ETSI/IQC Quantum Safe Cryptography Event

Preparing for the inevitable getting ready for the post-quantum world

Dr. Joanna Sliwa

Dr.-Ing. Konrad Wrona

Duarte Silva, Alim Solmaz Ph.D, Tsvetelina Shabanska

NATO Communications and Information Agency

14/02/2023

Agenda

- NATO Quantum technology strategy
- Approach to transition to post – quantum cryptography
    - Technology studies
- Summary

NATO quantum technology strategy

- Quantum Information Science (QIS) has the most revolutionary promise of all the applications of quantum technologies and is potentially a game changing technology for future military operational environment
    - QIS: the study of second-generation quantum enabled information science, including the R&D of quantum computers, algorithms, cryptography, programming languages, modelling, simulation, and knowledge applications

NATO Science & Technology Organisation (STO), *Quantum Review – Summary Report, 2021*

- Application of QIS can be both a threat and an advantage for the NATO Alliance

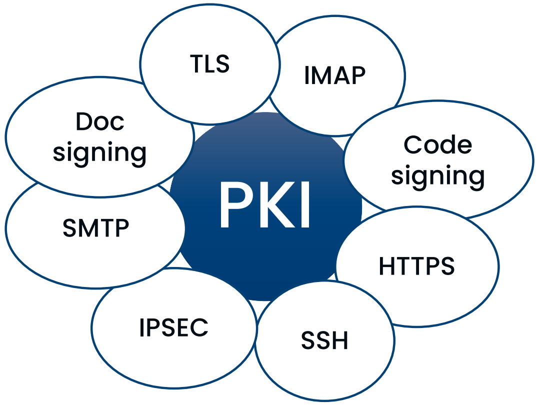
Quantum as a threat to cryptography

NATO Response to the Quantum Threat to Cryptography defines action plan on how information should be protected against the quantum threat

It covers systems of different classification levels

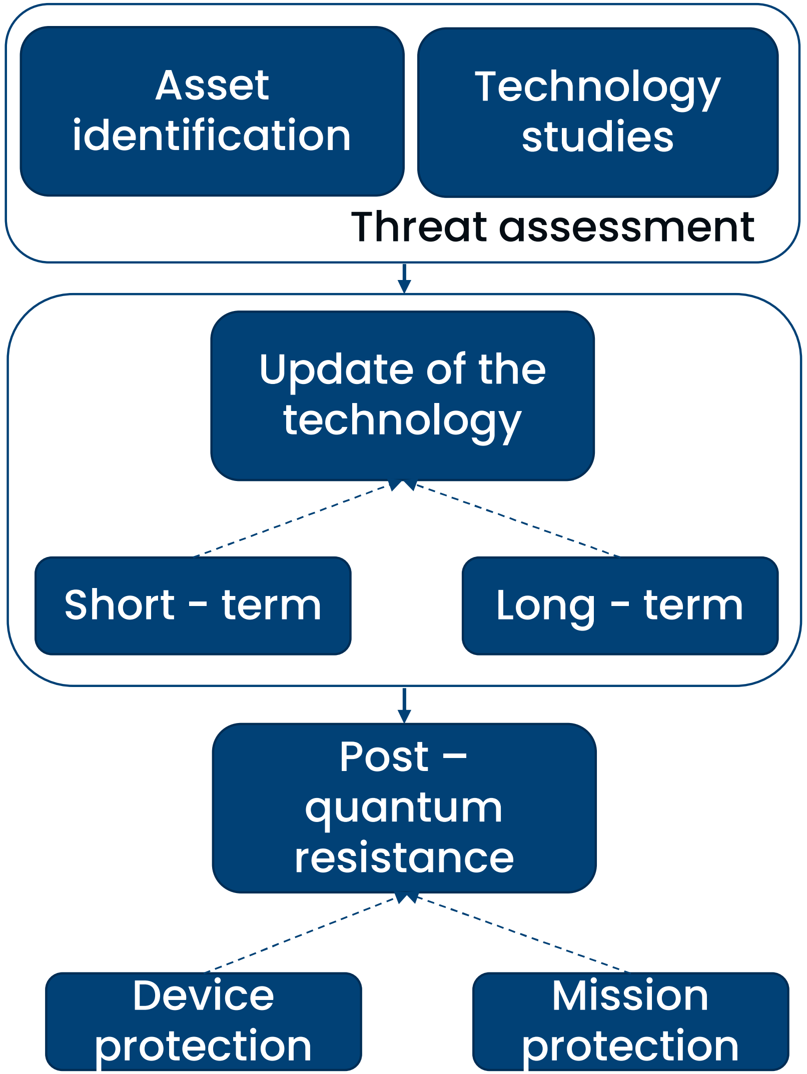
It assumes:

