The Process and Policy of the PQC Migration

Beware of the tragedy of the commons

Nitesh Bharosa

TU Delft
DIGICAMPUS

HAPKIDO Consortium: towards Quantum Safe PKI’s

NWO

5 year project
with 7+
partners

TU Delft

- Risks and Governance

CWI

- Cryptographic research

Microsoft

- Moving to higher TRL

kpn

- PKI management, test lab

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

- Digital government

ZYNYO.

- Provider of digital identification & signing services

TNO

- Coordination & integration

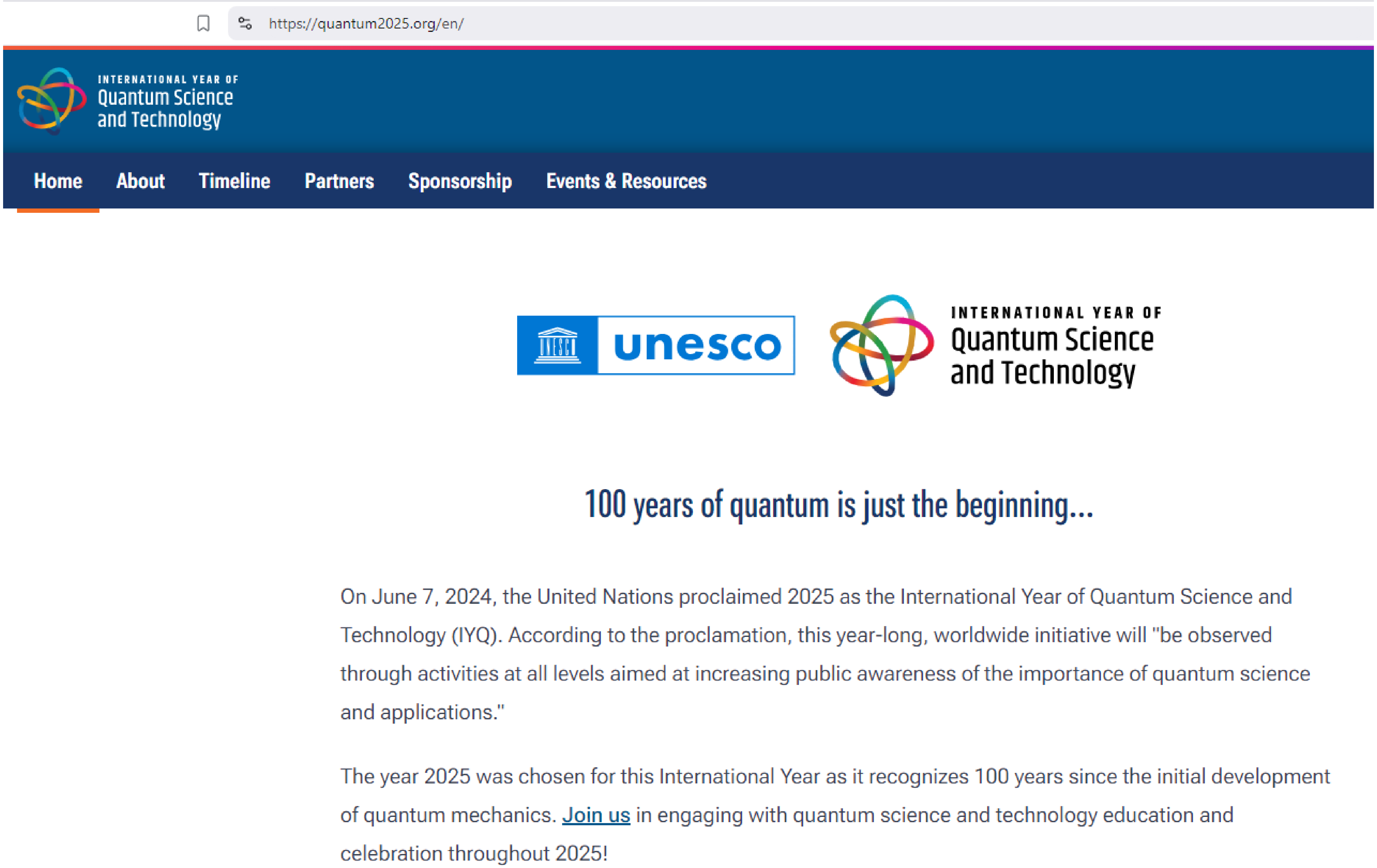
Agenda

I. What do we know?

II. What do we need to know?

III. How do we get there?

TUDelft

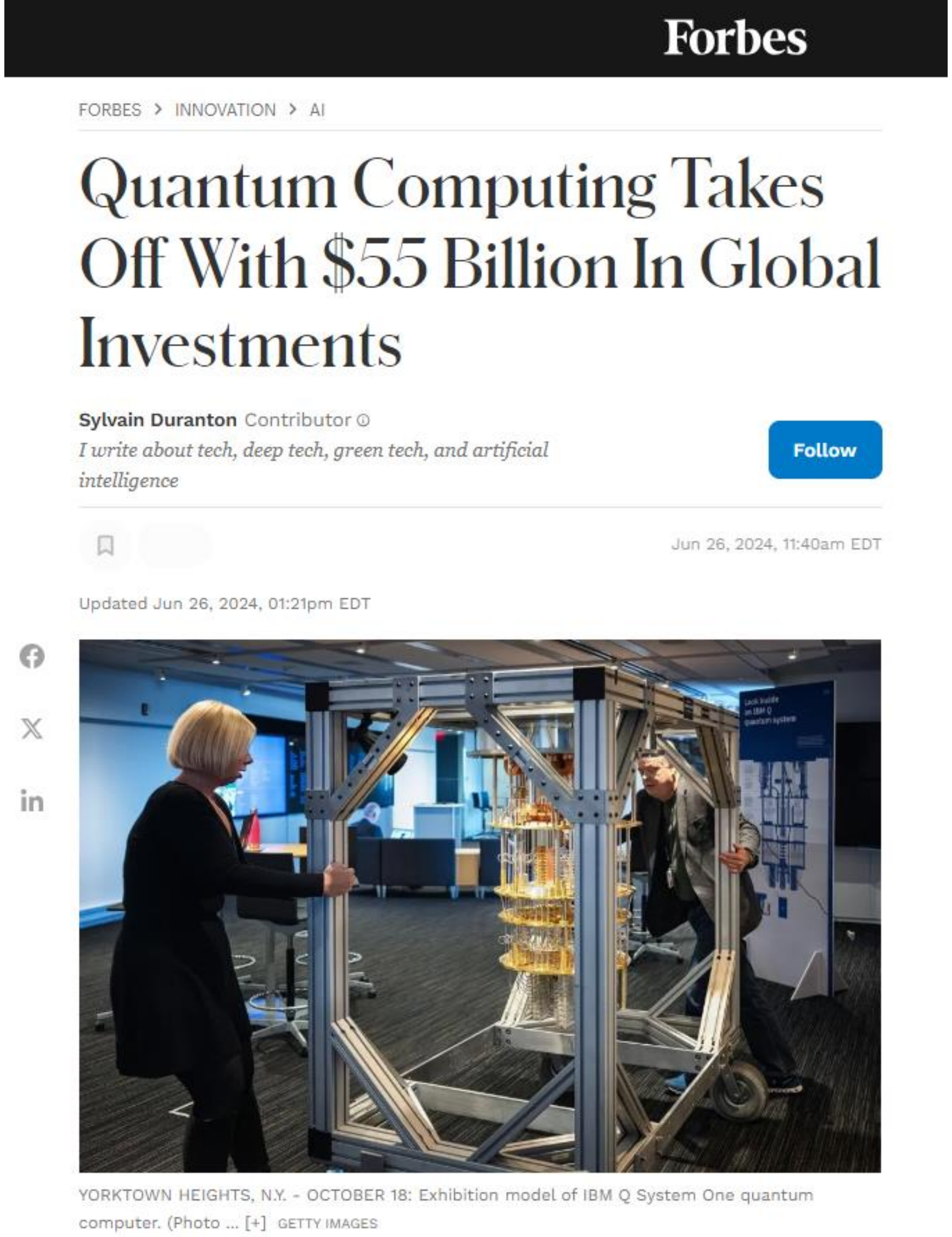

https://quantum2025.org/en/
INTERNATIONAL YEAR OF Quantum Science and Technology
Home
About
Timeline
Partners
Sponsorship
Events & Resources
unesco
INTERNATIONAL YEAR OF Quantum Science and Technology

100 years of quantum is just the beginning...

On June 7, 2024, the United Nations proclaimed 2025 as the International Year of Quantum Science and Technology (IYQ). According to the proclamation, this year-long, worldwide initiative will "be observed through activities at all levels aimed at increasing public awareness of the importance of quantum science and applications."

The year 2025 was chosen for this International Year as it recognizes 100 years since the initial development of quantum mechanics. Join us in engaging with quantum science and technology education and celebration throughout 2025!

