NAVIGATING THE GOVERNANCE ASPECTS OF THE PQC TRANSITION

Laima Jančiūtė PhD

PQCSA Workshop

Privacy in the Post-Quantum Era: Challenges and Migration Strategies

CPDP 2026 pre-event — May 19, 2026, Brussels

The value of encryption

- Coded language as part of human communication has been known for millennia (*S. Singh, "The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography", 1999*)
- "In today's world of ubiquitous computers and networks, it's hard to overstate the value of encryption" (*B. Schneier, "The Value of Encryption", 2016*)
- The internet's promise of universally connecting the world has resulted in a seemingly infinite space teeming with new and unknown adversaries, and cryptography is one of the few crucial mechanisms of defense possible in this new world" *(H. Halpin, "The Adversary: the Philosophy of Cryptography", 2025)*
- "People in the EU value encryption and express concern about unauthorised access to their private communications" *(FRA, 2026)*

Encryption and human rights

- UN HRC report on encryption and anonymity in digital communications, 2015; follow-up report 2018
- UNESCO, Human Rights and Encryption *(W. Schulz and J. van Hoboken, 2016)*
- UN Office of the High Commissioner for Human Rights, 'Apple-FBI Case Could Have Serious Global Ramifications for Human Rights: Zeid', 2016
- UN HRC report on the right to privacy in the digital age, sections II B and IV, 2022
- *Podchasov v Russia* (App No 33696/19) ECtHR 13 February 2024
- **Amnesty International**, 'Encryption a Matter of Human Rights', 2016
- **EDRi**, 'Position Paper on Encryption', 2016
- **EDRi**, 'Position Paper: State Access to Encrypted Data', 2022
- **Privacy International**, 'Securing Privacy: Privacy International on End-to-End Encryption', 2022
- K. Limniotis, "Cryptography as the means to protect fundamental human rights", 2021

Encryption and human rights

The right to privacy

- "…the right to be let alone-the most comprehensive of rights and the right most valued by civilized men" *(L. Brandeis, Olmstead et al. v. United States, 1928)*
- "Privacy is a gateway right that affects the ability to exercise almost every other right, in particular freedom of expression and freedom of assembly and association" (*Human Rights Watch, 2015*)
- A new digital right to post-quantum privacy *(QT Strategy of Spain, 2025, p. 80-81)*

The right to data protection

- Article 8 EU CFR, Article 16 TFEU
- The protection of personal data and digital privacy - *a 'super' fundamental right* in Europe *(O. Pollicino, Data Protection and Freedom of Expression Beyond EU Borders: EU Judicial Perspectives, 2021)*

Confidentiality of communications

- A distinct right in the constitutions of the majority of the EU MS *(EDPS, Opinion on the e-Privacy reform proposal, 2017, p. 7)*.

Encryption and human rights

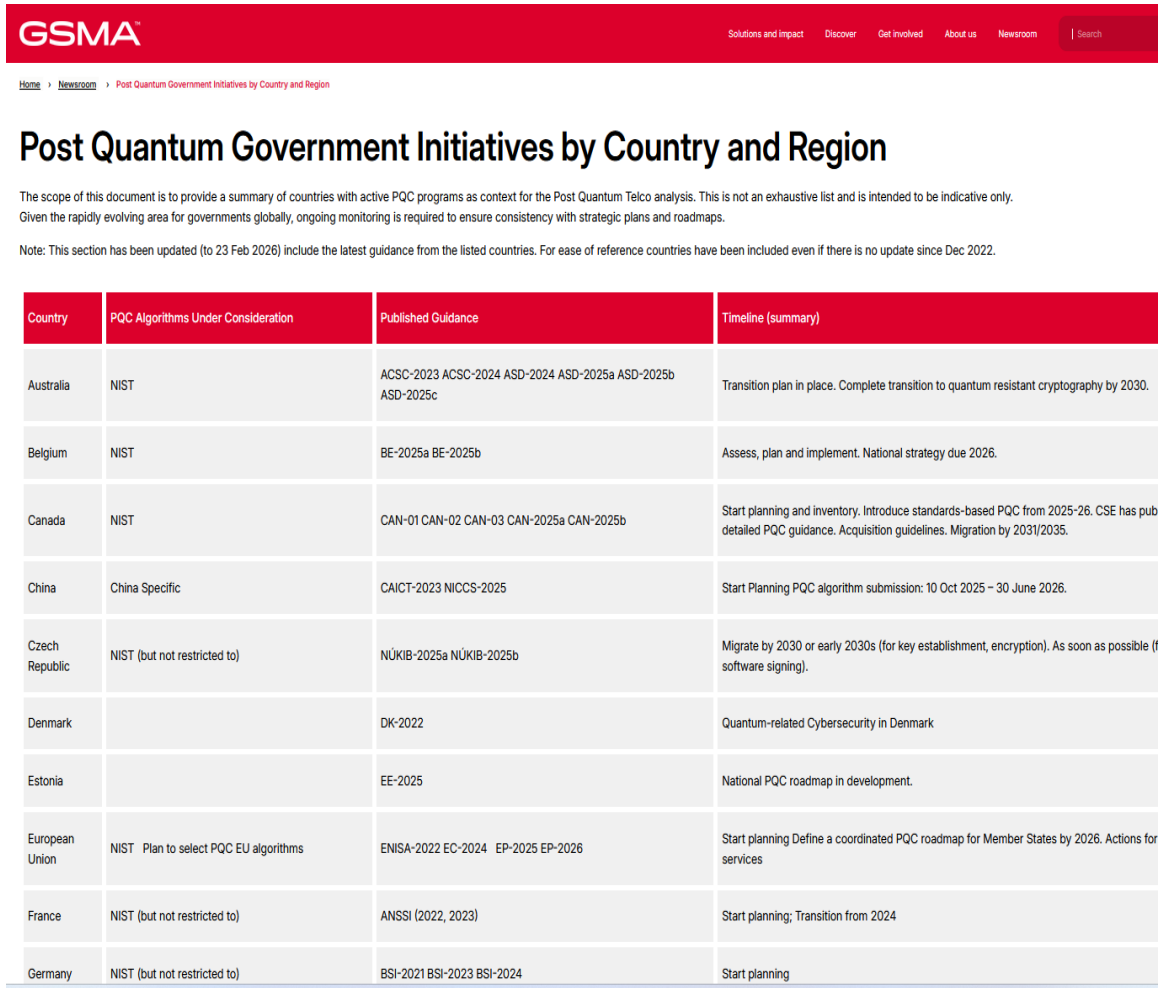
- to freedom of expression
- to peaceful assembly and association
- to a fair trial
- presumption of innocence
- privilege against self-incrimination
- and potentially other rights

A right to encrypt

- “It may now be time [...] to consider establishing a right to encrypt” *(G. Buttarelli, various speeches, 2016)*
- A statutory right to encryption *(Germany, law proposal, 2024)*

- D. Casacuberta, “El derecho a cifrar”, 2003
- S.W. Schlesinger and S. Yanisky-Ravid, “The Right to Data Encryption”, 2022
- J. Shurson, “A European Right to End-to-End Encryption?”, 2024
- P. Davis, “A Right to Encryption in the European Union’s Charter of Fundamental Rights”, 2025
- M. Wimmer and T.G. Moraes, “Quantum Computing, Digital Constitutionalism, and the Right to Encryption: Perspectives from Brazil”, 2022

PQC transition: government initiatives



GSMA

Solutions and impact | Discover | Get involved | About us | Newsroom | Search

Home › Newsroom › Post Quantum Government Initiatives by Country and Region

Post Quantum Government Initiatives by Country and Region

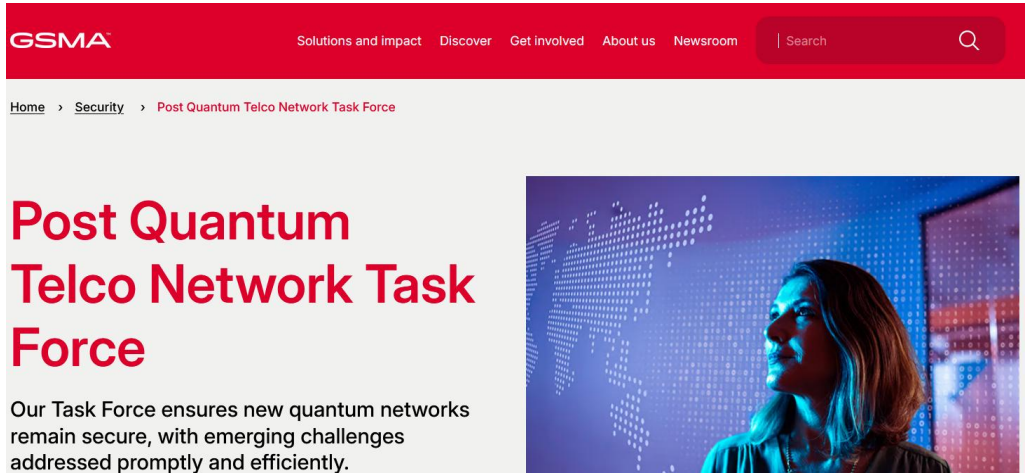
The scope of this document is to provide a summary of countries with active PQC programs as context for the Post Quantum Telco analysis. This is not an exhaustive list and is intended to be indicative only. Given the rapidly evolving area for governments globally, ongoing monitoring is required to ensure consistency with strategic plans and roadmaps.

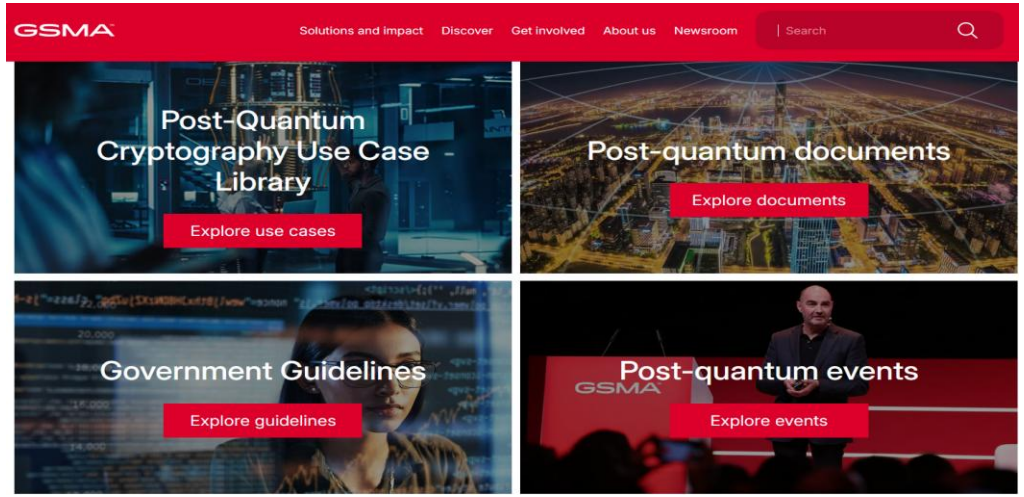
Note: This section has been updated (to 23 Feb 2026) include the latest guidance from the listed countries. For ease of reference countries have been included even if there is no update since Dec 2022.

