EUROPEAN POLICY CENTRE

DISCUSSION PAPER

EUROPE'S POLITICAL ECONOMY PROGRAMME

17 JULY 2023

A quantum cybersecurity agenda for Europe

Governing the transition to post-quantum cryptography

Andrea G. Rodríguez

Credit: CANVA

Table of contents

ABOUT THE AUTHOR

Andrea G. Rodríguez is Lead Digital Policy Analyst at the European Policy Centre.

ACKNOWLEDGEMENTS / DISCLAIMER

This Discussion Paper is the product of a workshop, interviews, and research conducted in the context of the EPC's 'Europe's Quantum Frontier' project. The project is structured as a task force bringing together actors across Europe's industry and policymaking community to work on EU policy questions and solutions for the development of a European quantum ecosystem. Previous workstreams have focused on quantum value chains. The EPC's work on this project is supported by Quantum Delta NL as a founding partner of the EPC task force.

The support the European Policy Centre receives for its ongoing operations, or specifically for its publications, does not constitute an endorsement of their contents, which reflect the views of the authors only. Supporters and partners cannot be held responsible for any use that may be made of the information contained therein.

Executive summary

Cybersecurity plays an important role in Europe's economic security by allowing digital communications and services to take place safely and securely. However, the rapid development of quantum computers creates a new set of challenges that compromise the level of security of everything happening online—of which quantum attacks on encryption are particularly worrisome. The advent of a cryptographically significant quantum computer is only a matter of time, and it is already changing the threat landscape with adversaries downloading encrypted information to be decrypted once the technology is available 'harvest attacks'.

Some actors, such as the United States and some—but not all—EU member states, are taking action to counter these emerging threats using the tools available, such as planning the migration to post-quantum encryption of sensitive information. Yet, a new EU Coordinated Action Plan will be necessary to ensure a harmonised transition to post-quantum encryption and bridge the gap between establishing a fully operational European quantum information infrastructure network (EuroQCI) project and the current needs of the European cybersecurity landscape to respond to 'harvest attacks' and future quantum attacks on encryption.

RECOMMENDATIONS FOR AN EU QUANTUM CYBERSECURITY AGENDA

1. Establish an EU Coordinated Action Plan on the quantum transition that outlines clear goals and timeframes and monitors the implementation of national migration plans to post-quantum encryption.

2. Establish a new expert group within the European Union Agency for Cybersecurity (ENISA) with seconded national experts to exchange good practices and identify obstacles to the transition to post-quantum encryption.

3. Assist in setting priorities for the transition to post-quantum encryption and push for cryptographic agility to respond to emerging vulnerabilities in post-quantum encryption systems.

4. Facilitate political coordination between the European Commission, EU member states, national cybersecurity agencies and ENISA to determine technological priorities and identify relevant use cases for quantum-safe technologies. This is particularly relevant at a time when some member states are individually evaluating the use of post-quantum encryption, quantum key distribution, or a combination of the two.

5. Facilitate technical coordination at the EU level to address research gaps in quantum-safe technologies, such as the need to develop quantum nodes to ensure long-range connections for quantum key distribution.

6. Explore the use of sandboxes to accelerate the development of near-term applications of quantum information technologies.

Introduction

Cybersecurity is an integral part of Europe's economic security, central to protecting and defending European interests, allowing the EU economy to operate at full speed, and citizens to navigate online services safely and securely. However, advances in quantum computing put at risk Europe's cybersecurity by rendering obsolete current encryption systems and creating new cybersecurity challenges. For Europe to be serious about its cybersecurity ambitions, it must develop a quantum cybersecurity agenda.

In recent years, the European Union has created a resourceful cyber policy. The aim has been to level up cybersecurity with particular attention to essential economic sectors, for example, by improving the coordination between private and public actors. Furthermore, the EU has invested in identifying emerging threats that can negatively impact cyber resilience or the ability to identify, protect, respond, and recover from cyberattacks.

