EUROPEAN POLICY CENTRE

DISCUSSION PAPER

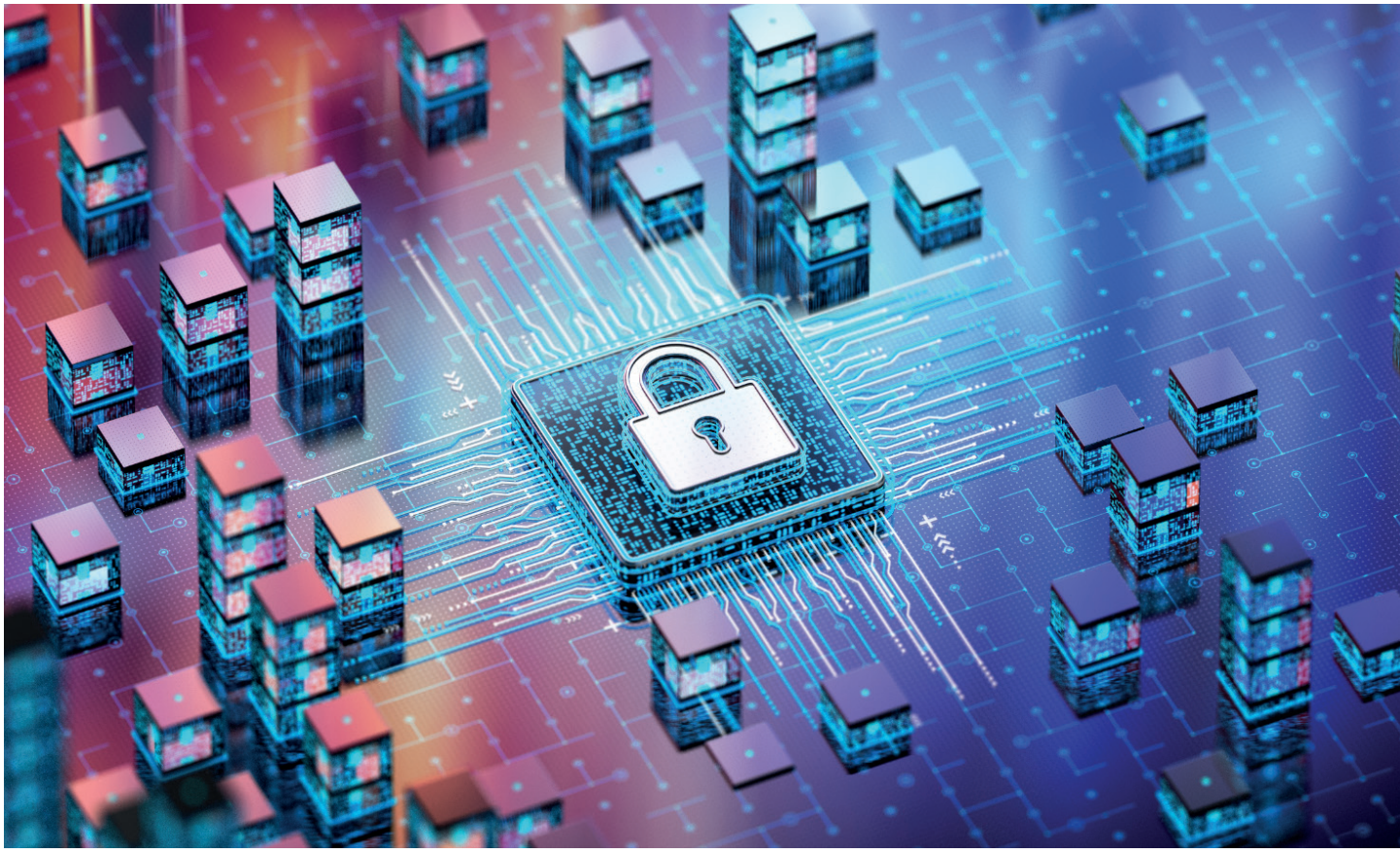
EUROPE'S POLITICAL ECONOMY PROGRAMME

17 JANUARY 2025

A quantum cybersecurity agenda for Europe II

Enabling policy and investment options for the quantum transition

Andrea G. Rodríguez



Credit: CANVA

Table of contents

ABOUT THE AUTHOR

Andrea G. Rodríguez is Associate Researcher at the Centre for European Policy Studies (CEPS).

ACKNOWLEDGEMENTS / DISCLAIMER

This Discussion Paper is the product of a workshop, several interviews, conversations and notes taken during 2024 and is framed under the "Europe's Quantum Frontier" project of the European Policy Centre. The project is structured as a task force that brings together a diverse range of actors to discuss pressing issues around quantum technologies and the EU agenda. This paper complements and builds on a previous one published in July 2023 with the same title "A quantum cybersecurity agenda for Europe". It aims to accompany the European Union in this pressing time to future-proof the EU's cybersecurity agenda. The EPC's work on this project is supported by Quantum Delta NL as a founding partner of the EPC task force. The author would like to thank Jesse Robbers, Ulrich Mans and Chris Kremidas-Courtney for their valuable input to this paper and EPC colleagues Johannes Greubel, Georg Riekeles and Beatrice White for their support with the project and publication.

