encryption methods that currently protect machine-to-machine communication, remote access protocols, firmware authentication, and data transmission within energy storage infrastructure rely on mathematical problems that classical computers cannot solve in any practical timeframe. Quantum computers, once they reach sufficient scale and stability, are expected to render several of these problems tractable. The algorithms most at risk include RSA and elliptic curve cryptography, both of which underpin the vast majority of public-key infrastructure deployed in critical systems today.

The timeline for this transition is uncertain, and that uncertainty is itself part of the problem. Estimates from leading research institutions suggest that cryptographically relevant quantum computers could emerge anywhere between the early 2030s and the mid-2040s. For operators making capital allocation decisions, this range is uncomfortably wide. Investment in new cryptographic infrastructure is expensive, time-consuming, and requires careful coordination across hardware, software, and operational layers. Beginning that process only when the threat materializes is not a viable strategy.

> ***There is a phenomenon known within the security community as 'harvest now, decrypt later.' Adversaries intercept and store encrypted communications today, with the intention of decrypting them once quantum capability becomes available. For energy infrastructure operators, this threat is not hypothetical: it is active and ongoing.***

Recognizing this dynamic, governments and standards bodies accelerated their work on post-quantum cryptography throughout the early 2020s. The convergence of regulatory activity, standards finalization, and growing awareness among infrastructure operators created a coherent, if still evolving, framework for action. This paper traces that framework and provides a practical guide to navigating it for organizations responsible for utility-scale energy assets.

Quantum Power and Cryptographic Vulnerability

Where Current Security Breaks Down

Quantum computing derives its power from the principles of quantum mechanics, specifically superposition and entanglement. Where a classical computer processes information in binary states, a quantum computer operates with quantum bits, or qubits, which can represent multiple states simultaneously. This property allows quantum computers to explore vast solution spaces in parallel, making them extraordinarily efficient at certain categories of mathematical problems. The most relevant of these categories for cryptography is the factoring of large integers and the computation of discrete logarithms, both of which form the mathematical foundation of widely used public-key encryption schemes.

The capacity to solve these problems at scale would not undermine all forms of cryptography equally. Symmetric encryption algorithms, including the Advanced Encryption Standard at 256-bit key lengths, remain resistant to known quantum attacks when implemented correctly. Hash functions used for data integrity verification retain significant security margins in the post-quantum era, provided key lengths are appropriately scaled. The vulnerability is concentrated in asymmetric, or public-key, cryptography, which is used extensively for key exchange, digital signatures, and authentication across virtually all networked systems.

Current quantum hardware remains far from the scale required to threaten production cryptographic systems. The most advanced quantum processors available operate with error rates that make sustained cryptographic attacks impractical. However, the trajectory of improvement is significant. Investment in quantum hardware from governments, technology companies, and venture capital has accelerated substantially, and academic progress in error correction, qubit coherence, and system integration has followed. The pace of development means that the gap between current capability and the threat threshold is narrowing, even if the precise timing of arrival at that threshold remains contested.

> ***The question is not whether quantum computers will eventually threaten current cryptographic standards, but how much preparation time remains before they do.***

Three distinct threat vectors are relevant to energy infrastructure operators. The first is the direct attack on encrypted communications, which becomes feasible once cryptographically relevant quantum hardware is available. The second is the harvest now, decrypt later threat, which is relevant to any data currently being transmitted over vulnerable channels. The third is the risk of supply chain compromise,

where quantum-capable adversaries could exploit vulnerabilities in hardware or software components sourced from third parties. Each of these vectors requires a different element of the response framework described in later sections.

ENERGY INFRASTRUCTURE AT RISK

The Cryptographic Exposure of Battery Storage Systems

More Than a Data Security Problem

Modern battery energy storage systems are sophisticated networked assets. A utility-scale storage park integrates battery management systems, energy management software, grid interconnection interfaces, remote monitoring and control capabilities, and communications links to grid operators and market platforms. Each of these integration points relies on cryptographic protocols to ensure that only authorized parties can issue commands, access data, or modify configuration parameters. The security of the entire installation is therefore only as strong as the cryptographic foundations underlying its most exposed communication pathways.

