QUANTUM
THINK TANK

Insight that protects. Foresight that leads

# Quantum Threat Overview

By Tooba Qasim
December 2025

www.cyberlondon.com | info@cyberlondon.com

## Are You Ready for 2026? Are You Quantum Secure and Prepared for AI-Driven, Quantum-Era Cyber Threats?

Are you confident that the systems protecting your data today will still protect it tomorrow? Do you know how long your organisation's sensitive information truly needs to remain confidential?
And if attackers became faster, more automated and more precise overnight, would your current security assumptions still hold?

Most organisations have never seriously asked these questions. And that is precisely why quantum security is no longer a distant research topic or a concern reserved for cryptographers. It is becoming a matter of timing, preparedness and long-term trust in digital systems.

If you are already working in cybersecurity or have recently started reading about quantum security, you may have come across the UK National Cyber Security Centre's timelines for migration to post-quantum cryptography and immediately realised that this is something serious.

But if you have never studied quantum computing, cryptography or advanced cybersecurity, those timelines might feel confusing, distant or even irrelevant.

This article is written for both groups.

Whether you are deeply technical or completely new to the topic, the aim here is simple: to explain **why these timelines exist, what they really mean in practice and why awareness today matters far more than most organisations realise, especially in a world where AI is already accelerating cyber threats**.

## Why the NCSC Quantum Timelines Matter

The **National Cyber Security Centre (NCSC)** has published guidance outlining how organisations should prepare for a future in which today's cryptographic protections may no longer be reliable. These timelines are not predictions of an imminent quantum catastrophe. They are a recognition of something far more practical: **security transitions take time**.

Cryptography is deeply embedded across modern digital environments. It protects websites, identity systems, internal networks, cloud services, software updates and data that may need to remain confidential for decades. Before an organisation can migrate to post-quantum cryptography, it must first understand where cryptography exists, which algorithms are in use, what data they protect and which vendors control critical security components.

The NCSC timelines exist because identifying, planning, testing and migrating cryptography across real-world systems typically takes many years, not months. Waiting until quantum computers are demonstrably capable of breaking encryption would leave organisations without enough time to respond safely.

You can read the NCSC's guidance on post-quantum cryptography timelines here: https://www.ncsc.gov.uk/guidance/pqc-migration-timelines

## Quantum Computing: Progress Without Panic

Quantum computing is no longer confined to theory or academic curiosity. Although today's machines cannot yet break real-world cryptography, progress in quantum hardware has been steady, visible and measurable.

Quantum computers differ fundamentally from classical computers. Classical systems process bits that are either zero or one. Quantum systems use **qubits**, which can exist in multiple states simultaneously through superposition and can be linked through entanglement. This allows quantum machines to solve certain classes of problems in ways classical computers cannot.

This does not mean quantum computers are faster at everything. It means they are exceptionally powerful for specific mathematical problems including some that underpin modern cryptography. That distinction is important: the concern is not about present-day capability but about future relevance combined with long-term data exposure.

## Recent Advancements in Quantum Hardware

In addition to understanding the timelines for cryptographic transition, it helps to look at how quickly quantum computing hardware is progressing not because quantum computers are ready to break encryption today but to appreciate the pace of innovation. In late 2024, Google Quantum AI unveiled its Willow processor, a superconducting quantum chip with 105 physical qubits, marking a substantial improvement over earlier generations and

demonstrating better error behaviour as the system scales. Willow has been used to perform benchmark computations that would be infeasible for classical supercomputers, signalling progress toward error-mitigation and larger-scale operations.

On the industrial front, IBM has made significant strides with its quantum roadmap, advancing beyond the early 100-qubit systems toward fault-tolerant architectures. In 2025, IBM highlighted progress with new processors such as "Nighthawk," expected to be available to users by the end of the year and designed with architectures that support increasing gate counts and error-resilient designs on the path to quantum advantage.

Beyond specific chips, IBM's broader quantum strategy envisions future generations of modular systems capable of linking multiple quantum processors and scaling into the thousands of qubits, with research aimed at delivering thousands of logical operations and paving the way for practical quantum-accelerated computing in the years ahead.

Taken together, these developments show that while we remain some distance from fully error-corrected, cryptography-breaking machines, **the underlying hardware is advancing at a pace that demands attention and long-term planning** as part of any robust cybersecurity strategy.

