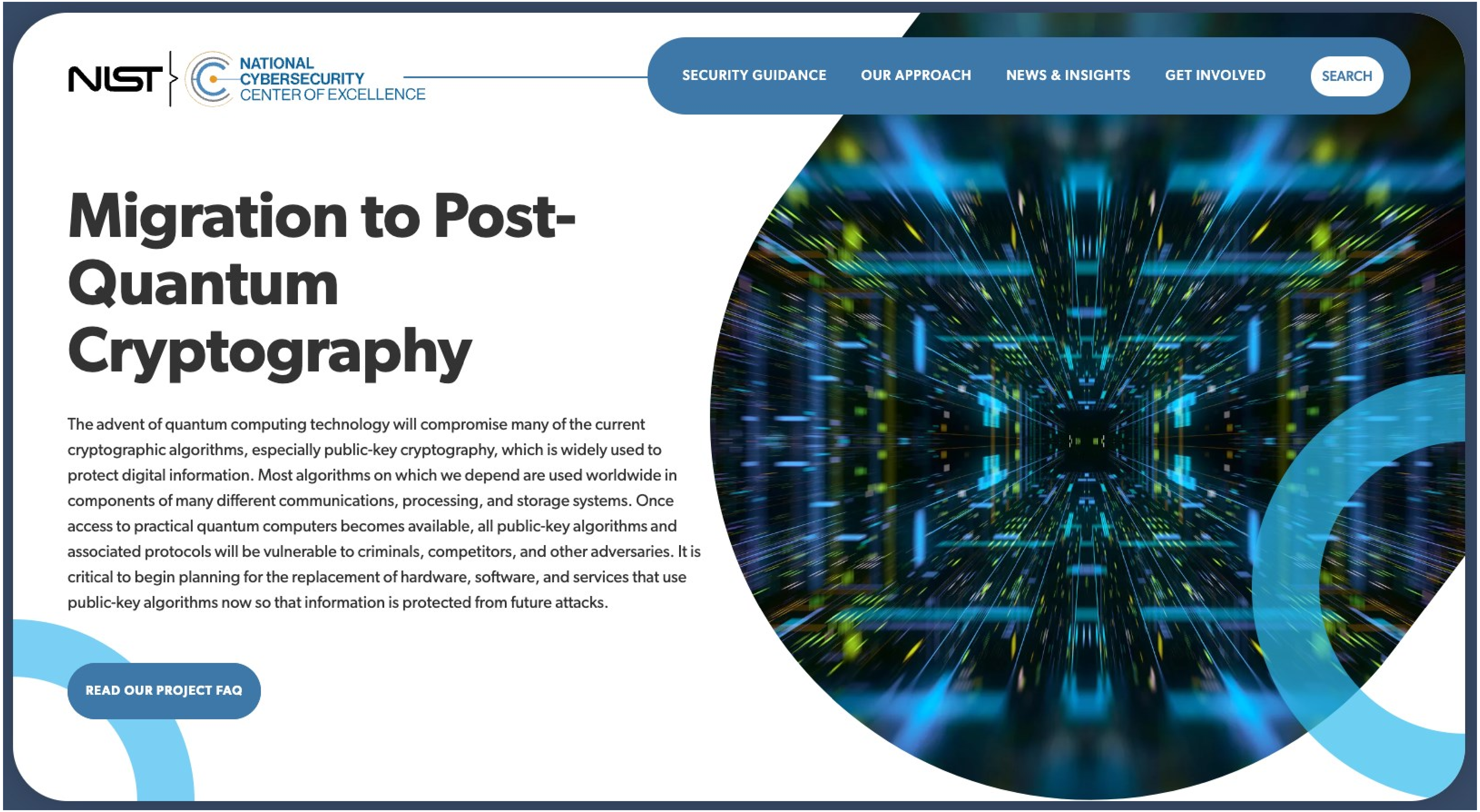
Quantum-Safe Journey

Migrating to PQC (Post-Quantum Cryptography)

Suvi Lampila
SSH Fellow

SSH



Migration to Post-Quantum Cryptography

The advent of quantum computing technology will compromise many of the current cryptographic algorithms, especially public-key cryptography, which is widely used to protect digital information. Most algorithms on which we depend are used worldwide in components of many different communications, processing, and storage systems. Once access to practical quantum computers becomes available, all public-key algorithms and associated protocols will be vulnerable to criminals, competitors, and other adversaries. It is critical to begin planning for the replacement of hardware, software, and services that use public-key algorithms now so that information is protected from future attacks.

