Workshop: 29 Jan 2025

Summary of Workshop on Ecosystem of Quantum-Safe Cryptography in the Netherlands

QISS, UvA
Ailsa Robertson

Overview

This report presents a summary and analysis of an interdisciplinary, multi-stakeholder workshop held in Amsterdam on 29 January 2025. This research is part of UvA's Quantum Impact on Societal Security (QISS) project on the transition to Quantum-Safe Cryptography (QSC), of which the overarching goal is to investigate the requirements for a successful and timely transition to QSC. As ecosystem of QSC is actively emerging, it is an opportune moment to conduct this study. Through the capture of a snapshot and its examination through a research lens, current developments may be effectively interpreted, and the trajectory of future development guided from an early stage.

The aim of this research is to uncover transition requirements by considering the complex, interconnected set of organisations involved in the transition from an ecosystem perspective. As part of this research, a workshop was organised to create an initial mapping of the ecosystem. The primary objective of the workshop was to propose actor types, and the secondary objectives were, for each actor type proposed, to describe their roles and responsibilities, as well as inhibitors of these roles and responsibilities. Participants of the workshop consisted of members of industry, government, research instutitions and branch organisations, providing representation from relevant stakeholder groups in the QSC ecosystem.

The presentation of findings follows the workshop structure. The first activity was an initial scoping exercise in order to align on key terms; details are given in **Scoping**. Then, the participants jointly created an initial ecosystem map; details are given in **Mapping**. Next, actor categories were proposed by the group; details are given in **Categories**. Then, an **Initial Analysis** summarises the deeper points which generated significant discussion, and provides a reflection on actor centrality. Finally, some short **Concluding Remarks** end this report. We highlight that the only analytic work performed in advance of the event was in the choice of participants, a process which we acknowledge introduces bias. All other findings emerged directly from the participants.

We reflect on the implications of this work. This study addresses the important issue of transition to QSC at a crucial moment, and highlights that it is a systemic and governance challenge rather than a purely technical one. In paricular, it fills a gap by providing an early, ecosystem-level mapping of actors, roles, and inhibitors, making socio-organisational challenges explicit. We propose that natural next steps include validating and refining the ecosystem map, translating identified challenges into concrete governance and policy interventions, and developing transition pathways that support coordinated, public-interest–oriented adoption.

Scoping

To enable a structured discussion, the boundaries of the ecosystem were first delineated. This was done by presenting a draft description of the ecosystem, accompanied by key terms: QSC, PQC, QKD, hybrid cryptography, cryptoagility and traditional cryptography. For definitions of these key terms, see the **PQC Migration Handbook**. Participants were then invited to comment, refine, and debate the wording until consensus was reached that the description adequately captured the ecosystem under consideration. The agreed description was:

The ecosystem of QSC in the Netherlands consists of the organisations that are ***responsible and accountable*** *for activities such as developing, testing, implementing, regulating, raising awareness, disseminating knowledge or financing in the migration to PQC, QKD or hybrid cryptography.*

Points of note from this discussion were:

- **Cryptoagility**: Although cryptoagility was included in the original description and considered by some participants to be the most important aspect of migration, it was ultimately excluded; the group did not view it as a core function of the ecosystem.

- **Normative Framing**: The original description was phrased descriptively (“organisations that have an active role in…”), but participants deliberately shifted it to a normative framing (“organisations that are responsible and accountable for…”). This suggests that participants viewed the migration not merely as an observed process, but as one that ‘should’ take place.

- **Terminology Choices**: Participants preferred the expressions “resistant to attack from a quantum computer” and “vulnerable to attack from a quantum computer” over the terms “quantum-safe” and “not quantum-safe.” This preference reflects both a desire for precision and an awareness of the nuances of the underlying technology.

- **Ambiguity of PQC**: It was noted that the term PQC carries multiple meanings in practice. In some contexts, it refers to the set of schemes designed in recent decades with the explicit aim of resisting quantum attacks. In others, it serves as an umbrella term for all schemes (including symmetric) that are resistant to quantum attack.

