

▶ **POST-QUANTUM CRYPTOGRAPHY MIGRATION MANUAL**

VINCENT DUNNING

16 juni 2022

› AGENDA

QUANTUM COMPUTERS

CRYPTOGRAPHY

TIMELINES

MIGRATION MANUAL

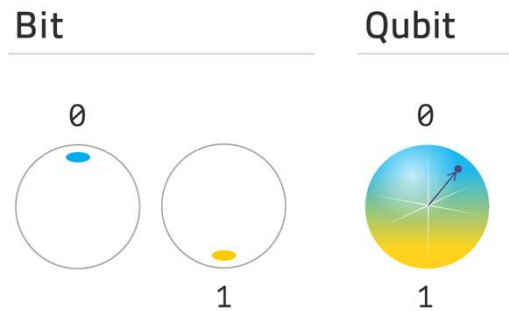
PERSONAS

ACTION STEPS

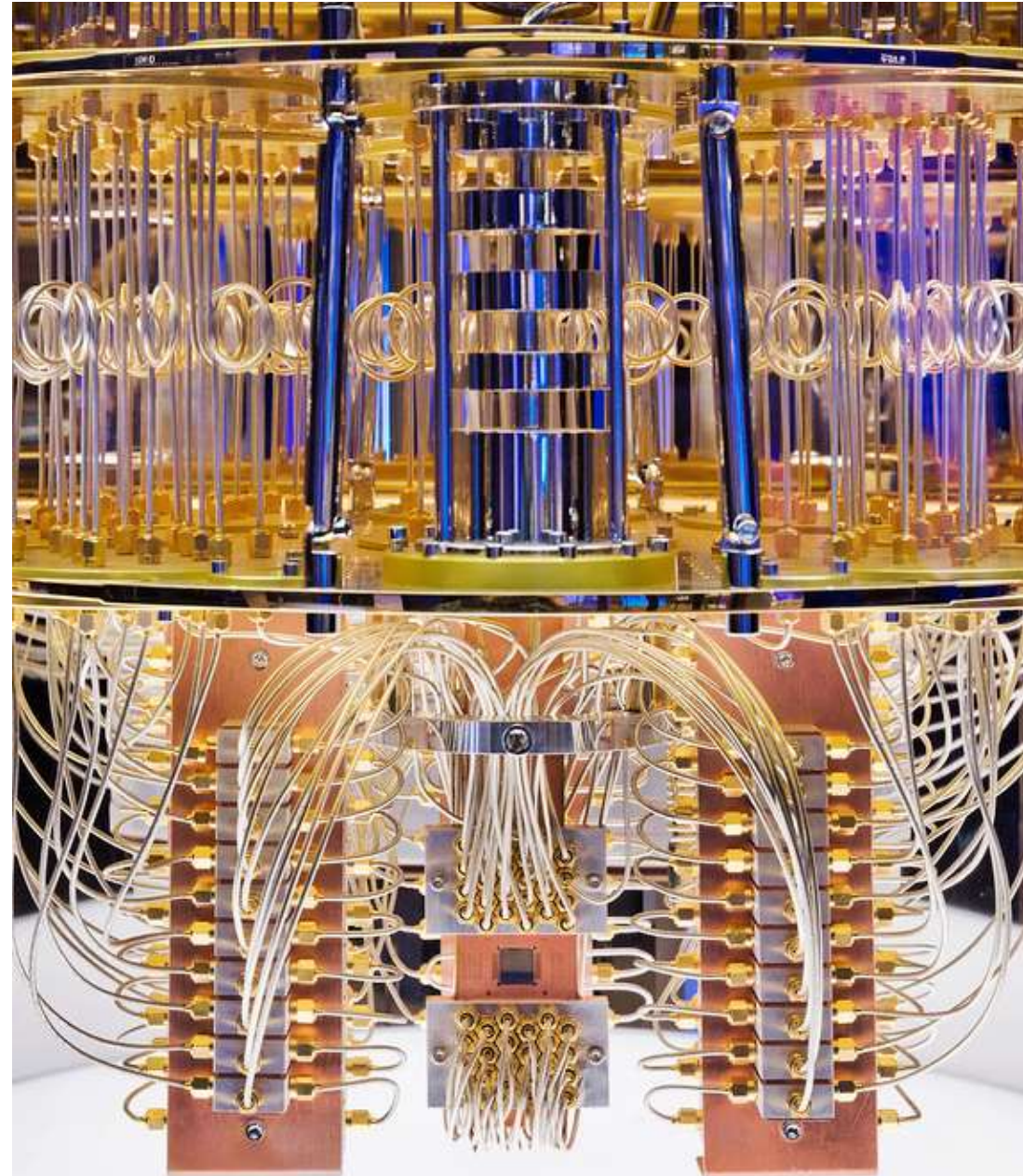
CONCLUSION

QUANTUM COMPUTERS

- › Use so-called *qubits* instead of bits



- › Work fundamentally different than traditional computers (not “supercomputer”)
- › Quantum algorithm potentially much faster than traditional algorithms with the same purpose