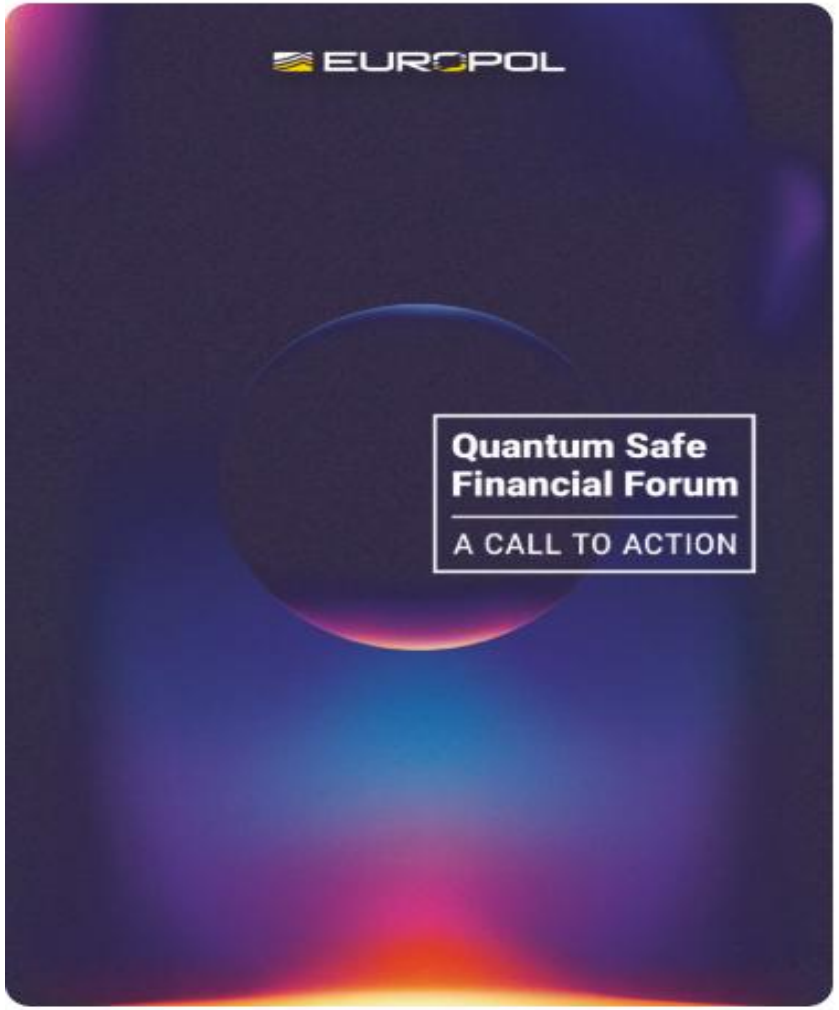
Country	PQC Algorithms Under Consideration	Published Guidance	Timeline (summary)
Australia	NIST	ACSC-2023 ACSC-2024 ASD-2024 ASD-2025a ASD-2025b ASD-2025c	Transition plan in place. Complete transition to quantum resistant cryptography by 2030.
Belgium	NIST	BE-2025a BE-2025b	Assess, plan and implement. National strategy due 2026.
Canada	NIST	CAN-01 CAN-02 CAN-03 CAN-2025a CAN-2025b	Start planning and inventory. Introduce standards-based PQC from 2025-26. CSE has pub detailed PQC guidance. Acquisition guidelines. Migration by 2031/2035.
China	China Specific	CAICT-2023 NICCS-2025	Start Planning PQC algorithm submission: 10 Oct 2025 – 30 June 2026.
Czech Republic	NIST (but not restricted to)	NÚKIB-2025a NÚKIB-2025b	Migrate by 2030 or early 2030s (for key establishment, encryption). As soon as possible (f software signing).
Denmark		DK-2022	Quantum-related Cybersecurity in Denmark
Estonia		EE-2025	National PQC roadmap in development.
European Union	NIST Plan to select PQC EU algorithms	ENISA-2022 EC-2024 EP-2025 EP-2026	Start planning Define a coordinated PQC roadmap for Member States by 2026. Actions for services
France	NIST (but not restricted to)	ANSSI (2022, 2023)	Start planning; Transition from 2024
Germany	NIST (but not restricted to)	BSI-2021 BSI-2023 BSI-2024	Start planning

- **Most countries** – full transition by **2035**; **earlier** transition timelines for **critical systems**
- ***Australia*** – *full migration by 2030*
- ***India*** - *full migration by 2033*
- ***US*** – *previously full migration (of federal systems) by 2035; set to accelerate? (US Cyber Strategy, 2026)*

