WHITEPAPER

The Clock

When will a quantum computer break today's public-key encryption, and should industrial operators prepare now or wait?

The latest expert survey puts a quantum computer able to break today's public-key encryption (a cryptographically relevant quantum computer, or CRQC) at more likely than not within about 15 years. The clock in the title is Mosca's: the years left before a CRQC, set against the years a migration takes. A controller installed in a substation or water treatment works this year may well still be in service by then. For data or keys that must stay safe for years, the protection period plus the migration time already exceeds the expected wait for a CRQC, even though much of the migration itself will have to wait for products.

ClaveQ · Quantum Clave Ltd Accurate as of 11 October 2026

6 sections, glossary and sources · about 13 min read

01 When will a quantum computer break today's public-key encryption?

AT A GLANCE

- A leading expert survey suggests a quantum computer that could break today's public-key encryption is more likely than not by about 2040.
- For data or keys that must stay safe for years, protection time plus migration time already runs past that point.
- Start finding where your systems rely on this encryption now: the UK's first target date, 2028, is guidance, and every later step depends on it.

Nobody can name the year, but there is structured expert opinion. Since 2019 the Global Risk Institute (GRI) and evolutionQ have surveyed quantum computing experts every year for the *Quantum Threat Timeline Report*.

The 2025 edition, published on 9 March 2026, surveyed 26 experts from academia and industry. Each was asked how likely it is that a quantum computer able to factor a 2048-bit number in under 24 hours (enough to break RSA-2048, a widely used key size) will be built within 5, 10, 15, 20 and 30 years. The report calls such a machine a CRQC.

The headline finding, in the report's own words: respondents “say it is quite possible (28-49%) that this will happen in the next 10 years, and likely (51-70%) in the next 15 years.” The report itself anchors the 10-year horizon at “roughly 2035”. [1]

Reading the word "likely" with care

Two details change how those numbers should be read. First, each range is not a confidence interval: the experts chose from seven answer bands, and the report averages their choices twice, once taking the bottom of every band (28% at ten years) and once the top (49%).

Second, the survey's own answer scale defines "Likely" as “> 70 % chance”. The 51-70% figure sits below that line. Read against the report's own definition, the experts' average view is that a CRQC is **more likely than not** by around 2040. That is the phrase this paper uses from here on.

Opinion is divided. At ten years, half the panel (13 of 26) put the chance below 30% and half at about 50% or higher (the survey's middle band, 30 to 70%). By twenty years, 24 of the 26 put it at about 50% or higher, and the report records “a remarkable shift towards a higher likelihood compared to recent similar surveys”. For the five-year horizon, though, its summary is that “the majority view the short-term risk as low”. [1]

---

02 *What a quantum computer would break, and when the harm begins*

A CRQC would break public-key cryptography (the maths that lets two parties agree a secret key, or check a signature, without having met). That covers RSA, elliptic-curve key exchange and ECDSA signatures.

Symmetric ciphers such as AES fare far better: the GRI report notes that the relevant quantum algorithm reduces their security “albeit not exponentially”. [1] The serious problem is public-key cryptography, which causes two kinds of harm on two timetables.

Confidentiality: the harm can start before a CRQC exists

An attacker can record encrypted traffic today and decrypt it once a CRQC is available. This is called **harvest now, decrypt later**. US Executive Order 14412 of June 2026 describes it plainly: “the risk of adversaries collecting United States information now, and decrypting it later once large-scale quantum

computers are operational.” [3] For confidentiality, exposure begins on the day the traffic is captured.

Authenticity: the harm starts on the day a CRQC exists

A digital signature proves who sent a message or who built a piece of software. Forging one needs the signer's private key, which a CRQC could work out from the matching public key. The danger is what an attacker could sign afterwards: a firmware image that a controller accepts as genuine, a software update, or a certificate that admits a rogue device to a network.