- Very high risk to asymmetric, or public key cryptography like the Rivest-Shamir-Adleman (RSA) and Elliptic-Curve Diffie-Hellman (ECDH) algorithms



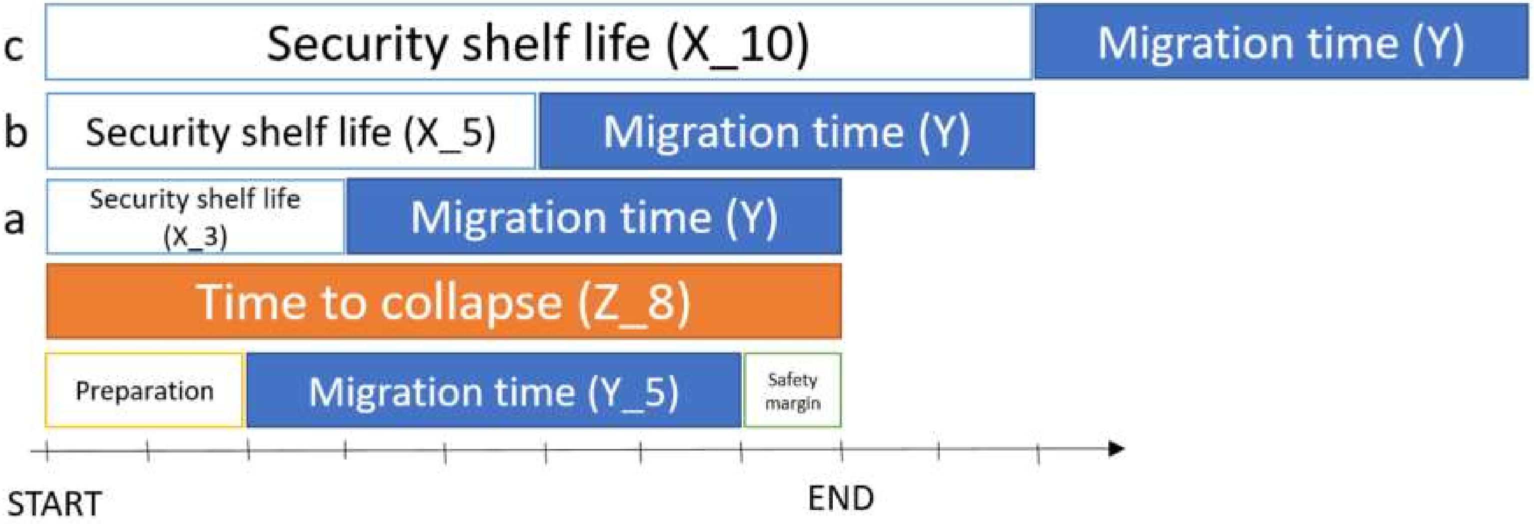
Transition plan

The overall objective is to ensure that NATO information and systems are not vulnerable to attack from a quantum computer

