De verstrekkende gevolgen van kwantumcomputing voor de overheid

Prof.dr.ir. Nitesh Bharosa

TU Delft DIGICAMPUS

Conclusie

- Kwantumcomputing heeft de potentie om een ontwrichtende impact te hebben op de (digitale) dienstverlening van overheid, banken en telecom.
  - En daarmee op de gehele maatschappij.
- Oproep:
  - Wacht niet op zekerheid over Q-Day. Kwantumveilige cryptografie (PQC) wordt binnen enkele jaren volwassen en landen die daarop voorbereid zijn kunnen de migratie sneller doorlopen.
  - Zorg voor een overkoepelende Governance. De Rijksoverheid dient een leidende rol nemen in de transitie naar kwantumveilige cryptografie.
  - Investeer meer in onderzoek naar kwantumveilige cryptografie (nu minder dan 1% t.o.v. onderzoek naar Kwantumcomputing).
  - Zorg voor Europese afstemming.

TU Delft

Vandaag: veel van onze digitale kritieke infrastructuren zijn afhankelijk van cryptografie

- DigiD, Mijn overheid, Berichtenbox, Digipoort, PKIoverheid, Diginetwerk, e-Herkenning, end-end communicatie
- Internet Bankieren, IDEAL, SWIFT, VISA, Mastercard
- Beldiensten, Internetdiensten, digitale televisie, WIFI, LORA
- Ook andere datadelings-infrastructuren in Zorg (LSP), Energie (ESDN), Hypotheken (HDN), Verzekeringen (ADN) etc.

Stel je eens dit persbericht in de toekomst voor

China is geslaagd in het ontwikkelen van een kwantumcomputer die Shor's algoritme kan toepassen voor het breken van huidige encryptie-technieken.

Het is Q-Day!

Technische impact van kwantumcomputers

- Veel meer rekenkracht + Shor's Algoritime = breken huidige cryptografie.
- Risico = waarschijnlijkheid kwantumcomputer X Impact.

Impact hoog op:

- **Vertrouwelijkheid** van verbindingen en gegevens niet meer gewaarborgd. Store now, decrypt later. Onthulling en misbruik.
- **Integriteit** niet meer gewaarborgd. Wie zit achter het bericht, is het echt en is het niet stiekem aangepast? Vervalsing van een digitale handtekening
- **Beschikbaarheid** van digitale diensten niet meer gegarandeerd.

Maatschappelijke impact

Overheid:

- Mensen kunnen geen veilig gebruik meer maken van DigiD
- Medewerkers van Defensie en in ziekenhuizen kunnen niet meer veilig inloggen
- Bedrijven kunnen niet meer veilig belastingaangifte doen

Banken:

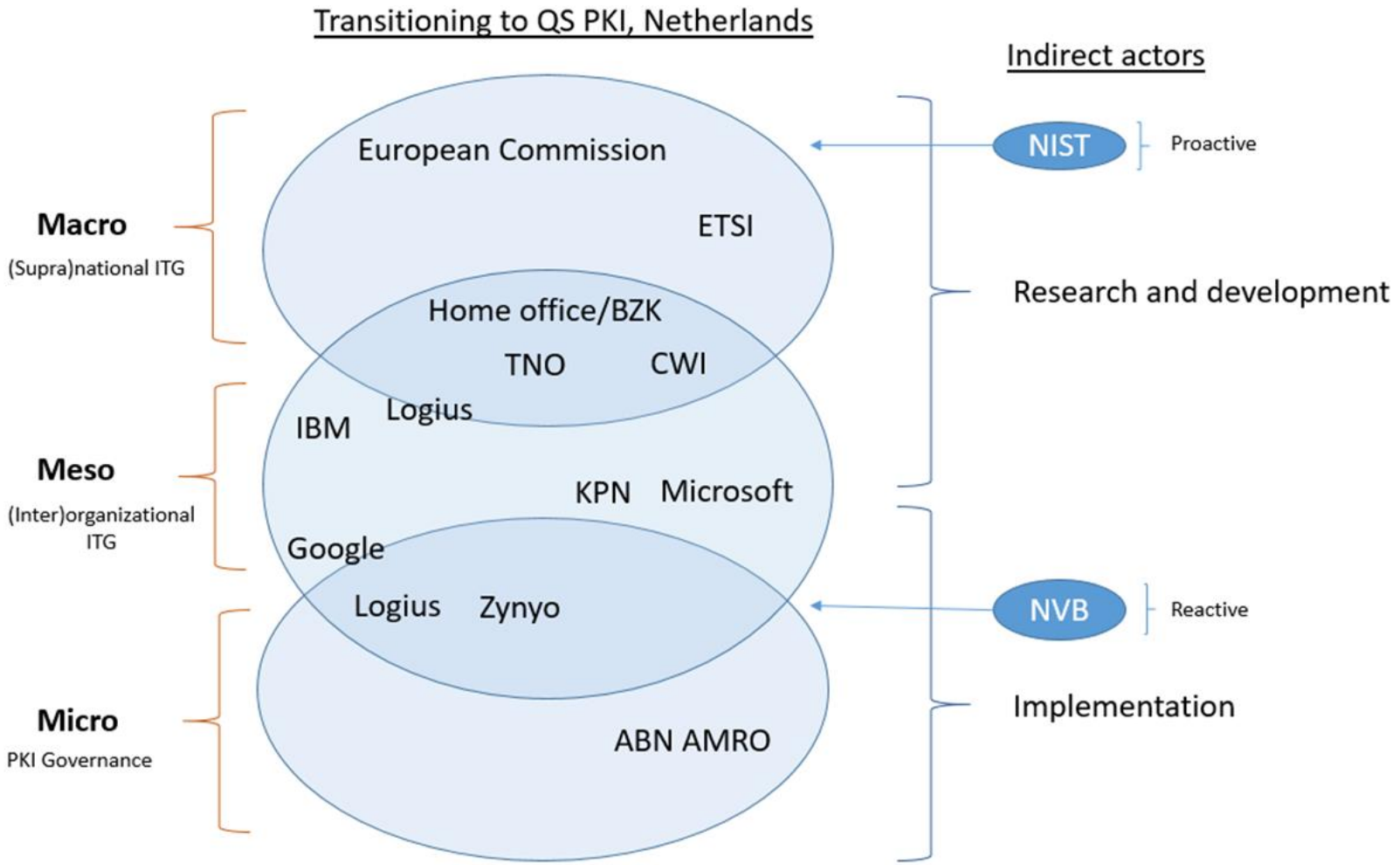
- Mensen kunnen geen geld meer overmaken
- Mensen kunnen niet meer pinnen bij de supermarket
- De integriteit van een hypotheek-overeenkomst is niet meer te garanderen

Telecom:

- Telefoongesprekken kunnen eenvoudig worden afgeluisterd
- Degene die belt met een bekend nummer kan iemand ander zijn
- Bedrijfsspionage

TU Delft

De complexe governance-opgave: er is geen overkoepelende gremium



Urgentie

- Niemand weet zeker wanneer Q-day komt.
- De overgang van SHA-1 naar SHA-2 in het bancaire stelsel heeft 10 jaar geduurd.
- Dit was een reguliere en voorspelbare update.
- Post kwantum cryptografie is geen reguliere update.
- Er zijn allerlei onzekerheden rond hardware, de performance van hybride architecturen en interoperabiliteit.
- Alleen al op vertrouwelijkheid te waarborgen (impact van store now, decrypt later) is het noodzakelijk om al bij de beschikbaarheid van post quantum cryptografie te migreren.

Wetenschappelijke onderbouwing

- Joseph, e.a. (2022). Transitioning organizations to post-quantum cryptography. Nature, 605(7909), 237–243.
- Kong, Janssen, Bharosa (2022). Challenges in the Transition towards a Quantum-safe Government. DG.O 2022: The 23rd Annual International Conference on Digital Government Research . P.282–292.
- Klunder, Bharosa, Meijaard, Klaver (2023). A Method for Analysing the Societal Risk of Quantum Computing. HAPKIDO deliverable 1.1.
- Meijaard, Spagnuelo, Bharosa (under review). The Societal Risk of Quantum Computing for Public-Key Infrastructures in Government, Banking and Telecom. HAPKIDO Deliverable 1.2.