The replacement algorithms already exist

On 13 August 2024 the US National Institute of Standards and Technology (NIST) published the first three post-quantum cryptography (PQC) standards: **FIPS 203 (ML-KEM)** for agreeing keys, **FIPS 204 (ML-DSA)**, the primary standard for digital signatures, and **FIPS 205 (SLH-DSA)**, a backup signature scheme.

NIST's advice at the time was direct: “We encourage system administrators to start integrating them into their systems immediately, because full integration will take time.” [4] What remains slow is everything around the algorithms: products, protocols and the testing needed before anything is installed (section 04).

---

03 *Mosca's test: is there enough time to finish?*

> THINK OF IT LIKE THIS
>
> You keep private papers in locked filing cabinets, and someone photocopies the locked drawers every night. One day a master key will exist. Your papers must stay private for X years; changing every lock takes Y years; the master key turns up in Z years. If X plus Y is more than Z, some papers will be read.
>
> Where the comparison stops working: for signatures, nothing needs copying in advance. The master key lets its holder forge new documents from the day it exists.

The precise version is Michele Mosca's inequality, first set out in 2013. The GRI report defines its three terms [1]:

TERM	GRI DEFINITION
X · shelf-life time	"the number of years the information should be protected for"
Y · migration time	"the number of years needed to safely and adequately migrate the cyber-system to a quantum-safe solution"

TERM	GRI DEFINITION
Z · threat time	"the number of years before the relevant threat actors will be able to break the quantum-vulnerable systems"

If X + Y is greater than Z, the report concludes, an organisation “may not be able to protect its assets” for as long as it needs to.

- **Z is uncertain**: the best estimate is a probability (section 01). In this paper the **expected wait** means the time until experts rate a CRQC as more likely than not: about 14 years from now, to around 2040.
- **Y is the only term an operator controls**, and nobody can estimate it without first knowing which systems use which cryptography. That is why the UK and EU sequences in section 05 begin with discovery and the US federal guidance opens with a strategy, planning and discovery phase [9]; NSA's CNSA 2.0 timetable, which starts with signing, is the exception.
- **For signatures, X means something slightly different.** A signature check can be trusted only for as long as the key behind it is safe. A controller that checks firmware against a key built into it relies on that key for the rest of its service life, so its X is the number of years it will stay in use. NSA notes that firmware-signing algorithms “are frequently locked in for the life of a system”. [8]

An illustrative calculation

The migration times below come from the EU roadmap's estimate that it “might easily take about 5 to 10 years to fully migrate all relevant systems”. [6] The equipment life comes from NIST's range for operational technology. [5]

CASE (ILLUSTRATIVE)	X	Y	PROTECTION NEEDED UNTIL	EXPERT VIEW AT THAT POINT [1]
Engineering data that must stay private for 10 years; migration finished quickly	10	5	About 2041	Past the point at which a CRQC is more likely than not (about 2040)
Controller installed in 2026 that trusts one fixed firmware-signing key for a 15-year life	15	n/a	About 2041	Past the point at which a CRQC is more likely than not

X and Y are assumptions for illustration, counted from 2026. Each organisation's values will differ.

Y alone, at 5 to 10 years, is shorter than the expected wait. The case for acting comes from adding X: for data or keys that must stay safe for years, the protection period plus the migration time already exceeds the expected wait, as every row above shows.

04 *Why industrial systems need more time to migrate*

Operational technology (OT: the control equipment and networks that run physical plant) differs from office IT in five ways that matter here. Each one makes Y longer.

1. Equipment stays in service for decades

NIST's guide to OT security, SP 800-82 Revision 3, says that typical IT components last “on the order of three to five years”, while for OT “the lifetime of the deployed technology is often in the order of 10 to 15 years and sometimes longer.” Elsewhere it adds: “The lifespan of an OT system can exceed 20 years.” [5] Equipment bought this year may therefore still be running in the 2040s.