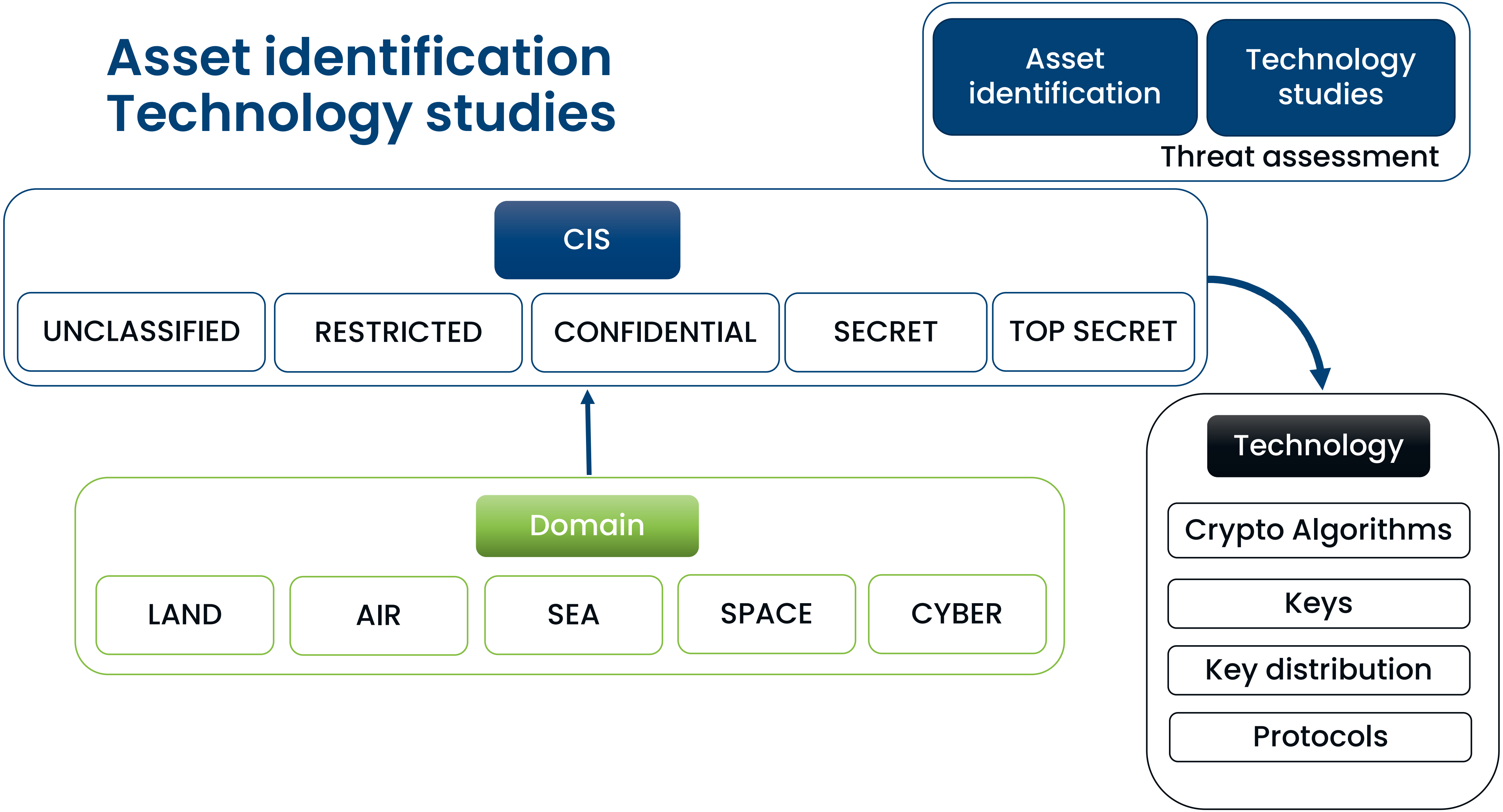


Preliminary steps

- Awareness and competence
- Cryptographic agility
- Planning timeframe
    - Consider “Harvest Now, Decrypt Later” attack