Executive summary

Developments in quantum computing present a big challenge to cybersecurity, creating the urgent need for the European Union (EU) to act proactively to safeguard digital infrastructure and the economy against future quantum-enabled cyberattacks. However, the response must consider vulnerabilities in digital supply chains, where network interconnectedness creates multiple points of entry for adversaries.

The EU's NIS 2 Directive offers a framework for addressing supply chain risks by expanding cybersecurity requirements across essential and non-essential sectors. In the quantum context, NIS 2 can play an essential role in coordinating and upgrading the level of cybersecurity of the whole European economy by mandating the transition to quantum-safe systems in the affected sectors first.

Time is of the essence. In securing the EU's economy against quantum-enabled cyberattacks, both quantum-key distribution (QKD) and post-quantum cryptography (PQC) have a role to play. Only by leveraging Europe's strengths and making use of the instruments available will Europe be ready for the era of quantum computing. With this in mind, this paper offers a series of policy recommendations:

1. Enhance **awareness** in the national cybersecurity agencies and industry on the importance of transitioning to quantum-safe systems, starting today.

2. Establish a **dual quantum-safe roadmap**. The main actions should include:

    a. Specific actions on the adoption of post-quantum cryptography, including mandatory risk assessments to identify vulnerabilities and the creation of a toolbox to help member states and organisations transition to PQC.

    b. Specific actions on quantum key distribution, including supporting the implementation of scalable use cases and the creation of metropolitical and cross-border quantum networks.

3. The Commission should use the **NIS 2 framework to set priority sectors**, identify bottlenecks and coordinate the transition to quantum-safe systems.

4. Introduce quantum-safe as a **requisite in public procurement** to mitigate attacks on the supply chain.

5. Use the **European Cybersecurity Competence Centre (ECCC) to distribute funding** among public sector and industry players to kick-start the transition to post-quantum cryptography.

6. Use **InvestEU and the Digital Europe Programme to fund** the PQC transition in the short-term.

7. Make sure that **developments in cybersecurity certification** include the notion of "quantum-safe" infrastructure.

Introduction

The European way of life relies on strong cybersecurity. Cybersecurity is essential to ensure individual rights, to create trust in the digital economy, and to prevent unauthorised access to sensitive information. As countries ramp up their investments in quantum technologies, technological breakthroughs bring an encryption-breaking quantum computer closer to reality. There is a need to put in place relevant strategies to protect, detect, defend and recover from quantum attacks – and there is growing urgency to it.[1] In designing these responses, there are several things policymakers should take into consideration.

First, their scope *and the actors* that should be involved. Europe's cybersecurity architecture is a complex network of collaboration and burden-sharing between EU institutions, member states and the private sector. This multiplicity of actors raises concerns about the resilience of the current architecture and the EU's readiness to mitigate and respond to quantum attacks. As Europe's cybersecurity system evolves to accommodate new challenges, it will also have to evolve to ensure readiness against quantum attacks.

Second, the *instruments* that are required for such a response. Even though Europe's cybersecurity architecture can be seen as one of the biggest successes in coordinating policy with funding and stakeholder cooperation, there are various major challenges ahead when preparing for the effects of quantum computing on cybersecurity. One aspect concerns *which use* different technological solutions should have in responding to the evolution of the threat landscape when adversaries have access to quantum capabilities. Another is *which resources* should be employed to ensure an adequate level of readiness.

Current debates around national security and quantum technology show that policy options will have to reconcile post-quantum cryptography (PQC) with quantum key distribution (QKD) – necessary to ensure that Europe uses all the tools at its disposal to ensure a long-lasting response to challenges from quantum computing. This involves the weighted analysis of where each of the solutions can be most useful, bearing in mind their current limitations.

Current debates around national security and quantum technology show that policy options will have to reconcile post-quantum cryptography (PQC) with quantum key distribution (QKD).

This paper reflects on what responses will be necessary in the medium and long term to ensure that Europe remains effective in countering cybersecurity threats far beyond the point when a universal quantum computer is available and in the hands of geopolitical adversaries. Quantum-enabled cyberattacks, such as quantum attacks on encryption or new sophisticated malware developed using quantum machine learning are already on the horizon, and policy should start rolling out mitigation strategies for both the short and long term.

This paper includes three separate sections. The first section reflects on the evolution of the threat landscape, paying particular attention to cyberattacks on the supply chain. It takes the example of the Solar Winds cyberattack and the response of the European Commission with the release of the ICT toolbox on securing the ICT supply chain. The second section raises the question of the need for a roadmap to mitigate the impact of quantum-enabled cyberattacks. It investigates advancements in the implementation of post-quantum cryptography and the development of quantum networks in Europe. It also discusses a dual roadmap for quantum cybersecurity, combining quantum-safe solutions PQC and QKD. The last part reflects on how to finance the quantum transition looking at the current structures and mechanisms.

CHOOSING BETWEEN PQC VS QKD

The development of quantum computing has increased the interest of countries and organisations like NATO in how to secure future communication networks from new quantum cybersecurity threats. However, there is no standard reply to this challenge and occasionally debates are centred on whether to use one instrument (e.g. post-quantum cryptography) or another (e.g. quantum key distribution). Since the publication of the last paper in the European Policy Centre series on quantum and cybersecurity in July 2023,[2] new initiatives have emerged, with discussions around quantum communications advancing in the EU and beyond.