Post Quantum Cryptography

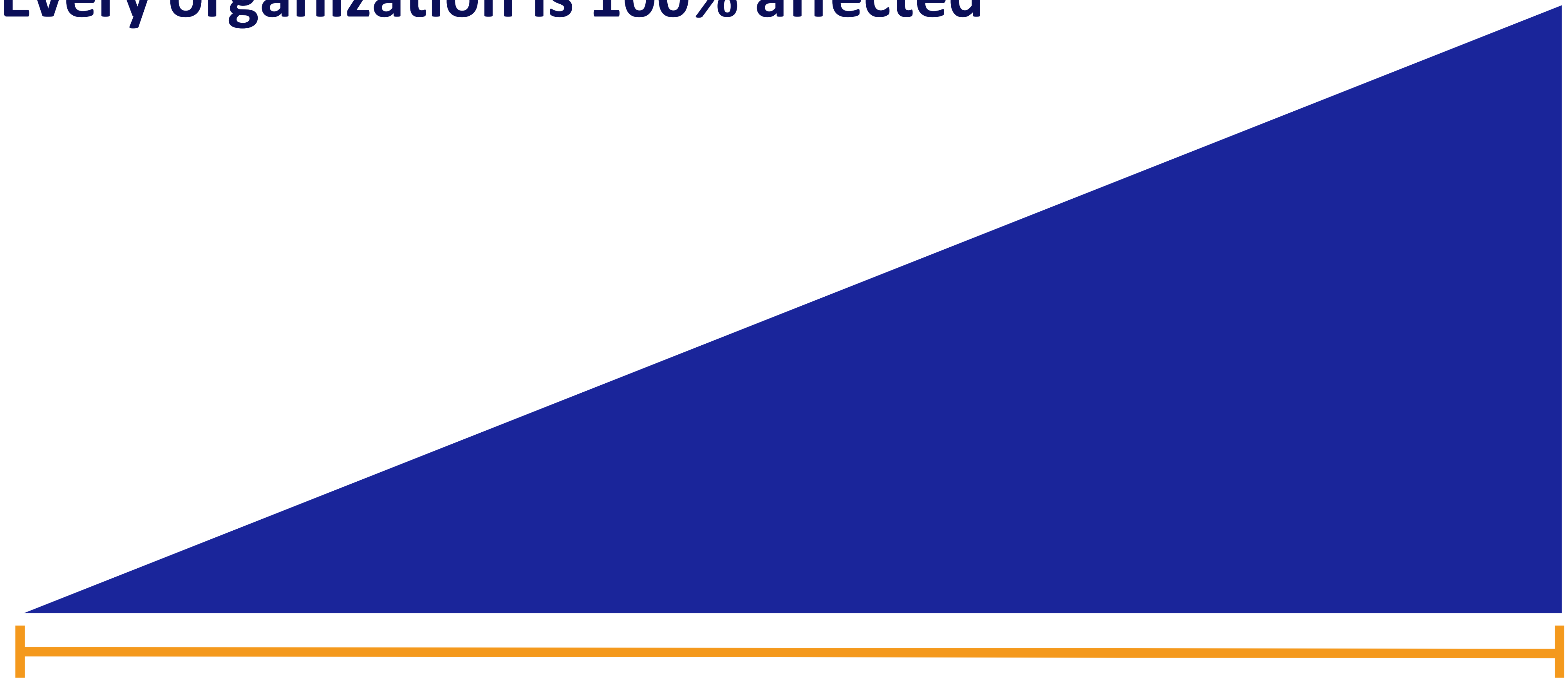
~~P~~ost Quantum

Quantum Safe

Cryptography

NOW

Every organization is 100% affected



Embarrassing

Existential Crisis

Large-scale quantum computers do not exist yet, but your secrets do.