## Why Today's Cryptography Becomes a Long-Term Risk

Much of the digital world depends on public-key cryptography, particularly RSA and elliptic curve cryptography. These algorithms protect secure websites, online banking, digital certificates, encrypted email, software updates, virtual private networks, and cloud authentication systems.

Their security is based on mathematical problems that are extremely difficult for classical computers to solve. Quantum algorithms, most notably **Shor's algorithm**, change that assumption. Once sufficiently powerful quantum computers exist, those mathematical problems become solvable in practical timeframes.

This does not cause immediate collapse. Instead, it introduces a **long-term structural weakness** into systems designed under classical assumptions. The risk is not sudden failure but the gradual erosion of confidence in cryptographic guarantees over time.

## Harvest Now, Decrypt Later: A Risk That Already Exists

One of the most important concepts to understand is "harvest now, decrypt later."

Attackers do not need quantum computers today to benefit from them in the future. They can already intercept encrypted communications, steal encrypted databases, collect backups and store that data indefinitely. When quantum capabilities mature, they can return to that information and decrypt it retroactively.

This is particularly dangerous for data that must remain confidential for long periods, including personal identity information, medical and genomic records, financial histories, intellectual property, legal documents, and sensitive government data. From a risk perspective, **the exposure begins the moment data is collected**, not when quantum computers arrive.

## Where AI Changes the Equation

While cryptographically capable quantum computers are still on the horizon, **artificial intelligence is already reshaping cyber operations today**.

AI is being used to automate reconnaissance, accelerate vulnerability discovery, generate highly convincing phishing content and optimise attack paths at scale. This does not create "quantum attacks," but it does significantly increase the speed and efficiency with which attackers can identify valuable targets and long-lived data.

In practical terms, AI reduces the time attackers need to map environments, identify cryptographic dependencies, locate weak protections and prioritise systems whose data will remain valuable for many years. When future quantum decryption capabilities eventually arrive, the groundwork for exploitation may already be in place.

## Why Awareness Must Come First

Many organisations still think post-quantum cryptography is a future technical upgrade. In reality, the first challenge is awareness.

Most organisations cannot clearly say where cryptography is used, which algorithms protect which data, how long that data must remain confidential, or which third parties manage cryptographic controls. Without this understanding, preparation is impossible.

This is why awareness is the first phase of the **Logic Train framework**. It is not about fear or hype. It is about understanding what exists today and how it may age in a rapidly evolving threat environment.

## Global Signals Are Aligning

The UK is not acting alone.

The **National Institute of Standards and Technology (NIST)** has standardised multiple post-quantum cryptographic algorithms, setting a global baseline for future-safe encryption.

https://csrc.nist.gov/projects/post-quantum-cryptography

The **European Telecommunications Standards Institute (ETSI)** has been developing quantum-safe and hybrid cryptographic specifications for years, focusing on practical deployment and interoperability.

https://www.etsi.org/technologies/quantum-safe-cryptography

Together with NCSC guidance, these efforts send a consistent message: **early awareness and planning are essential**.

## Why Waiting Is the Real Risk

The greatest risk is not that quantum computers will appear suddenly. The real risk is assuming there will be time to respond later.

Post-quantum migration involves discovering cryptographic dependencies, updating legacy systems, testing hybrid approaches, coordinating with vendors, updating governance and aligning with evolving standards. All of this takes years. The NCSC timelines are not alarmist; they are realistic.

## Concluding Reflections

From our perspective, the most dangerous misconception about quantum security is that it belongs only to specialists or future teams. It does not. It belongs to anyone responsible for long-term digital trust.

Awareness does not require deep knowledge of quantum physics or artificial intelligence. It requires recognising that the assumptions underpinning today's security systems are changing and that preparation must begin before urgency arrives.

This article is not meant to alarm. It is meant to focus attention. Awareness is the first step, and without it, every later step becomes harder. That is why this series begins here.

---

**About the author:** Tooba Qasim is a PhD researcher in cybersecurity at City St George's, University of London. Her research includes authentication challenges in Quantum Key

Distribution (QKD), analysis of post-quantum cryptography (PQC) algorithms in security protocols and exploring the security and performance of PQC on hardware and resource-constrained devices.