European Union

Following the publication of the EU's Economic Security Strategy in June 2023,[3] the European Commission published a list of critical technologies[4] key to safeguarding Europe's economic base and competitiveness. Out of the 10 technologies identified, the Commission highlighted four (AI, advanced semiconductors, biotechnologies, and quantum technologies) as having the most immediate risks of technology leakage and security. These four technologies were identified as a priority in the creation of mitigation measures to ensure that Europe can develop and access

them while curbing the transfer of sensitive knowledge to geopolitical adversaries. Following this categorisation, the 2024 annual work programme for standardisation further guides EU action into quantum technologies by prioritising advancing standardisation works around quantum communications and modular quantum computers in 2024.

While the European Commission set the direction to protect the quantum communications ecosystem in Europe and advance in the standardisation process to speed up its adoption, at the end of January 2024 France, Germany, Sweden and the Netherlands published a joint position paper pushing for the transition to post-quantum cryptography. The paper builds from the increased urgency to take action to mitigate the challenges to cybersecurity posed by the quick development of quantum computing, in particular, harvest-now-decrypt-later attacks in which adversaries download encrypted information that they cannot read now in the hope that technology will be available soon.

Whereas these four countries agree that QKD has promising applications, describing it as an "interesting technology" (p. 6), they also agree that it is technologically limited and presents unprecedented challenges for adoption, such as the high cost of using specialised hardware. Moreover, they note that QKD is not suitable for practical use in most cases in its current form, citing the lack of advanced standardisation processes and the lack of QKD security proofs. Still, the countries agree on the need to continue investments and develop experience in physical quantum network technologies. In the course of 2024, the position paper has received letters of support of other EU countries, such as the Czech Republic.

In April 2024, the Commission published a recommendation for a Coordinated Implementation Roadmap on the transition to PQC, mandating member states to create solid strategies and recommending the establishment of a sub-group on the NIS Coordination Group to synchronise efforts. In parallel to this, in the last few months, the EU has pursued its cybersecurity agenda with the signing into law of important policy developments such as the Cyber Resilience Act that creates cybersecurity conditions for connected devices.

NATO

Across the Atlantic, quantum cybersecurity is also gaining momentum. At the end of 2023, NATO allies agreed on a quantum strategy. In it, they recognise that quantum applications harm deterrence and defence, and for that reason have become "an element of strategic competition". Even though minor details about the strategy have been made public, NATO has identified quantum attacks on encryption as an area of concern. Consequently, it has recommended the transition to quantum-safe cryptography as a desired outcome, opening the door to quantum key distribution as well. In fact, NATO has recently begun testing QKD technology. This push for secure communications comes at a time when it launched its defence accelerator, DIANA, which is currently funding solutions to improve the confidentiality, integrity and availability of streamed data in a manner resilient to quantum attacks.

United States

Developments in the United States have been two-fold. On the one hand, the NIST process towards the standardisation of post-quantum encryption algorithms continues with the publication of the first set of PQC standards in 2024. On the other hand, there have been major developments towards creating metropolitan quantum networks, though the weight of quantum key distribution technologies in them is inherently limited. In May 2023, the United States launched the QuANET programme, a 51-month programme to develop and deploy hybrid quantum-classical networks. However, QuANET's ambition is not to establish a QKD-enabled network but rather a classical network in which quantum solutions are increasingly incorporated and that explicitly seeks solutions that go beyond QKD. This position, favouring classical solutions and relegating QKD innovation to a second place, goes hand in hand with the US's National Security Agency recommendations to prioritise post-quantum encryption over quantum key distribution, a technology that the NSA sees as limited and providing insufficient proof of security.

Responding to quantum cybersecurity challenges in the supply chain

Interconnectivity is one of the main characteristics of today's world. Countries, companies and individuals are interlinked in the creation of complex digital networks connecting infrastructure and services. This interconnectedness fosters collaboration among those actors and efficiency but also introduces new vulnerabilities, as is well known by the cybersecurity community. A cyberattack on a single entity within a supply chain can ripple through the entire network, causing widespread disruption and financial loss. If unprepared, once a universal quantum computer is available, the risks of spillover effects in the cybersecurity of supply chains multiply.

Broadly speaking, supply chain risk refers to the likelihood of any disruption to the normal operation of the chain. In quantifying risk, cybersecurity actors consider factors like those affecting the environment they are operating in, technical factors such as pre-arranged connectivity configurations, but also their relationship to third parties. Supply chain attacks often profit from the trust between the different actors in a chain that allows attackers to bypass the cybersecurity of a vendor by targeting the weakest link. A well-known example to the cybersecurity community is the 2020 SolarWinds cyberattack.

The SolarWinds cyberattack is not the only supply chain attack that has ever happened nor the most disruptive one, but it shows what the costs of unpreparedness were. Later reports place the beginning of the campaign in September 2019,[5] the moment in which the malware was distributed in March 2020, and the moment of response after detecting the vulnerability in December 2020. That means that attackers were inside the networks and left to their free will for over a year; something that policy prevented[6] in subsequent cyberattacks such as the one on the Colonial pipeline in 2021 (2 days) or the discovery of the Apache Log4j vulnerability (hours/1 day). The Colonial pipeline hack, for instance, was possible because of the exposed password of one of the employees. In the future, adversaries with quantum capabilities could be able to exercise brute force with a higher degree of success to crack passwords, which could make paradigmatic examples like these recur more often.