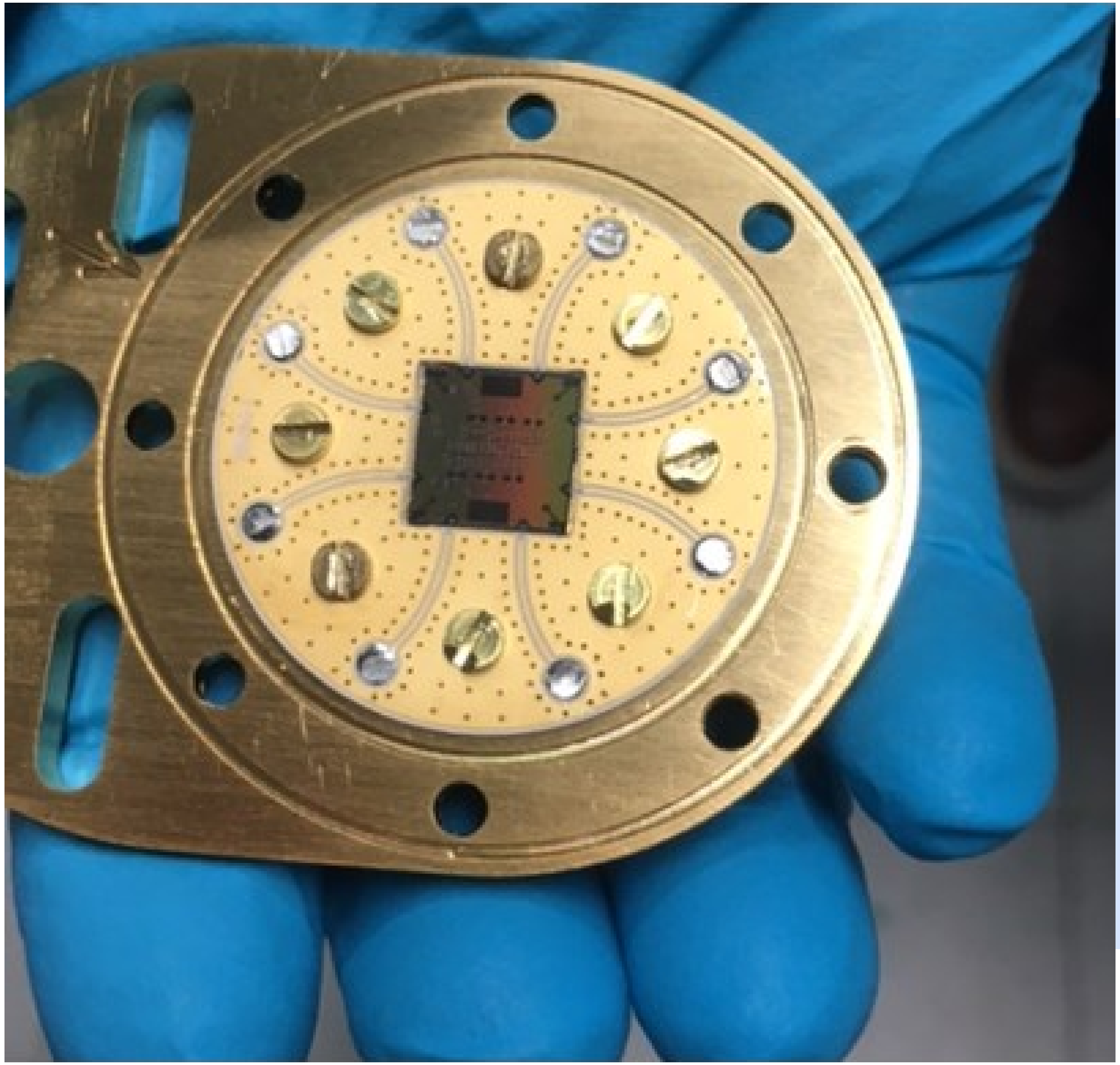