Ecosystem Mapping

In order to establish a shared understanding of the ecosystem, participants were first asked to compile individual lists of ten organisations that they considered to be part of the ecosystem. This activity was undertaken independently to minimise the potential for group influence. Following the completion of the individual lists, duplicates were removed and the remaining organisations were consolidated. Participants were subsequently invited to group these organisations into categories in a manner that felt most appropriate.

Although it had been anticipated that three to four high-level categories would emerge, the exercise ultimately produced a more differentiated picture. A total of twelve distinct categories were identified, each reflecting a specific role within the ecosystem. These categories are listed in **Appendix A.3**.

Roles & Responsibilities

The participants had already started considering roles and responsibilities implicitly as part of forming actor categories. The list of 12 categories was split between the three breakout groups, and each group attempted to list all roles and responsibilities of these actors in the migration. The roles and responsibilities are listed in **Appendix A.4**.

Points of note from this discussion were:

- **Promoters**: The participants identified a group of actors who stimulated development in the ecosystem. This was often a role held alongside another role (e.g. Financier). This group was originally called Lobbyists, but the group ultimately labelled them Promoters.

- **Network Operators**: Whether or not Network Operators have a distinct role in this migration was contested. Consensus was reached that these actors only have a distinct role for QKD; otherwise, they are simply End Users.

- **End Users**: The group considered every organisation in the Netherlands to be an End User, as each will have to make its own internal migration. However, the group identified a subcategory they labelled Special End Users. These are End Users which were large enough to exert influence on the ecosystem, e.g. due to their buying power. Although not mentioned during the mapping exercise, Ericsson was named as an example of a Special End User.

Initial Analysis

Five major themes emerged during the discussion of roles and responsibilities; these are outlined below. These themes will be analysed in depth in an upcoming academic paper, accompanied by recommendations for the stimulation of development of this ecosystem for public good.

1. Migrating to Immature Cryptography

Participants highlighted the substantial institutional inertia that hinders the adoption of new cryptographic solutions. This inertia is compounded by the relative immaturity of emerging schemes. The maturity of cryptographic systems depends heavily on rigorous cryptanalysis dedicated research efforts aimed at breaking them. Yet, funding for such ‘attack research’ remains limited. Expanding support for cryptanalysis was identified as a critical enabler of trust and adoption.

2. Prompting Action from End Users

Driving the migration requires effective communication with decision-makers in organisations, particularly CISOs. While awareness of the quantum threat was recognised as a first step, participants noted that this does not necessarily translate into action. Even motivated organisations often delay migration due to the lack of mature tooling and practical pathways. Bridging this gap between awareness and implementation remains a significant challenge.

3. Carrots and Sticks

Two breakout groups framed migration levers as “carrots and sticks.” At present, incentives for early movers are minimal, and formal mandates, such as regulations or timelines, are absent in the Dutch context. Participants suggested that mandates are more likely to emerge at the EU level. A balanced transition strategy would combine meaningful incentives with well-timed mandates, supported by clear expectations and milestones for organisations.

4. Preventing Fragmentation

Fragmentation of cryptographic approaches, already visible in hybrid schemes, was identified as a major risk. Unless interoperability is made a high priority, countries and organisations will pursue divergent paths. Ensuring alignment will require coordination among international standardisation bodies; a process that is both technically complex and politically sensitive, with implications for national autonomy.

Initial Analysis, Continued

5. Open Source

Most organisations are expected to rely on open source PQC during their migration. While such open development is deeply valuable, concerns were raised about accountability and security. No single actor is formally responsible for ensuring the quality and resilience of open source solutions, leaving them vulnerable to risks such as malicious code updates. A proposed solution was to assign formal responsibility for maintenance and quality assurance to companies that benefit from using open source PQC.

Inferring Centrality

Charts in **Appendices A.1** and **A.2** show the organisations with highest mentions. We infer a level of ecosystem centrality from this data.

- **Research & Education** had the highest number of total mentions (31) and the highest number of unique mentions (10). This category also contained the two organisations with most mentions: **TNO** (9) and **CWI** (8). Although these may have been influenced by the fact that the workshop was facilitated by CWI and TNO, these should still be considered central actors.