The EU roadmap draws the procurement conclusion. It is “highly recommended to ensure that products entering the market with an expected lifetime beyond 2030 should be upgradable to PQC”, and that the mechanism for software and firmware updates “should incorporate post-quantum signature schemes for integrity and authenticity.” [6]

2. Every change has to be tested and scheduled

NIST notes that OT assets “reflect massive investments in operational, reliability, and safety testing”, and that outages “must often be planned and scheduled days or weeks in advance.” [5] The UK's National Cyber Security Centre (NCSC) advises that changes to physical infrastructure “should be done, as far as possible, to coincide with other infrastructure maintenance and improvements.” [2] A new cryptographic library in a controller is a change like any other: it waits for a maintenance window and passes the same tests first.

3. Post-quantum products for industrial protocols will arrive later

For sectors that rely on OT, the NCSC expects “fewer PQC products becoming available in the near future.” It also names industrial control system (ICS) protocols as one of two areas where post-quantum protocol development will be hardest, because of “legacy protocols in use in ICS that have never been brought up to modern cryptographic standards.” [2]

4. Control systems care more about authenticity than confidentiality

Most process data is of little value to a thief, while a forged firmware image or a rogue device admitted to the network could be dangerous. The NCSC makes this point about fielded OT devices: “the integrity of the data is likely to be critical, since faulty sensor readings or commands can lead to ICS failures.” [2]

Many control connections carry no encryption or authentication at all: a risk today with or without a quantum computer, and one discovery should find. The quantum risk falls on the authentication that does use public-key cryptography: firmware and software signing, certificates in remote-access VPNs and jump hosts, OPC UA certificates, CIP Security and Modbus/TCP Security (both built on TLS), and the optional certificate-based key change in DNP3 Secure Authentication.

The practical consequence is that confidentiality and authentication should be rated separately.

5. Post-quantum keys and signatures are larger

An ML-DSA signature is 2,420 to 4,627 bytes, depending on the security level [11], and an ML-KEM-768 public key is 1,184 bytes [10]. An elliptic-curve P-256 signature is 64 bytes. On a controller with little spare memory or processing power, inside a fixed-size industrial protocol frame, or over a serial or radio link to an outstation, that overhead matters. The NCSC notes that industrial IoT devices "might be resource-constrained" and "might not be upgradeable". [2] Some devices will need new hardware, not just a software update.

---

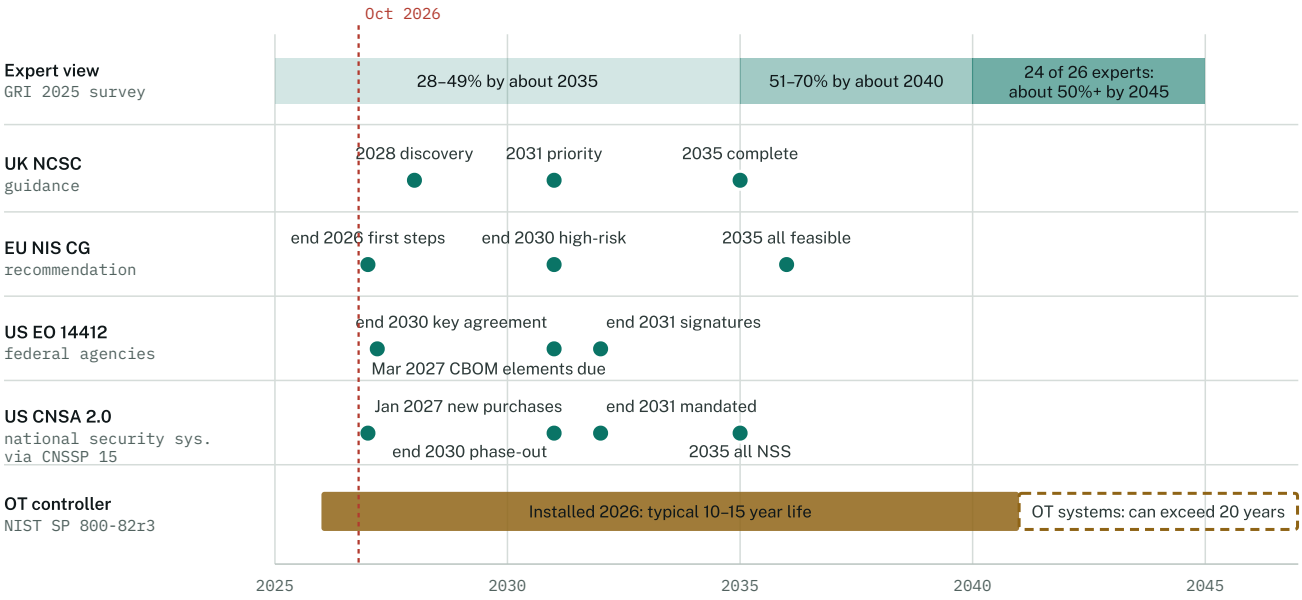
05 *Government target dates, and how binding each one is*