Big Money by Big Tech



Forbes

FORBES > INNOVATION > AI

Quantum Computing Takes Off With $55 Billion In Global Investments

Sylvain Duranton Contributor ⓘ

I write about tech, deep tech, green tech, and artificial intelligence

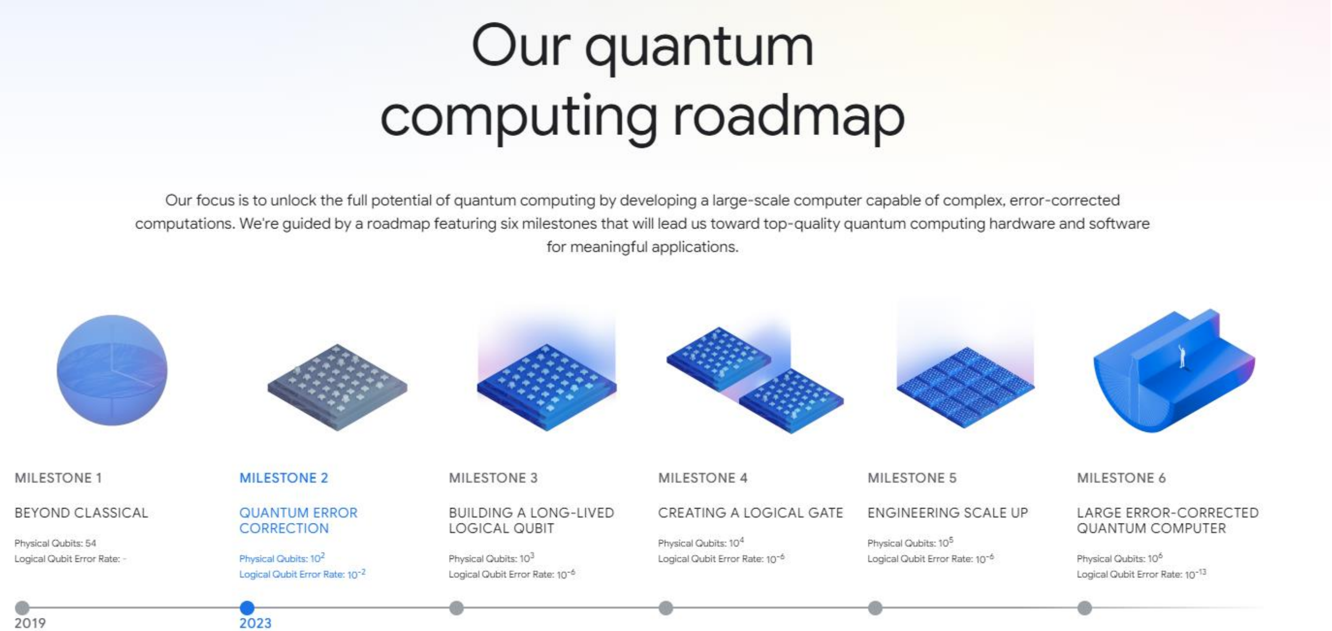
Follow

Jun 26, 2024, 11:40am EDT

Updated Jun 26, 2024, 01:21pm EDT

YORKTOWN HEIGHTS, N.Y. - OCTOBER 18: Exhibition model of IBM Q System One quantum computer. (Photo ... [+] GETTY IMAGES

BigTech seems to deliver on their own milestones....



Our quantum computing roadmap

Our focus is to unlock the full potential of quantum computing by developing a large-scale computer capable of complex, error-corrected computations. We're guided by a roadmap featuring six milestones that will lead us toward top-quality quantum computing hardware and software for meaningful applications.

MILESTONE 1

BEYOND CLASSICAL

Physical Qubits: 54
Logical Qubit Error Rate: -

2019

MILESTONE 2

QUANTUM ERROR CORRECTION

Physical Qubits: 10^2
Logical Qubit Error Rate: 10^{-2}

2023

MILESTONE 3

BUILDING A LONG-LIVED LOGICAL QUBIT

Physical Qubits: 10^3
Logical Qubit Error Rate: 10^{-6}

MILESTONE 4

CREATING A LOGICAL GATE

Physical Qubits: 10^4
Logical Qubit Error Rate: 10^{-6}

MILESTONE 5

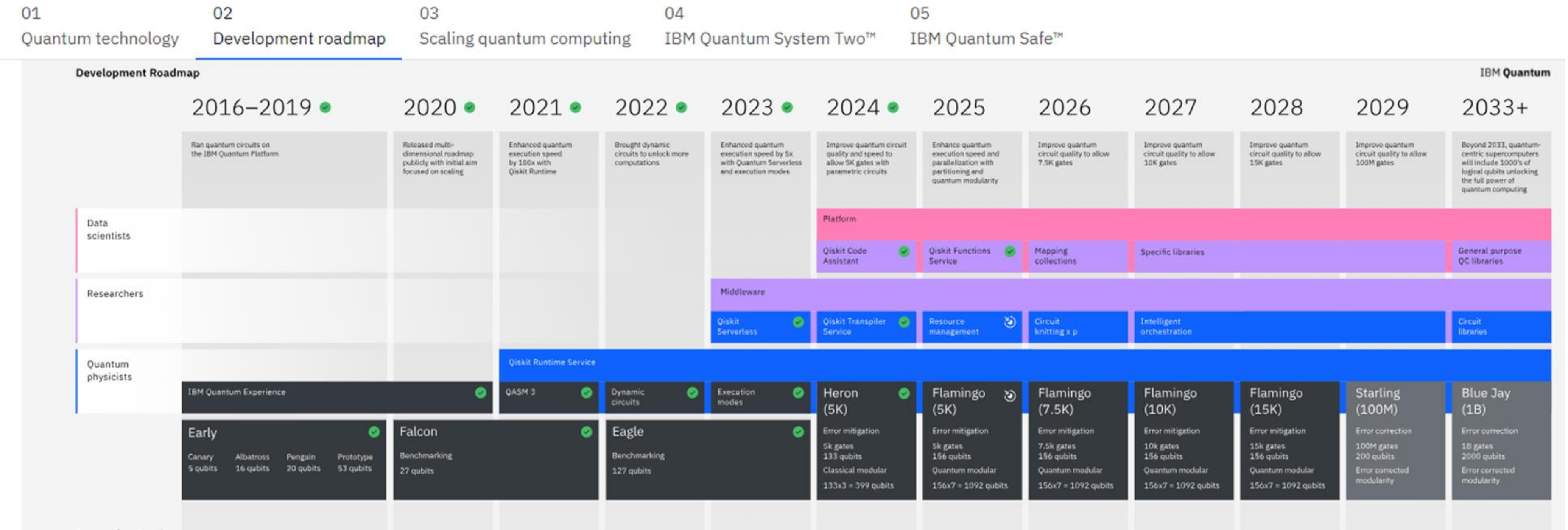
ENGINEERING SCALE UP

Physical Qubits: 10^5
Logical Qubit Error Rate: 10^{-6}

MILESTONE 6

LARGE ERROR-CORRECTED QUANTUM COMPUTER

Physical Qubits: 10^6
Logical Qubit Error Rate: 10^{-13}



01 Quantum technology
02 Development roadmap
03 Scaling quantum computing
04 IBM Quantum System Two™
05 IBM Quantum Safe™

Development Roadmap

IBM **Quantum**

2016–2019 ✓
Ran quantum circuits on the IBM Quantum Platform

2020 ✓
Released multi-dimensional roadmap publicly with initial aim focused on scaling

2021 ✓
Enhanced quantum execution speed by 100x with Qiskit Runtime

2022 ✓
Brought dynamic circuits to unlock more computations

2023 ✓
Enhanced quantum execution speed by 5x with Quantum Serverless and execution modes

2024 ✓
Improve quantum circuit quality and speed to allow 5K gates with parametric circuits

2025
Enhance quantum execution speed and parallelization with partitioning and quantum modularity

2026
Improve quantum circuit quality to allow 7.5K gates

2027
Improve quantum circuit quality to allow 10K gates

2028
Improve quantum circuit quality to allow 15K gates

2029
Improve quantum circuit quality to allow 100M gates

2033+
Beyond 2033, quantum-centric supercomputers will include 1000's of logical qubits unlocking the full power of quantum computing

Data scientists

Platform

Qiskit Code Assistant ✓
Qiskit Functions Service ✓
Mapping collections
Specific libraries
General purpose QC libraries

Researchers

Middleware

Qiskit Serverless ✓
Qiskit Transpiler Service ✓
Resource management
Circuit knitting x p
Intelligent orchestration
Circuit libraries

Quantum physicists

Qiskit Runtime Service

IBM Quantum Experience ✓
QASM 3 ✓
Dynamic circuits ✓
Execution modes ✓

Early ✓
Canary 5 qubits
Albatross 16 qubits
Penguin 20 qubits
Prototype 53 qubits

Falcon ✓
Benchmarking
27 qubits

Eagle ✓
Benchmarking
127 qubits

Heron (5K) ✓
Error mitigation
5k gates
133 qubits
Classical modular
133x3 = 399 qubits

Flamingo (5K)
Error mitigation
5k gates
156 qubits
Quantum modular
156x7 = 1092 qubits

Flamingo (7.5K)
Error mitigation
7.5k gates
156 qubits
Quantum modular
156x7 = 1092 qubits