Battery management systems present a particular concern because they operate at the boundary between the digital control layer and the physical chemistry of the cells themselves. Commands issued through the BMS can affect charging rates, discharge cycles, temperature management, and safety mechanisms. The consequences of unauthorized access or command injection range from accelerated degradation of battery assets to, in the most serious cases, conditions that compromise the physical safety of the installation. Ensuring the integrity of the authentication mechanisms that protect BMS access is therefore not merely a data security matter: it is an operational safety imperative.

Grid interconnection interfaces add a further dimension of exposure. Communications between storage facilities and grid management systems typically traverse external networks and rely on encrypted channels to ensure that instructions to charge, discharge, or curtail output are authentic and unmodified. As energy storage assets are increasingly called upon to provide grid services such as frequency response, voltage regulation, and capacity management, the integrity of these communications becomes operationally critical. A compromised channel could allow an adversary to issue false instructions that affect grid stability at scale, particularly in markets where storage assets represent a significant proportion of available balancing capacity.

Remote monitoring and management capabilities, while essential to the commercial operation of distributed energy storage assets, expand the attack surface further. Operators and investors require

visibility into the operational performance of storage parks, including state-of-charge data, cycle counts, temperature profiles, and revenue metrics. Where this data is transmitted over encrypted connections that rely on public-key cryptography, it falls within the harvest now, decrypt later threat envelope. Commercially sensitive operational data intercepted today could reveal competitive intelligence or patterns of behaviour that inform future attacks.

Supply chain integrity represents an often-overlooked dimension of quantum risk. The hardware and software components that make up a utility-scale storage installation are sourced from a global market. Where provenance is poorly documented or components originate from high-risk jurisdictions, the possibility of embedded vulnerabilities cannot be discounted. Robust supply chain traceability is therefore a structural element of quantum resilience, not merely a conventional procurement concern.

POST-QUANTUM CRYPTOGRAPHY

The Emerging Standard

From Research to Finalized Specification

Post-quantum cryptography, abbreviated as PQC, refers to cryptographic algorithms designed to resist attacks from both classical and quantum computers. Unlike quantum key distribution, which requires specialized hardware and dedicated optical infrastructure, PQC algorithms are software-based and can be implemented on conventional computing hardware. This characteristic makes them far more practical for widespread deployment across existing infrastructure and represents the primary migration pathway for most organizations.

The process of standardizing PQC algorithms has been led by the U.S. National Institute of Standards and Technology, which initiated a public evaluation programme in 2016. After multiple rounds of analysis, testing, and community scrutiny, NIST selected a suite of algorithms for standardization in 2022 and finalized the first set of standards in 2024. The selected algorithms address both digital signatures and key encapsulation mechanisms, covering the principal use cases where public-key cryptography is currently deployed. The finalized standards represent a significant milestone, providing organizations with a stable technical foundation on which to base migration planning.

The transition to PQC is not a straightforward algorithmic swap. In practice, it requires a systematic inventory of all systems using cryptographic functions, an assessment of the sensitivity and longevity of the data those systems protect, a prioritized migration plan that sequences the transition from most to least critical, and an extended period of hybrid operation during which both classical and post-quantum

algorithms run in parallel. This hybrid approach is important because PQC algorithms have different performance characteristics from their classical counterparts, and some legacy hardware may not support the computational requirements of the new standards without modification or replacement.

> ***Post-quantum cryptography is not a distant aspiration: it is a finalized standard awaiting deployment across the infrastructure that supports modern energy systems.***

The transition is further complicated by the interdependency of cryptographic systems. A utility-scale storage facility does not operate its cryptographic infrastructure in isolation: it communicates with grid operators, cloud platforms, equipment vendors, and market systems, each of which runs its own cryptographic stack. Achieving end-to-end post-quantum security therefore requires coordination across an ecosystem of counterparties, not simply an internal upgrade programme. Early engagement with vendors and market platforms on their own PQC migration timelines is a necessary part of any serious transition planning effort.

THE TRANSITION FRAMEWORK

Four Steps for Infrastructure Operators

From Discovery to Execution

Organizations responsible for critical energy infrastructure require a structured approach to the post-quantum transition. The following four-step framework provides a practical sequence that balances the urgency of action with the operational realities of managing complex, long-lived assets. It is intended as a starting point rather than a comprehensive technical specification, and organizations should expect to engage specialist advisors as they move from assessment into implementation.