Asset identification
Technology studies



Asset identification

Technology studies

Threat assessment

CIS

UNCLASSIFIED

RESTRICTED

CONFIDENTIAL

SECRET

TOP SECRET

Domain

LAND

AIR

SEA

SPACE

CYBER

Technology

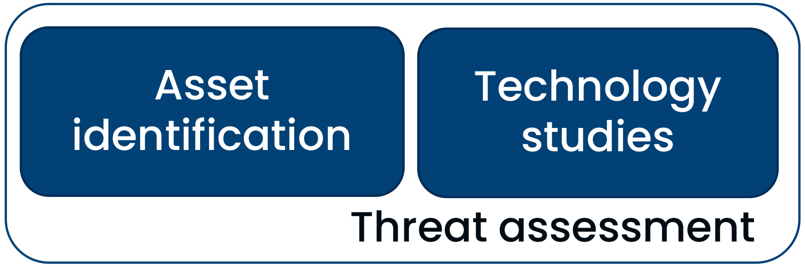
Crypto Algorithms

Keys

Key distribution

Protocols

Technology studies
NCIA + CMRE

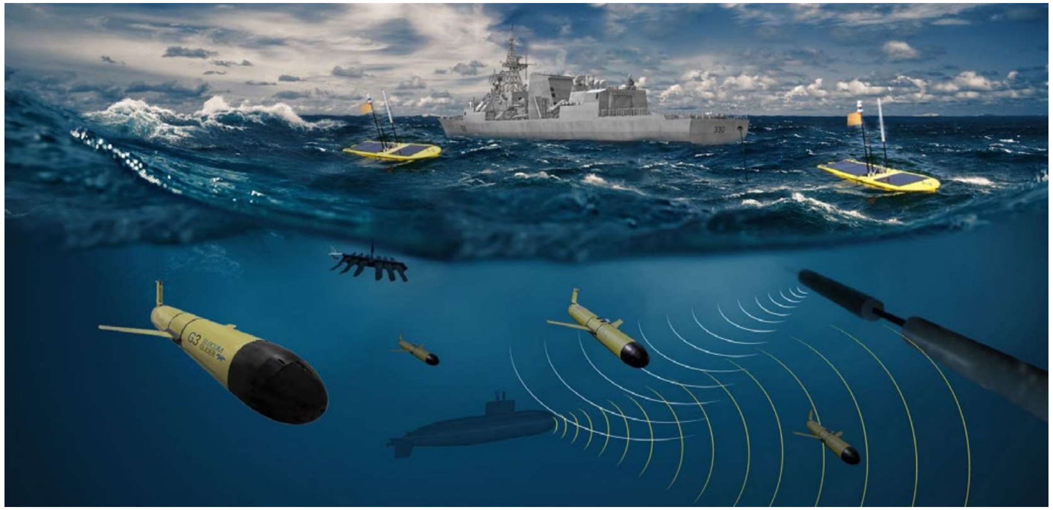


Asset identification

Technology studies

Threat assessment

- Assumptions: mobile, constrained devices (low energy, low throughput, limited CPU and RAM)
- Verification of post – quantum cryptographic algorithms' overhead in terms of their energy consumption and identification of challenges of their application in constrained IoT devices
- Planning of new communications schemes for underwater communication

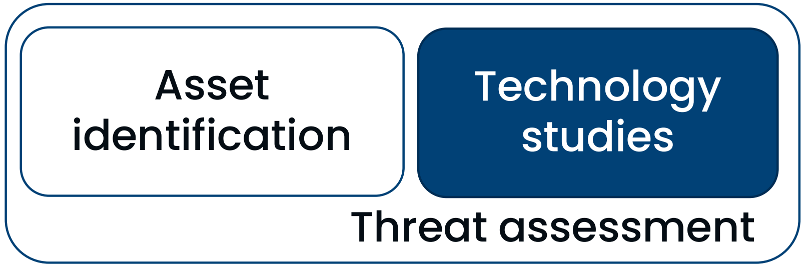


NATO OTAN

SCIENCE & TECHNOLOGY ORGANIZATION
CENTRE FOR MARITIME RESEARCH & EXPERIMENTATION

S&T organization CMRE

Technology studies
QRNG



When implementing new cryptography, independently evaluate and validate solutions