In the EU, the cybersecurity policy architecture has been increasingly adopting a whole-of-supply-chain approach with the promulgation of new policies to fill resilience gaps and increase the cybersecurity requirements of all interconnected devices. This approach has accelerated in recent years, against the backdrop of heightened geopolitical tensions and rising supply chain attacks.

In 2022, the Council of the EU presented its conclusions on ICT supply chain security also in light of the consequences for cybersecurity of the Russian aggression against Ukraine. Among the recommendations, it urged member states to assess, map and take an active posture on the mitigation of strategic dependencies in ICT products and services. It also urged the EU as a whole to use all the instruments at hand to adapt to the evolving cyber threat landscape, explicitly mentioning supply chain attacks as the biggest area of concern, also in light of developments of emerging technologies.[7]

However, the only emerging technology explicitly mentioned was 5G networks, citing positively how the EU's 5G toolbox had facilitated mitigating 5G cybersecurity risks by providing an agile risk-based

Table 1: Short comparison of the EU's NIS Directive and NIS 2 Directive

	NIS Directive	NIS 2 Directive
Adopted	6 July 2016	27 December 2022
Entry into force	9 May 2018	16 January 2023*
Overall goal	Achieving a high level of cybersecuriy in essential sectors	Aims for a more comprehensive approach by: 1. Enhancing critical infrastructure resilience 2. Improving incident response 3. Strengthening cybersecurity in the digital supply chain
Scope	Operators of essential services in critical sectors	Expands the list of NIS1 sectors and adds digital service providers, public administations, and other important entities such as medium-sized and large entities in non-essential sectors deemed critical for the economy or society
Security measures	Basic security and incident reporting obligations	Stronger obligations including: 1. Risk management 2. Supply chain security assessments 3. Incident reponse plans and stricter deadlines for reporting 4. Encryption and access controls
Compliance & enforcement	Implementation varied across member states, which led to inconsistencies	Introduces new harmonised rules for implementation across the EU and stronger enforcement mechanisms with stricter penalties

approach and concrete measures. For context, the 5G toolbox was, along with all US policies responding to the 2020-2021 supply chain cyberattacks, a *reaction* to the security concerns.[8] Because of the negative effects of quantum on cybersecurity,[9] Europe cannot afford to be reactive again; there is still time to make the EU a proactive player in sight of this challenge.

FILLING SUPPLY CHAIN CYBERSECURITY GAPS WITH THE NIS 2 DIRECTIVE

The Council's conclusions on ICT security urged the EU to pay closer attention to the cybersecurity of supply chains at a moment when key files were being discussed. Barely a month and a half after its publication, the NIS 2 Directive was adopted. This directive was an update to the original Networks and Information Directive of 2016, which established strong cybersecurity requirements for a restricted list of critical sectors to ensure a common and advanced level of cybersecurity. While limited in scope, it provided a solid foundation to increase coordination and improve resilience and became the backbone of Europe's cybersecurity architecture. The NIS 2 Directive added new sectors to the shopping list and increased cybersecurity measures among other important updates (see: Table 1).

The new sectors covered under NIS 2 give the regulation a new sense of relevance while addressing supply chain risks. While its predecessor only applied to essential service operators, under NIS 2 digital service providers (DSPs) such as online marketplaces, or cloud computing service providers were added, as well as the space sector or public administrations and other important entities for the economy. This allows for a broader coverage of critical digital network infrastructure which has, in turn, a positive effect in increasing the ability of the EU to detect, defend and recover from cyber incidents.

NIS 2 places a strong emphasis on data security and, although it does not explicitly cover encryption, it indirectly features as a key element for the cybersecurity requirements mandated by NIS 2. For example, strong encryption can be a key measure for mitigating risks to unauthorised access to sensitive data, or a key element to securing sensitive operational data, and certainly to securing communication channels.

As the deadline for quantum attacks on encryption comes closer - by estimates 2030 – the NIS 2 directive is a useful point of reference for the quantum transition. In fact, the recent Coordination Implementation Roadmap on the transition to post-quantum cryptography[10] published in April 2024 notes the relevance of NIS 2, but falls short of looking into the directive for further inspiration by only focusing on the coordinating role of the NIS Coordination Group. The NIS 2 Directive could play a bigger role in the transition to quantum-safe as well as in the creation of a new quantum cybersecurity agenda for Europe that upgrades the existing cybersecurity agenda with specific measures to counter the challenges posed by quantum computing.

LESSONS FROM NIS 2 FOR QUANTUM CYBERSECURITY

The cybersecurity threat landscape is constantly evolving, and considerations of the impact of quantum computing on cybersecurity cannot be a separate part of Europe's existing cybersecurity and digital infrastructure agendas. In addition to the quantum risk analysis, the cybersecurity agenda needs to start seriously considering the instruments available as a remedy. These will make current information systems more secure, even in the event of quantum attacks, such as quantum key distribution and post-quantum cryptography.