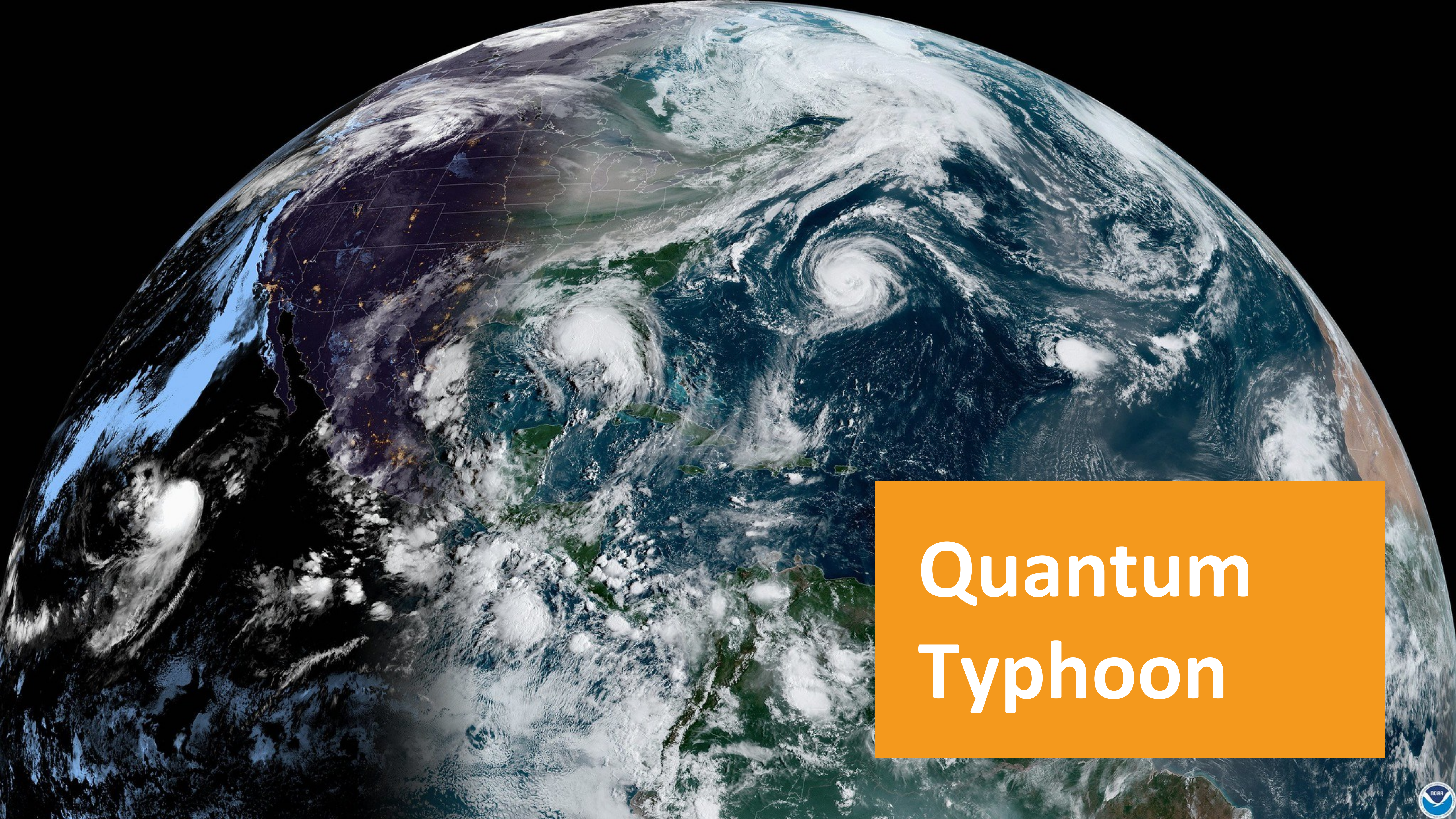