Nevertheless, the impact of quantum computing on Europe's cybersecurity and data protection has been mainly left out of the conversation despite sporadic mentions in some policy documents, such as the 2020 EU Cybersecurity Strategy or the 2022 Union Secure Connectivity Programme. Quantum computing, a field developing rapidly, will disrupt online security by compromising cryptography—the algorithms that keep information safe—or by facilitating cyberattacks such as those on digital identities.

The EU can leverage its experience and successes in cybersecurity, such as identifying key players and relevant actors, and encourage its industrial base to address current strategic vulnerabilities in key quantum-safe technologies, like quantum key distribution (QKD) and post-quantum cryptography (PQC).

Background: Quantum computing and challenges to today's cybersecurity

Quantum computers use quantum mechanics to code and perform operations on digital information. These properties make quantum computers work differently from classical computers, opening up a new set of challenges for cybersecurity.

One of the most urgent directly impacts how information is secured, transmitted, and consumed online. Cryptography is the backbone of secure digital communications. From web searches to sensitive intelligence, in the way that encryption goes, mathematical algorithms codify information and ensure that communication happens only between pre-authorised parties and that the message is accessible and remains unaltered. These three properties—confidentiality, integrity, and availability—are the basis of information security.

Research suggests that by 2026, there is a 1 in 7 chance that quantum computers will break the most used cryptographic systems, which will go as high as 50% by 2031.[1] However, research published[2] in early 2023 by Chinese scholars suggests that it could happen even before.

Table 1: Examples of most commonly used cryptographic systems and their resistance to quantum attacks.[3]

Cryptography standard (in-use)	Function	Post-quantum security level	Examples of today's use
RSA-2048	Encryption & signature	Broken	Internet traffic, including the webpages of all European Institutions, banks, energy, and transport companies.
RSA-3072	Encryption & signature	Broken	VPNs, financial transactions, minimum security level required for intelligence secrets, e-passports.
DH-3072	Key exchange	Broken	Internet protocols such as SSL/TLS, SSH, and IPSec.
256-bit ECDSA	Signature	Broken	Used in Bitcoin and Ethereum exchanges, Companies' internal communications.

All cryptography algorithms in this table were also listed as vulnerable by the White House in the November 2022 migration memorandum - examples of use retrieved by the author.

Cyberattacks on encryption using quantum computers would allow adversaries to decode encrypted information, interfere with communications, and access networks and information systems without permission, thereby opening the door to stealing and sharing previously confidential information.

Given that the prospects of a cryptographically significant quantum computer—one able to break encryption—are not a question of if but rather when, cybercriminals and geopolitical adversaries are rushing to obtain sensitive encrypted information that cannot be read today to be de-coded once quantum computers are available.

These types of cyberattacks, known as 'harvest attacks' or 'download now-decrypt later', are already a risk to European security. In 2022, Belgium passed a law to declassify documents following a 20, 30, and 50-year rule, depending on the level of secrecy. In France, documents should generally be ready for public access after 50 years, and similar examples can be found in other EU countries. However, an adversary using a quantum computer could steal, read, and disseminate information before it reaches the public eye—as soon as seven years.

Cryptography attacks can also negatively impact the European economy and the competitiveness of European companies. Quantum computers will increase the probability of intellectual property theft or data breaches as cryptography attacks become more frequent, and companies responsible for critical infrastructure, such as transportation, energy distribution systems, or communications, will be particularly vulnerable. Cyberattacks on critical infrastructure can have far-reaching consequences, with spillover effects on other economic sectors and international security. Only the recovery from the 2020 SolarWinds cyberattack[4] could cost the global economy up to $100 billion.

Governing the quantum transition: The US and the EU approach

These emerging cybersecurity challenges have urged policy responses in several countries. Because of the urgency of quantum attacks on encryption, many of these policies have been specifically aimed at identifying vulnerabilities of the cryptographic systems in use and exploring the use of quantum-safe technologies, particularly post-quantum encryption and quantum key distribution (see: Box 1).

BOX 1: COMPARISON OF THE USE OF QUANTUM KEY DISTRIBUTION AND POST-QUANTUM ENCRYPTION FOR CYBERSECURITY

As countries prepare their cybersecurity structures for quantum computers, there are still questions about which technologies are better to secure information. To this day, the two most promising are quantum key distribution and post-quantum cryptography both of them offering a different set of advantages and disadvantages over the other.