PQC transition: sectoral initiatives

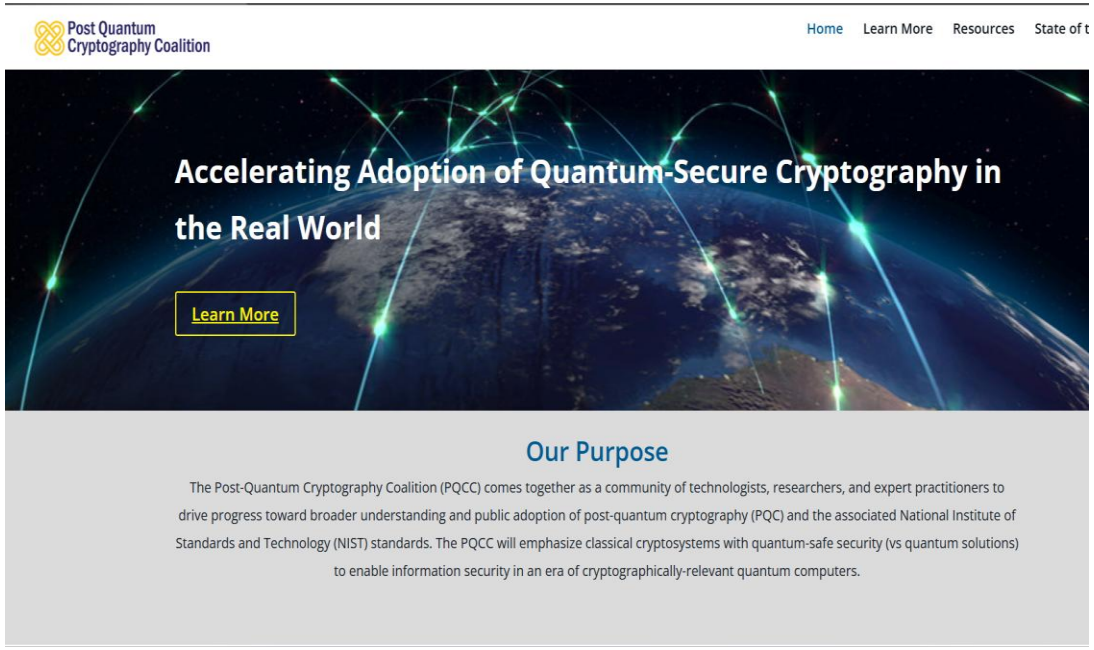




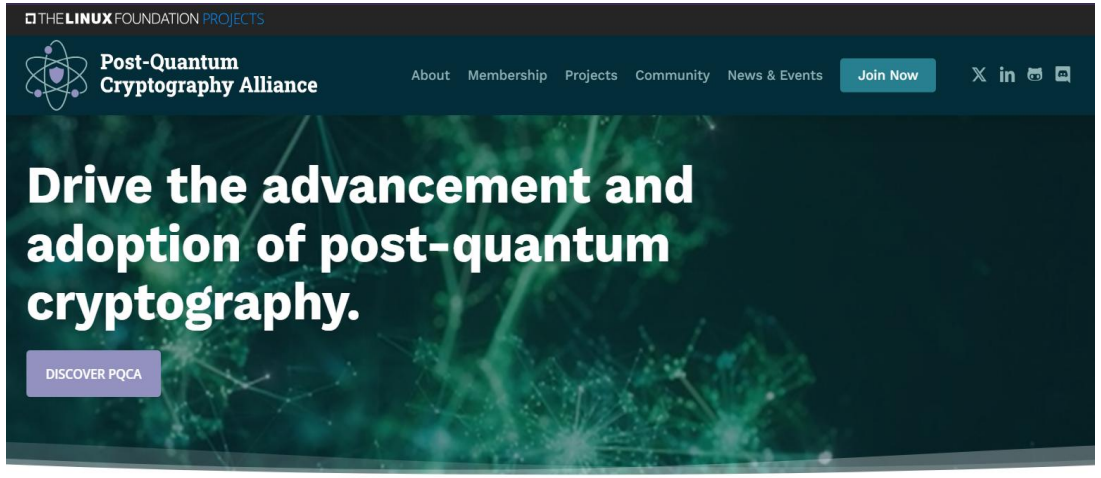


Other collective initiatives

Post Quantum Cryptography Coalition

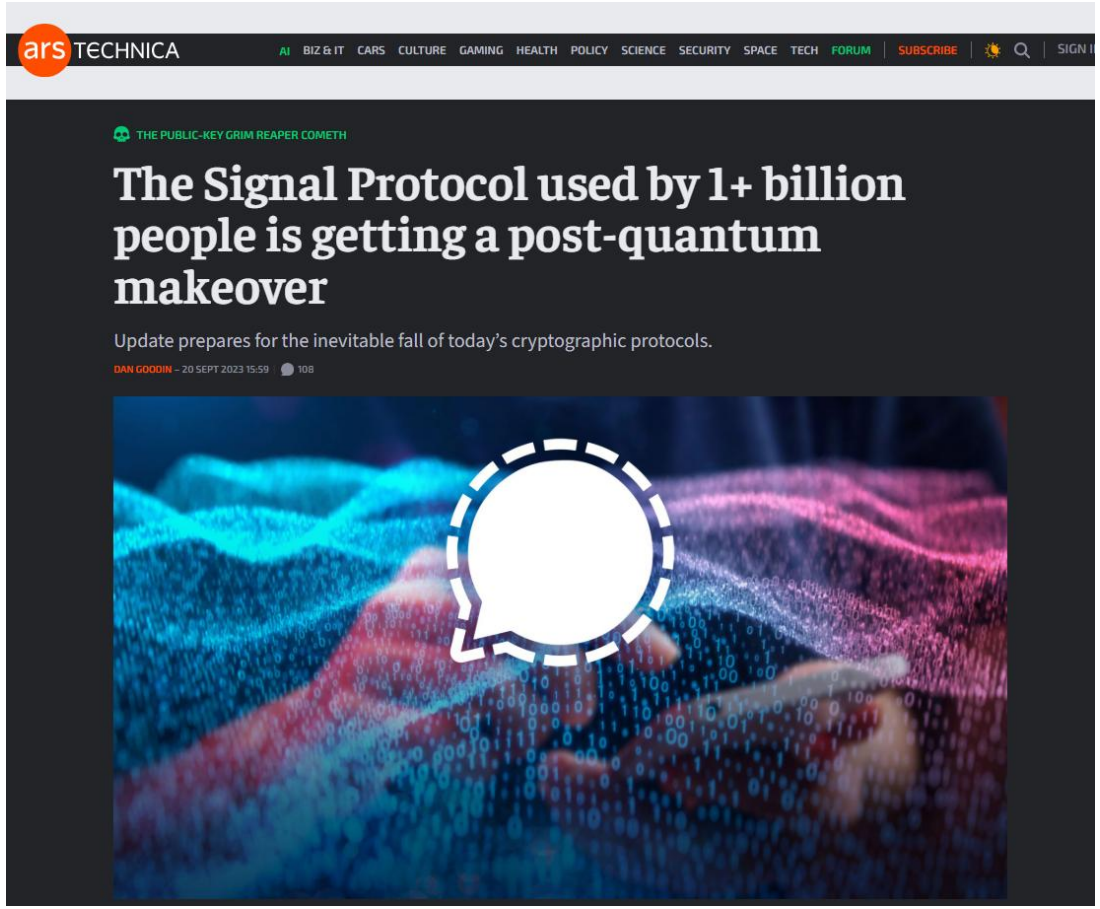


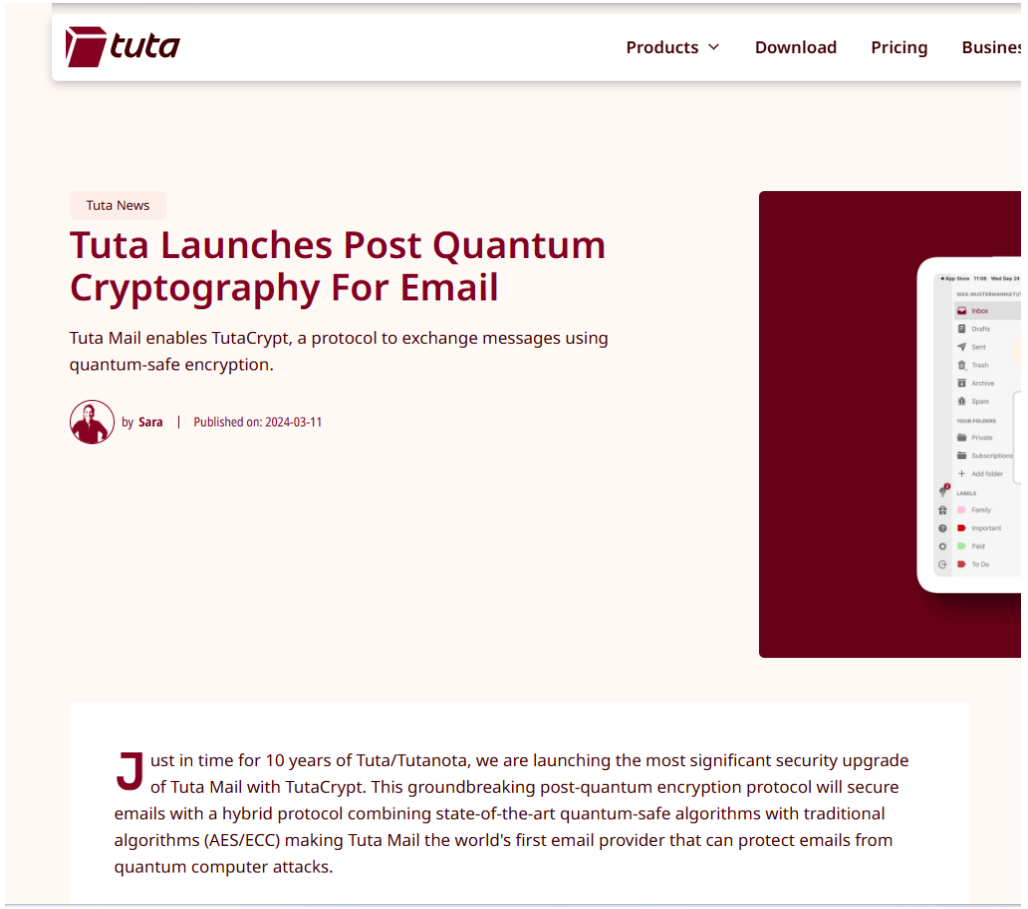
Post-Quantum Cryptography Alliance



The alliance seeks to address cryptographic security challenges posed by quantum computing by producing high-assurance software implementations of standardized algorithms and supporting the continued development and standardization of new post-quantum algorithms with software for evaluation and prototyping.

PQC deployment – encrypted comms





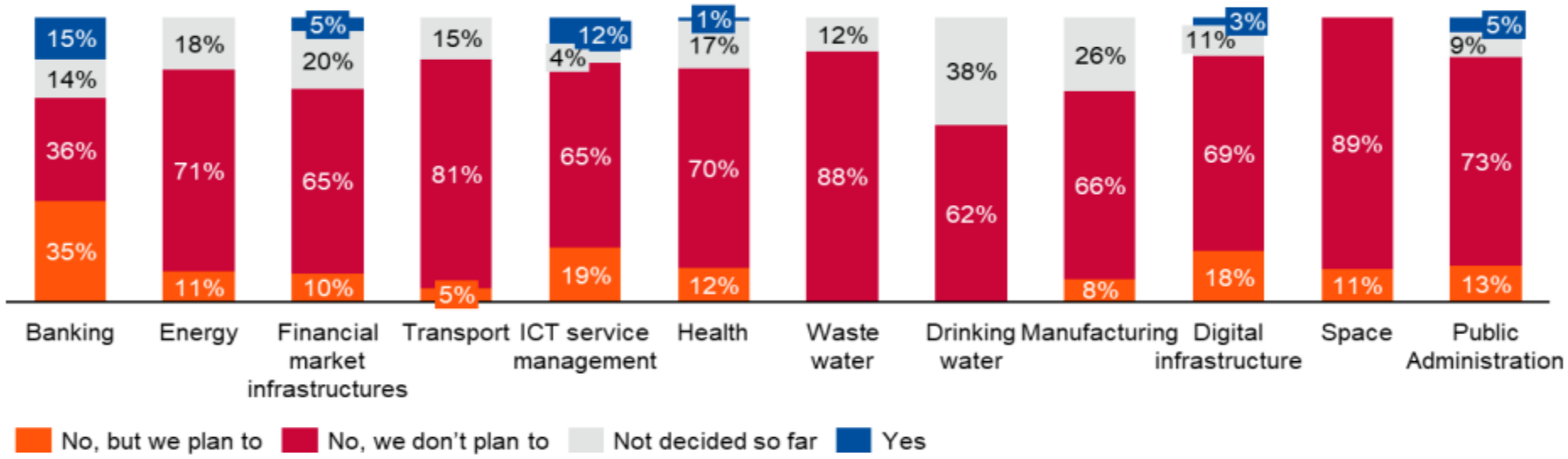
Surveys on quantum-readiness

- Over 2/3 of European cyber and IT professionals are worried about the quantum threat to cybersecurity risks, but **only 4%** of surveyed organisations have a quantum mitigation strategy in place *(ISACA, 2025)*.

- “While 69% of organizations recognize the risk quantum computing poses to current encryption standards, **only 5%** have implemented quantum-safe encryption” *(DigiCert, 2025)*

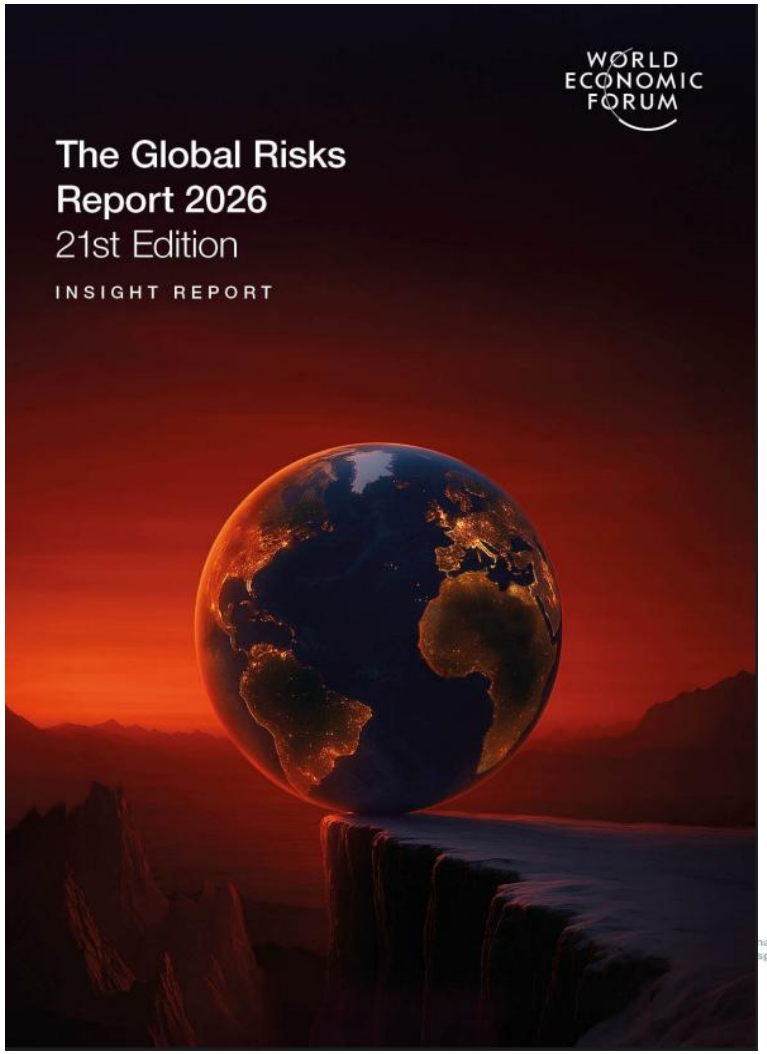
Investment in PQC in the EU critical sectors

Figure 26: Investment in Post-Quantum Cryptography, per NIS2 sector



(ENISA, NIS investments, 2024, p. 31)

Cryptographic complacency



Quantum technologies stand to offer huge economic and social benefits. However, major risks are also on the horizon, potentially within a decade. These include cryptographic challenges (encryption and authentication) with potentially cascading impacts; new extremes in concentration of economic and business power; and an amplification of security risks.

