Paving the road towards quantum-safe communications for the Alliance

Quest-IS: Quantum Communications – Towards a Quantum Internet Infrastructure

Dr Joanna SLIWA, Dr. Ing. Konrad WRONA, Mikolaj PIETRUCZUK, NATO Cyber Security Center, NCIA

Agenda

- Innovation in NATO context
- Innovation Continuum exercises
- Cryptographic agility and resilience
- An outline of the experimental validation planned for the NATO Innovation Continuum 2025 (IC25)

Innovation in NATO context

Allied Command Transformation
Norfolk, Virginia | USA

NATO's Strategic Warfare Development Command
- Strategic Thinking
- Development of Capabilities

Innovation
- S&T
- Outreach
- Producers

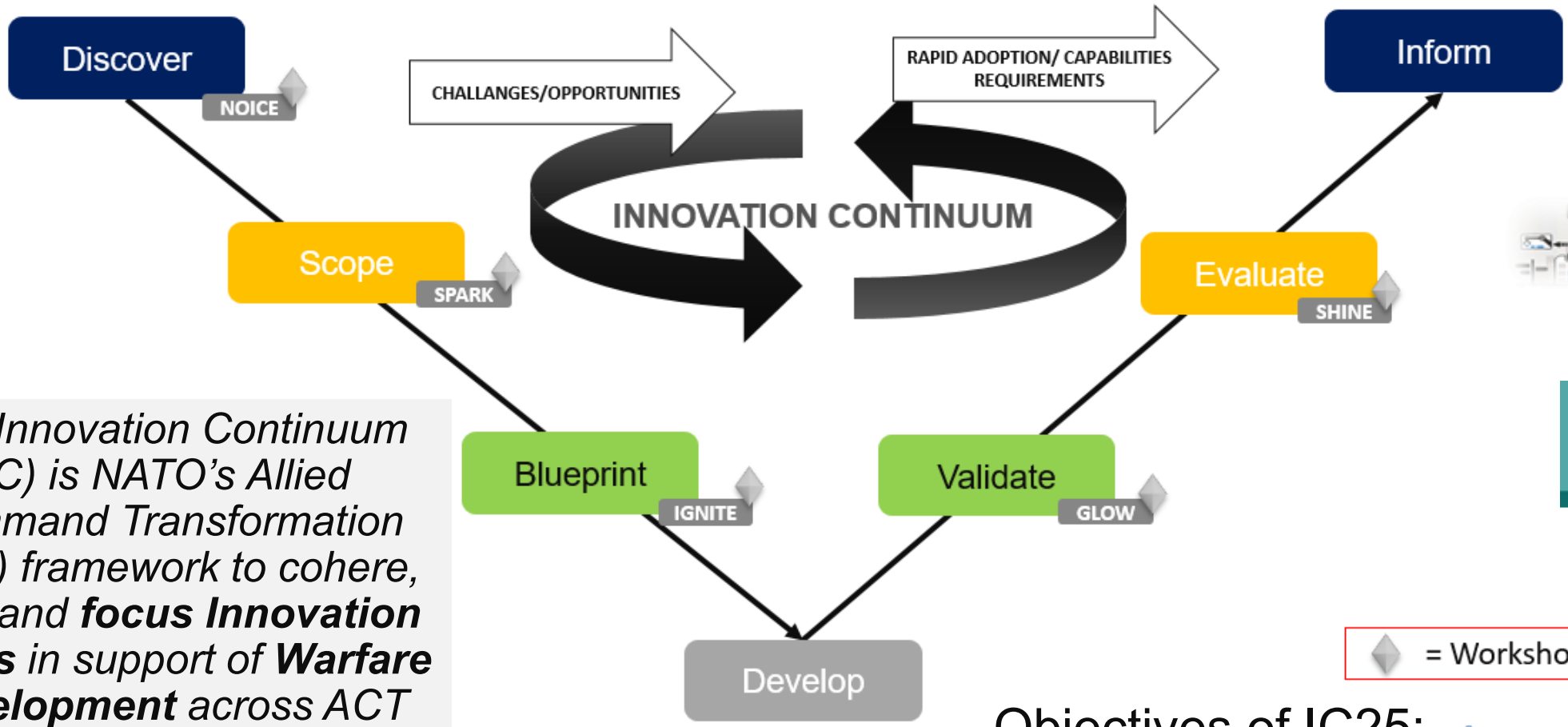
- Understanding & leverage of S&T
- Outreach & Engagement
- In-house innovation activity

Science & Technology Organization
Centre for Maritime Research & Experimentation (CMRE)
La Spezia | Italy

Emerging and Disruptive Technologies (EDTs)

Artificial Intelligence (AI)	Robotics and Autonomous Systems	Biotech-nologies & Human Enhance-ments	Electronics & Electro-magnetics*	Energy & Propulsion	Hypersonics	Next Generation Communi-cation Networks	Novel Materials and Advanced Manufac-turing	Quantum	Space