- **Regulators** can also be viewed as central, as they also had a high number of total mentions (24), proportionally greater than the unique mentions (8).

- We can infer that **Min EZ** (5) and **QDNL** (4) can be viewed as central **Promoters**; **NXP** (5) and **PQShield** (3) can be viewed as prominent **Manufacturers**.

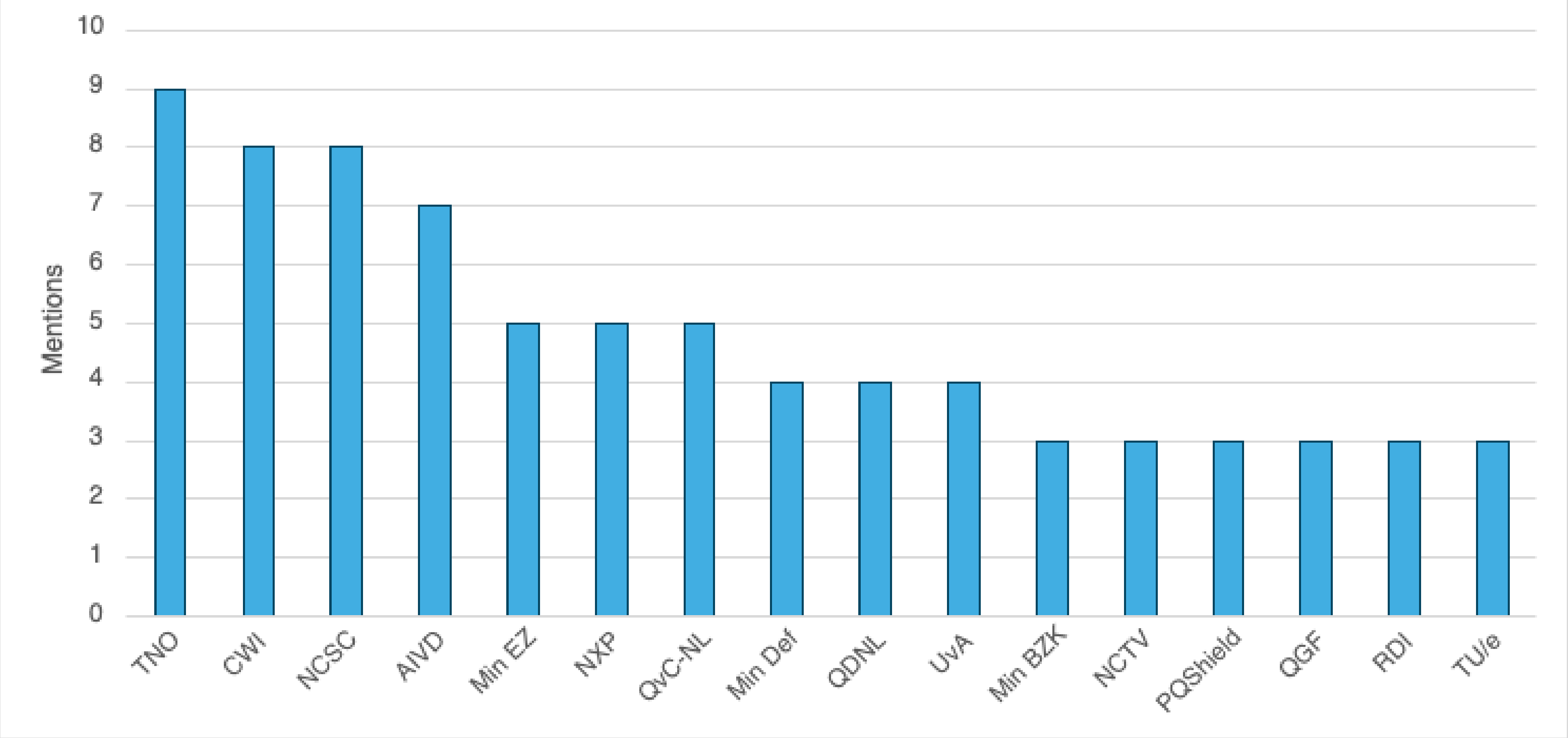
- **Migration Service Providers** can be viewed as an emerging category, as the number of mentions was very low (total 4, unique 2). However, **Quantum Gateway Foundation** (3) is a prominent member of this category.