Cryptographic complacency

Cryptographic risks are looming from expected quantum computing attacks on classical mathematics-based cryptography. The latter underlies current user authentication as well as data protection, storage and transmission, affecting the digital lives of all organizations and individuals.

The quantum algorithm that exists today (known as Shor's algorithm) already poses a theoretical threat to classical mathematics-based cryptography. Importantly, there are two specific threat vectors and impacts: First is decryption of private data, which will threaten Personally Identifiable Information (PII) and data privacy (e.g. medical data) as well as intellectual property data. This threat is immediate, due to so-called "harvest now, decrypt later" campaigns, whereby encrypted data is stolen and stored until quantum technology becomes sufficiently advanced to decrypt it.[117]

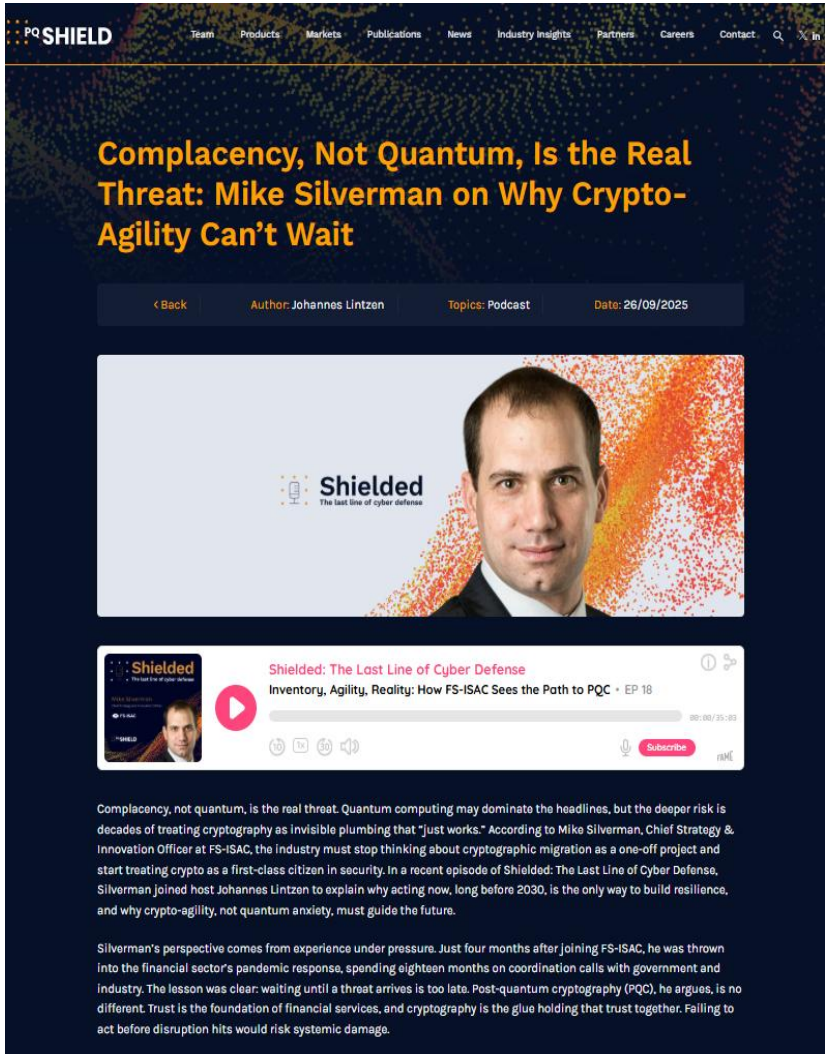
The second threat relates to breaking the cryptographic system that lets people, devices or services prove who they are online. Shor's algorithm threatens to break this so-called "public-key infrastructure" as it is based on asymmetric keys and allows the impersonation of identities. All forms of digital authentication – including impersonation of online wallets for blockchain, authentication of digital contracts, trust establishment between a credit card and the issuing bank, or trust establishment between digital devices – will be at risk. National critical infrastructure could be at risk, too, since hostile actors could, for example, potentially take over self-driving vehicles or utilities. This threat is a longer-term one, as it does not depend on data, rather on whether quantum protection is in place at the time that a quantum attack becomes possible.

Shor's algorithm is waiting for a quantum computer powerful enough to run it, and progress towards this objective is quickening thanks to AI. According to a survey conducted in 2024, 53% of quantum experts believe that within a decade there will be at least a 50% likelihood of a quantum computer being able to break RSA-2048, a type of public-key classical mathematics-based cryptography[118] within 24 hours.[119] Time is thus of essence in preparing for this milestone, often termed "Q-day".[120]

The US National Institute of Standards and Technology (NIST) in 2024 took the lead[121] in issuing a set of standards for post-quantum cryptography (PQC),[122] which is currently serving as a benchmark for other jurisdictions, focused on implementing new PQC algorithms that are resistant to Shor's algorithm. EU Member states have also developed a roadmap for the transition to PQC.[123]

However, many organizations appear to be lagging when it comes to understanding the potential impacts of quantum, both positive and negative. Only 12% of employers surveyed view quantum and encryption as critical technologies that will transform their organizations.[124] Moreover, it is estimated that only 5% of organizations have quantum-safe encryption (i.e. to protect against Shor's algorithm) in place.[125] According to IBM's Quantum Safe Readiness Index, which assesses organizations' level of readiness across quantum-safe discovery, observability and transformation, the average quantum-safe readiness score is only 25 out of 100, where 100 is the safest.[126]

While large companies and some governments may have the know-how and resources to implement protections in time, many smaller companies



Stimulating quantum-readiness

- 96% of participants “stated that regulatory requirements would encourage investment decisions in favour of more quantum-safe cryptography” *(BSI/KPMG, “Market survey on cryptography and quantum computing”, 2023, p. 7)*

- “Clear directives or actions from regulators would trigger immediate action” (*Global Risk Institute/evolutionQ, Quantum threat timeline 2025: executive perspectives on barriers to action, 2025*)

Towards PQC as a crypto standard by default

- “From the BSI's point of view, the question of "if" or "when" there will be quantum computers is no longer paramount. First post-quantum algorithms have been selected by NIST for standardisation and post-quantum cryptography will be used by default. Therefore, the migration to post-quantum cryptography should be pushed forward.” (BSI website)

- “preparing for the quantum threat should be considered an integral aspect of cyber security risk management”; organisations are urged to “make the transition to post-quantum cryptography a top priority” (Joint statement - Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography, 2024)

- **Deprecation of public-key quantum-vulnerable algorithms after 2030, completely disallowing quantum-vulnerable cryptography after 2035** (NIST, 2024)

- Starting from 2027, ANSSI will no longer be accepting applications for security visas on security products that do not have PQC integrated (ANSSI, 2025).

EU PQC research and deployment funding

Horizon Europe and Digital Europe

- **2024:** *Standardisation and awareness of the European transition to post-quantum cryptography* (DE)
- **2024:** *Roadmap for the transition of European public administrations to a post-quantum cryptography era* (DE)
- ***2024:*** *Deployment of Post Quantum Cryptography in systems in industrial sectors* (DE)
- **2025:** *Integration of Post-Quantum Cryptography (PQC) algorithms into high-level protocols* (HE)
- **2025:** *Security of implementations of Post Quantum Cryptography algorithms* (HE)
- **2025:** *Security evaluations of Post-Quantum Cryptography (PQC) primitives* (HE)

EU legislation

Implementing appropriate security measures to ensure the level of security commensurate with the risks, taking into account the state-of-the-art; privacy-by-design, security-by-design:

- **GDPR** (Regulation (EU) 2016/679), Article 32(1) and 25 (1) and (2)
- **e-Privacy** (Directive 2002/58/EC), Article 4(1)
- **NIS 2** (Directive (EU) 2022/2555), Article 21(1) and (2)(h)
- **DORA** (Regulation (EU) 2022/2554), Article 9 and Delegated Regulation (EU) 2024/1774 (9) and Article 6 and 7
- **e-IDAS 2** (Regulation (EU) 2024/1183), (31), (73) and Article 24(2)(e)
- **CRA** (Regulation (EU) 2024/2847), Article 6, Article 13(1) and (2), Article 19(1) and Annex I, Part I (1) and (2)(e)

Suplementing legislation

Commission Implementing Regulation (EU) 2024/2690

Technical and methodological requirements of cybersecurity risk-management measures under NIS 2

Annex, Section 9. Cryptography

- 9.2 (b): mandates to follow, “where appropriate, a cryptographic agility approach”
- 9.3: regular revision and updates of policies and procedures regarding the use of cryptography based on the state of the art

Commission Delegated Regulation (EU) 2024/1774

Regulatory technical standards under DORA

Section 4. Encryption and cryptography

- Article 6(3): “… the selection of cryptographic techniques and use practices, taking into account leading practices…”
- Article 6(4): “…updating or changing, where necessary, the cryptographic technology on the basis of developments in cryptanalysis” ensuring “that the cryptographic technology remains resilient against cyber threats”
- Recital (9): “…remain abreast of relevant developments in cryptanalysis and consider leading practices and standards… follow a flexible approach, based on risk mitigation and monitoring, to deal with the dynamic landscape of cryptographic threats, **including threats from quantum advancements**”

State-of-the-art

"In the context of Article 25 [GDPR], the reference to "state of the art" **imposes an obligation** on controllers, when determining the appropriate technical and organisational measures, **to take account of the current progress in technology that is available in the market. The requirement is for controllers to have knowledge of, and stay up to date on technological advances … and how to implement and update the measures and safeguards … taking into account the evolving technological landscape. …In the face of technological advancements…a measure that once provided an adequate level of protection no longer does. Neglecting to keep up to date with technological changes could therefore result in a lack of compliance with Article 25 [GDPR]**"

"Existing and recognized frameworks, standards, certifications, codes of conduct, etc. in different fields may play a role in indicating the current "state of the art" within the given field of use. Where such standards exist and provide a high level of protection for the data subject in compliance with – **or go beyond – legal requirements**, controllers should take them into account in the design and implementation of data protection measures".