The first step is cryptographic discovery. Many organizations, including those with mature security practices, lack a complete picture of where cryptographic algorithms are deployed across their systems, applications, and communication interfaces. Cryptography is embedded in operating systems, firmware, network protocols, authentication mechanisms, and application layers in ways that are not always visible to operational or IT teams. A systematic cryptographic discovery exercise, which catalogues every instance of public-key cryptography in use, is the necessary foundation for all subsequent steps. Without this inventory, prioritization is impossible and migration planning lacks a factual basis.

The second step is data sensitivity assessment. Not all data protected by public-key cryptography carries the same risk profile in the post-quantum context. Operational data with a short useful life may represent a low priority for quantum-safe migration, even if it is currently transmitted over vulnerable channels. By

contrast, data with a long shelf life, including contractual information, proprietary performance benchmarks, grid topology data, or strategic operational parameters, warrants priority attention because it falls squarely within the harvest now, decrypt later threat envelope. Mapping data sensitivity to the cryptographic systems identified in step one yields a risk matrix that drives prioritization decisions.

The third step is system mapping and dependency analysis. Once the cryptographic inventory and data sensitivity assessment are complete, organizations should map the dependencies between their internal systems and the external platforms, vendors, and grid interfaces with which they communicate. This mapping will identify where post-quantum migration requires unilateral action, where it requires coordination with counterparties, and where legacy hardware or software constraints may slow or complicate the transition. It will also surface the most critical interdependencies, specifically those where a failure of cryptographic integrity in one system could propagate consequences across a wider operational ecosystem.

The fourth step is transition planning and execution. Drawing on the outputs of the first three steps, organizations can develop a phased cryptographic transition plan that sequences migration efforts by risk priority, coordinates with counterparties on shared timelines, identifies hardware or software components requiring replacement, and establishes a testing and validation programme to confirm that post-quantum implementations perform correctly under operational conditions. The plan should also address the hybrid operation period and include contingency arrangements for the possibility that migration timelines are compressed by unexpected acceleration in quantum hardware development.

ADJACENT QUANTUM OPPORTUNITIES

Communication, Sensing, and Optimisation

Beyond the Cryptographic Threat

While the primary focus of this paper is the cryptographic threat posed by quantum computing, the quantum technology landscape encompasses two additional domains that are likely to have significant implications for energy infrastructure over the coming decades. Quantum communication and quantum sensing represent opportunities rather than threats, but they share with quantum computing the characteristic that early awareness and considered positioning will yield substantial advantages over reactive adoption.

Quantum key distribution represents the most mature application of quantum communication technology. It exploits the properties of quantum mechanics to establish cryptographic keys between two

parties in a manner that is physically detectable if intercepted. Unlike PQC, which relies on mathematical complexity, QKD relies on the laws of physics to guarantee security. Current QKD implementations require dedicated optical fibre links or line-of-sight free-space channels, which limits their immediate applicability to point-to-point connections between facilities. For energy infrastructure, near-term applications are most plausible in connections between major substations or between storage facilities and central control systems.

Quantum sensing exploits the extreme sensitivity of quantum systems to physical perturbations. Quantum magnetometers, gravimeters, and accelerometers are already being explored for applications including underground infrastructure mapping, grid monitoring, and the detection of physical tampering with buried cables or conduits. For energy storage operators, quantum sensing technologies could eventually enable non-invasive inspection of battery chemistry, more precise monitoring of structural integrity in large-scale installations, and enhanced detection of physical intrusion. These applications remain largely at the research and early demonstration stage, but the pace of development has accelerated substantially.

Quantum computing, once available at sufficient scale, is expected to transform optimization problems in energy management, grid balancing, and storage dispatch that are currently addressed with classical heuristics. The combinatorial complexity of optimizing large numbers of distributed storage assets across variable renewable generation, dynamic demand, and market signals is precisely the class of problem that quantum optimization algorithms are designed to address. Organizations that have developed familiarity with quantum technology through their security transition programmes will be better positioned to evaluate and adopt these optimization capabilities as they mature.