As EU policy has adapted to new types of cyber operations (e.g. supply chain attacks) and new technologies (e.g. 5G) the same logic will have to apply to challenges arising from quantum computing. Some of these actions will necessarily include an update to the EU's cybersecurity agenda with the review of current instruments and policies to include consideration of third-party risks also in a quantum context.

As EU policy has adapted to new types of cyber operations (e.g. supply chain attacks) and new technologies (e.g. 5G) the same logic will have to apply to challenges arising from quantum computing.

To date, the NIS 2 Directive but also other relevant policies such as the EU Cyber Resilience Act offer a good point of departure to consider special obligations for critical digital infrastructure and requirements for all interconnected devices. In fact, several lessons can be drawn from the EU's cybersecurity agenda for the quantum transition.

Clearly, the biggest success of the NIS 2 Directive has been defining which areas are critical for the security of European networks as a whole. In this sense, what NIS 2 provides is a list of priority digital infrastructure followed by a series of obligations to ensure that they are sufficiently protected. In the case of the quantum transition, considerations around it should go beyond whether or not there is a need to implement quantum-safe solutions, to identify which sectors should be mandated to become quantum-safe first. In that sense, NIS 2 does not only become a point of reference but also a suitable instrument in which some of these new obligations could be included, such as the need to incorporate post-quantum encryption or to identify use cases for the establishment of quantum key distribution channels once the technology is ready.

Another lesson from NIS 2 is helping clarify the role of the different actors in the quantum transition. Even though the European Commission in its recommendation on the transition to PQC[11] gives a prominent role to member states, these all have internally different configurations which could lead to delays in advancements towards becoming quantum-safe. Under NIS 2, member states need to designate or establish a competent authority to oversee cybersecurity and compliance with the obligations (Article 8 NIS 2 Directive). A similar approach to the quantum transition could help speed up the implementation of quantum-safe solutions and the identification of bottlenecks that require attention.

Similarly, as EU member states advance in the creation of structures to coordinate the transition, the creation of a Europe-wide database with the vulnerable infrastructure could be useful in avoiding the duplication of efforts and identifying supply chain vulnerabilities. This task could be assigned to the sub-group on post-quantum encryption that has been created under the NIS Cooperation Group.

In addition to this, quantum risks should be incorporated into the risk-assessment obligations of priority digital infrastructure to ensure that appropriate measures are taken before quantum computing is advanced enough to create significant damage. Here again, NIS 2 provides a useful framework for the entities covered under its scope as it also mandates EU-level coordinated risk assessments on critical supply chains. This holistic approach will be necessary to prevent adversaries from taking advantage of the partial implementation of quantum transition roadmaps or other issues compromising cybersecurity as a whole.

A dual roadmap (PQC-QKD) for quantum cybersecurity

Europe faces the enormous task of reconciling hyperconnectivity (advanced levels of digitalisation and dependence on digital infrastructure for everyday business) with the need to upgrade existing infrastructure to mitigate unprecedented new risks coming from the possibility of quantum computing breaking current encryption systems. In this longer-term vision of cybersecurity, Europe will have to think about how to use the available resources and technologies to create an additional layer of security against quantum attacks. Despite the mentions of quantum technologies in the priorities of the second von der Leyen term and

BOX 1: QUANTUM KEY DISTRIBUTION VS POST-QUANTUM CRYPTOGRAPHY

As countries ready their cybersecurity structures for quantum computers, there are still questions about which technologies are better for securing information. Today, the two most promising are quantum key distribution (QKD) and post-quantum cryptography (PQC), with each offering a different set of advantages and disadvantages.

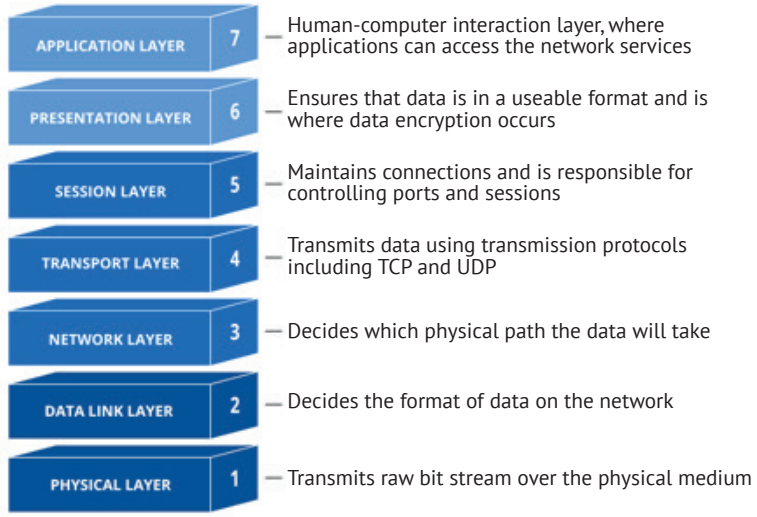
Quantum key distribution (QKD) enables two parties to establish a secure communication channel based on quantum physics. Because of the properties of quantum bits (qubits), data shared cannot be copied, which protects against information theft during communications. Moreover, any disturbance or interference in the communication channel could be perceived by the parties that can suddenly 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 (currently limited to around 200km) and the need to use trusted nodes to solve this, to go beyond 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 (PQC), as a classical computing solution, is a more mature activity area and offers several advantages over quantum key distribution. At the same time, 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 NIST competition is still ongoing. In other words, no practical proof exists that more sophisticated decryption algorithms, besides those already known and run by quantum computers, would not break post-quantum cryptography being developed today.