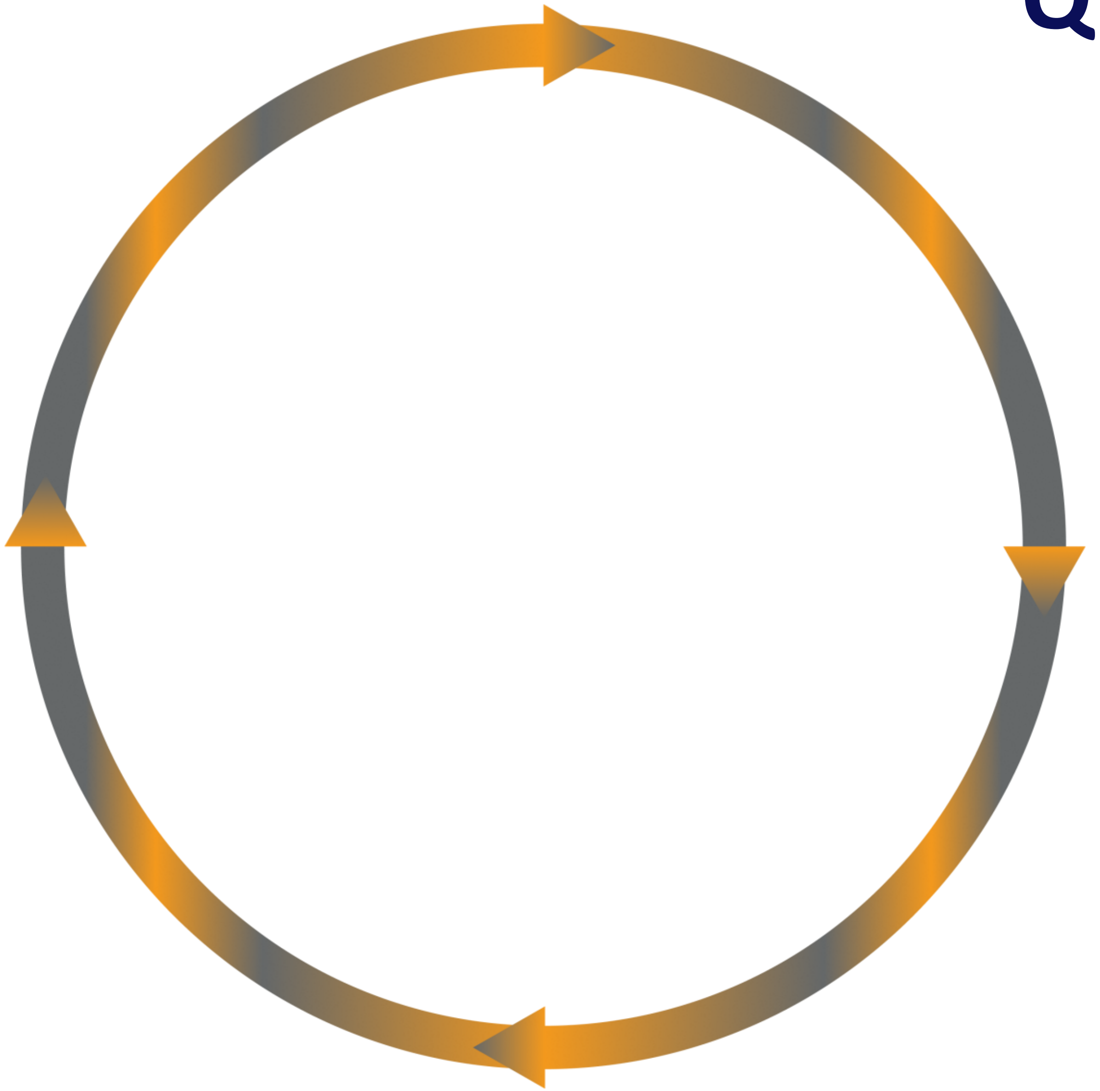
Photo: Jorma Mellin 2021, IQM QPU



Quantum Typhoon

Harvest now, decrypt later is retroactive and often invisible attack.