Practical engagement with quantum technology does not require in-house expertise in quantum physics. Assessment tools developed by specialist organizations, including the Exploratory Quantum Technology Assessment developed by the Centre for Quantum and Society within the Dutch Quantum Delta NL network, provide a structured methodology for organizations wishing to evaluate the impact of quantum technology on their business and to develop a prioritized action plan. Engaging with such resources is a low-barrier starting point for organizations that have not yet systematically addressed their quantum exposure.

Quantum Readiness as Asset Protection

A Rational and Time-Limited Decision

The financial case for quantum readiness in energy infrastructure is best understood not as an incremental security expenditure but as a form of asset protection and future-proofing. Battery energy storage parks represent capital-intensive, long-lived investments. A utility-scale storage facility commissioned today is expected to generate revenue and provide grid services for fifteen to twenty years or more. The cryptographic infrastructure embedded in that facility, if not designed with post-quantum resilience in mind, may require costly and operationally disruptive remediation within the same timeframe. Early integration of PQC-compatible architecture into new projects eliminates this future liability.

For investors evaluating energy storage assets, cryptographic security posture is an increasingly relevant dimension of technical due diligence. As the regulatory landscape around quantum resilience firms up, assets that cannot demonstrate a credible migration pathway toward post-quantum compliance will face growing pressure from institutional investors, insurance providers, and grid operators. By contrast, assets built on architectures that incorporate modern security principles, including cryptographic agility and supply chain traceability, represent lower long-term risk profiles and are better positioned to meet emerging standards without disruptive capital remediation.

> ***Quantum readiness is not a cost centre: it is a form of asset protection for infrastructure designed to operate across multiple decades.***

The cost of inaction is asymmetric. The investment required to conduct a cryptographic inventory, develop a migration plan, and begin the transition to post-quantum standards is modest relative to the total capital deployed in a utility-scale storage project. The cost of a security failure resulting from cryptographic compromise includes not only the direct remediation expense but also reputational damage, potential regulatory sanction, operational downtime, and the erosion of counterparty trust. Against this asymmetry, proactive investment in quantum readiness is straightforwardly rational.

For developers and operators of energy storage parks, quantum readiness also represents a differentiation opportunity in a market where security credentials are becoming a procurement and partnership criterion. Grid operators, offtakers, and co-investors increasingly scrutinize the security architecture of the assets they connect to or fund. Demonstrating a structured, evidence-based approach to quantum risk positions an operator as a credible long-term steward of critical infrastructure, and that

positioning carries commercial value that extends well beyond the direct cost of the security investment itself.

TIMING AND URGENCY

The Window Is Narrowing

Why Deferred Action Is Not Neutral

The most common objection to investing in quantum readiness today is that the threat remains in the future. This objection misunderstands the structure of the risk. The harvest now, decrypt later threat is present tense: adversaries are intercepting and storing encrypted data now, in anticipation of quantum decryption capability that does not yet exist but is widely expected to arrive. Organizations that defer their security response until quantum computers are operationally available will find that the data they transmitted in the intervening period is already compromised. The correct reference point for urgency is not the emergence of the threat but the sensitivity and longevity of the data already in transit.

Regulatory timelines add a further dimension of urgency. The finalization of NIST post-quantum standards in 2024 created a technical foundation for regulatory requirements that are now taking shape. Government agencies in multiple jurisdictions have published or are developing mandates that require operators of critical infrastructure to complete cryptographic inventories, develop migration plans, and implement post-quantum algorithms within defined timeframes. Organizations that have not begun this work face a compressed timeline to compliance, with less flexibility to prioritize and sequence their migration efforts than those who started earlier.

The supply of expertise in post-quantum cryptography implementation is currently constrained relative to anticipated demand. As regulatory deadlines approach and as awareness among infrastructure operators increases, competition for qualified specialists in PQC assessment, implementation, and validation will intensify. Organizations that begin their transition planning now benefit from greater access to expertise, more considered timelines, and the ability to shape vendor and counterparty roadmaps rather than simply adapt to them. First-mover advantage in post-quantum readiness is a genuine and time-limited opportunity.