Figure 1

LAYERS OF AN INFORMATION SYSTEM. PICTURE FROM CLOUDFLARE ABOUT THE OSI MODEL SETUP OF CLASSICAL DATA INFRASTRUCTURE



Source: Cloudflare.

the pledges to improve quantum capacities by Tech Sovereignty, Security and Democracy Commissioner Henna Virkkunen, quantum cybersecurity remains largely absent as a topic.

Indeed, post-quantum cryptography is a useful tool to prevent quantum attacks on encryption and mitigate the effects of harvest attacks by ensuring that encoded information downloaded now by adversaries will not be read even as universal quantum computers become available. However, post-quantum cryptography is not infallible either.

Post-quantum encryption protects the data exchange but does not offer additional safeguards in the transport and physical levels of an information system (see: Figure 1). Moreover, as their level of security is tested merely on paper since universal quantum computers are not available yet, post-quantum encryption could be potentially compromised in the future. A larger quantum computer could potentially harvest PQC-protected data and also break that encryption algorithm, because PQC only protects the data layer. For that reason, countries such as France have prepared a 3-step approach[12] to the quantum transition including a "middle step" in which they prioritise current "classical" cryptographic systems that are believed to be quantum-resistant.

Moreover, there are additional questions about how post-quantum cryptography affects performance that could also create some barriers to its implementation. Post-quantum encryption algorithms can be computationally intensive, which can lead to longer times for encryption and decryption,[13] which can be problematic. As research

Figure 2

THE QUANTUM NETWORK STACK[14]

Application	
Transport	Qubit transmission
Network	Long distance entanglement
Link	Robust entanglement generation
Physical	Attempt entanglement generation

advances into optimising PQC algorithms, performance issues might delay the speed at which post-quantum cryptography is implemented and multiply the resistance towards doing so.

Another alternative in securing cybersecurity in the age of quantum computing is the use of quantum networks. Although the EU remains a world leader in this technology, there is increased consensus on the fact that quantum key distribution (QKD) is not technologically ready yet to be implemented,[15] though advancements are happening at speed with an increasing number of products arriving on the market. The limitations affecting QKD make it even more unlikely for it to be deployed in the short term. However, continued research could make it an interesting alternative for a select number of use cases.

In the future, QKD networks could become the core of European ultra-secure communications and a vital resource for some parts of the economy, such as in digital infrastructure, or more specifically in the telecommunications sector.

In the future, QKD networks could become the core of European ultra-secure communications and a vital resource for some parts of the economy, such as in digital infrastructure, or more specifically in the telecommunications sector. QKD offers new levels of protection in all layers, as it works under the principles of quantum physics.

Though it will require a sizable investment in new hardware, quantum networks could be a solution to a world with off-the-shelves quantum computers that continuously require classical networks to adapt to the threat landscape. By offering advanced cybersecurity covering even the transport and physical layers, and preventing the most common cybercrimes, such as data theft, quantum networks will be fundamental to maintaining secure communications between governments, critical infrastructure, and even the military. QKD protects against harvest attacks which are an important concern. However, as QKD develops, there are a lot of steps to be fulfilled to prepare for quantum networks.

The first one is continued investment. Even though returns will not be seen for at least five years, Europe is in pole position in the development of relevant cases and in testing and piloting quantum networks.[16] Jumping from targeted experiments to the development and testing of quantum networks is a necessary next step to accelerate the incorporation of quantum networks into Europe's digital infrastructure. This will require new investments and renewed commitment to the development of European quantum networks. In parallel, it will be necessary for the European Commission to keep advancing its connectivity programme and keep investing in wiring the European continent in fibre optic networks, which are the base infrastructure for possible future QKD networks and follow-up technologies like Quantum Entangled Networks and the Quantum Internet.

As challenges multiply and the EU enters a new term, the European Commission will have to think about expanding its PQC roadmap to incorporate both technologies: QKD *and* PQC. Though with different degrees of reliability and maturity at the moment, both solutions complement each other and will be necessary to ensure Europe is protected in the face of quantum attacks. While getting hands-on with the transition to post-quantum cryptography is urgent, advancing quantum networks means supporting the creation of an additional layer of security that will become critical in the future for resilience.

Financing the transition

The implementation of quantum-safe solutions will be an additional cost to companies playing a critical role in Europe's economy. The White House has reported that migration to post-quantum cryptography alone in the public sector will cost US Federal Agencies $7.1 billion.[17] While financing cybersecurity solutions in the EU has been on the agenda for a while, the perception of quantum cybersecurity topics as a matter of research and development has prevented the topic from being added to these discussions. Nonetheless, there are several funding instruments allowing companies to invest more in cybersecurity[18] that could start, already today, to help advance the quantum cybersecurity agenda in Europe.

The InvestEU programme mobilises public and private investments through an EU budget guarantee of €26.2 billion. Its Strategic European Security Initiative[19] (€8 billion) aims to fund dual-use projects that have an impact on the security of infrastructure. This instrument could be instrumental in finding reliable use cases for quantum networks.