(EDPB, "Guidelines 4/2019 on Article 25 Data Protection by Design and by Default", 2020, p. 8)

State-of-the-art

- “With the ongoing development of extremely powerful quantum computers, methods that are classified as secure today may become obsolete in the near feature. Therefore, the ideal solution is one that is already compatible with post-quantum cryptographic algorithms (PQC**)**” (*ENISA/TeleTrust, “Guideline ‘State of the art’, technical and organizational measures, 2019 p. 41; see also here*)

- Personal data transferred to non-EU countries should be protected against “HNDL” scenarios, including quantum decryption (*EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, 2021 p. 30*)

- “…it is necessary to manage obsolescence and the possibility of encryption algorithms being broken. The computational effort needed to break encryption systems, and the possibility of technical advances such as cryptanalytically-relevant quantum computers, should be balanced with regard to the sensitivity and value of the data…Depending on the risk, measures to enhance the encryption system…should be planned in advance” (*EDPB, “Guidelines 02/2025 on processing of personal data through blockchain technologies”, 2025, p. 19*)

- “The development of practical, widely deployable post-quantum cryptography would mean that the use of quantum vulnerable mechanisms would no longer be best practice” *(SOG-IS, “SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms”, 2023)*; PQC included in EU-level crypto guidelines (*ENISA/SOG-IS, “Agreed Cryptographic Mechanisms ”, 2025*)

Eu-level actions

- **April 2024 – *European Commission Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography* –** to create a Roadmap by April 2026

- **EU PQC Workstream**, co-chaired by France, Germany and the Netherlands within the NIS Cooperation Group.

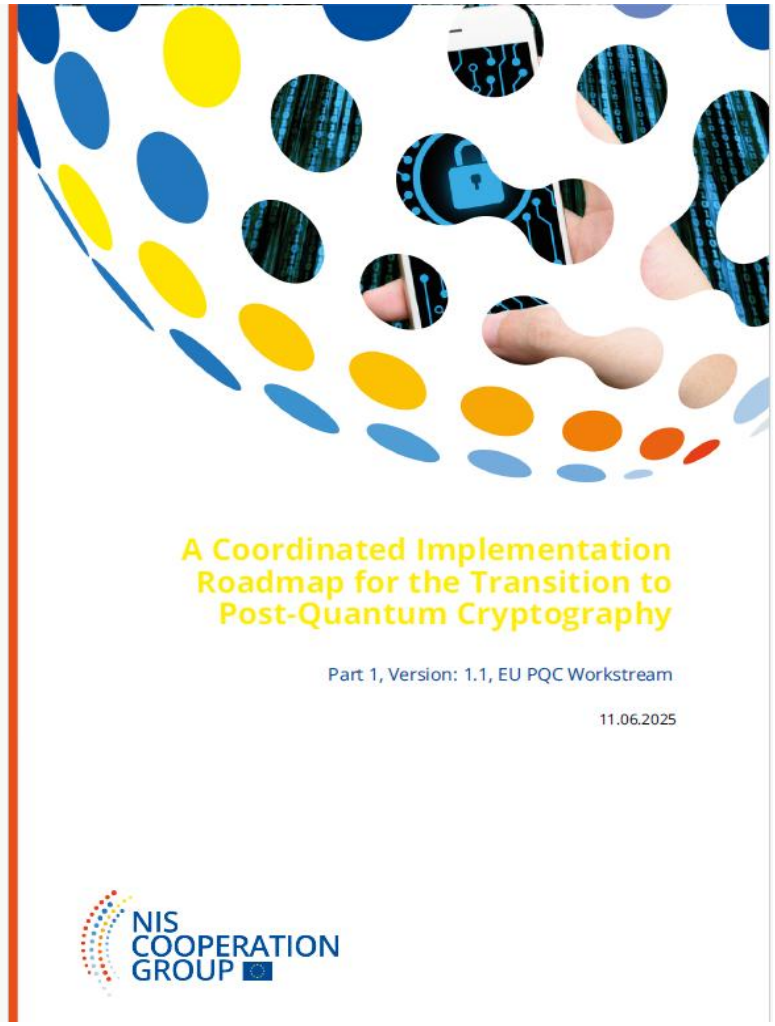
- **November 2024** - Joint statement: *Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography*

- **June 2025** - *A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography*, "high-level concept paper"

Eu-level actions

Timelines:

- **By the end of 2026:** Initial national PQC transition roadmaps have been established by all MS
- **By the end of 2030:** The PQC transition for high-risk use cases has been completed; quantum-safe software and firmware upgrades are enabled by default
- **By the end of 2035:** The PQC transition for medium-risk use cases has been completed; the PQC transition for low-risk use cases has been completed as much as feasible



National initiatives: resources, guidelines, recommendations

The Netherlands

- **AIVD, 2014:** “It is wise to start preparing data encryption for the arrival of quantum computers at an early stage”, *Quantum Computing Fact Sheet*
- **NCSC, 2017:** “Factsheet Post-Quantum Cryptografie”, updated 2023.
- **NCSC, 2022:** “Guidelines for quantum-safe transport-layer encryption”
- **AIVD, 2022:** “*Prepare for the threat of quantum computers*”
- **AIVD/NCSC 2024:** “*Kicking off your quantum migration program*”

National initiatives: resources, guidelines, recommendations

Germany

- **BSI, 2020:** “Migration to Post Quantum Cryptography”
- **BSI, 2021: “**Quantum-safe cryptography – fundamentals, current developments and recommendations”
- **BSI:** regularly updated technical crypto guidelines series *TR-02102-1*.

National initiatives: resources, guidelines, recommendations

France

- **ANSSI, 2020 and 2021:** Cryptographic guidance with PQC mention
- **ANSSI, 2022 and 2023:** “ANSSI views on the Post-Quantum Cryptography transition”
- **ANSSI, 2025: FAQ on PQC**
- **ANSSI, 2026: “**ANSSI’s views on crypto-agility for developers and system architects”
- **ANSSI, 2026:** PQC transition technical guides for SSHV2, IPsec, TLS 1.3

National initiatives: a holistic approach

- **BSI/KPMG:** “Market survey on cryptography and quantum computing”, 2023
- **BSI:** regularly updated study “Status of quantum computer development”
- **ANSSI:** three PQC market-readiness studies 2024a, 2024b and 2025
- **AIVD/CWI/TNO 2023: “**The PQC Migration Handbook”, updated 2024

National initiatives: resources, guidelines, recommendations

Other countries

- **CCN (Spain), 2022:** “Recommendations for a safe post-quantum transition”
- **LHC (Luxembourg), 2023:** “Post quantum security”
- **NÚKIB (Czechia), 2023:** “Minimum Requirements for cryptographic algorithms – Cryptographic security recommendations”, updated **2025** + **Annex** “Quantum threat and quantum-resistant cryptography”
- **ACN (Italy), 2024:** “Crittografia Post-Quantum e Quantistica, Preparazione alla Minaccia Quantistica”
- **NBÚ (Slovakia), 2025:** “Odporúčania pre kryptografické algoritmy”

National initiatives: legal mandates

Hungary

- **Since** 2022, a requirement for critical entities to apply PQC (Act L of 2013, 1. § (1) 49. and 50.)

- Superseded by Act LXIX of 2024 (Chapter V, 51. § - 56. §)

Lithuania

- **By April** 2027**:** an obligation for essential cybersecurity entities to complete the crypto-inventory, to identify high-risk systems and to develop plans for the implementation of PQC

- **By 2030:** migration of high-risk systems is imposed (in either stand-alone or hybrid mode); **by 2035** – the rest of information systems of cyber security actors to apply only PQC
- Accompanying guidelines and crypto-inventory guidelines

Taking stock: “a policy gap”

- Policy goals are set at the strategic level, but PQC is not explicitly mandated at the EU level; a lack of precise requirements may defer action (*Pupillo L. et all, “Strengthening the EU transition to a quantum-safe world. Technology, market, governance and policy challenges”, 2025, p. 29*)

- “Member States have varying capacities and urgency levels… Without a binding EU-wide mandate, the speed of transition may depend on local political will and awareness” (*Ibid*)

- “The planned deprecation of certain algorithm implementations and full disallowance of current public-key cryptographic algorithms, increase the urgency of initiating actions for the migration to [PQC]” (*Recital (8), NIS 2 amendments proposal, 2026*)

- A requirement for Member States to incorporate policies for the transition to PQC into their national cybersecurity strategies (*Article 7(2)(k) and Recital (8), NIS 2 amendments proposal, 2026*)

Taking stock: “a policy gap”

- **Stronger action at the EU level is needed: a joint streamlined clarification as regards PQC as a required standard across all relevant legal instruments**

- Misalignments: a lack of clear emphasis on PQC in the context of Technical implementation guidance On Commission Implementing Regulation (EU) 2024/2690 (*ENISA, 2025, p.117-120*)

- ENISA should play a more prominent and consistent role in promoting PQC transition

- More involvement of data protection authorities in the PQC transition governance processes