- › In 1990 2 qubits, nowadays ~100 qubits



› MODERN CRYPTOGRAPHY

› Symmetric cryptography

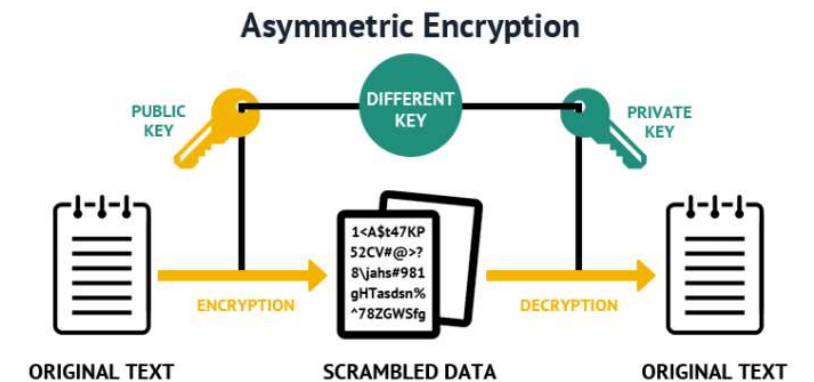
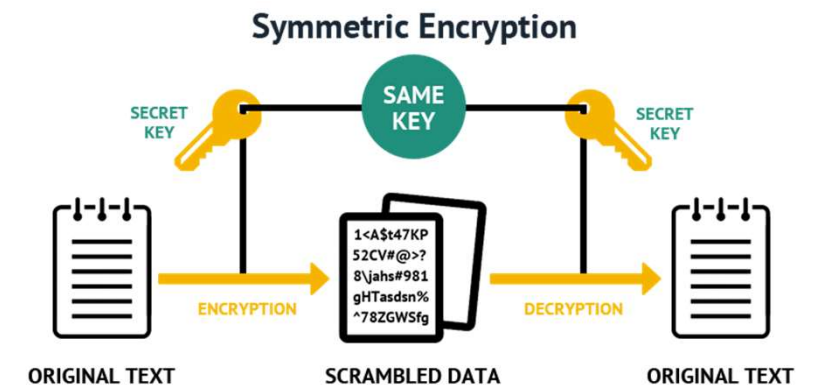
- › One key for both encryption and decryption
- › Require agreement on this shared key

Weakened by quantum attacks

› Asymmetric (“public-key”) cryptography

- › Separate keys for encryption (*public key*) and decryption (*private key*)
- › Security based on “hard” problems
- › Often used to setup shared symmetric key