Four sets of target dates are most often cited. They agree broadly on timing and differ widely in legal force. None of them is UK law.

BODY AND DOCUMENT	TARGET DATES	WHO IT APPLIES TO	LEGAL FORCE
UK NCSC Timelines for migration to PQC, 20 March 2025 [2]	By 2028: define goals, "carry out a full discovery exercise", build an initial plan. By 2031: "early, highest-priority PQC migration activities". By 2035: complete migration of all systems, services and products.	Mainly large organisations and critical national infrastructure, including industrial control systems; "all organisations should work towards these key dates."	**Guidance.** The NCSC calls them "indicative timelines" and "key target dates".
EU NIS Cooperation Group Coordinated Implementation Roadmap, v1.1, 11 June 2025 [6]	End of 2026: national first steps and roadmaps. High-risk use cases "as soon as possible, no later than the end of 2030". 2035: "as many	EU Member States. Critical infrastructure and NIS2 entities "should refer to" it.	**Non-binding recommendation** under the Commission's April 2024 Recommendation on PQC; the roadmap calls its dates "recommended".

BODY AND DOCUMENT	TARGET DATES	WHO IT APPLIES TO	LEGAL FORCE
	systems as practically feasible".		
US Executive Order 14412 22 June 2026 [3]	High-value and high-impact federal systems: post-quantum key establishment by 31 December 2030; signatures by 31 December 2031. CISA and NIST to publish minimum elements for a CBOM within 270 days, around March 2027.	US federal agencies. A proposed procurement rule, due around December 2026, would require covered contractors to meet NIST's FIPS, "including all applicable FIPS incorporating PQC compliant algorithms", by 31 December 2030.	**Executive order directing US federal agencies.** OMB has issued the guidance it called for (M-26-15) [9]. No direct obligation on UK operators; UK suppliers to the US government may be caught by the procurement rule if it is adopted. CBOM guidance unpublished as of 11 October 2026.
US NSA, CNSA 2.0 and CNSSP 15 Advisory, September 2022 [7]; FAQ, December 2024 [8]; CNSSP 15, March 2025	CNSSP 15, as summarised by NSA [8]: new acquisitions CNSA 2.0 compliant from 1 January 2027; equipment that cannot support it phased out by 31 December 2030; CNSA 2.0 mandated by 31 December 2031. NSA's 2022 timetable [7]: signing to "exclusively use CNSA 2.0 by 2030"; constrained devices 2033; all by 2035.	US National Security Systems and their suppliers.	**NSA advisory (2022) setting expected target dates; the 2027, 2030 and 2031 target dates are made binding for US national security systems through CNSSP 15.** Does not apply to other systems.

FIGURE 1 · EXPERT ODDS, GOVERNMENT TARGET DATES AND EQUIPMENT LIFE



Expert probability of a CRQC [1] compared with government target dates [2][3][6][7][8][9] and the service life of an industrial controller [5]. Expert horizons are counted from the survey, which the report anchors at about 2035 for ten years. Government markers show target dates, not predictions. The controller bar is illustrative.

The NCSC did not choose 2035 by forecasting a CRQC. It chose it because “10 years is a sufficient period” for standards and products to mature and be widely adopted. [2] In Mosca's terms, the government dates are estimates of Y. On the GRI figures, 2035 falls when the experts' average is 28 to 49%.