- Quantum Safe Random Number Generator implemented in hardware
    - Not all chips are created equal, even in the same family
    - Software sometimes is built on assumptions of the hardware used
    - Test suites developed to validate the quality for RNGs are still valid for QRNGs
        - FIPS-140-3 (Security Requirements for Cryptographic Modules)
        - NIST SP 800-22 (Statistical Test Suite for Random and PRNG for Cryptographic Applications)
        - NIST SP 800-90B (Entropy Estimation Tests)
    - If it fails in randomness tests, it is insecure
        - Post-processing needed ?

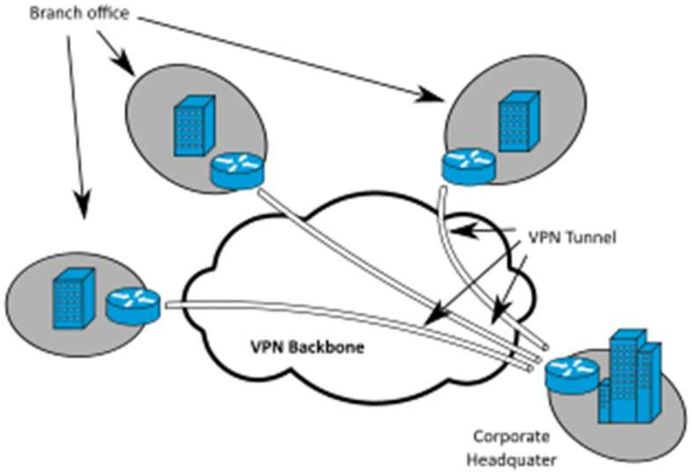
Technology studies VPN

Asset identification

Technology studies

Threat assessment

- Quantum-safe algorithms implemented in OpenVPN:
  - NIST reference implementations (e.g. CRYSTALS-KYBER, NTRU, SABER)
  - Data leakage – what if the protocol or the hosts establishing the connection is exposed?
  - Resiliency and robustness
  - Messages sizes
  - Connection establishment time



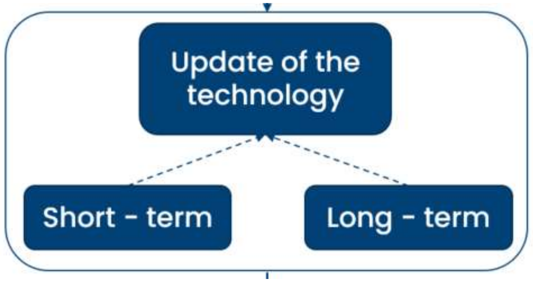
VPN

Outermost layer defense mechanism

Vulnerable to external attackers (nation state actors)

Store-now decrypt-later attacks

What are possible solutions?



Symmetric key crypto

Interim solution with trade-offs

Scaling is a big challenge

Hybrid solution

Combine:

- Classical asymmetric crypto
- Symmetric crypto
- Post-quantum asymmetric crypto