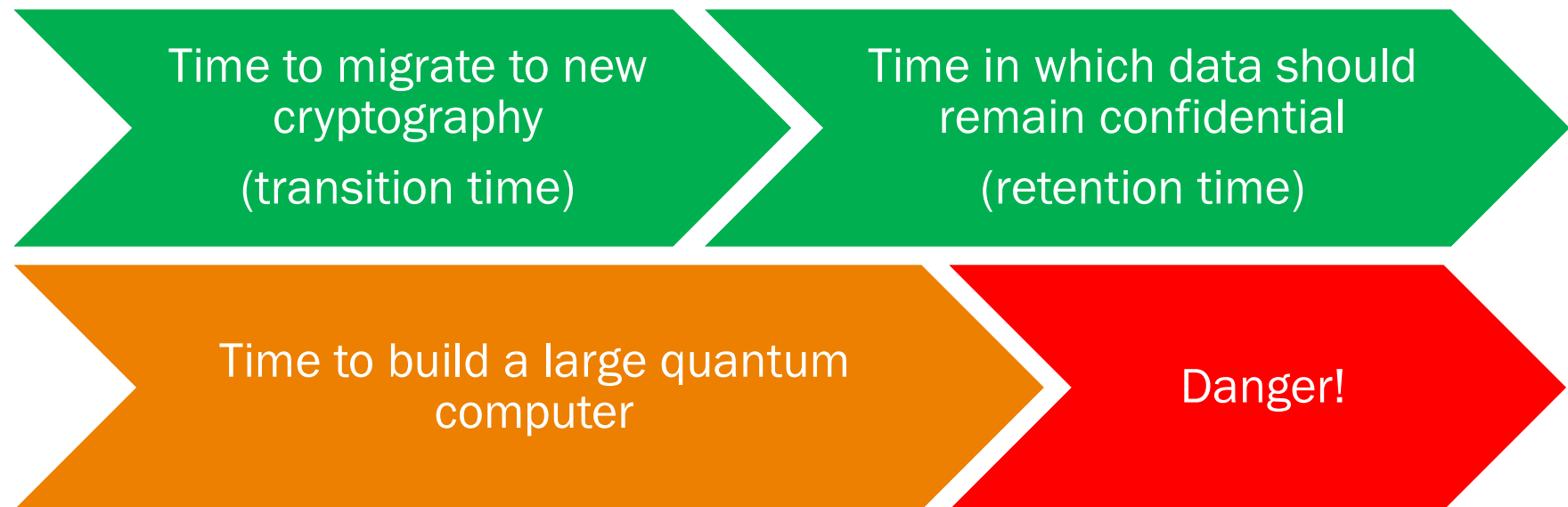
Broken by quantum attacks



› TIMELINES

WHY SHOULD WE CARE?

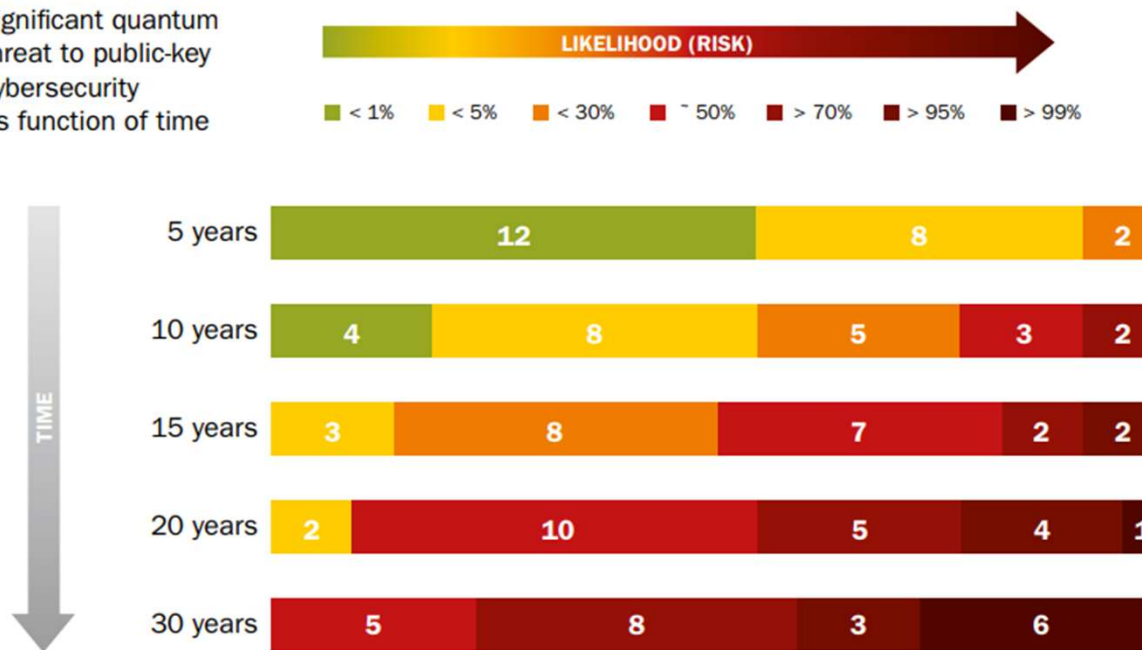
› Mosca's inequality (2015): Estimation of urgency