Quantum-Safe Journey



1 **Discovery** Identify Critical Assets

2 **Prioritize** & Plan Migration Path

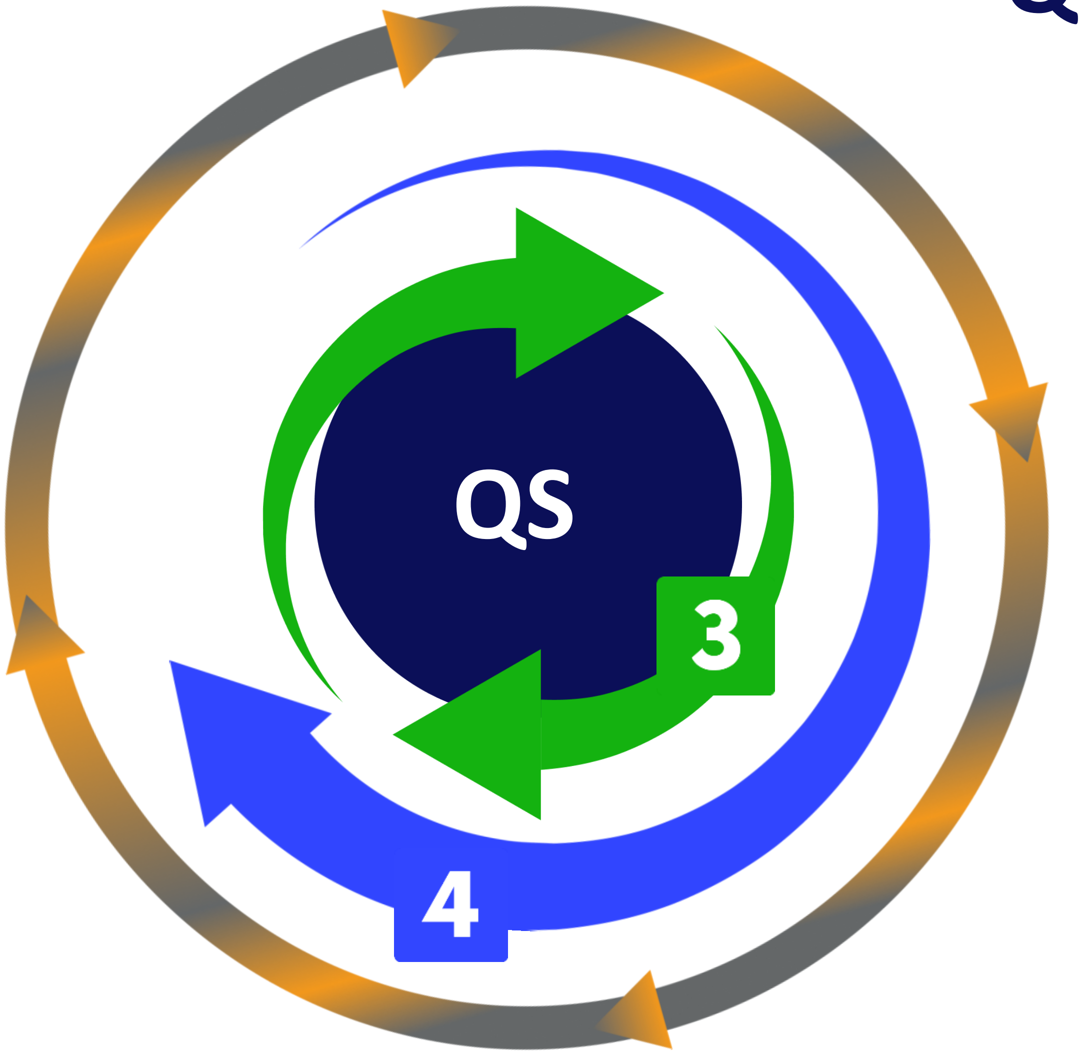
Quantum-Safe Journey

1 **Discovery** Identify Critical Assets

2 **Prioritize** & Plan Migration Path

3 **Deploy** Hybrid Key Exchange (PQC KEM + ECDH)