Requires changes to many established protocols

Post-quantum asymmetric key crypto

Long term solution

Relatively new and less extensively tested compared to classical crypto

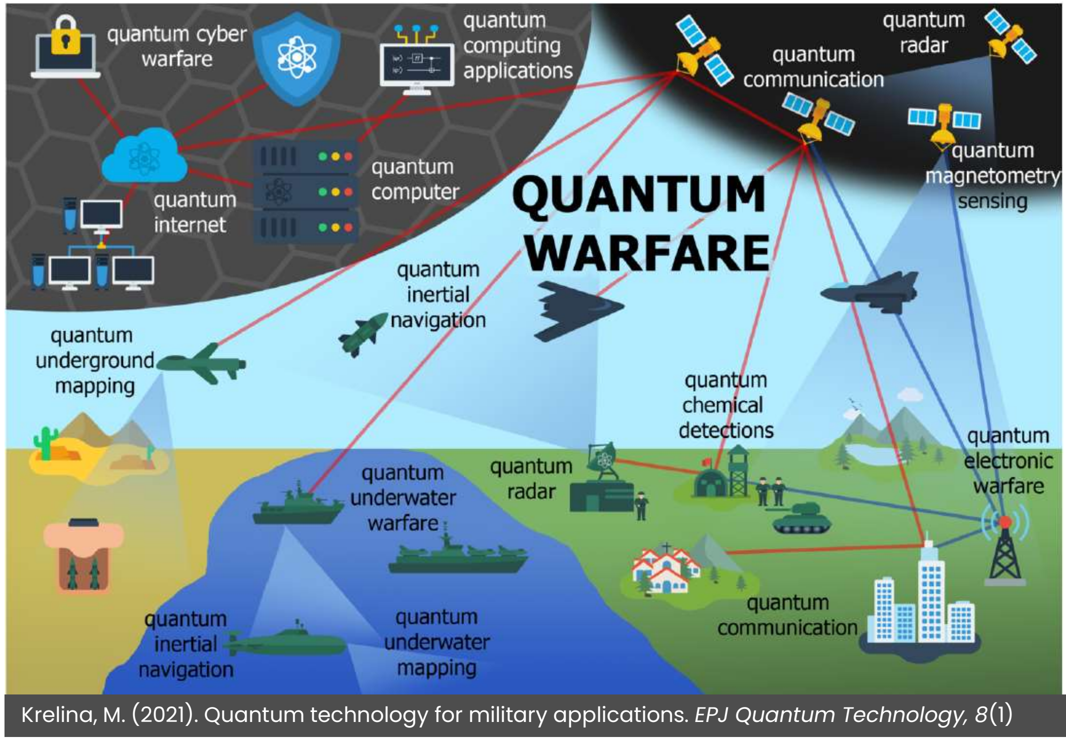
Recently revealed winners of the 3rd round of the NIST Post–Quantum competition

Quantum as an advantage

Quantum technologies support significant advancements primarily in:

- Quantum Sensing, Position, Navigation & Timing
- Quantum Communications
- Quantum Key Distribution
- Quantum Random Number Generators
- Quantum Information Science

These Emerging and Disruptive Technologies (EDTs) have the potential to drive innovations in diverse military applications


quantum cyber warfare
quantum computing applications
quantum communication
quantum radar
quantum internet
quantum computer
quantum magnetometry sensing
QUANTUM WARFARE
quantum inertial navigation
quantum underground mapping
quantum chemical detections
quantum underwater warfare
quantum radar
quantum electronic warfare
quantum communication
quantum inertial navigation
quantum underwater mapping

Krelina, M. (2021). Quantum technology for military applications. *EPJ Quantum Technology*, *8*(1)

Summary (1/2)

