Post-Quantum

Cryptography Conference

A quantum cybersecurity agenda for Europe

Andrea Garcia Rodriguez

Lead Digital Policy Analyst at European Policy Centre (EPC)

ENTRUST HID PKI Consortium

A Quantum Cybersecurity Agenda for Europe

Governing the transition to post-quantum cryptography

PKI Conference, 07 November 2023
Andrea G. Rodríguez, Lead Digital Policy Analyst

EPC
EUROPEAN POLICY CENTRE

Quantum computing impacts the cyber threat landscape

Cyberattacks using quantum computers will have a direct impact on the cyber threat landscape, facilitating **new types of malware and more disruptive cyberattacks** (e.g. using quantum AI).

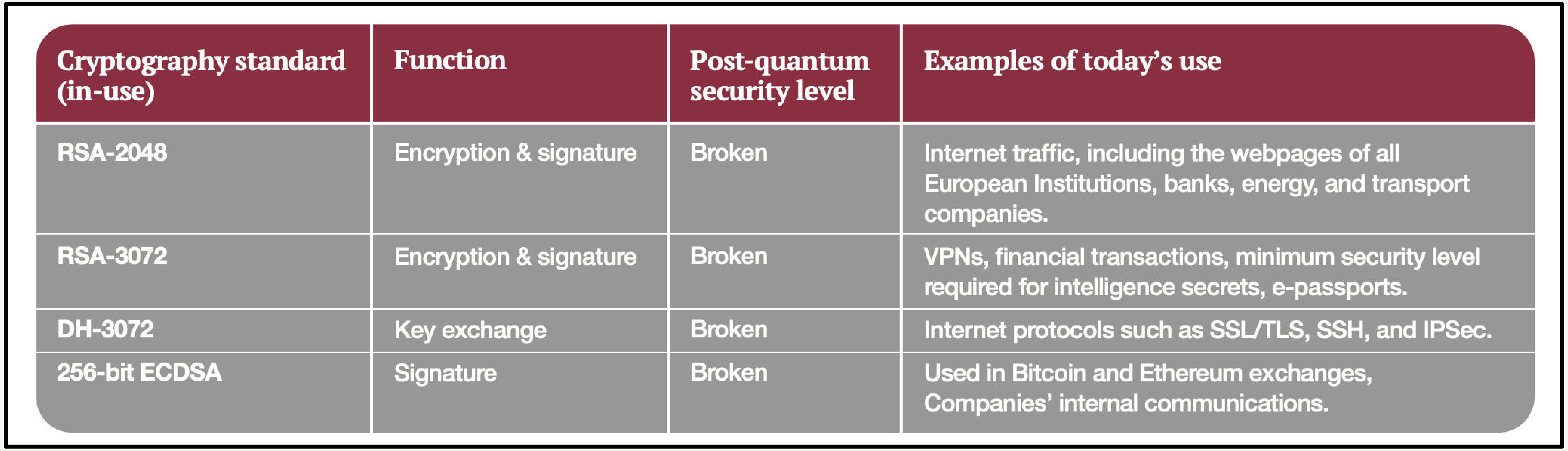
Of those, ‘harvest attacks’ (download-now-decrypt-later) are especially concerning. It is already too late to *prevent* them, but we can *mitigate* their impact. Some examples of disruptions:

- National security
- European economy and competitiveness
- Democratic well-being

By 2026 there is a **1 in 7 chance** of breaking of most commonly used encryption systems

Estimation of cybercrime in 2020 was **€5,5 trillion, the GDP of Germany and Spain** combined