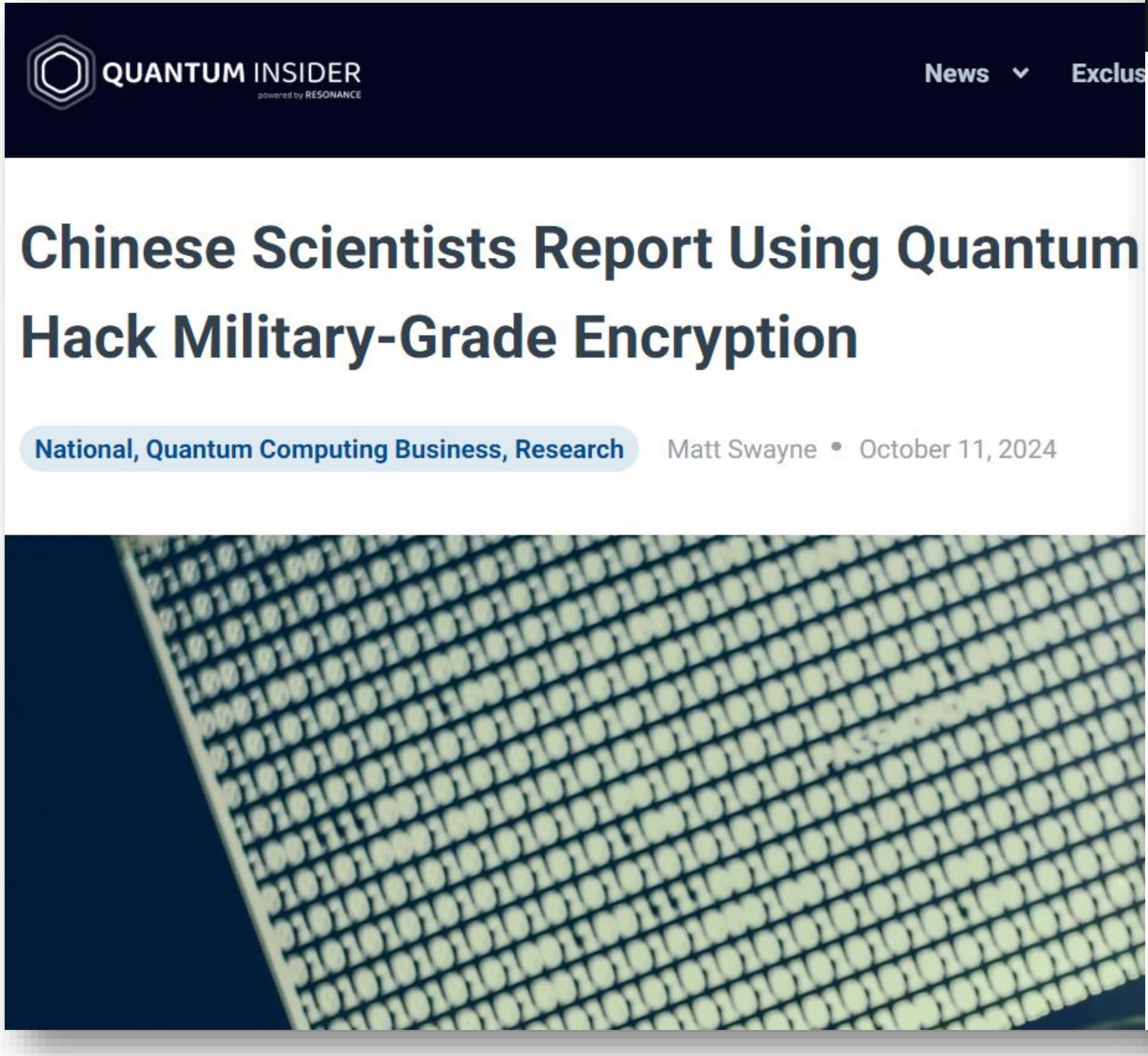
Flamingo (10K)
Error mitigation
10k gates
156 qubits
Quantum modular
156x7 = 1092 qubits

Flamingo (15K)
Error mitigation
15k gates
156 qubits
Quantum modular
156x7 = 1092 qubits

Starling (100M)
Error correction
100M gates
200 qubits
Error corrected modularity

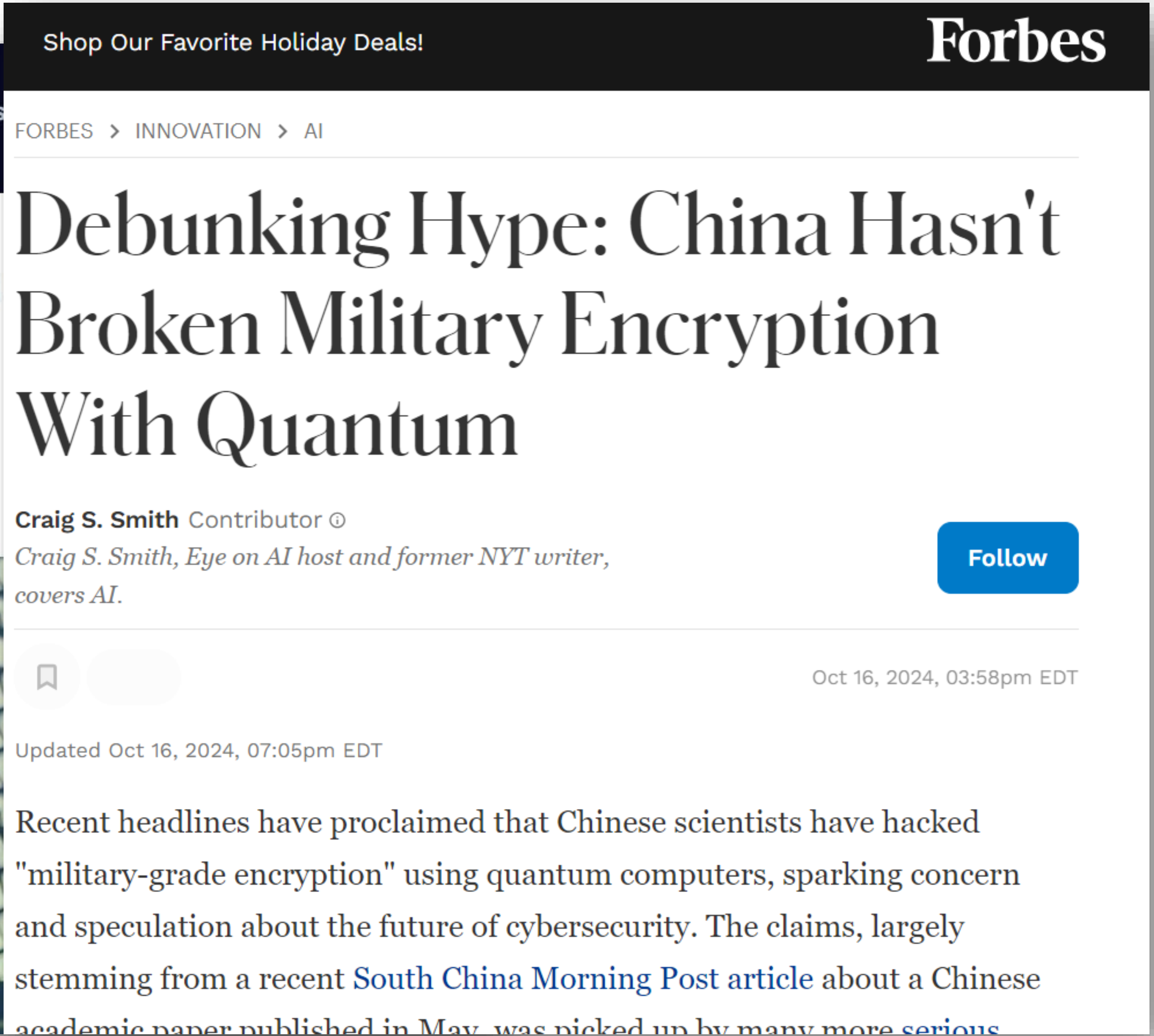
Blue Jay (1B)
Error correction
1B gates
2000 qubits
Error corrected modularity

My fear



Chinese Scientists Report Using Quantum Hack Military-Grade Encryption

National, Quantum Computing Business, Research · Matt Swayne • October 11, 2024



Debunking Hype: China Hasn't Broken Military Encryption With Quantum

Craig S. Smith Contributor ⓘ

Craig S. Smith, Eye on AI host and former NYT writer, covers AI.