› TIMELINES

WHEN WILL A QUANTUM COMPUTER BECOME AVAILABLE?

Expert opinions on the likelihood of a significant quantum threat to public-key cybersecurity as function of time



Numbers reflect how many experts (out of 22) assigned a certain probability range.

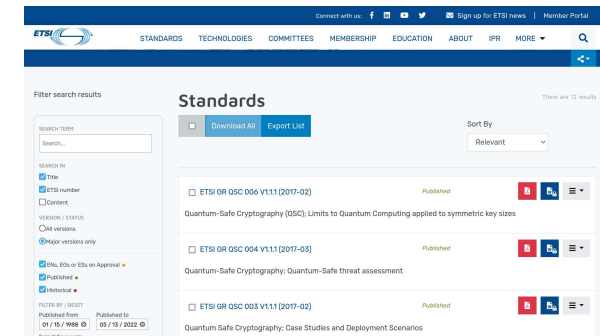
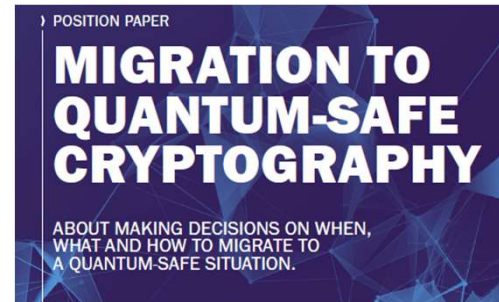
Source:
M. Mosca and M. Piani,
Quantum Threat
Timeline Report, Global
Risk Institute, 2019

Figure 2: Expert opinions on breaking RSA-2048 with a quantum computer

› TIMELINES

WHAT IS BEING DONE ALREADY?

- › TNO: position paper on migration
- › AIVD: Recommendations for mitigating risks of quantum computer
- › NIST standards (2024?)
- › ETSI: Analysis and best practices for post-quantum cryptography
- › ENISA
- › BSI



› **PQC MIGRATION MANUAL**

CONCRETE ADVICE

- › “Should I even worry already?”
- › Different organisations have different “personas”
- › Based on persona certain action steps should be taken
- › Some personas do not have to worry right now...