Post-quantum world

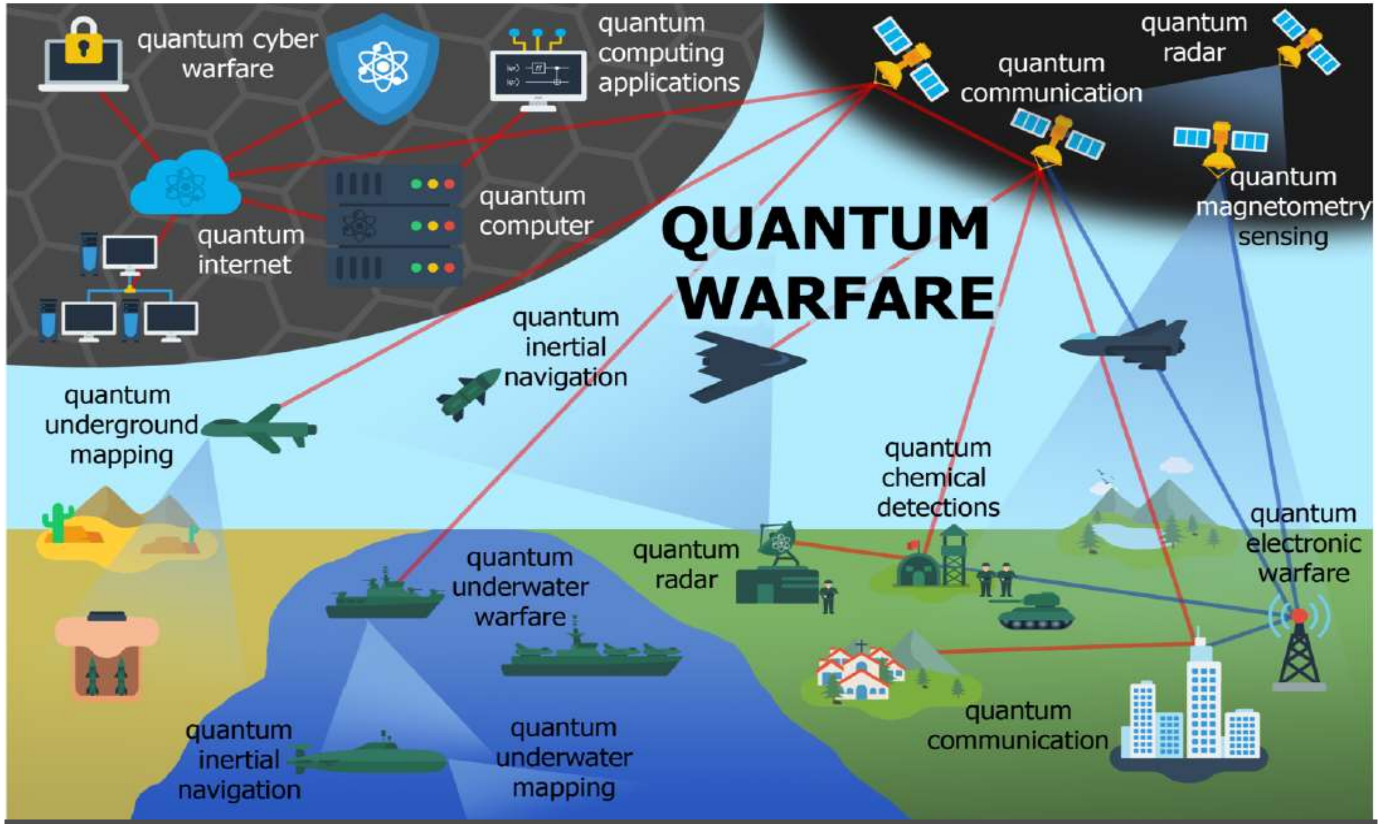
Quantum – resistant CIS infrastructure

- Complex infrastructure requires coordinated approach to transition
- A number of NATO systems is based on symmetric cryptography
- Potentially vulnerable assets have been identified and technology studies are taking place in order to select the best short – terms and long term measures
- NATO needs standardized solutions to continuously provide interoperability among the Allied forces
    - NATO uses public standards
    - NATO produces Standardization Agreements, so called STANAGS

Summary (2/2)

Post-quantum world

Quantum superiority


quantum cyber warfare
quantum computing applications
quantum communication
quantum radar
quantum internet
quantum computer
quantum magnetometry sensing
QUANTUM WARFARE
quantum inertial navigation
quantum underground mapping
quantum chemical detections
quantum radar
quantum underwater warfare
quantum electronic warfare
quantum communication
quantum inertial navigation
quantum underwater mapping

Krelina, M. (2021). Quantum technology for military applications. *EPJ Quantum Technology, 8*(1)

Thank you for your attention

joanna.sliwa@ncia.nato.int
konrad.wrona@ncia.nato.int