Quantum key distribution enables two parties to establish a secure communication channel based on quantum physics. Because of the properties of quantum bits (qubits), data shared cannot be copied, which protects against information theft during communications. Moreover, any disturbance or interference in the communication channel could be perceived by the parties that can at the moment decide to stop communicating. This offers a unique advantage against eavesdropping, where a third party 'listens' to the conversation.

However, while eavesdropping can be detected, QKD requires pre-sharing encryption keys, which can create an authentication problem. An unauthorised party could potentially supplant the identity of one of the parties ('man-in-the-middle'). Moreover, QKD requires specific infrastructure, which increases the time and cost of the transition, and its sensibility to eavesdropping could increase the risk of denial of service (DoS) cyberattacks. Also, there are still multiple challenges to widespread adoption, such as the distance at which communication can happen (hardly over 200km nowadays) and the need to use trusted nodes to solve this, to go over 200km. For all these reasons, while QKD applications are promising and can add value in the long-term, they are generally perceived as still in the early stages of development.

Post-quantum cryptography is a more mature area of activity and offers several advantages over quantum key distribution, though it also has theoretical and practical challenges. PQC can be defined as a set of cryptographic algorithms which are believed to be quantum resistant. These algorithms run on classical hardware, which makes their deployment much faster and cheaper as, in a few words, it would involve little more than a software update. However, PQC protocols have the same vulnerabilities as current cryptographic systems, and further technological advancements could allow for the retrospective decryption of these algorithms, hence the reason why the Nation Institute for Standards and Technology (NIST) competition is still ongoing. In other words, no practical proof exists that more sophisticated decryption algorithms, besides the ones already known run by quantum computers, would not break post-quantum cryptography being developed today.

The US arguably leads the transition to post-quantum cybersecurity (see: Table 2), in which post-quantum cryptography will be the protagonist. In 2016, the US NIST initiated a standardisation process of post-quantum cryptography algorithms, noticing the fast development of quantum computing and its potential impact on information security. Out of the many algorithms submitted in 2022, NIST selected four of them with the perspective of finalising standardisation efforts in 2024.

In parallel with the standardisation process, the US has sped up the number of policies dedicated to securing sensitive information against quantum cyberattacks. In 2022, the US passed the Quantum Cybersecurity Preparedness Act,[5] which sets up a roadmap to migrate government information to post-quantum cryptography. Furthermore, the White House issued a series of memorandums[6] urging federal agencies to report an inventory of cryptographic systems and start the transition to post-quantum cryptography.

In 2023, the new US National Cybersecurity Strategy[7] established protection against quantum cyberattacks as a strategic objective. This priority encompasses the use of post-quantum cryptography and the need to replace vulnerable hardware, software, and applications that could be compromised. On top of that, the US Congress is in the process of debating a new law that would create public-private sandboxes to accelerate the development of promising near-term applications of quantum technologies.[8]

Meanwhile, the European Union's efforts to secure information from quantum cyberattacks lack a clear strategy about how to deal with short-term threats, such as 'harvest attacks'. Moreover, there are questions about the role that quantum technologies will have in securing European networks against quantum cyberattacks. While the US predominates the use of post-quantum cryptography, policy-wise, the EU has only focused so far on quantum key distribution, despite mentions of the importance of post-quantum cryptography for cyber resilience in the 2020 Cybersecurity Strategy.

This has undoubtedly hindered the EU's ability to establish global standards for post-quantum cryptography, a process that the US is leading and benefits from European research. Of the 19 researchers within the four groups whose algorithms have been selected by NIST for standardisation, 13 are affiliated with European research institutions. On top of that, EU standardisation bodies joined the race late for PQC standards, which has resulted in these organisations following the facto the advancements made by NIST.[9]

In 2022, ENISA published an integration study of post-quantum cryptography[10] and the EU Commission allocated €11 million for research on PQC.[11] But the EU Commission's call expects results by 2026, two years after the expected end of the NIST process, and the ENISA paper is about the challenges to implementing PQC on digital systems, but it is a research paper. Europe has come in late.