Quantum-Safe Journey



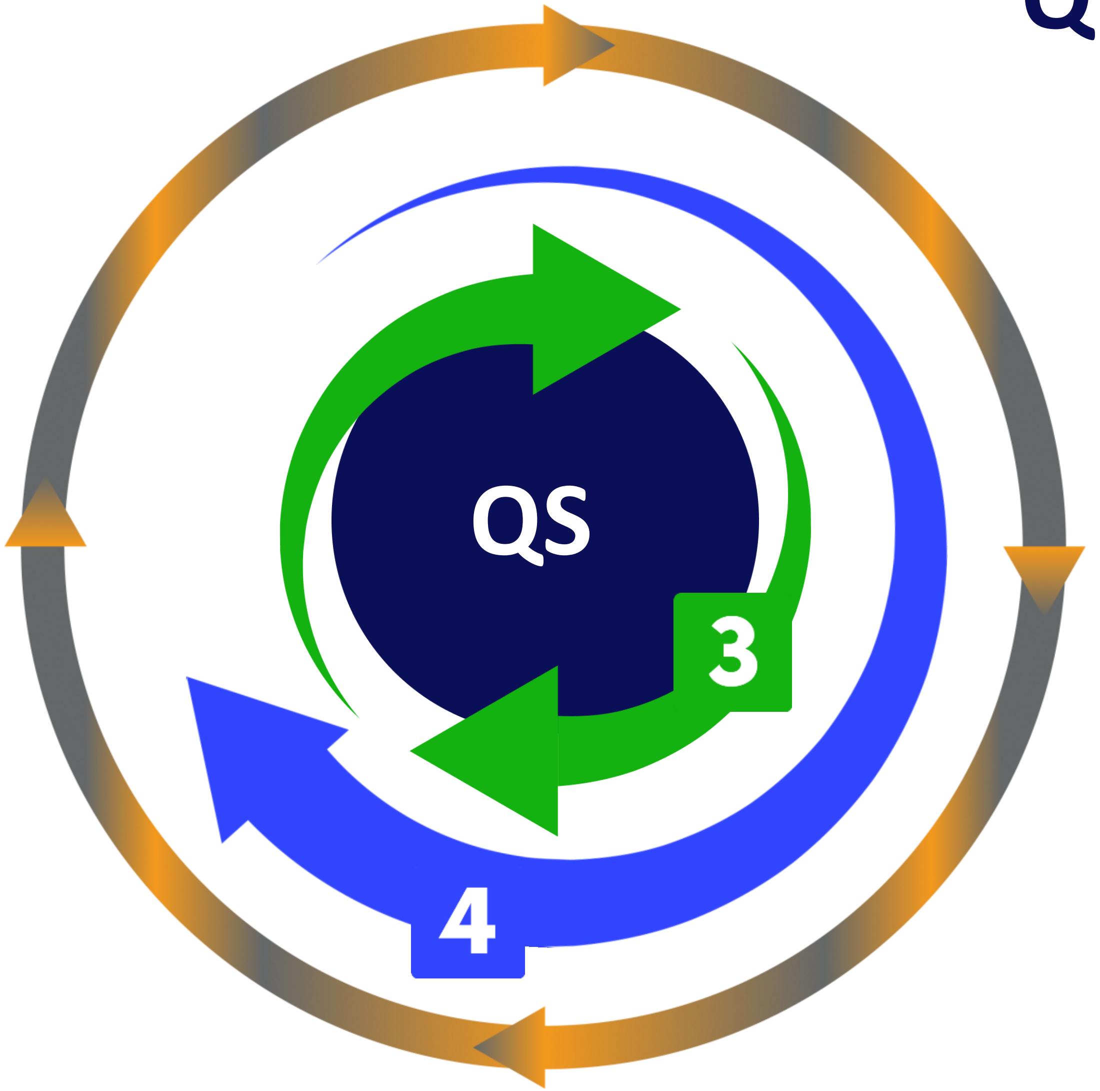
1 **Discovery** Identify Critical Assets