The (fuzzy) (geo)politics of algo choices

- (8) “For a harmonized implementation of [PQC] across the Union it is essential to develop common European standards and develop a framework for identifying and selecting [PQC] algorithms to be deployed in the digital networks and services across the Union” (*Commission Recommendation (EU) 2024/1101 on coordinated PQC transition roadmap*)
- 1(2) “support the evaluation and selection of relevant [PQC] EU algorithms with the help of cybersecurity experts, and further adoption of such algorithms as Union standards that should be implemented across the Union as part of the [PQC] Coordinated Implementation Roadmap” (*Commission Recommendation (EU) 2024/1101 on coordinated PQC transition roadmap*)
- (42) “ENISA should contribute to the development and evaluation of cryptographic algorithms, in particular in the area of post-quantum cryptography” and “may establish a process to solicit and evaluate algorithms for cryptographic algorithms by relevant stakeholders” (*CSA 2 proposal, 2026*)
- Article 18(3) ENISA should cooperate with the European standardisation bodies to standardise schemes positively evaluated though its process (*CSA 2 proposal, 2026*)

The (fuzzy) (geo)politics of algo choices

- (2) Encryption - a key technology for achieving resilience and **technological sovereignty**, among others (*Commission Recommendation (EU) 2024/1101 on coordinated PQC transition roadmap*)

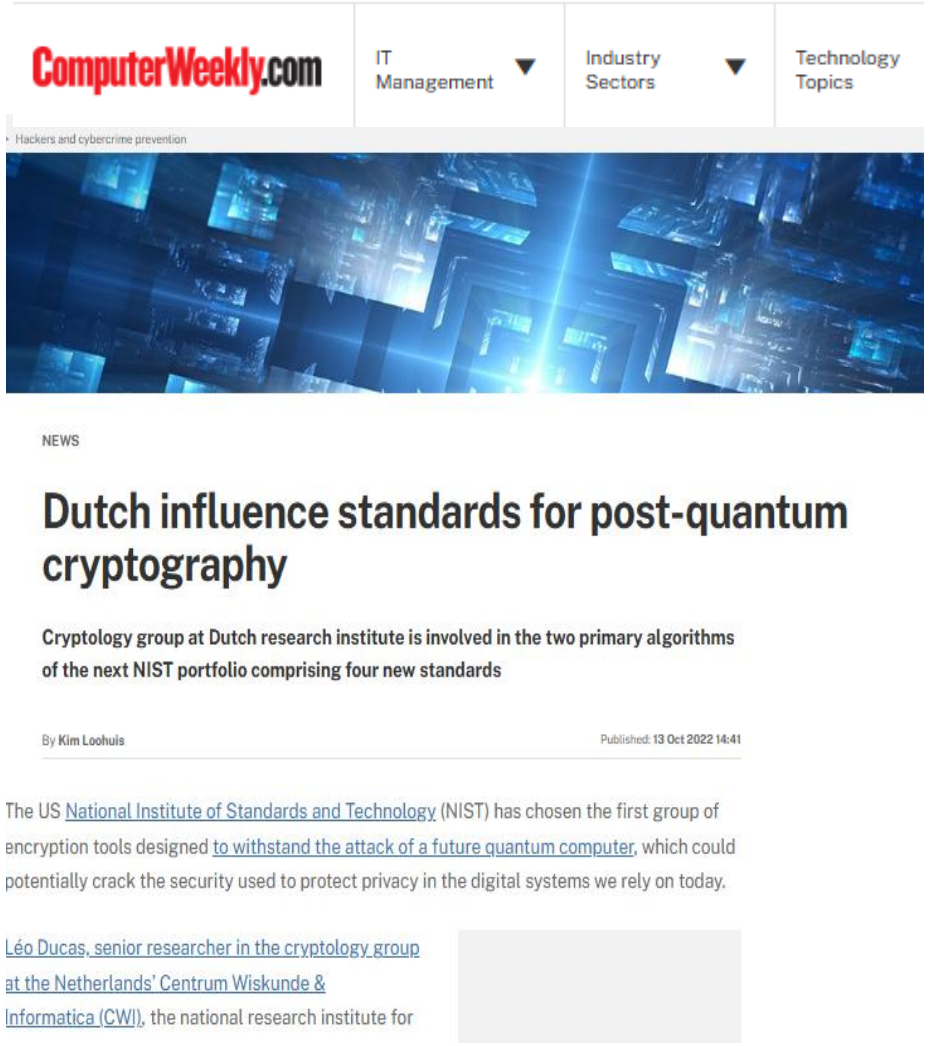
- US NIST – the main PQC standardisation venue and *de facto* global crypto standards setter for decades (*L. Chen and M. Scholl, "The Cornerstone of Cybersecurity – Cryptographic Standards and a 50-Year Evolution", 2022*)

- "The NSA and NIST: a toxic relationship" (*R. Hagemann, 2016*)

But

- Significant contribution of EU researchers within the NIST PQC standardization process

Significant European contribution in PQC standardisation



ComputerWeekly.com | IT Management | Industry Sectors | Technology Topics

Hackers and cybercrime prevention

NEWS

Dutch influence standards for post-quantum cryptography

Cryptology group at Dutch research institute is involved in the two primary algorithms of the next NIST portfolio comprising four new standards

By Kim Loohuis Published: 13 Oct 2022 14:41

The US National Institute of Standards and Technology (NIST) has chosen the first group of encryption tools designed to withstand the attack of a future quantum computer, which could potentially crack the security used to protect privacy in the digital systems we rely on today.

Léo Ducas, senior researcher in the cryptology group at the Netherlands' Centrum Wiskunde & Informatica (CWI), the national research institute for

HQC Home Resources Team

HQC Team (by joining date then alphabetical order)

- Philippe Gaborit - University of Limoges (FR)
- Carlos Aguilar Melchor - SandboxAQ (USA)
- Nicolas Aragon - Naquidis Center (FR)
- Slim Bettaieb - Technology Innovation Institute (UAE)
- Loïc Bidoux - Technology Innovation Institute (UAE)
- Olivier Blazy - Ecole Polytechnique (FR)
- Jean-Christophe Deneuville - ENAC, University of Toulouse (FR)
- Edoardo Persichetti - Florida Atlantic University (USA)
- Gilles Zémor - IMB, University of Bordeaux (FR)
- Jurjen Bos - Worldline (NL)
- Arnaud Dion - ISAE-SUPAERO, Toulouse University (FR)
- Jérôme Lacan - ISAE-SUPAERO, Toulouse University (FR)
- Jean-Marc Robert - University of Toulon (FR)
- Pascal Véron - University of Toulon (FR)
- Paulo L. Barreto - University of Washington Tacoma (USA)
- Santosh Ghosh - NVIDIA (USA)
- Shay Gueron - University of Haifa, Israel and Meta (USA)
- Tim Güneysu - Ruhr-Universität Bochum and DFKI (DE)
- Rafael Misoczki - Meta (USA)
- Jan Richter-Brokmann - Ruhr-Universität Bochum (DE)
- Nicolas Sendrier - INRIA (FR)
- Jean-Pierre Tillich - INRIA (FR)
- Valentin Vasseur - Thales (FR)

The (fuzzy) (geo)politics of algo choices

- "… the evaluation of algorithms as candidates for standards is being done in the context of the competition led by NIST, supported by the EU through EU-funded research" (*European Commission, "Rolling plan for ICT standardisation", 2025, p. 29*)

- "BSI welcomes the NIST process as a method of defining standards in a transparent international process that can then be used worldwide. It is particularly opposed to a separate process for standardising German or European algorithms. A "proliferation" of international standards would both hamper interoperability and reduce the market opportunities of crypto producers. In addition, a splitting of personnel and research resources would lead to a lower evaluation quality for those algorithms that are ultimately selected" *(BSI, "Quantum-safe cryptography – fundamentals, current developments and recommendations", 2022, p. 34*)

The (fuzzy) (geo)politics of algo choices

- NIST PQC selections endorsed by national and EU-level crypto guidelines

Beyond NIST

- “For practical recommendations for quantum-resistant cryptography in the near future, we also find other candidates in the KEM/Encryption category essential, namely **Classic McEliece** (3rd and 4th round candidate) and **FrodoKEM** (alternate 3rd round candidate). The reason why this is so is closely related to their security. They have in principle higher theoretical security guarantees than the winner in this category, CRYSTALS-Kyber. And the reasons why they have not (yet) been selected for standardization are related to some of their practical properties” (*NÚKIB, “Quantum threat and quantum-resistant cryptography”, 2025, p. 18*)
- Some national authorities endorse both FrodoKEM and Classic McEliece, some only one of them, only FrodoKEM features in the current EU-level crypto quidelines

The (fuzzy) (geo)politics of algo choices

- NIST PQC selections endorsed by national and EU-level crypto guidelines

Beyond NIST

- “For practical recommendations for quantum-resistant cryptography in the near future, we also find other candidates in the KEM/Encryption category essential, namely **Classic McEliece** (3rd and 4th round candidate) and **FrodoKEM** (alternate 3rd round candidate). The reason why this is so is closely related to their security. They have in principle higher theoretical security guarantees than the winner in this category, CRYSTALS-Kyber. And the reasons why they have not (yet) been selected for standardization are related to some of their practical properties” (*NÚKIB, “Quantum threat and quantum-resistant cryptography”, 2025, p. 18*)
- Some national authorities endorse both FrodoKEM and Classic McEliece, some only one of them, only FrodoKEM features in the current EU-level crypto quidelines

PQC transition and the EU competence

- (11) “On the basis of the information thus obtained and all other available information, the Commission will assess the effects of this Recommendation and determine whether additional steps, including proposing binding acts of Union law, are required” (*Commission Recommendation (EU) 2024/1101 on coordinated PQC transition roadmap*)

- 3 (10) “On the basis of those and all other available information the Commission will assess the designed measures and the operation of the network of Member States’ representatives and determine whether additional actions, including proposing binding acts of Union law, are required” (*Commission Recommendation (EU) 2024/1101 on coordinated PQC transition roadmap*)

- NIS 2 amendments proposal, 2026

Market-framing of non-market issues

Taylor & Francis Online

Journals · Search · Publish

Home ► All Journals ► Politics & International Relations ► Journal of European Public Policy ► List of Issues ► Volume 7, Issue 2 ► Competing frames in the European Commiss

Journal of European Public Policy ›

Volume 7, 2000 - Issue 2

Enter keywords, authors, DOI, etc

Submit an article | Journal homepage

Original Articles

Competing frames in the European Commission - the case of the defence industry and equipment issue

Ulrika Morth

Pages 173-189 | Published online: 04 Feb 2011

Cite this article https://doi.org/10.1080/135017600343151

References | Citations | Metrics | Reprints & Permissions | Read this article

Abstract

It is argued that frame competition plays an important part in EU policymaking, especially within the European Commission. The case of a cross-pillar issue, the issue of defence industry and equipment, shows how two frames – market and defence – compete on the legal and political approaches to this issue. Frame competition is something more than just conflicts of interests. It also functions as an important identity-building and sense-making process in multi-organizations, which are typified more by ambiguity and inconsistency than by clarity and consistency. By approaching the European Commission from a multi-organizational perspective, the frame competition process is regarded as an essential component in the cohesion process. The empirical analysis shows that framing is not static, but that frames can change and result in a reframing. By reframing the defence industry and equipment issue, the Commission has managed the conflict between the market and defence frames.