If the dates assume roughly ten years of migration and an OT estate needs longer (section 04), its operator has to start earlier and treat them as the latest acceptable finish.

Some companies are moving faster than government dates. In March 2026 Google, describing itself as “a pioneer in both quantum and PQC”, set a 2029 timeline for its own post-quantum migration, putting authentication services first, and recommended “that other engineering teams follow suit.” [12] Google gives no date for when a CRQC will exist; 2029 is its own engineering target, not guidance.

06 *Prepare now or wait? A decision table for operators*

The case for waiting deserves a fair hearing. Post-quantum products for industrial protocols are scarce. Standards for some protocols are still being written. And a hurried change carries its own danger: the GRI report warns that “a rushed transition to post-quantum security systems may lead to the introduction of new vulnerabilities”. [1]

Those are good reasons to leave working controllers alone this year. They do not justify delaying discovery. Discovery needs no new algorithm and touches no controller, and working from a copy of the traffic sends nothing onto the control network. Installing the copy point, a network TAP or a SPAN (mirror) port on a switch, is itself a change: it goes through the site's normal approval process, and some TAPs interrupt the link if they lose power. Once that is done, discovery is the input to every later decision.

WHEN	WHAT TO DO	WHY IT CANNOT WAIT LONGER
This year (2026–27)	Name an owner for the migration. Start discovery across OT and IT: which connections use public-key cryptography, which use none, and where signing keys are built into devices. For equipment expected to run beyond 2030, ask suppliers for a dated post-quantum roadmap and a firmware-update mechanism that can take new signature algorithms, and weight both in tender evaluation.	Equipment bought now may stay in service into the late 2030s and, sometimes, the 2040s, when a CRQC is more likely than not [1][5]. The EU asks for upgradability beyond 2030 (section 04) [6].
By 2028	Complete discovery, set migration goals and write an initial plan. Rate confidentiality and authentication separately. Identify long-lived hardware roots of trust (keys fixed in a device that anchor everything it trusts), which the NCSC lists for this phase.	This is the NCSC's first target date [2]. Without an inventory, the 2031 work cannot be prioritised.
By 2031	Finish the highest-priority migrations. A verification key fixed in a fielded device cannot be migrated: plan to replace the device at refresh and, in the meantime, restrict and monitor the network paths and people that can push firmware to it. Fold the remaining changes into planned maintenance and equipment refresh.	NCSC guidance asks for highest-priority migration by 2031 [2]; the EU recommends high-risk use cases by the end of 2030 [6]. US national security systems face CNSA 2.0 dates made binding through CNSSP 15 from 2027 (section 05) [8].

For an office network, waiting a year or two for better products may cost little; for an industrial estate the arithmetic is different. If migration takes the 5 to 10 years the EU estimates, an operator that starts discovery in 2029 is planning to finish between about 2034 and 2039. That is close to the expected wait of about 2040. **For data or keys that must stay safe for years, such as long-lived confidential data and the keys that sign firmware or admit remote access, the protection period plus the migration time already exceeds the expected wait for a CRQC. Discovery should start now.**

07 Glossary

CBOM

Cryptographic bill of materials: a machine-readable list of the cryptography a product uses.

CIP Security

Security add-on for the EtherNet/IP industrial protocol, built on the encryption secure websites use.

CNSA 2.0

The US NSA's quantum-resistant algorithm suite for national security systems.

CNSSP 15

US policy that makes the CNSA 2.0 dates binding, for national security systems only.

CRQC

Cryptographically relevant quantum computer: one powerful enough to break today's public-key encryption.

DNP3 Secure Authentication

Optional part of DNP3, a utility control protocol, that lets devices check who sent a command.

FIPS

Federal Information Processing Standards: US government standards published by NIST, including the post-quantum ones.

Modbus/TCP Security

Secure version of the Modbus/TCP industrial protocol, built on the encryption secure websites use.