Another funding option includes the Digital Europe Programme. Designed to promote the digital transformation of the continent, out of the five pillars it funds, the cybersecurity pillar has the most significant budget (€1.6 billion). This "cybersecurity and trust" pillar aims to boost European cyber defences. Because of the

weight of encryption in ensuring the confidentiality, integrity and availability of critical data, financing the implementation of post-quantum encryption seems a logical spillover for the programme to ensure digital trust. The Connecting Europe Facility (CEF) and IRIS2 space programme are logical follow-ups to finance the transition.

Financing the quantum transition not only will help prepare Europe for future cybersecurity threats emerging from the quantum computing landscape but will also have a positive effect on the industrial fabric of the EU. New companies could be established to help move forward the transition to quantum-safe systems, thus creating new jobs, but also decreasing the EU's dependencies on foreign quantum-safe solutions. In sum, the benefits of financing the quantum transition will inevitably go beyond cybersecurity, enhancing competitiveness and digital trust.

Looking ahead: policy recommendations for the new term

Some assessments of when the effects of quantum computing will be felt in cybersecurity place it in 2027, right in the middle of this European Commission term.[20] If the estimation allows for a little room for manoeuvre, this suggests that during this Commission term, companies and governments could potentially face a quantum cybersecurity risk one way or another. This also means that the instruments at hand to respond to, and recover from, these risks are the ones that currently exist. The best way to increase Europe's resilience, therefore, is to use existing tools and refine them to respond to cyberattacks as well as to provide some detailed planning for the quantum transition.

Recommendation 1: Enhance awareness in national cybersecurity agencies and the industry about quantum cybersecurity.

Quantum computing is a major factor affecting the cyber threat landscape. Despite it being a developing emerging technology, there is an urgent need to treat its effects on cybersecurity as a research and development issue and to do so as an emerging cybersecurity challenge. The way that Europe thinks about the effects of Artificial Intelligence on cybersecurity can be a source of inspiration. AI is now embedded into risk assessments and into cyber threat reports. Cybersecurity developments and developments in quantum computing must go hand in hand.

Recommendation 2: Establish a Dual Roadmap for the Quantum Transition (PQC-QKD) at the EU level.

Post-quantum cryptography and quantum-key distribution are complementary solutions and hence should be part of the same roadmap to ensure that Europe maximises the benefits of quantum networks and PQC solutions. Such a roadmap should establish clear goals and must be agile considering the differences in maturity and development of PQC and QKD as well as other aspects including:

- Institutional leadership: In this Commission term, PQC and QKD solutions must make it to the portfolios of DG CONNECT, DG DEFIS and DG GROW, and have a bigger share in the actions of the EU Agency for Cybersecurity (ENISA). In addition to this, the international aspects of quantum cybersecurity should be included in the cyber diplomacy division of the EU's External Action Service (EEAS).

- The hybrid implementation of PQC and QKD during the next European Commission to mitigate the effects of harvest attacks and to ensure there exists an ultra-secure alternative for the exchange of sensitive information.

In addition to these general aspects, the roadmap should include specific provisions for post-quantum cryptography and quantum key distribution. In particular, in the period 2024-2029 the roadmap should ensure the following:

For the post-quantum cryptography transition

- By 2025, in addition to the publication of the Coordinated Implementation Plan on Post-Quantum Cryptography, the European Commission should mandate risk assessments of quantum cybersecurity vulnerabilities in key sectors and areas of the European economy. To that end, the European Commission should keep the NIS 2 Directive as a point of reference, paying special attention to how quantum risks spill over in critical digital infrastructure such as the cloud.

- By Autumn 2025, the European Commission should publish a PQC toolbox to help member states and organisations move on to post-quantum encryption. This toolbox should be built in cooperation with ENISA, member states' cybersecurity agencies, the NIS Cooperation Group and the sub-group on PQC, and the intelligence and national security communities.

- By the end of 2027, all operators of essential services and public administrations must be able to certify that all sensitive information is PQC-protected.

For quantum network developments

The EU must keep supporting developments in quantum key distribution in line with the goals established in the Quantum Flagship's 2030 Strategic Research Agenda. These developments must be centred on the search for scalable use cases relevant to European cybersecurity, such as the case of ultra-secure telecommunication networks. In addition, it will be important to keep supporting investments in the EUROQCI network and the IRIS2 network, to boost their deployment and support the creation of metropolitan and cross-border QKD networks to develop the quantum internet.

Moreover, as QKD network base infrastructure is fibre optic cables, it will be important to keep investing in European connectivity, in particular in the FLAP+ region (Frankfurt, London, Amsterdam, Paris and Dublin) that concentrates the largest numbers of data centres and is the core of Europe's digital infrastructure potential.

Lastly, it will be important to position the quantum communication roadmap, including technologies like QKD, quantum networks and the quantum internet, as a high priority in the Quantum Declaration launched in March 2024.

Recommendation 3: The Commission should use the NIS 2 framework to set priority sectors, identify bottlenecks and coordinate the transition to quantum-safe systems.