Oct 16, 2024, 03:58pm EDT

Updated Oct 16, 2024, 07:05pm EDT

Recent headlines have proclaimed that Chinese scientists have hacked "military-grade encryption" using quantum computers, sparking concern and speculation about the future of cybersecurity. The claims, largely stemming from a recent South China Morning Post article about a Chinese academic paper published in May, was picked up by many more serious

I. What do we know? The risks posed by quantum computing

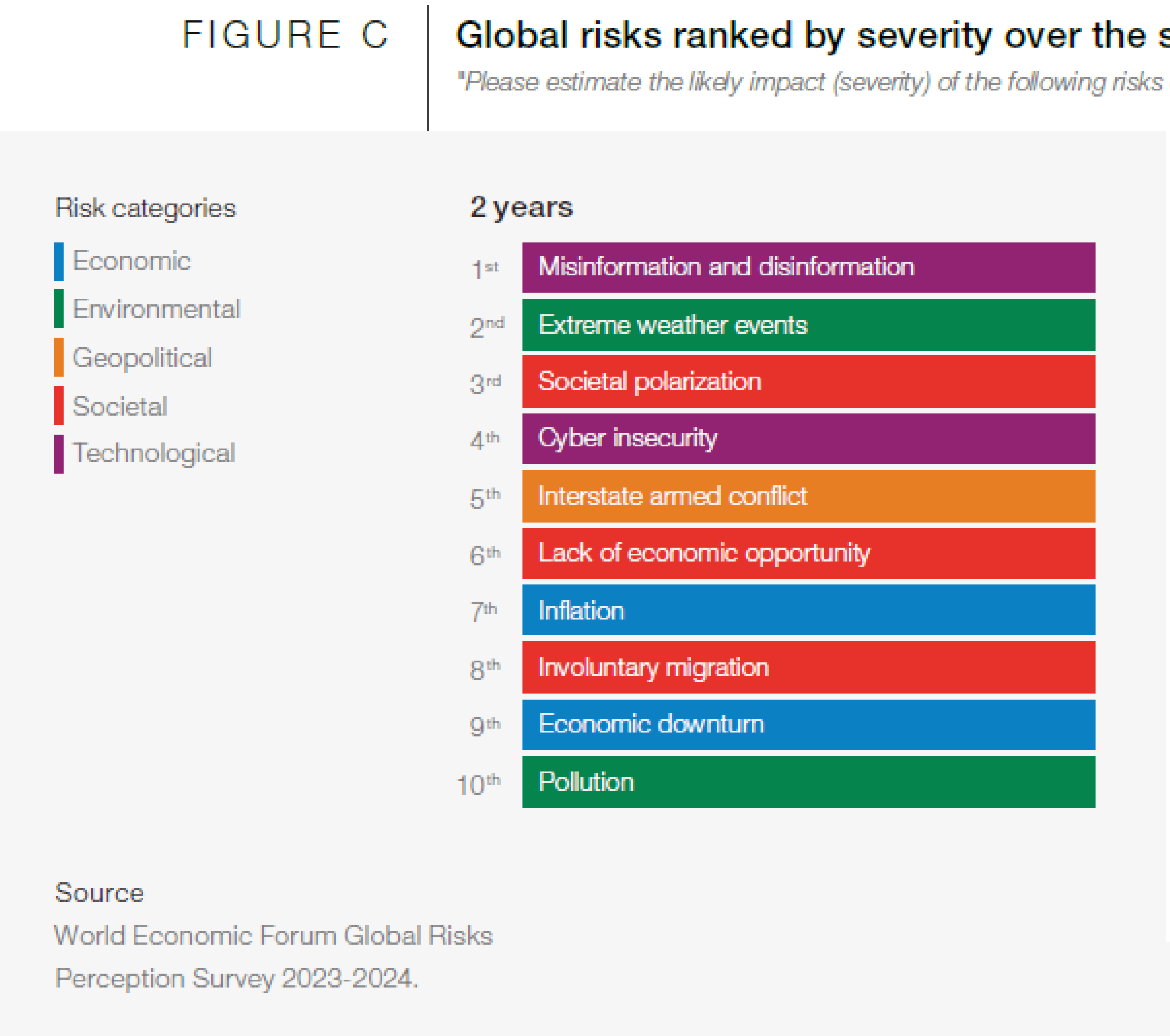


FIGURE C

Global risks ranked by severity over the short and long term

"Please estimate the likely impact (severity) of the following risks over a 2-year and 10-year period."

Risk categories

- 🟦 Economic
- 🟩 Environmental
- 🟧 Geopolitical
- 🟥 Societal
- 🟪 Technological

	2 years
1st	🟪 Misinformation and disinformation
2nd	🟩 Extreme weather events
3rd	🟥 Societal polarization
4th	🟪 Cyber insecurity
5th	🟧 Interstate armed conflict
6th	🟥 Lack of economic opportunity
7th	🟦 Inflation
8th	🟥 Involuntary migration
9th	🟦 Economic downturn
10th	🟩 Pollution

Source

World Economic Forum Global Risks Perception Survey 2023-2024.

Simmering geopolitical tensions combined with technology will drive new security risks (p9. WEF Global Risks Report 2024)

“Breakthrough in quantum computing Quantum computing could break and remake monopolies over compute power, posing radical risks in its development Criminal actors have already launched harvest attacks (SNDL) ….. Trade secrets across multiple industries, including pharmaceuticals and technological hardware, could be compromised. Large or even global infrastructure – such as banks, power grids and hospitals – could also be paralyzed…..”

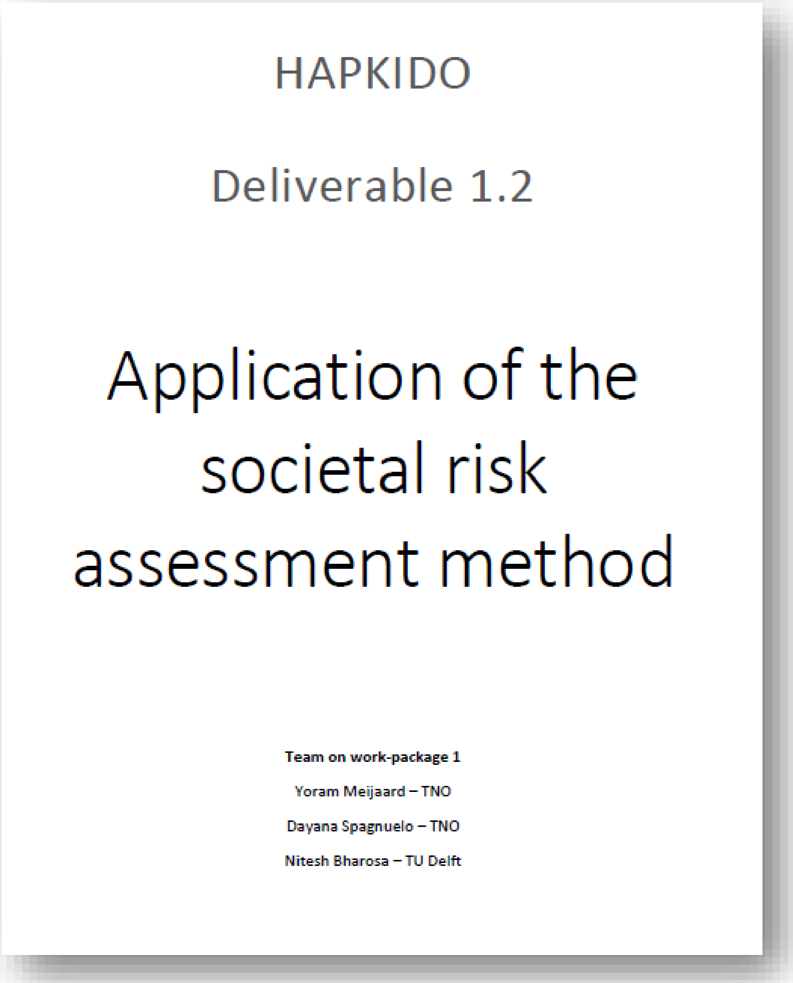
Societal impact can be devastating

HAPKIDO impact assessments:

I. Banking

II. Government

III. Telecom



HAPKIDO

Deliverable 1.2

Application of the societal risk assessment method

Team on work-package 1

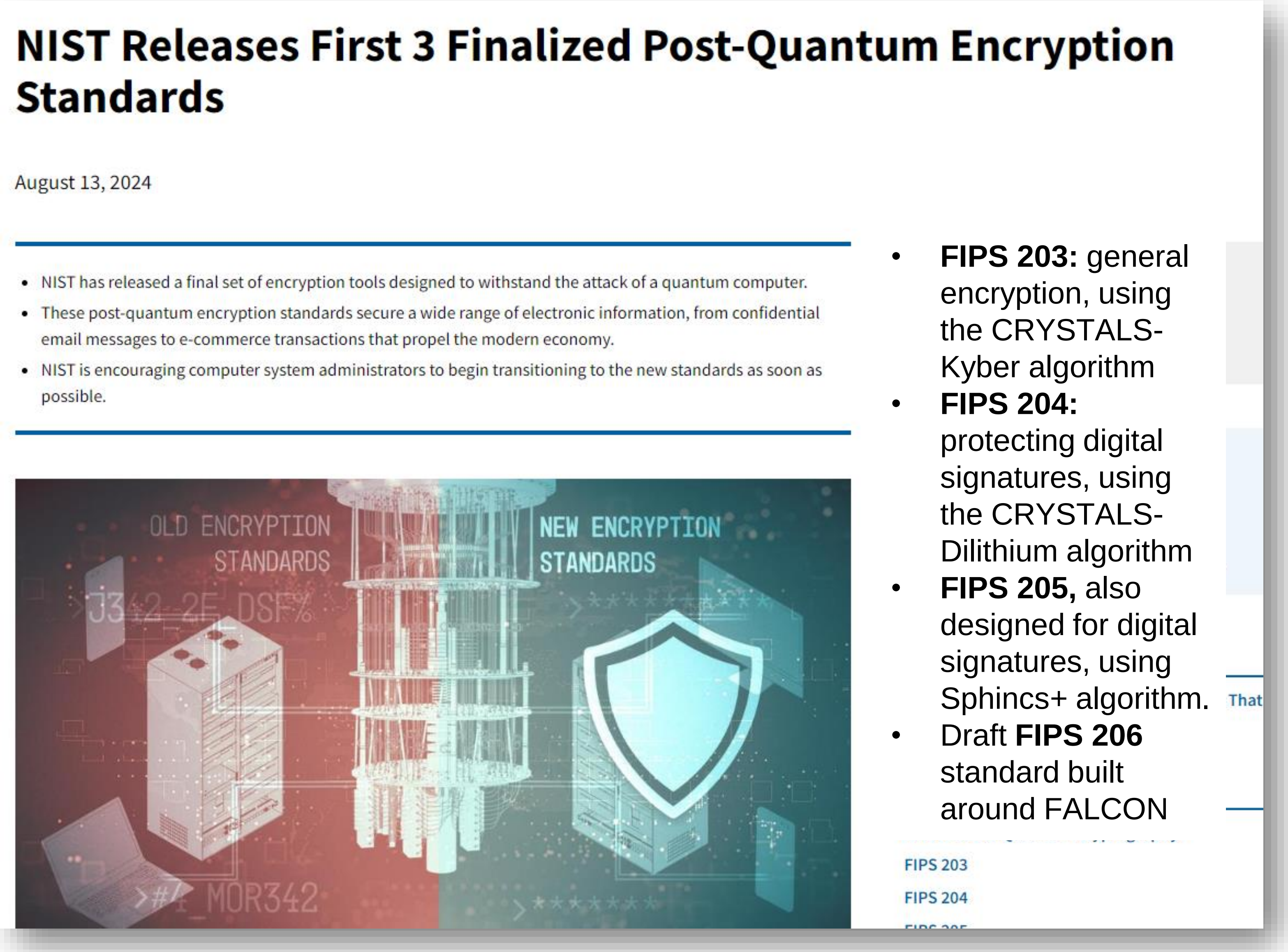
Yoram Meijaard – TNO

Dayana Spagnuelo – TNO

Nitesh Bharosa – TU Delft

https://hapkido.tno.nl/deliverables/application-societal-risk-assessment/

New PQC standards are on the horizon



NIST Releases First 3 Finalized Post-Quantum Encryption Standards

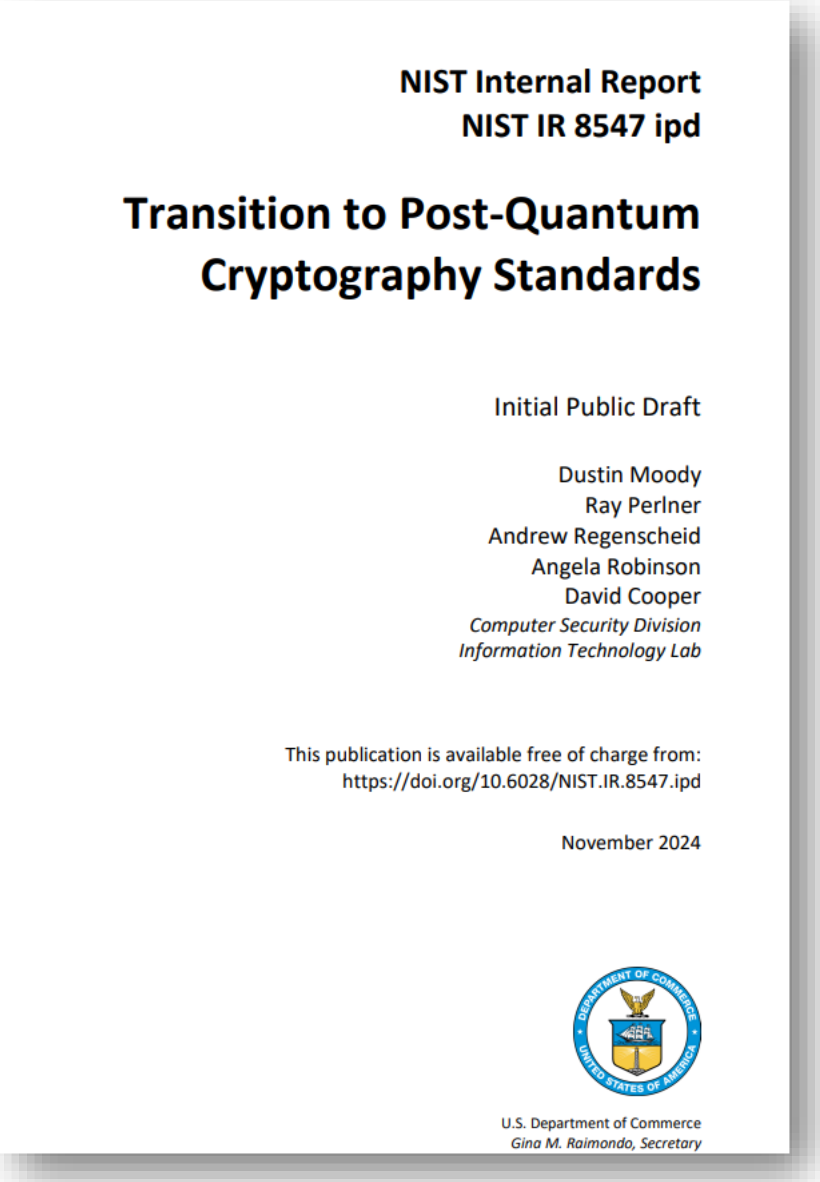
August 13, 2024

- NIST has released a final set of encryption tools designed to withstand the attack of a quantum computer.
- These post-quantum encryption standards secure a wide range of electronic information, from confidential email messages to e-commerce transactions that propel the modern economy.
- NIST is encouraging computer system administrators to begin transitioning to the new standards as soon as possible.

That

FIPS 203
FIPS 204
FIPS 205

- **FIPS 203:** general encryption, using the CRYSTALS-Kyber algorithm
- **FIPS 204:** protecting digital signatures, using the CRYSTALS-Dilithium algorithm
- **FIPS 205,** also designed for digital signatures, using Sphincs+ algorithm.
- Draft **FIPS 206** standard built around FALCON



NIST Internal Report
NIST IR 8547 ipd

Transition to Post-Quantum Cryptography Standards

Initial Public Draft

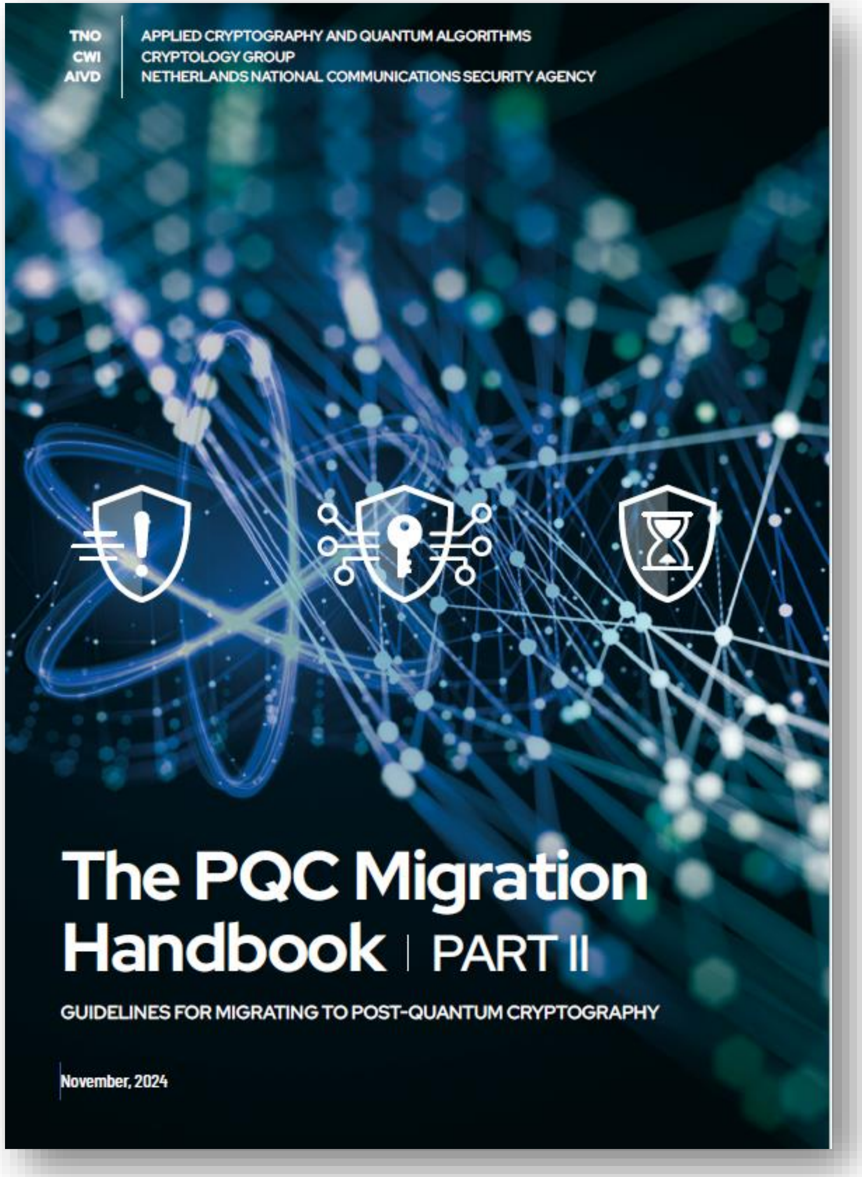
Dustin Moody
Ray Perlner
Andrew Regenscheid
Angela Robinson
David Cooper
Computer Security Division
Information Technology Lab