Table 2: Comparative table of quantum cybersecurity initiatives

	United States	European Union	EU member states
Standardisation process	Since 2016 (NIST). Standardisation finished by 2024.	Ongoing: no clear results. Likely to follow NIST standards.	Participate in NIST and European standardisation efforts.
Quantum cybersecurity agenda	2022 Quantum Cybersecurity Preparedness Act. 2023 National Cybersecurity Strategy.	No	No
Roadmap to quantum-proof systems	2022 NSM-10 and M-23-03 (White House). 2022 Quantum Cybersecurity Preparedness Act.	No	Some
Support for quantum-safe technologies	National Quantum Initiative. 2023 Quantum Sandbox for Near-Term Applications.	2022 Ultra Secure Connectivity Programme. EU Quantum Flagship EuroQCI Horizon Europe.	All member states are part of the EuroQCI network. 12/27 have national quantum programmes in the form of direct strategic state-led R&D programmes, or national strategies.

The strengths of Europe lie in the EuroQCI project. However, even though it could become the backbone of secure communications in the future, its focus on quantum key distribution will not solve the pressing challenges that quantum computing creates for European cybersecurity today.

EuroQCI is a flagship project in the EU that aims to provide secure communications by 2027. This has drawn a lot of attention from member states. All of the 27 are signatories of this project, which in 2021 saw the first interstate quantum-safe communication (100.5km) between Trieste (Italy), Ljubljana (Slovenia), and Zagreb (Croatia).[12]

The focus on the EuroQCI network and its promising applications divert policymakers from paying attention to today's needs of the European cybersecurity agenda about quantum cybersecurity threats.

To support and amplify the geographical range of EuroQCI, in 2022, the EU passed the Union Secure Connectivity Programme regulation,[13] which mandates the development of a space segment for EuroQCI, the IRIS2 space constellation. IRIS2 will be built upon the GOVSATCOM infrastructure. When completed, IRIS2 could become a flagship space programme along with Copernico and Galileo.

Yet, it is arguable that the focus of the EuroQCI network and its promising applications divert policymakers from paying attention to today's needs of the European cybersecurity agenda about quantum cybersecurity threats. Furthermore, as the supporting technology of the EuroQCI is a quantum key distribution, there are questions about whether the EU will be able to meet the 2027 deadline for operational capacity. Moreover, even when fully deployed, the EuroQCI will have limited functionality compared to the functionality of PQC. The EuroQCI network is meant to secure governmental communications and critical infrastructure, which does not necessarily prevent threats to other critical areas for cybersecurity, such as third-party or supply chain cyberattacks.

Policy recommendations for an EU fit for the quantum age

The narrow focus at the EU level on how to mitigate short-term quantum cybersecurity challenges, especially 'harvest attacks' and quantum attacks on encryption, leaves member states as the frontline actors in the quantum transition. This can create asymmetries between bigger and smaller countries, thereby weakening the overall level of cybersecurity in the European Union.

As of 2023, only a few EU countries have made public plans to counter emerging quantum cybersecurity threats, and fewer have put in place strategies to mitigate them, as in the case of Germany. Moreover, the cybersecurity budget and the number of specialists available differ between countries, leaving smaller states with 'champion units' in charge of compliance with current cybersecurity regulations and little space and resources to consider mitigating emerging threats.

As the EU advances in the integration of the European economy, a cyberattack on any part of it, let it be at the individual, company, or small or bigger government, has spillover effects on the cybersecurity of the rest of the Union. Therefore, as quantum computers develop, European action will be needed to prevent cybersecurity loopholes that can be used as attack vectors and ensure that all member states are equally resilient to quantum cyberattacks.

These are the reasons why a Coordinated Action Plan on the quantum transition is urgently needed that outlines clear goals and timeframes and monitors the implementation of national migration plans to post-quantum encryption. This Coordinated Action Plan would bridge the gap between the far-looking objective of establishing a fully operational EuroQCI network and the current needs of the European cybersecurity landscape to respond to short-term quantum cybersecurity threats like 'harvest attacks' or quantum attacks on encryption.