Concluding Remarks

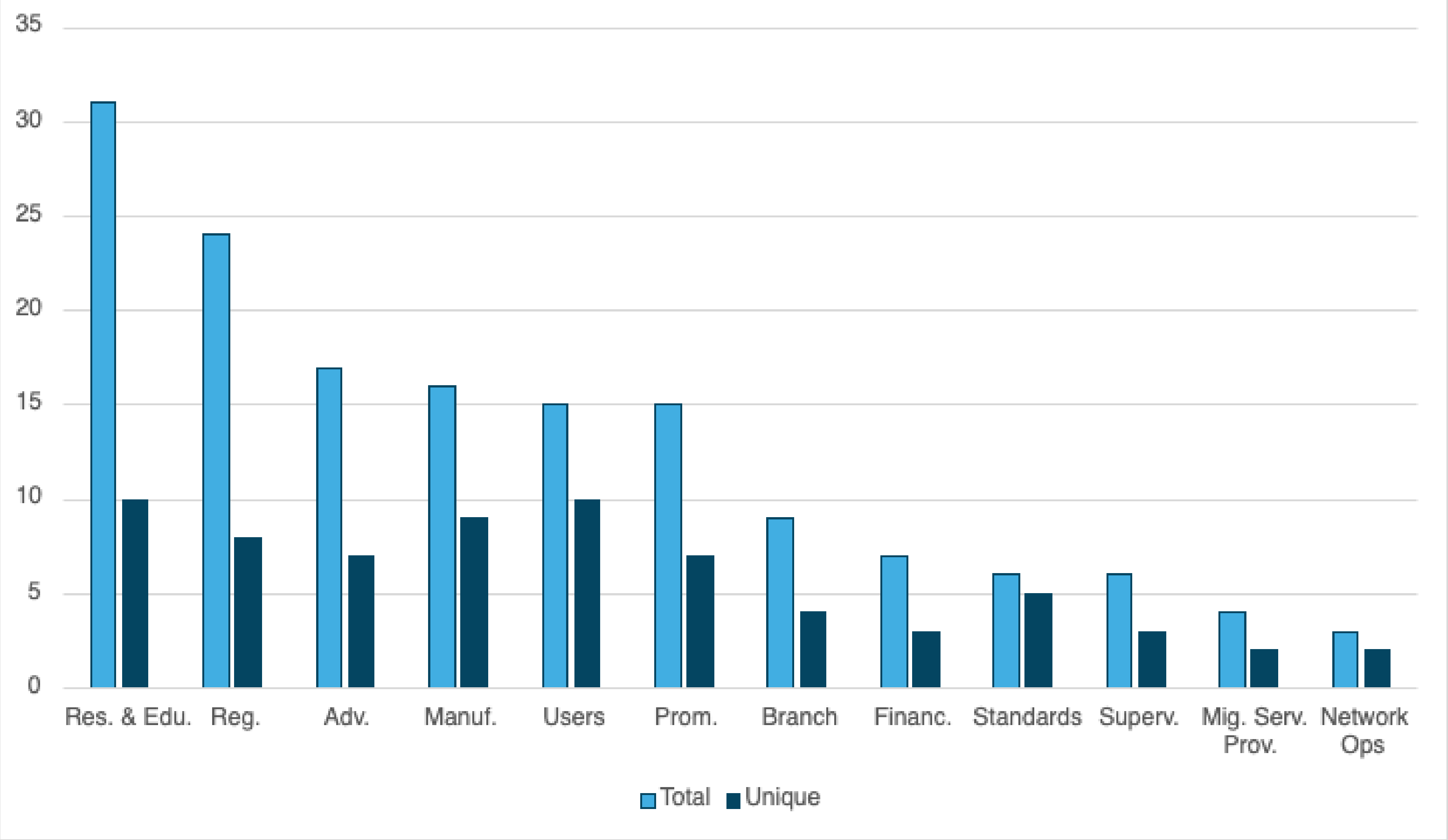
This research highlights that the migration to quantum-safe cryptography is not simply a technical challenge but a systemic one, involving governance, incentives, and coordination. Participants emphasised that without deliberate intervention, the transition risks being shaped by commercial interests and fragmented initiatives. By contrast, a carefully designed ecosystem, supported by targeted incentives, robust standards, and shared responsibility, could accelerate progress while serving the broader public good.