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8547.ipd

November 2024

U.S. Department of Commerce
Gina M. Raimondo, Secretary

Handbook for migration to PQC: great step

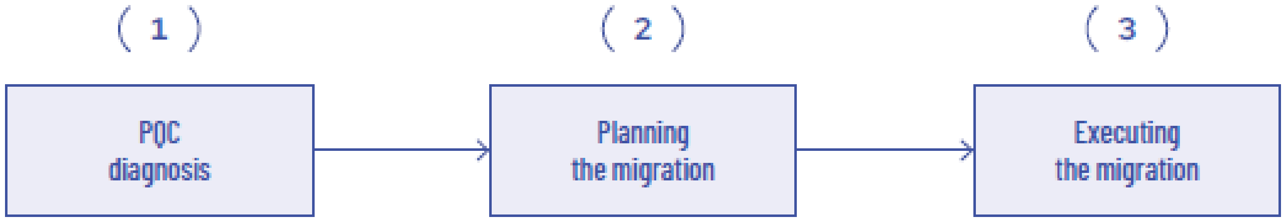


TNO APPLIED CRYPTOGRAPHY AND QUANTUM ALGORITHMS
CWI CRYPTOLOGY GROUP
AIVD NETHERLANDS NATIONAL COMMUNICATIONS SECURITY AGENCY

The PQC Migration Handbook | PART II

GUIDELINES FOR MIGRATING TO POST-QUANTUM CRYPTOGRAPHY

November, 2024

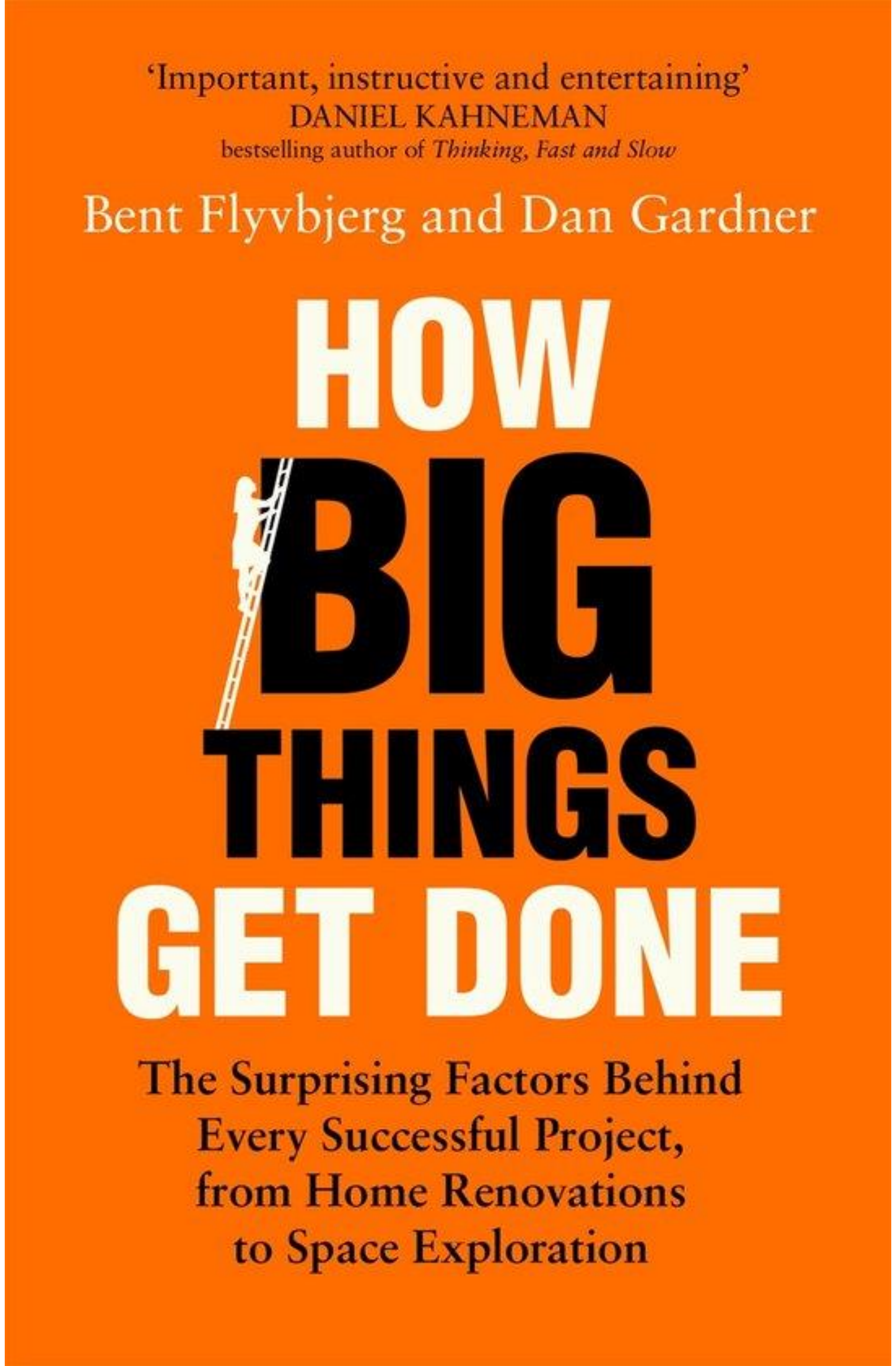


(1) PQC diagnosis

(2) Planning the migration

(3) Executing the migration

It’s not going to be easy

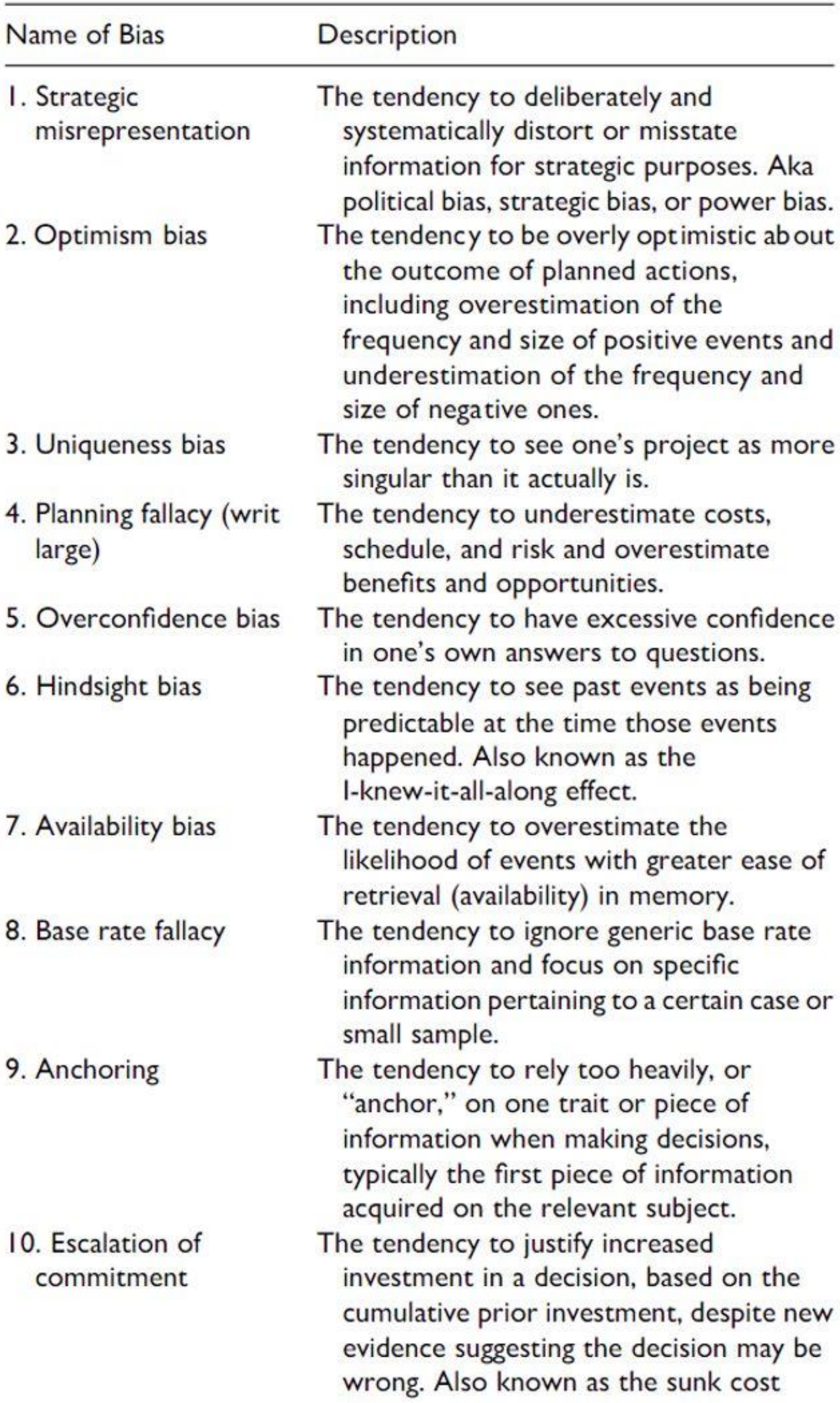


‘Important, instructive and entertaining’
DANIEL KAHNEMAN
bestselling author of *Thinking, Fast and Slow*