PERSONAS

3 CATEGORIES



Urgent adopters

- Sensitive information
- Long-lived systems
- Critical infrastructure



Cryptographic experts

- Standards
- Suppliers of cryptographic solutions
- Dependencies



Regular adopters

- No risk right now
- Can wait for verified implementations & standards

› ACTIONS



1. DIAGNOSIS

- CRYPTOGRAPHIC INVENTORY
- SMOOTHENS MIGRATION & UPDATES
- ALSO FOR REGULAR ADOPTERS



2. PLANNING

- DEPENDENCIES BETWEEN CRYPTOGRAPHIC ASSETS
- ALTERNATIVES
- BUSINESS PROCESSES

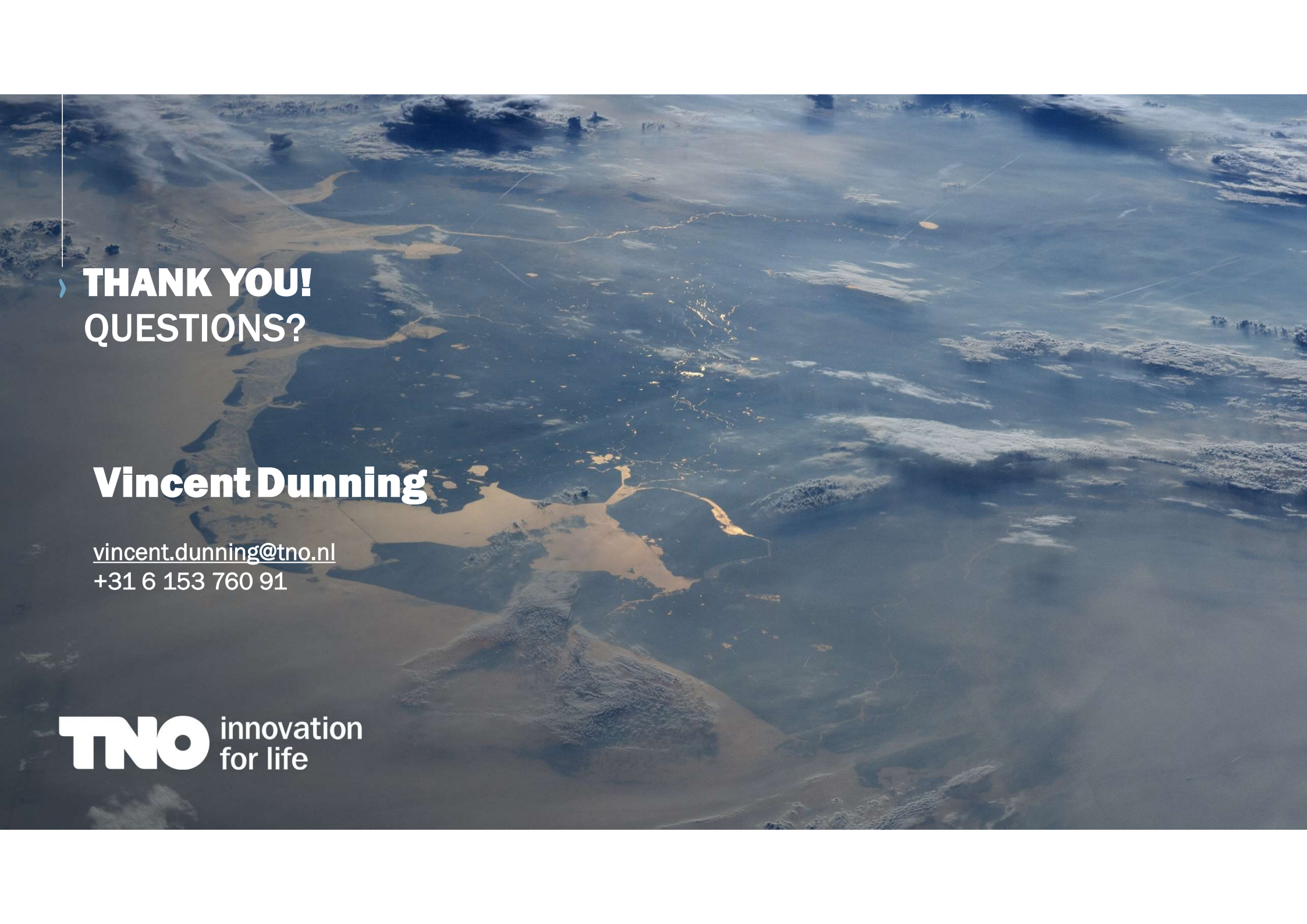


3. EXECUTION

- ISOLATION & DOWNTIME
- AGILITY

› CONCLUSION

- › Quantum computers threaten modern cryptography
- › For some organisations action is required already
 - › “Store-now-decrypt-later”
 - › Long-lived systems
- › Manual to identify the urgency & concrete action steps



› **THANK YOU!**
QUESTIONS?

Vincent Dunning

vincent.dunning@tno.nl
+31 6 153 760 91

TNO innovation
for life