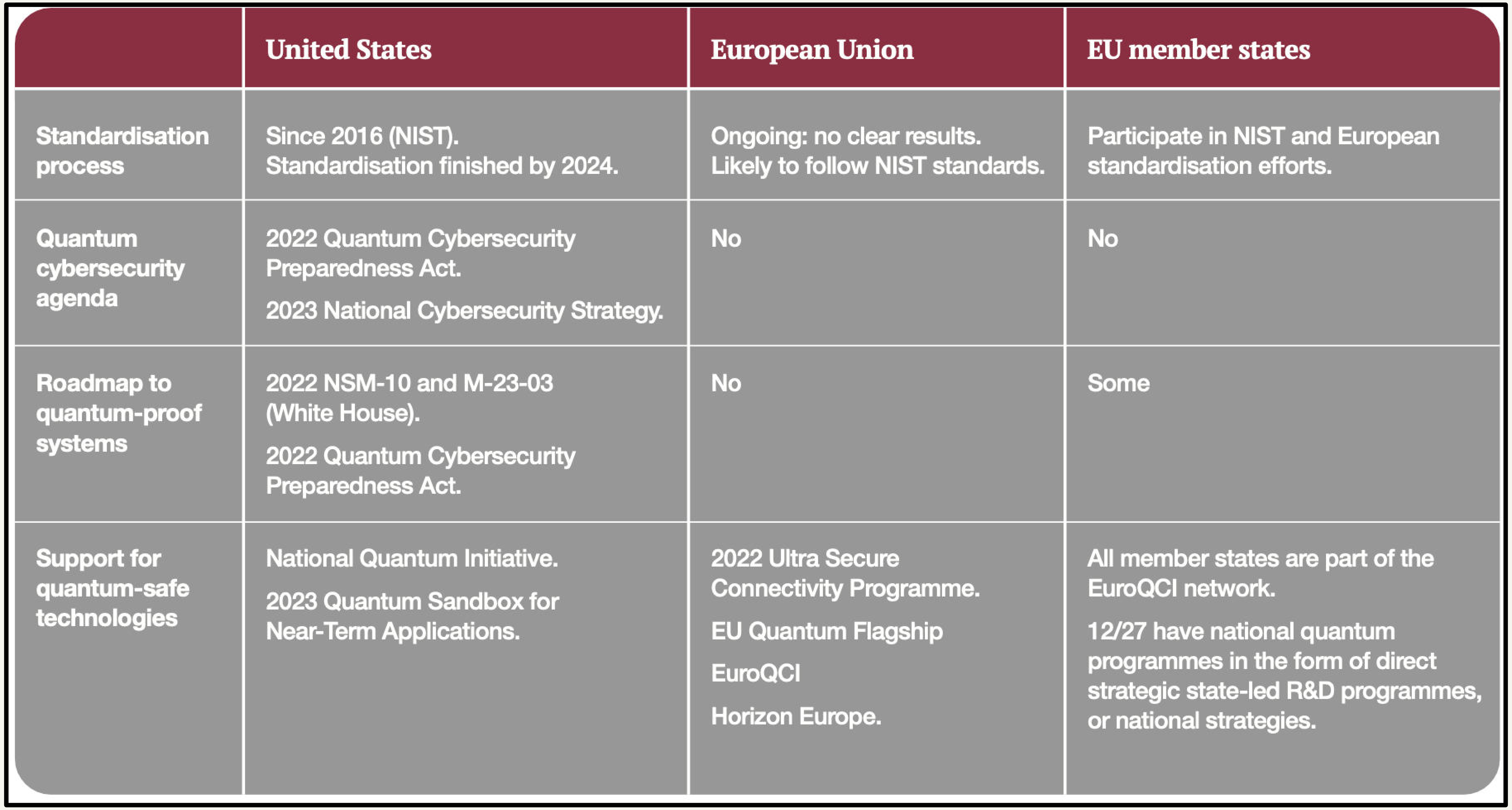
EC 2024-2029: First wave of disruption



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.

There is **high confidence** that these effects will be felt during the next European Commission term. However, **Europe is ill-prepared** to respond to these challenges.

EU coordination is crucial but MMSS lead



	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.

A quantum cybersecurity agenda

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

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 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.

A Coordinated Action Plan on the Quantum Transition

Why?

- To bridge the gap between **EUROQCI** and the **current needs** of the EU's cybersecurity landscape
- To help **switch the mindset** for quantum technologies: from R&D to an important element in the policy debate
- To outline **clear goals and timeframes**
- To help **prioritise** areas of action
- To **encourage** the creation of national migration plans to PQC
- To **monitor** the implementation of national migration plans

Other urgent measures

- A new expert group within ENISA with **seconded national experts**
- Assistance in setting **priorities** for the PQC transition and a push for **crypto-agility**
- **Political coordination** to determine technological priorities and **identify** use cases
- **Technical coordination** to address research gaps
- Sandboxes to accelerate near-term quantum applications

E-mail: a.rodriguez@epc.eu

Twitter (x): @agarcod

EPC
EUROPEAN POLICY CENTRE

Post-Quantum Cryptography Conference

PKI Consortium

ENTRUST

HID

PQ SHIELD

Fortanix

KEYFACTOR

NOREG

QRL

THALES

d-trust.

01 COMMUNIQUE

amsterdam convention bureau

ascertia

亞洲誠信 TRUSTAsia