Bent Flyvbjerg and Dan Gardner

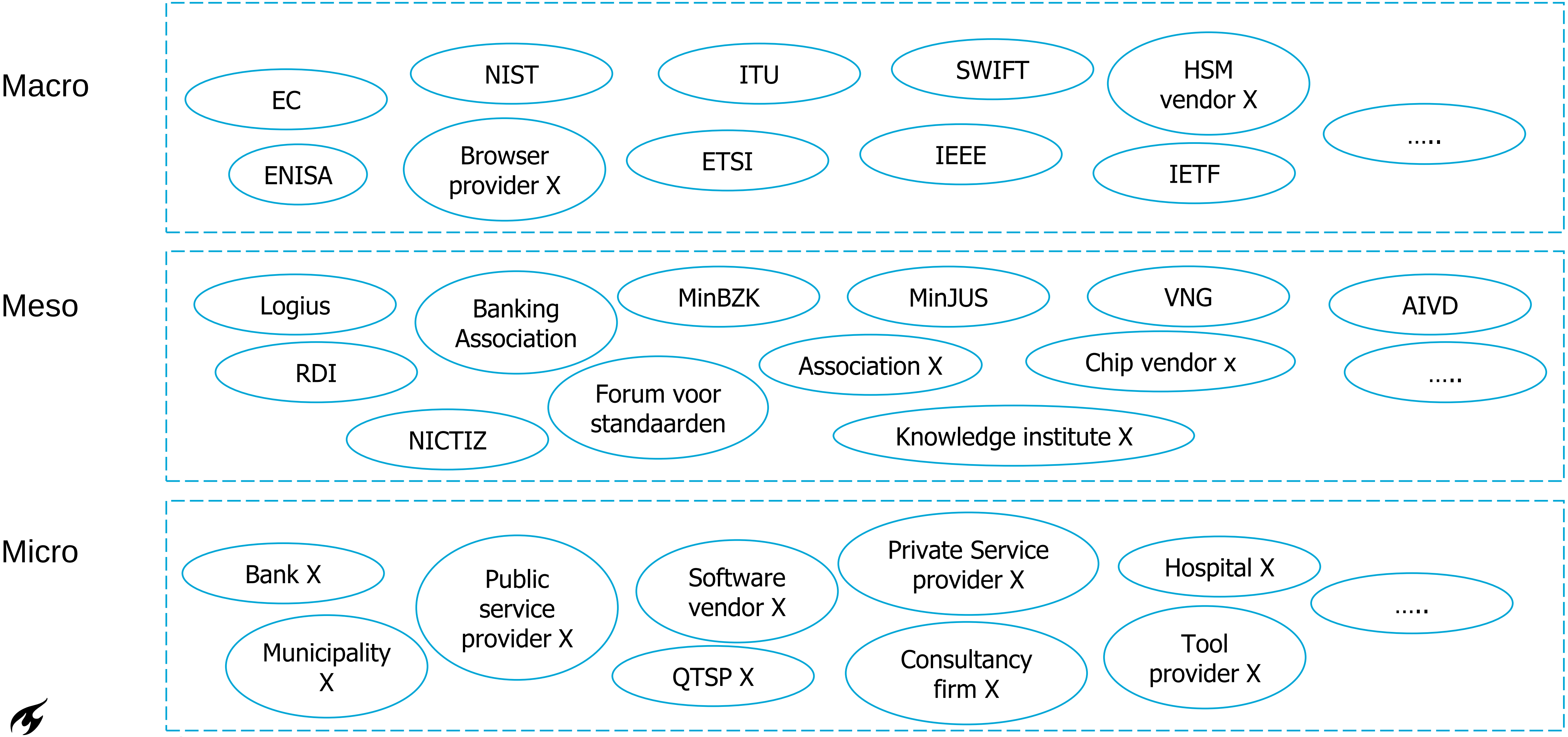
HOW BIG THINGS GET DONE

The Surprising Factors Behind Every Successful Project, from Home Renovations to Space Exploration



Name of Bias	Description
1. Strategic misrepresentation	The tendency to deliberately and systematically distort or misstate information for strategic purposes. Aka political bias, strategic bias, or power bias.
2. Optimism bias	The tendency to be overly optimistic about the outcome of planned actions, including overestimation of the frequency and size of positive events and underestimation of the frequency and size of negative ones.
3. Uniqueness bias	The tendency to see one’s project as more singular than it actually is.
4. Planning fallacy (writ large)	The tendency to underestimate costs, schedule, and risk and overestimate benefits and opportunities.
5. Overconfidence bias	The tendency to have excessive confidence in one’s own answers to questions.
6. Hindsight bias	The tendency to see past events as being predictable at the time those events happened. Also known as the I-knew-it-all-along effect.
7. Availability bias	The tendency to overestimate the likelihood of events with greater ease of retrieval (availability) in memory.
8. Base rate fallacy	The tendency to ignore generic base rate information and focus on specific information pertaining to a certain case or small sample.
9. Anchoring	The tendency to rely too heavily, or “anchor,” on one trait or piece of information when making decisions, typically the first piece of information acquired on the relevant subject.
10. Escalation of commitment	The tendency to justify increased investment in a decision, based on the cumulative prior investment, despite new evidence suggesting the decision may be wrong. Also known as the sunk cost

The communities are fragmented



TU Delft

II. What do we need to know?

I. What is the impact of the NIST standards on our PKIs?
II. How will PKIs and digital infrastructures (software and hardware) respond to the PQC standards?
III. What obstacles awaits organizations when following the transition handbook?
IV. How to align European, National vs. sectoral transition governance?
V. What will move the needle from ‘wait and see’ to a sense of urgency?
VI. What roles should governments play?
VII. What are the incentives for moving the key actors: the standard setters, demand and supply?
VIII. What will be transition cost be? How to share the cost?
IX. How do we foster inter-organisational crypto agility?
X. ….

III. How do we get there? Some propositions from Hapkido: move

From ‘wait and see’ strategy to a higher sense of urgency.

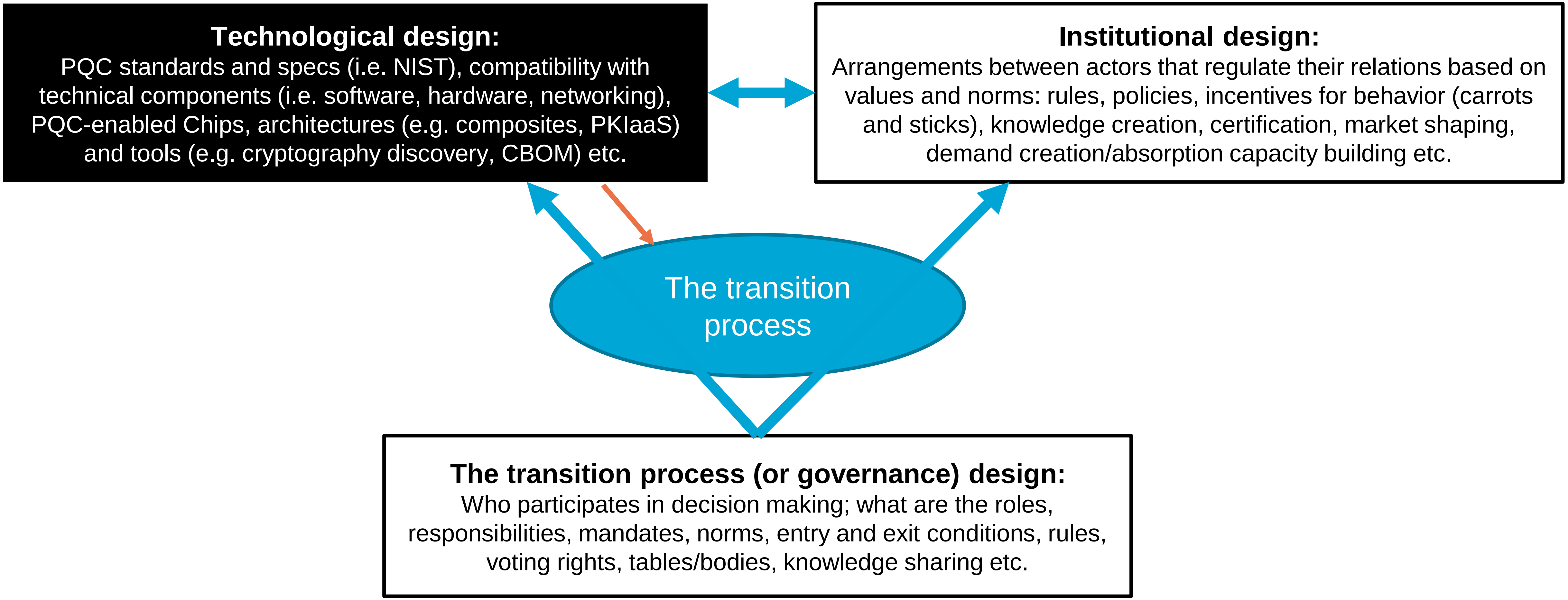
From looking for positive business cases to societal risks.