Keywords:

Defence Industry Equipment | European Commission | Multi-ORGANIZATION

Previous article | View issue table of contents | Next article

Related

People rea

In every integrati

Daniel Fic

Journal of

Published

Discours doing cri

Merlijn va

Critical Pol

Published

POLICY F

BLOOMSBURY COLLECTIONS

Home | Subjects | Discover | Open Access | About | For Librarians

EU Data Protection and 'Treaty-base Games': When Fundamental Rights are Wearing Market-making Clothes

Author: Laima Jančiūtė

DOI: 10.5040/9781509919376.ch-001

Page Range: 1–32

ABSTRACT

At odds with the European rights-based approach context in which it is embedded, the EU Directive 95/46/EC (the world's most influential privacy and data protection instrument that in 2018 will be replaced by the newly adopted GDPR) was created and has been functioning as a market-making tool. The constitutional basis for the rights-based approach to fully unfold at the EU level came along with the Lisbon Treaty. However, the governance of the rights to privacy and data protection maintains a lot of market-issue elements, and certain path dependencies emerged throughout the two decades after adoption of Directive 95/46/EC. These dynamics are determined by a complex interplay between various dimensions: the evolution of the EU politics as such (macro), the evolution of the human rights governance in the EU (meso) and the development of privacy and data protection norms and instruments namely (micro). The above represents an interesting case for analysis and will be explained with the aid of the neo-institutional theory, which allows to show how norms creation has always been intertwined with or even driven by the strategic interests of various actors. It also allows to gain insights into the constraints and possibilities determined by the market-making governance of data protection. This paper links the market-framing context of the Directive 95/46/EC to the so-called 'treaty-base games' known in the EU politics as one of the creative strategies in overcoming institutional constraints.

Crypto – genuinely a cross-pillar issue

- "Encryption technologies are increasingly integrated into commercial systems and applications"; "it will become an integral part of personal and business computing"; significance for e-commerce, fundamental rights and the development of Information Society (*Commission Communication "Ensuring security and trust in electronic communication - Towards a European framework for digital signatures and encryption", 1997*)

- Protection of a series of fundamental rights; objectives of the Digital Single Market, among others *(Commission Recommendation (EU) 2024/1101 on coordinated PQC transition roadmap*)

- Provisions on encryption in the EU Cybersecurity and digital *acquis*

“Europeanisation” of cybersecurity

EUROPEAN CYBER SECURITY: HISTORY OF A CULTURAL TRANSFORMATION

In the first half of 2022, France will hold the presidency of the Council of the European Union. An opportunity which, in terms of cyber security, offers the prospect of increasing the momentum started in the last few years. In preparation for this time, certain key words can be heard at ANSSI: ambition, scaling up, cooperation, solidarity, digital sovereignty. Just a decade ago, such intentions didn't come so naturally. Let's take a look back at an area which, year on year, has become considerably "Europeanised". ➔

↓
"ALL STATES ARE MATURING AND DEVELOPING THEIR CAPACITY TO COOPERATE. THE EXCHANGE OF INFORMATION REALLY IS IN OUR DNA."
↑

LOUIS ROUXEL
CERT-FR cooperation activities manager

● are maturing and developing their capacity to cooperate. The exchange of information really is in our DNA."

FROM A TECHNICAL TO A STRATEGIC LEVEL

It is with this well-crafted directive that, what Anne Tricaud calls the "European transformation" of the agency, begins. "We were able to see that the NIS directive enabled us to strengthen the level of security throughout the Union, to protect more players, to coordinate with our partners ... and thus to help strengthen national security. So we started to think that dealing with cyber matters on a European scale... that was a very good idea!"

Especially since NIS also allows the creation of a strategic cooperation group. Initially designed to discuss the implementation of the directive, the forum has evolved to accommodate broader topics, such as securing 5G technology. A subject which knows all too well the interests of the major world powers, sometimes opposing positions, against which Europe must adopt a consistent stance. Antoine Berthier, sectorial coordinator responsible for telecoms at ANSSI, takes stock: "We have reached a balanced position by focusing on technical and safety issues. Each country has conducted its risk analysis to bring out a set of recommendations." For Yves Verhoeven, the creation of this instrument is a dual success: "Firstly, because it is the result of intelligent cooperation between the Commission and the member states in the face of a great technological challenge of our time. And secondly, because it constitutes a first illustration of what European digital sovereignty can be: neither naive nor autarkic."

More recently, the group served as an incubator ... for CyCLONe.[3] Dedicated to crisis management, this fledgeling network brings together the European counterparts of ANSSI's Director-General. "In 2018, the organisation of a crisis management exercise at European level highlighted the need for cooperation at a more strategic level than the CSIRTs Network, which has more of a technical vocation", explains Agathe Favetto. In addition to this observation was the desire expressed by Guillaume Poupard to be able to prepare for a major crisis with his European counterparts. The Blue OLEx event, organised in Paris in 2019, then allowed a first meeting and, subsequently, the formal creation of CyCLONe.

"We have not yet had to put it to the test" states Guillaume Poupard, reassuringly. "But the preparation work we are doing today will save so much time when the moment comes." More able to take a step back from technical incidents, to have an overview of the impacts and to provide political advice, CyCLONe continues to improve, also by developing its interactions with the CSIRTs Network.

A UNIFYING AGENCY

We can say that NIS paved the way for all the initiatives that followed for the construction of genuine European cybersecurity. That with the solid foundations it laid, all the blocks that have been put together since then can't help but fit together naturally.

But let's take a little step back. A first stone was, in fact, laid several years before the turning point of the famous European directive, almost as if to mark the place where it was to be built. As early as 2004, an institution was conceived as a means to strengthen cooperation between the states of the continent; a European cybersecurity agency: ENISA[4].

Several years before the acceptance of the very concept of European cybersecurity and the first steps in this ●

[3] Cyber Crisis Liaison Organisation Network

[4] European Union Agency for Cybersecurity

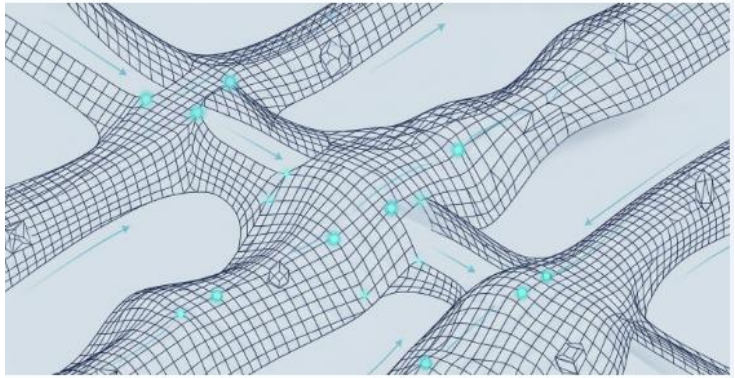
Scientific uncertainty

QUANTUM INSIDER

News Resources Product Advisory Marketing About Us

Q-Day Just Got Closer: Three Papers In Three Months Are Rewriting The Quantum Threat Timeline

Quantum Business, Research Resonance • March 31, 2026



The Three Papers

The Research That Made It Possible

The Trajectory

The Policy and Regulatory Landscape

What This Means for Organizations

The quantum resources needed to break modern encryption have dropped by an order of magnitude since May 2025. Here is what happened, what it means, and what organizations should do about it.

In fewer than twelve months, three research papers have sharply reduced the estimated quantum resources required to break the cryptographic systems that protect the global digital economy. Together, they represent the most significant shift in quantum threat assessment since Peter Shor published his factoring algorithm in 1994.

The punchline: what once required 20 million qubits now requires fewer than one million for RSA, potentially fewer than 100,000 under newer architectures, and fewer than 500,000 for the elliptic curve cryptography that protects every major cryptocurrency and most digital signatures. One of the papers was so sensitive that its authors chose not to publish the actual attack circuits, instead releasing a cryptographic proof that the circuits work without revealing how they work. If you are a CISO, CTO, or policymaker still treating quantum risk as a future problem, that decision should give you pause.

The Three Papers

GIDNEY (MAY 2025): RSA-2048 IN UNDER A MILLION QUBITS

Craig Gidney of Google Quantum AI published a paper showing that a quantum computer with fewer than one million noisy physical qubits could factor a 2048-bit RSA

BBC

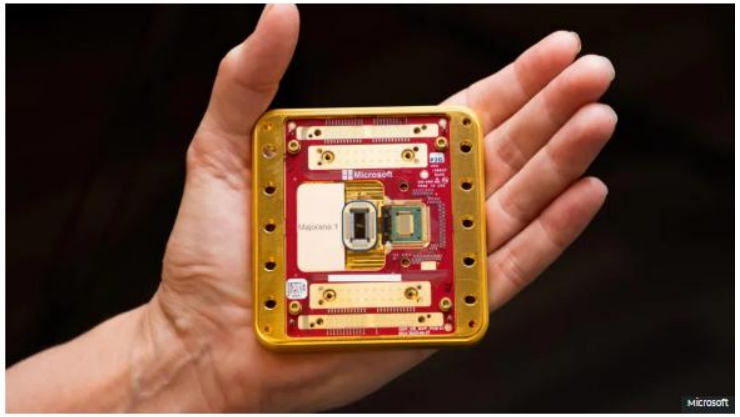
Home News Sport Business Technology Health Culture Arts Travel Earth Audio Video Live

Powerful quantum computers in years not decades, says Microsoft

19 February 2025

share save Add as preferred on Google

Chris Vallance
senior technology reporter



Microsoft has unveiled a new chip called Majorana 1 that it says will enable the creation of quantum computers able to solve "meaningful, industrial-scale problems in years, not decades".