2 **Prioritize** & Plan Migration Path

3 **Deploy** Hybrid Key Exchange (PQC KEM + ECDH)

4 **Discovery** Authentication Key & Certificate Inventory

Quantum-Safe Journey



1 **Discovery** Identify Critical Assets

2 **Prioritize** & Plan Migration Path

3 **Deploy** Hybrid Key Exchange (PQC KEM + ECDH)

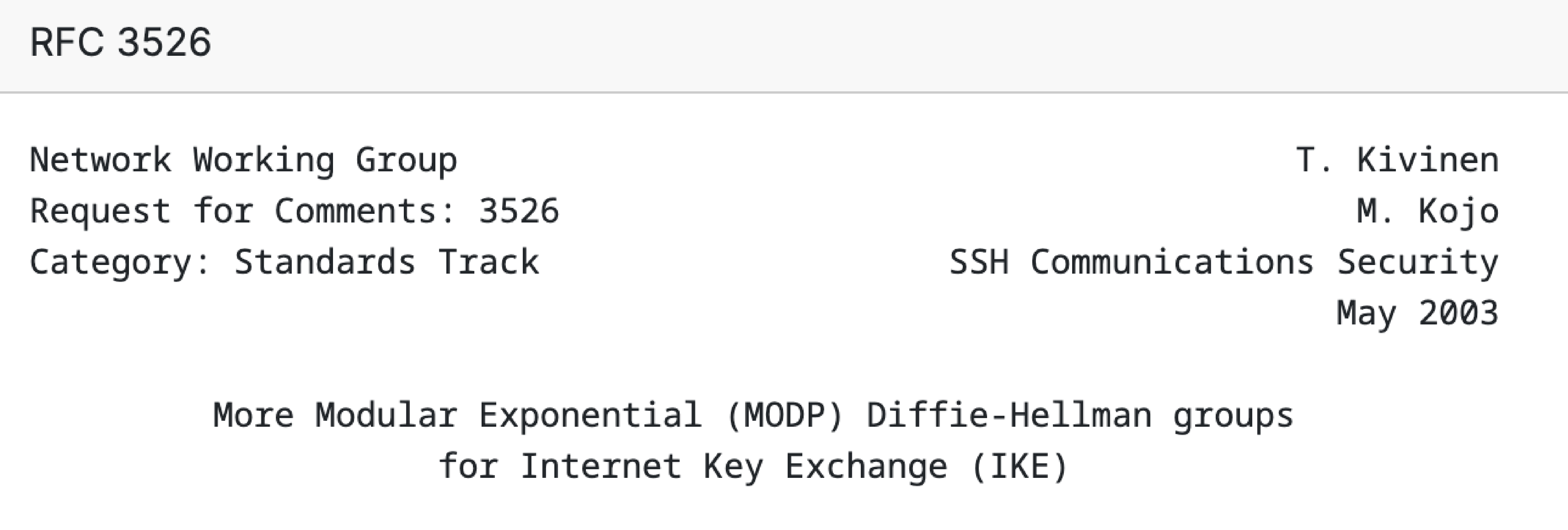
4 **Discovery** Authentication Key & Certificate Inventory

5 **Deploy** PQC Authentication Keys & Certificates
(Before Day One of Quantum Computer)

SSH

“Please don’t break RSA 2048 before I retire.”

Diffie-Hellman Groups also affected when RSA breaks



RFC 3526

```
Network Working Group                                         T. Kivinen
Request for Comments: 3526                                       M. Kojo
Category: Standards Track                    SSH Communications Security
                                                                May 2003

          More Modular Exponential (MODP) Diffie-Hellman groups
                      for Internet Key Exchange (IKE)
```

Prioritize Quantum-Safe Key Exchange

SSH

Quantum-Safe

NOW