From certainty-seeking to continuous learning and growth.

From technocentric transition planning to a holistic approach

From organisational roadmaps to collective coordination.

From technocentric transition planning to a holistic approach



Technological design:
PQC standards and specs (i.e. NIST), compatibility with technical components (i.e. software, hardware, networking), PQC-enabled Chips, architectures (e.g. composites, PKIaaS) and tools (e.g. cryptography discovery, CBOM) etc.

Institutional design:
Arrangements between actors that regulate their relations based on values and norms: rules, policies, incentives for behavior (carrots and sticks), knowledge creation, certification, market shaping, demand creation/absorption capacity building etc.

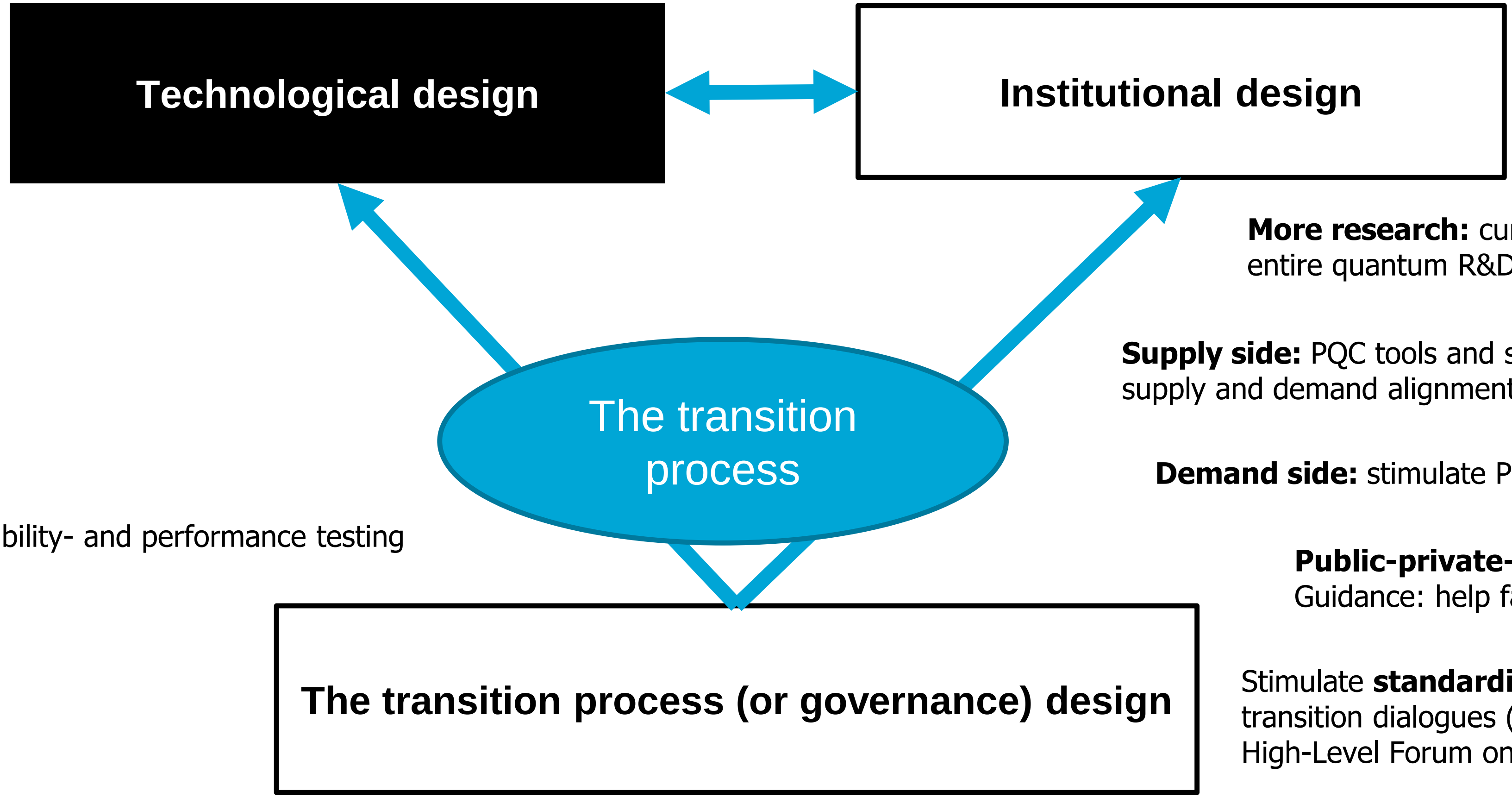
The transition process

The transition process (or governance) design:
Who participates in decision making; what are the roles, responsibilities, mandates, norms, entry and exit conditions, rules, voting rights, tables/bodies, knowledge sharing etc.

TU Delft

Based on: Koppenjan, JFM., & Groenewegen, JPM. (2005). Institutional Design for Complex Technological Systems. *International Journal of Technology, Policy and Management*, *5*(3), 240-257.

Some non-technical priorities



Technological design

Institutional design

The transition process

The transition process (or governance) design

More research: currently ca. 1% of the entire quantum R&D budget on PQC

Supply side: PQC tools and services, consulting, helping supply and demand alignment

Demand side: stimulate PQC absorption capacity building

Public-private-academic Expertise Centre: Guidance: help facilitate the absorption of PQC.

Stimulate **standardization bodies** to start transition dialogues (e.g. Forum Standaardisatie, High-Level Forum on European Standardisation)

Organize interoperability- and performance testing

Public sector leadership: co-create a **national trust framework** (afsprakenstelsel) for using PQC in various PKIs

Inspiration from a nobel prize winner: Governing the commons

- Collective Action Theory
- PKIs as ‘digital commons’, or resources that benefit many members of a society
  - Shared benefits for the community
  - Collective maintenance responsibility
  - Network effects: more users, more value
- Beware of ‘**Tragedy of the commons’:** pursuing short term self-interest (e.g. let others work on the transition and incur the cost) over common interest (e.g. lets invest together) erodes trust in the entire PKI system potentially leading to future collapse.

OSTROM'S 8 PRINCIPLES FOR MANAGING A COMMONS

(1)

STRONG GROUP IDENTITY AND UNDERSTANDING OF PURPOSE

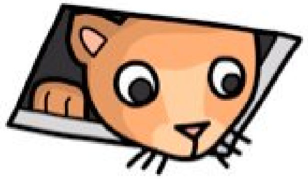
(2)

FAIR DISTRIBUTION OF COSTS AND BENEFITS

(3)

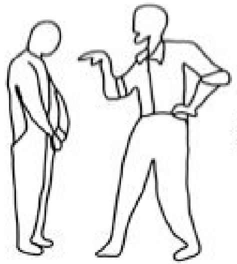
FAIR AND INCLUSIVE DECISION MAKING

(4)



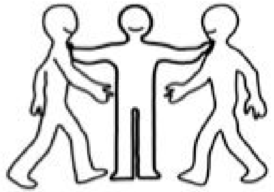
MONITORING AGREED UPON BEHAVIORS

(5)



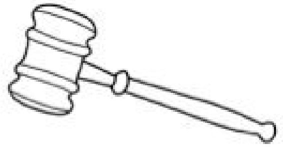
GRADUATED SANCTIONS FOR MISBEHAVIORS

(6)



FAST AND FAIR CONFLICT RESOLUTION

(7)



AUTHORITY TO SELF-GOVERN

(8)

APPROPRIATE RELATIONS WITH OTHER GROUPS

Conclusions

1. We are entering an important and difficult phase in the PQC era: the technical standards are drafted, but how to proceed from here?
2. The transition process is not only about the technical design. Don’t forget the institutional design (e.g., incentives and market building) and the governance design (who decides on what, when and how).
3. Govern PKIs as digital commons and beware of the tragedy of the commons.
4. Research is an effective vehicle for connecting the fragmented actor landscape. Stimulate and participate in research programs.

Amara's Law – "We tend to overestimate the effect of a technology in the short run and underestimate the effect in the long run."

Thank you!

N.Bharosa@tudelft.nl
https://hapkido.tno.nl/