OPC UA

A widely used industrial data-exchange standard whose security identifies machines by digital certificate.

Post-quantum cryptography (PQC)

Encryption and signature methods designed to stay secure against a future quantum computer.

Public-key cryptography

The maths that lets two parties agree a secret key, or check a signature, without having met.

SPAN port

A switch setting that sends a copy of chosen traffic to a monitoring port.

TAP

A small device fitted to one cable that sends a copy of its traffic to a monitor.

TLS

Transport Layer Security: the encryption behind secure websites, also used by some industrial protocols.

08 Sources

All sources were opened and checked in October 2026. Quotations are reproduced as they appear in the source.

#	PUBLISHER	DOCUMENT	DATE	SUPPORTS
[1]	Global Risk Institute (M. Mosca and M. Piani)	*Quantum Threat Timeline Report 2025* ↗ Full report (PDF) ↗	9 March 2026	§01 expert timeline, "likely"; §02; §03 X, Y, Z; §06
[2]	UK National Cyber Security Centre	*Timelines for migration to post-quantum cryptography* ↗	20 March 2025	§04 OT constraints; §05 UK dates; §06
[3]	The White House	Executive Order 14412, *Securing the Nation Against Advanced Cryptographic Attacks* ↗	22 June 2026	§02 harvest now, decrypt later; §05 US dates, CBOM
[4]	NIST	*NIST Releases First 3 Finalized Post-Quantum Encryption Standards* ↗	13 August 2024	§02 PQC standards
[5]	NIST	SP 800-82 Revision 3, *Guide to Operational Technology (OT) Security* (PDF) ↗	September 2023	Cover, §03, §04 equipment life, testing; §06
[6]	NIS Cooperation Group, EU PQC Workstream	*A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography*, Part 1, v1.1 ↗	11 June 2025	§03 migration time; §04; §05 EU dates; §06
[7]	US National Security Agency	*Announcing the Commercial National Security Algorithm Suite 2.0*, Cybersecurity Advisory (PDF) ↗	September 2022	§05 NSA's expected timetable
[8]	US National Security Agency	*The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ*, v2.1 (PDF) ↗	December 2024	§03 signing keys locked in; §05, §06 CNSSP 15 dates
[9]	US Office of Management and Budget	M-26-15, *Execution of the Migration to Post-Quantum Cryptography* (PDF) ↗	24 June 2026	§03, §05 OMB guidance
[10]	NIST	FIPS 203, *Module-Lattice-Based Key-Encapsulation Mechanism Standard* (PDF) ↗	August 2024	§04 ML-KEM key size
[11]	NIST	FIPS 204, *Module-Lattice-Based Digital Signature Standard* (PDF) ↗	August 2024	§04 ML-DSA signature sizes
[12]	Google (H. Adkins, S. Schmieg), company blog	*Quantum frontiers may be closer than they appear* ↗	25 March 2026	§05 company migration target

About this paper

Published by ClaveQ, which builds discovery tools that inventory the cryptography in use on industrial networks from a copy of their traffic and record it as a CycloneDX cryptographic bill of materials. Nothing in this paper depends on any product; the steps in section 06 apply whichever tools an operator uses.

Read the other ClaveQ whitepapers on post-quantum security for industrial systems:
claveq.com/whitepapers.html

COPYRIGHT AND TERMS OF USE

Copyright	© 2026 Quantum Clave Ltd, trading as ClaveQ. Company no. 17340121. All rights reserved, except as below.
Sharing	You may copy and share this paper in full and unmodified, with this notice intact. Please do not edit it, remove our name, or sell it.
Quotations and sources	Quotations from published sources are reproduced with attribution for the purposes of review and comment. Named products and organisations belong to their owners; mention does not imply endorsement.
Trade mark	ClaveQ® is a registered trade mark of Quantum Clave Ltd in the United Kingdom.
Disclaimer	This paper is general information, accurate as of October 2026. It is not legal, regulatory or compliance advice. Check current guidance before acting on it.