Appendix

A.1 High Organisation Mentions



A.2 Comparative Mentions



A.3 Ecosystem Actors

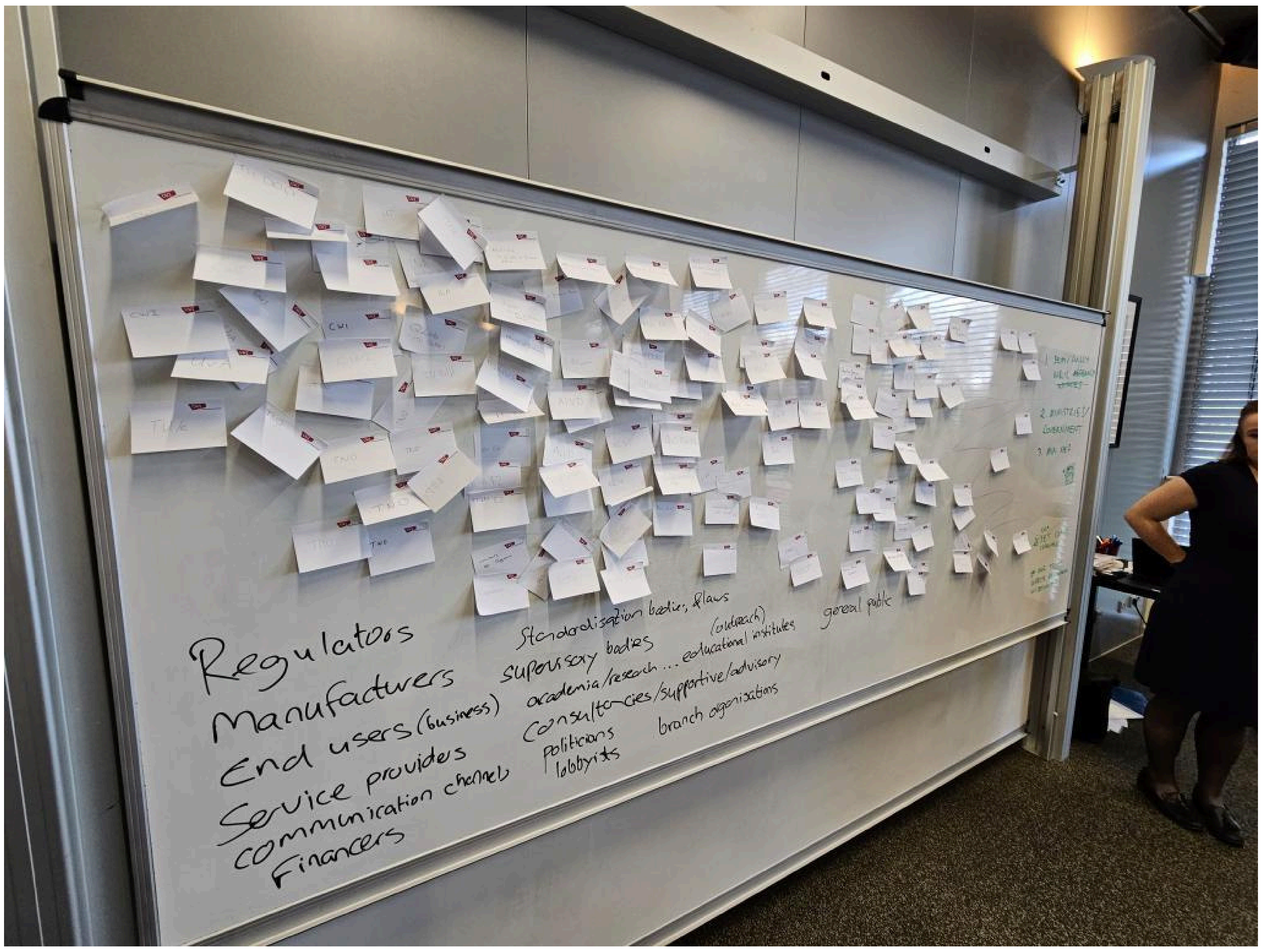
Category	Examples	Count Total	Count Unique
Research & Education	TNO (9), CWI (8), UvA (4), TU/e (3), TU Delft (2), Security Academy (1), SURF (1), UT (1), QLab (1), Quantum-Safe Consortium (1).	31	10
Regulators	AIVD (7), QvC-NL (5), NCTV (3), Min BZK (3), European Commission (2), NBV (2), NATO (1), Tweede Kamer (1).	24	8
Advisory	NCSC (8), Min BZ (2), NBV (2), Capgemini (2), Deloitte (1), Clingendael (1), Rathenau (1).	17	7
Manufacturers (crypto. components)	NXP (5), PQShield (3), Q*Bird (2), ASML (1), Thales (1), Fox Crypto (1), Cubiqs (1), Riscure (1), Compumatica (1).	16	9
End Users*	*[*Should be all organisations.]* Min Def (4), Min I&W (2), Min BZ (2), Tennet (1), Worldline (1), VNG (1), TPO (1), Alliander (1), Min J&V (1), Google (1).	15	10
Promoters	Min EZ (5), QDNL(4), dcypher (2), NCC-NL (1), PKI Consortium (1), EuroQCI (1), CC Nederland (1).	15	7
Branch Organisations	QvC-NL (5), NVB (2), Tech NL (1), Veb. Voz (1).	9	4
Financers	Min EZ (5), NWO (1), *American Federal Government [inclusion in ecosystem was contested] (1).*	7	3
Standardisation Bodies	IETF (1), ISOs (1), ETSI (1), NEN (1), *NIST [inclusion in ecosystem was contested] (2).*	6	5
Supervisors	RDI (3), DNB (2) & ESAs (1).	6	3
Migration Service Providers	Quantum Gateway Foundation (3), Fox-IT (1).	4	2
Network Operators	KPN (2), BBNET (1).	3	2