It is the latest development in quantum computing - tech which uses principles of particle physics to create a new type of computer able to solve problems ordinary computers cannot.

Creating quantum computers powerful enough to solve important real-world problems is very challenging - and some experts believe them to be decades away.

Microsoft says this timetable can now be sped up because of the "transformative" progress it has made in developing the new chip involving a "topological conductor", based on a new material it has produced.

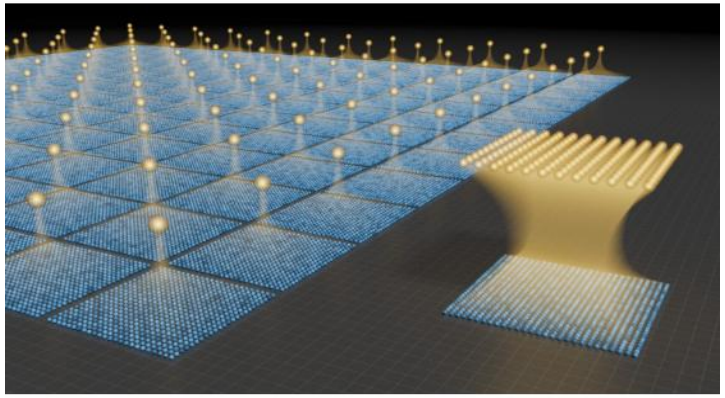
The firm believes its topoconductor has the potential to be as revolutionary as the semiconductor was in the history of computing.

QUANTUM INSIDER

News Resources Product Advisory Marketing About Us

Research Team Finds Useful Quantum Computers Could Be Built With As Few As 10,000 Qubits

Research Matt Swayne • March 31, 2026

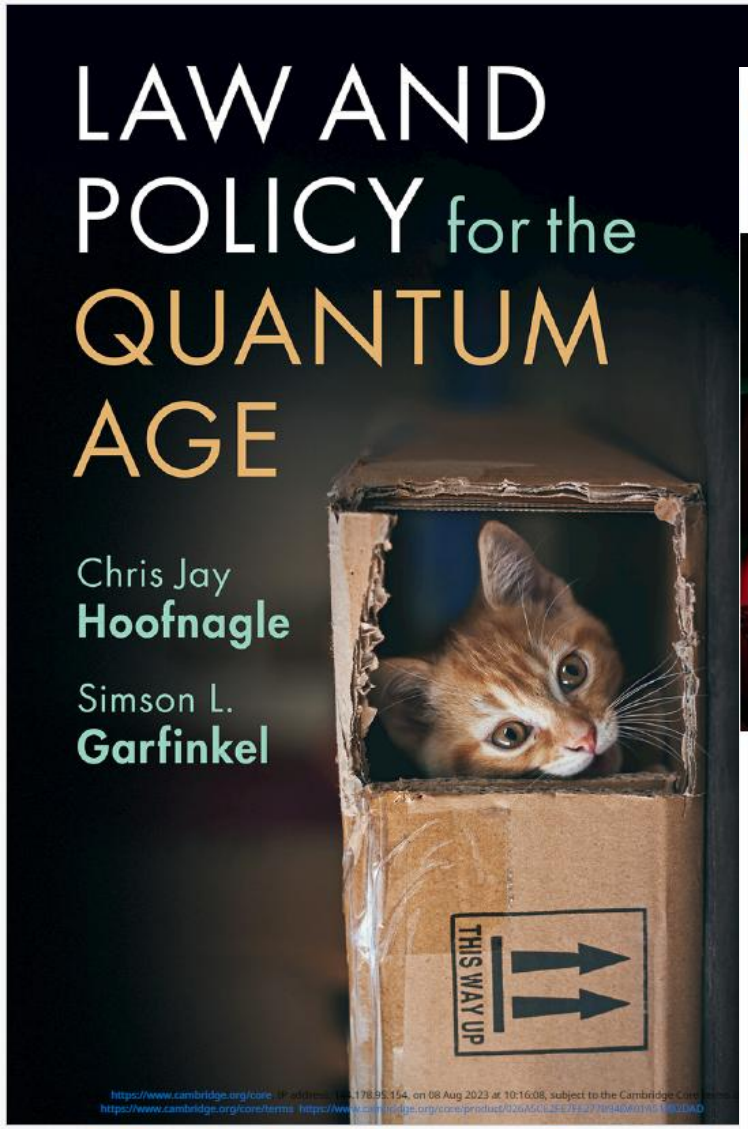


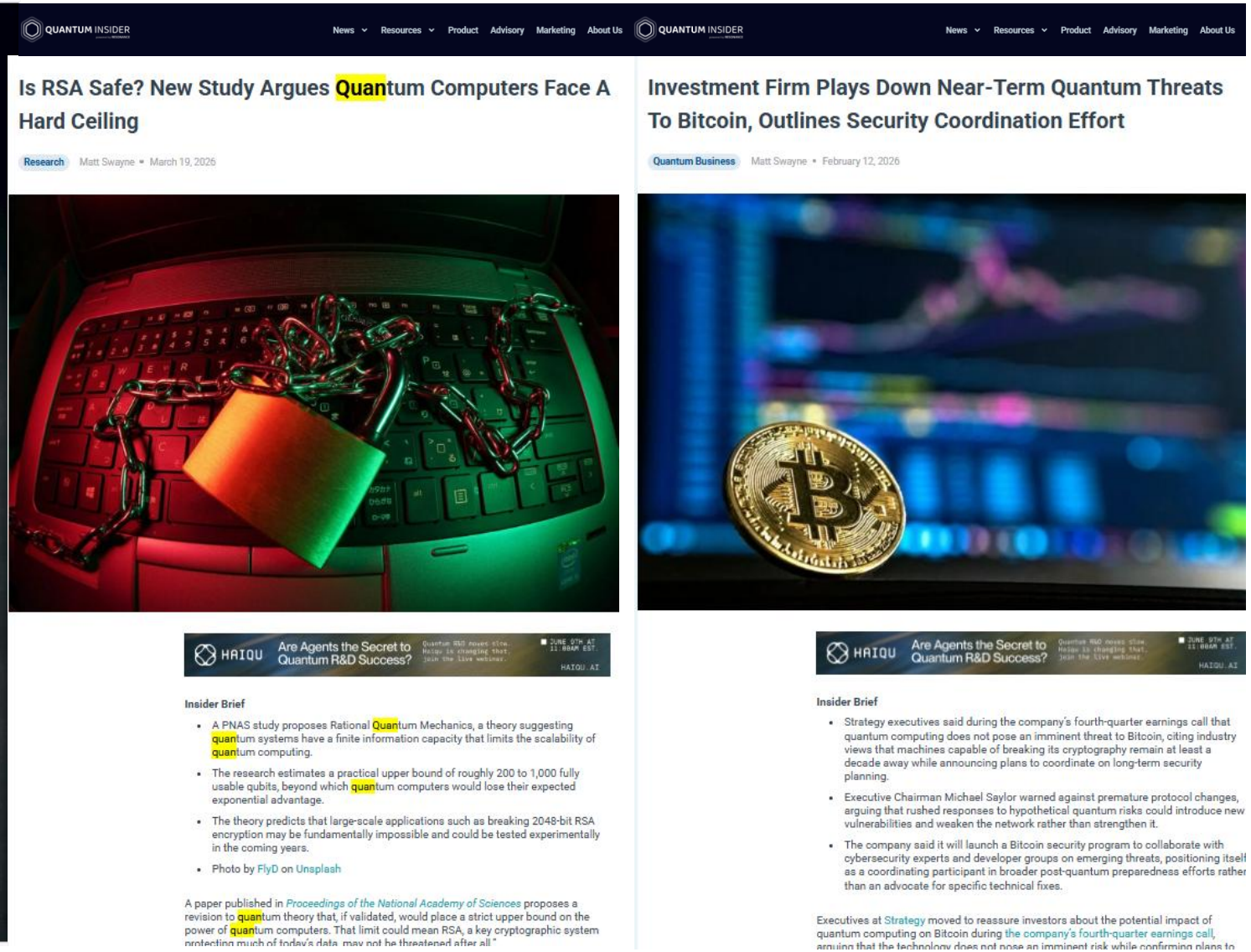
Insider Brief

- New research from Caltech and Oratomic suggests fault-tolerant quantum computers could require only 10,000–20,000 qubits—far fewer than previously thought—potentially accelerating timelines to within this decade.
- The team developed an ultra-efficient quantum error-correction architecture using neutral atom systems, reducing the number of physical qubits per logical qubit from around 1,000 to as few as five.
- The findings imply faster progress toward practical quantum machines capable of breaking current encryption methods, increasing urgency for migration to quantum-resistant cryptography.
- Image: Previous error-correction schemes, depicted on the left, require hundreds of physical qubits per logical qubit. The new scheme, depicted on the right, reduces this overhead by more than 100-fold. (Caltech/Robert Hurt,IPAC-SELab)

PRESS RELEASE — Quantum computers of the future may be closer to reality thanks to new research from Caltech and Oratomic, a Caltech-linked start-up company. Theorists and experimentalists teamed up to develop a new approach for reducing the errors that riddle today's rudimentary quantum computers. Whereas these machines were previously thought to require millions of qubits to work properly (qubits being the quantum equivalent to 1's and 0's in classical computers), the new results indicate that a fully realized quantum computer could be built with as few as 10,000 to 20,000 qubits. The need for fewer qubits means that quantum computers could, in theory, be operational by the end of the decade.

Scientific uncertainty





Precautionary principle

- The consequences of a false negative cannot be afforded
- “In the context of financial stability and cybersecurity, the precautionary principle requires … action already when there is a *risk* to the stability of the financial system. The mere possibility of damage is enough; a concrete probability is not required” *(C. Calliess and A.Baumgarten, “Cybersecurity in the EU The Example of the Financial Sector: A Legal Perspective”, 2020,* p.1156 *original emphasis)*
- “For a wide variety of organizations, the costs of delayed preparation are likely to exceed those of adopting quantum-safe cryptography early” *(WEF, The global risks report, 2026, p. 58)*

THANK YOU !!!