The EU's efforts to bolster cybersecurity within its borders offer insights[14] about how to navigate quantum cybersecurity risks. As part of its efforts to establish a cybersecurity agenda, Europe has identified critical stakeholders, set goals in capacity building, created special obligations for essential sectors, and promoted better coordination among national cybersecurity agencies, government entities, the intelligence community, and the EU.

The EU can facilitate coordination in two ways. First, it can lead the efforts to enhance technical coordination to address research gaps in developing quantum-safe technologies, such as the need to develop quantum nodes[15] to ensure long-range connections for quantum key distribution.

Moreover, by aligning strategic objectives between member states and the European Commission, the EU can foster stronger cooperation between national cybersecurity agencies and ENISA to determine technological priorities and identify relevant use cases for quantum technologies. This would be fundamental in a time when some member states are individually evaluating the use of post-quantum cryptography, quantum key distribution or a combination of the two to secure their systems, especially when clear divergences in use exist.

While experts and some member states such as Germany, Spain, or the Netherlands agree that a combined QKD-PQC approach which favours post-quantum cryptography is the way to go, other European actors, such as France, are reluctant to the future use of QKD.[16] European coordination at the technical level could be instrumental in sharing information and best practices and reaching a common approach to the quantum transition. Likewise, to help accelerate promises but not yet mature applications, such as in the case of QKD, the European Union in coordination with member states could explore the use of sandboxes, following the developments of the US 2023 Quantum Sandbox for Near-Term Applications Act but adapting it to European needs.

Second, the EU could provide the political coordination needed to support a harmonised transition to post-quantum encryption to mitigate the risks of encryption attacks. A crucial step towards cyber resilience in the face of quantum computing will be developing a detailed migration plan that moves information susceptible to quantum attacks on encryption (see, for example, Table 1) to post-quantum encryption. The first step will be the elaboration of cryptographic inventories, to which collaboration with the private sector will be essential, especially in developing and procuring digital tools able to scan information systems and register which cryptographic systems are in use.

A crucial step towards cyber resilience in the face of quantum computing will be developing a detailed migration plan that moves information susceptible to quantum attacks on encryption (see, for example, Table 1) to post-quantum encryption.

Subsequently, the EU can assist in setting priorities, such as giving prominence to operators of essential economic sectors and government information and establishing the need for cryptographic agility. As the robustness of post-quantum encryption has not been tested in a real environment with quantum computers, cryptographic agility allows for swiftly replacing or updating cryptography in the event of a breach or a vulnerability that can compromise information security. In fact, researchers have already found security flaws in NIST-proposed PQC algorithms for standardisation.[17]

Lastly, Europe can leverage the expertise of national cybersecurity agencies, experts, and the private sector by establishing a new expert group within ENISA where seconded national experts in post-quantum encryption can exchange good practices and encourage the establishment of migration plans. Similar groups have been created before, such as the ENISA's National Cyber Security Strategy group to align cybersecurity priorities between member states.

The challenges that quantum computing poses for European cybersecurity might seem far away, but the ability of the EU to detect, protect, defend, and recover from them in the future starts by pursuing necessary actions to mitigate them now. Therefore, a quantum cybersecurity agenda is essential for Europe's economic security in a fast-developing geopolitical environment and is in Europe's hands to act now.

[1] Mosca, Michele (2016), Quantum Computing: A New Threat to Cybersecurity. Global Risk Institute. In addition, see: Table 1.

[2] Waters, Richard (2023), "Chinese researchers claim to find a way to break encryption using quantum computers", *Financial Times*, January 5.

[3] Bernstein, Daniel J. and Tanja Lange (2017), "Post-quantum cryptography", *Nature* 549: 188-194.

[4] The 2020 SolarWinds cyberattack was a supply chain attack in which hackers gained access to the systems of multiple government agencies and private companies by compromising SolarWinds, a leading software provider. The company clients received a malware-infected file as a software update, allowing attackers to gain access to sensitive information and networks. The attack was attributed to a Russian hacking group and is considered one of the most significant cyberattacks in history.