The March 2026 landscape represents a pivotal moment in this trajectory. The standards are finalized, the regulatory direction is clear, and the ecosystem of PQC-capable products and services is maturing rapidly. The transition from awareness to action is now the central challenge for organizations responsible for critical energy infrastructure. The framework described in this paper is designed to

support that transition in a structured, prioritized, and operationally realistic manner. The time for preparatory assessment is available now: it will not remain available indefinitely.

MARCH 2026 UPDATE

From Draft Standards to Finalized Mandates

What Has Changed Since 2023

Since initial publication in 2023, the post-quantum landscape has advanced materially. NIST finalized its first three post-quantum cryptographic standards in August 2024, publishing FIPS 203 (ML-KEM, for key encapsulation), FIPS 204 (ML-DSA, for digital signatures), and FIPS 205 (SLH-DSA, an alternative signature scheme). These standards provide the stable technical foundation that was absent during early quantum readiness planning and remove a key source of uncertainty for organizations developing migration roadmaps. The publication of finalized standards has also accelerated the development of compliant libraries, toolkits, and validated hardware security modules from major vendors, lowering the practical barrier to adoption.

At the regulatory level, the European Union's Cyber Resilience Act, which entered into force in late 2024, embeds security-by-design obligations for manufacturers of networked products, including components used in energy storage systems. The NIS2 Directive has substantially expanded the population of critical infrastructure operators subject to mandatory security requirements. Several member states have published guidance specifically addressing post-quantum cryptography migration for operators of essential services, with timelines that align with the 2030 to 2035 window identified by leading standards bodies as the probable outer limit of safe reliance on current public-key cryptography.

The quantum hardware development landscape has also shifted since 2023. Multiple research groups and commercial developers have demonstrated processors with substantially improved qubit counts and reduced error rates. While none of these systems is yet capable of running cryptographically relevant attacks at scale, the trajectory of improvement has been faster than many conservative estimates anticipated. The consensus among security researchers has accordingly shifted, and the urgency of beginning migration planning has increased correspondingly.

At 247 Energy, the March 2026 update to this paper reflects our continued commitment to leading on security in the energy storage sector. Our in-house software development practice, combined with our dedicated hardware firewall architecture and our policy of 70 percent European component sourcing, positions us to integrate post-quantum cryptographic standards into our battery management and

communications infrastructure ahead of regulatory deadlines. We regard this as a founding principle of how we build and operate storage parks, and as an essential element of the trust we ask of our investors and grid counterparties.

247 ENERGY

Quantum Readiness as a Design Principle

247 Energy NV is a developer, builder, and co-investor in utility-scale Battery Energy Storage Parks. The company operates from its base in Belgium and is active across Belgian and surrounding European markets, with a project pipeline of 505 MW currently in development. 247 Energy occupies a distinctive position in the market by retaining a direct investment stake alongside its capital partners in every project it develops, aligning incentives across the full project lifecycle from development through to operation.

The company builds its competitive advantage on three structural pillars. First, proprietary software development for battery management and energy management systems eliminates dependence on black-box vendor stacks and provides full visibility into system logic. Second, a hardware-first security architecture places a dedicated physical firewall between battery management systems and all external communication interfaces. Third, a deliberate supply chain strategy sources more than 70 percent of components from European suppliers, providing documented provenance and reducing exposure to geopolitically sensitive supply chain risk.

247 Energy's approach to quantum readiness is an extension of its broader security philosophy. The company views post-quantum cryptography not as a compliance obligation to be addressed when mandated, but as an engineering standard to be embedded in system architecture from the outset. Projects in development are being assessed against the four-step framework described in this paper, and the technology team is engaged with the evolving NIST and European standards ecosystem to ensure that migration pathways are designed into the systems it builds.

247 Energy welcomes engagement from institutional investors, infrastructure funds, and strategic partners who share its conviction that utility-scale energy storage, built on principles of operational excellence and security leadership, represents a compelling long-term infrastructure investment. The company's co-investment model ensures that its own capital is committed alongside that of its partners, providing a structural alignment of interests that underpins every partnership it enters.

247 Energy NV | Schaarbeekstraat 20E/11 | 9120 Beveren, Belgium

+32 3331 0000 | storage@247.energy | 247.energy