The question of the quantum transition inevitably starts with "where". The NIS 2 Directive offers a handful of experience in establishing strong cybersecurity requirements for sensitive sectors of the European economy. Using NIS 2 as a framework, the EU should prioritise the sectors contained therein and incorporate quantum-safe as the only means to ensure robust cybersecurity. In addition, similarly to what was done under NIS 2, the EU must ensure the creation of an EU-wide database of vulnerable infrastructure to ensure that the continent advances as one into the quantum-safe era.

Recommendation 4: Introduce 'quantum-safe' as a requisite in public procurement to prevent supply chain attacks.

The level of cybersecurity is as strong as the weakest link in the chain. For that reason, the Commission and European governments must incorporate a quantum supply chain risk mindset into their public procurement processes. Moreover, as the implementation of public contracts can take several years, not including quantum-safe as a requisite now can have negative consequences in the future as providers being chosen now will, unless required to be quantum-safe, potentially pose a cybersecurity risk.

Recommendation 5: Use the European Cybersecurity Competence Centre (ECCC) to distribute funding among the public sector and industry players to start the transition to post-quantum cryptography.

Recommendation 6: Use current financing instruments such as InvestEU and the Digital Europe Programme to fund the dual PQC-QKD transition.

PQC and QKD represent an additional layer to cybersecurity, therefore fitting into the scope of these solutions can improve companies' digital resilience.

Recommendation 7: Make quantum-safe a requirement for the EU's cybersecurity certification scheme.

In January 2024, the EU adopted the first ever European cybersecurity certification scheme,[21] a set of unified rules to certify ICT products in their lifecycle. Quantum attacks will have a disruptive effect on the European economy and security. For that reason, further developments in the creation of relevant protocols and rules should incorporate quantum-safe by default to increase the resilience of the whole cybersecurity supply chain against quantum attacks.

As the new European Commission gets up and running, it faces the challenge of ensuring that Europe's cybersecurity infrastructure is resilient against the threats posed by quantum computing. The urgency to transition to quantum-safe systems is undeniable, as well as the need for this transition to be comprehensive and EU-coordinated. Leveraging frameworks like the NIS 2 Directive to identify priority sectors and streamline the integration of quantum-safe solutions, the new EU executive will have a well-tested place to start. To safeguard the European digital ecosystem, the Commission must act swiftly and decisively, ensuring a proactive, innovative and unified approach to quantum cybersecurity. Only then can Europe's single market and its position as a leader in global digital security be maintained in the years to come.

[1] Kremidas-Courtney, Chris (2024), "How can Europe be ready for the Quantum Age?", Brussels: European Policy Centre.

[2] G. Rodríguez, Andrea (2023), "A quantum cybersecurity agenda for Europe: governing the transition to post-quantum cryptography", Brussels: European Policy Centre.

[3] European Commission (2023), European Economic Security Strategy, Brussels, JOIN(2023) 20 final.

[4] European Commission (2023), Commission recommendation on critical technology areas for the EU's economic security for further risk assessment with Member States, Strasbourg, C(2023) 6689 final.

[5] *U.S. Government Accountability Office*, "SolarWinds Cyberattack Demands Significant Federal and Private Sector Response (infographic)" (accessed 7 January 2025).

[6] See, for example: *White House*, "Executive Order on Improving the Nation's Cybersecurity", (accessed 7 January 2025).

[7] *Council of the European Union*, "The Council agrees to strengthen the security of ICT supply chains" (accessed 7 January 2025).

[8] *U.S. Department of State*, "The Clean Network" (accessed 7 January 2025).

[9] G. Rodríguez, Andrea (2023), "A quantum cybersecurity agenda for Europe: governing the transition to post-quantum cryptography", Brussels: European Policy Centre.

[10] *European Commission*, "Recommendation on a Coordinated Roadmap for the transition to Post-Quantum Cryptography" (accessed 7 January 2025).

[11] *European Commission*, "Recommendation on a Coordinated Roadmap for the transition to Post-Quantum Cryptography" (accessed 7 January 2025).

[12] *Government of France*, "ANSSI views on the Post-Quantum Cryptography Transition", (accessed 7 January 2025).

[13] Horpenyuk, Andriy; Opirskyy, Ivan, and Vorobets, Pavlo (2023), "Analysis of Problems and Prospects of Implementation of Post-Quantum Cryptographic Algorithms", *CEUR Workshop Proceedings*, vol. 4504, n.4, pp. 44.

[14] Source: *QuTech*, "Wehner Group" (accessed 7 January 2025)

[15] E.g., *NSA*, "Quantum Key Distribution (QKD) and Quantum Cryptography (QC)" (accessed 7 January 2025).

[16] E.g.: *Eurofiber*, "Eurofiber joins development of secure quantum encrypted fiber network in port of Rotterdam", (accessed 7 January 2025).

[17] *Quantum Insider*, "White House Report: U.S. Federal Agencies Brace for $7,1 Billion Post-Quantum Cryptography Migration" (accessed 7 January 2025).

[18] European Investment Bank (2022), "European Cybersecurity Investment Platform", Luxembourg.

[19] *European Investment Bank*, "Strengthening Europe's security and defence industry" (accessed 7 January 2025).

[20] See, for example: *Global Risk Institute*, "Quantum Computing: A New Threat to Cybersecurity" (accessed 7 January 2025).

[21] *European Commission*, "First EU-wide cybersecurity certification scheme to make European digital space safer" (accessed 7 January 2025).

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