A.4 Roles & Responsibilities

Category	Roles & Reponsibilities
Research & Education	Develop knowledge, disseminate knowledge, certify migration tools/services.
Manufacturers (crypto. components)	Develop quantum-resilient hardware/software; adopt new standards; experiment/test; follow market demand.
Standardisation Bodies	Influence regulators; provide advice to governments; communicate with other standards agencies to ensure compatibility of standards; set standards for adoption.
End Users	Comply to existing standards/regulations; incorporate quantum threat in risk assessment; understand own needs; express demands to vendors; create migration strategy; create internal cryptography policy; analyse urgency of use cases; estimate transition cost; allocate budget; upskill FTEs; adopt new standards/regulations; develop internal policy; identify migration barriers; adopt/buy tooling/services; make cryptography inventory; implement; experiment/test; maintain cryptography and cryptoagility.
Advisory	Explain/interpret incentives; 'translate' regulation; recommend migration tools.
Regulators	Set regulation; enforce compliance; create transition policy; mandate interoperability; set minimum transition requirements.
Promoters	Facilitate matchmaking for research calls; stimulate development/ innovation.
Branch Organisations	Set milestones for reaching minimum requirements; recommend migration tools; share best practice.
Financers	Finance research (both fundamental and applied); finance valorisation activities; steer innovation.
Supervisors	Enforce compliance of End Users; 'translate' regulation.
Migration Service Providers	Develop scalable migration services; respond to demand from users; create cryptography inventory tooling; offer standard and bespoke migration services.
Network Operators	Offer reliable QKD networks.