[5] US Congress (2022), Quantum Computing Cybersecurity Preparedness Act, Washington D.C.

[6] White House (2022), "Memorandum for the Heads of Executive Departments and Agencies: Migrating to Post-Quantum Cryptography", November 18, Washington D.C.

[7] White House (2023), National Cybersecurity Strategy, Washington D.C.

[8] US Congress (2023), Quantum Sandbox for Near-Term Applications Act, Washington D.C.

[9] See for example ETSI's review of NIST algorithms or CEN-CENELEC standardisation roadmap acknowledging NIST.

[10] ENISA (2022), Post-Quantum Cryptography — Integration Study. [online] Available at: https://www.enisa.europa.eu/publications/post-quantum-cryptography-integration-study.

[11] European Commission (2022), "Transition towards Quantum-Resistant Cryptography", Funding and Tender Opportunities Portal. [online] Available at: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl3-2022-cs-01-03.

[12] EU Quantum Flagship (2021), "First intergovernmental quantum communication", [online] Available at: https://qt.eu/news/2021/first-intergovernmental-quantum-communication.

[13] European Commission (2022), Regulation of the European Parliament and of the Council establishing the Union Secure Connectivity Programme for the period 2023-2027, Strasbourg: France.

[14] The European Union plays an essential coordinating role in Europe's cybersecurity. Policies like NIS 2 or the Cyber Resilience Act have helped governments identify priorities and establish ambitious cybersecurity requirements for the areas deemed more sensitive for Europe's economic security. Hence, it is arguable that the EU is equipped with sufficient experience in coordinating cybersecurity preparedness and response to also play a key role in the transition to quantum-safe systems.

[15] Quantum nodes would receive, store, and transmit information in quantum states but the technology is not there yet. Current quantum networks use trusted nodes that receive information in quantum states, store them in classical states, and transmit them in quantum states again. This adds a new layer of vulnerability as attackers could read and steal information once put back in zeroes and ones.

[16] Agence nationale de la sécurité des systems d'information (2022) "ANSSI views on the post-quantum cryptography transition", [online] Available at: https://www.ssi.gouv.fr/en/publication/anssi-views-on-the-post-quantum-cryptography-transition/.

[17] Gable, Jim, Shannon Gray, and Denis Mandich (2023), "Is PQC broken already? Implications of the successful break of a NIST finalist", [online] Available at: https://cloudsecurityalliance.org/blog/2023/04/03/is-pqc-broken-already-implications-of-the-successful-break-of-a-nist-finalist/.

NOTES

NOTES

The **European Policy Centre** is an independent, not-for-profit think tank dedicated to fostering European integration through analysis and debate, supporting and challenging European decison-makers at all levels to make informed decisions based on sound evidence and analysis, and providing a platform for engaging partners, stakeholders and citizens in EU policymaking and in the debate about the future of Europe.

The **EPC's Europe's Political Economy Programme** (EPE) is dedicated to covering topics related to EU economic governance, the single market, industrial and digital policies, and strategic autonomy in a context of deep geo-economic and technological shifts. The Programme has contributed actively to these debates over past years, leveraging its convening power, analysis and multistakeholder taskforce model. EPE analysts pioneered the concept of a 'wartime economy' following Russia's invasion of Ukraine, and the Programme is currently running projects focusing on the EU's ambitions and the private sector's capacity to deliver on the "triple" green, digital and economic security transitions. As fast-advancing components of 'economic security', digital and emerging technologies, such as quantum, are priority areas of focus. Linked to the changing international context, the Programme also focuses on trade policy, the transatlantic agenda, notably the EU-US Trade and Technology Council, China, and the EU's close economic partnerships (UK, EEA, Switzerland). The EPE Programme consists of a young and dynamic team, with recent recruitments bolstering analytical capacities linked to economic growth and crises, resilience and recovery, emerging tech and cybersecurity.

With the strategic support of King Baudouin Foundation
Working together for a better society