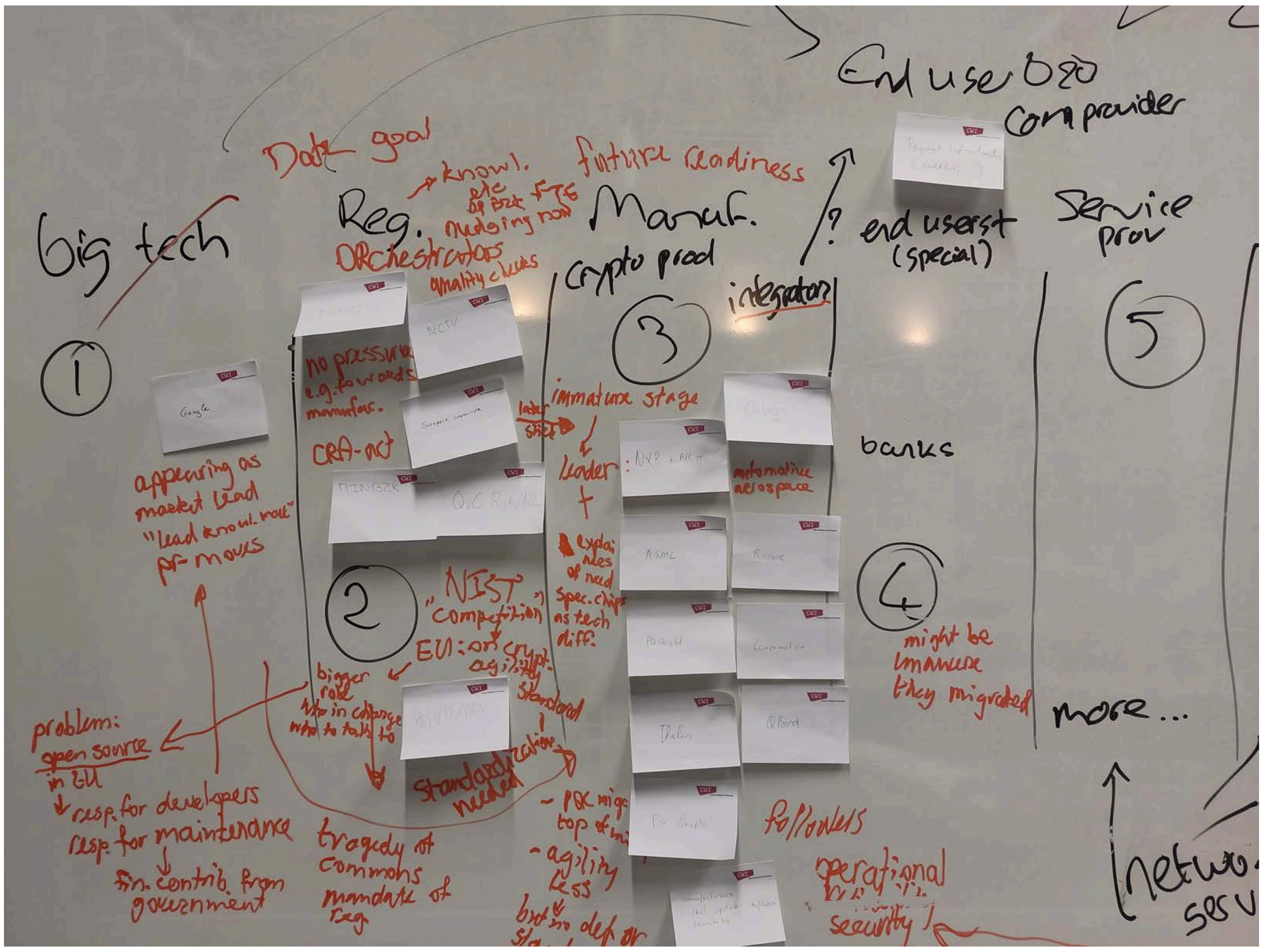
A.5 Event Photos

A.5.1: Arranging organisations into natural categories.



A.5.2: Final picture once grouping reached saturation.

A.5.3: Naming the proposed categories (featured face is of a QISS researcher).



A.5.4: Notes made during discussion in Breakout Group 3.