Innovation Continuum exercises



Industry

Academia

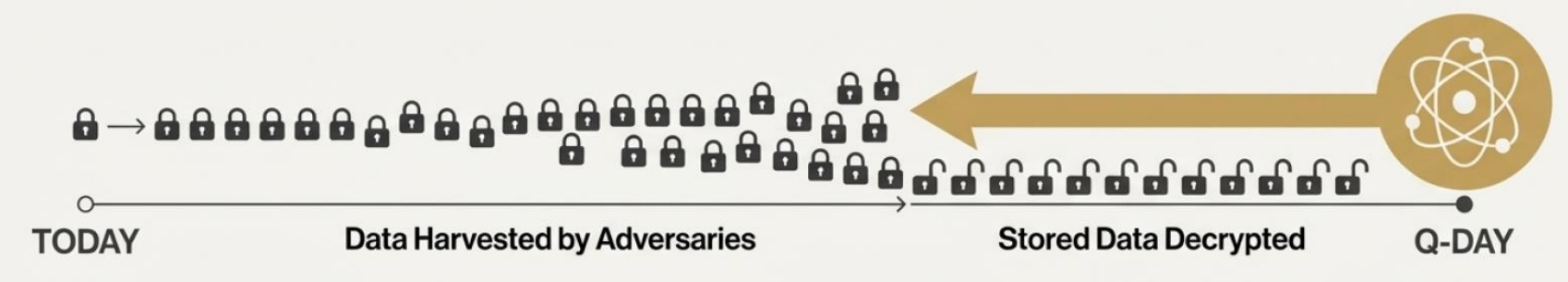
◆ = Workshop Event

*The Innovation Continuum (IC) is NATO's Allied Command Transformation (ACT) framework to cohere, align and **focus Innovation efforts** in support of **Warfare Development** across ACT and the NATO enterprise, from foresight to war-fight*

Objectives of IC25: 6

- Quantum – safe NATO CISs
- Cyber Resilience

Cryptographic agility and resilience



The threat

- In a relevant future (5 to 10 years?), a cryptographically relevant quantum computer can break most of the currently used, not quantum-resistant, asymmetric encryption algorithms
- Or a genius can break the underlying mathematical problem
- Or our implementation is just flawed
- The threat actors are active now!
  - Harvest Now Decrypt Later attacks

- **The Solution: Proactive, Agile, Diversified Defense**
  - Becoming Proactive: swiftly employing post-quantum cryptography to existing systems
  - Staying Agile: prepared for any new major breakthrough in cryptanalysis or unknown vulnerabilities in implementation
  - Diversifying: Quantum Key Distribution adds security based on principles of quantum physics

Proactive, Agile, Diversified Defense by Design

How can we build a future-proof, resilient and secure communications infrastructure that can adapt to the uncertain and evolving threat landscape?

- Built-in crypto agility

  The ability to transition between different cryptographic primitives (encryption algorithms, hash functions, or digital signature schemes) swiftly and securely without disruptive changes to the system's infrastructure

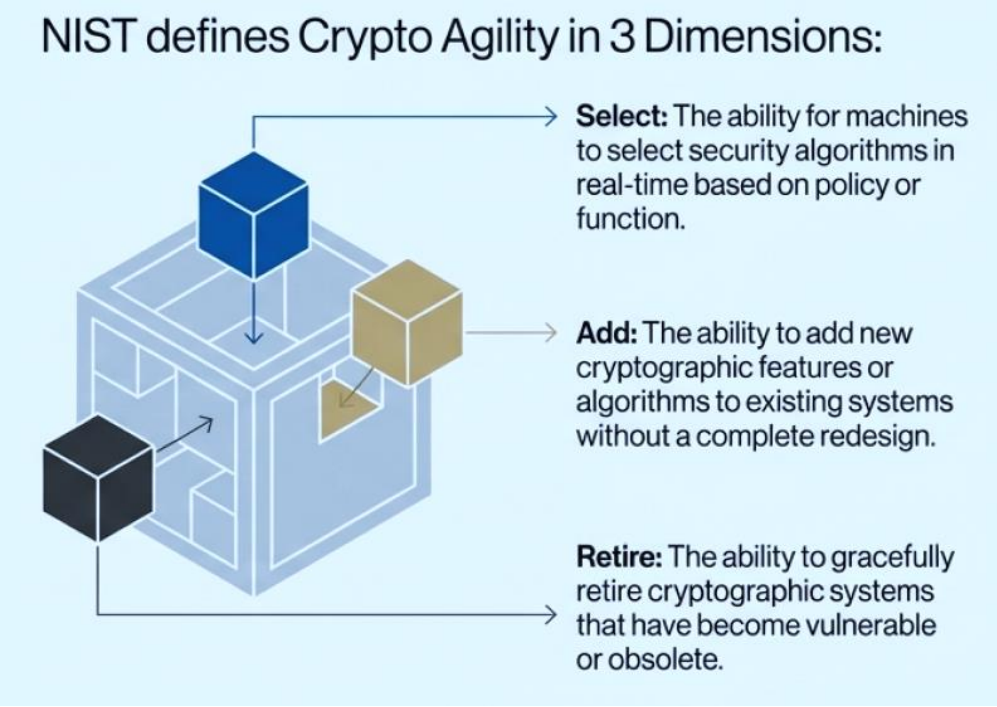
- Why?

  Critical incident response mechanism

  Allows to swiftly deprecate vulnerable primitive and replace it with a more secure alternative

  Fundamental requirement for resilient NATO crypto-systems

  In the long term – the foundation of the Cyber Resilience by Design



Evaluation – IC25, Istanbul TUR

Experiment 1: Design for Agility & Resilience

Establishing a foundational architecture that decouples key management from data transmission.

Experiment 2: Secure Mobile Platforms

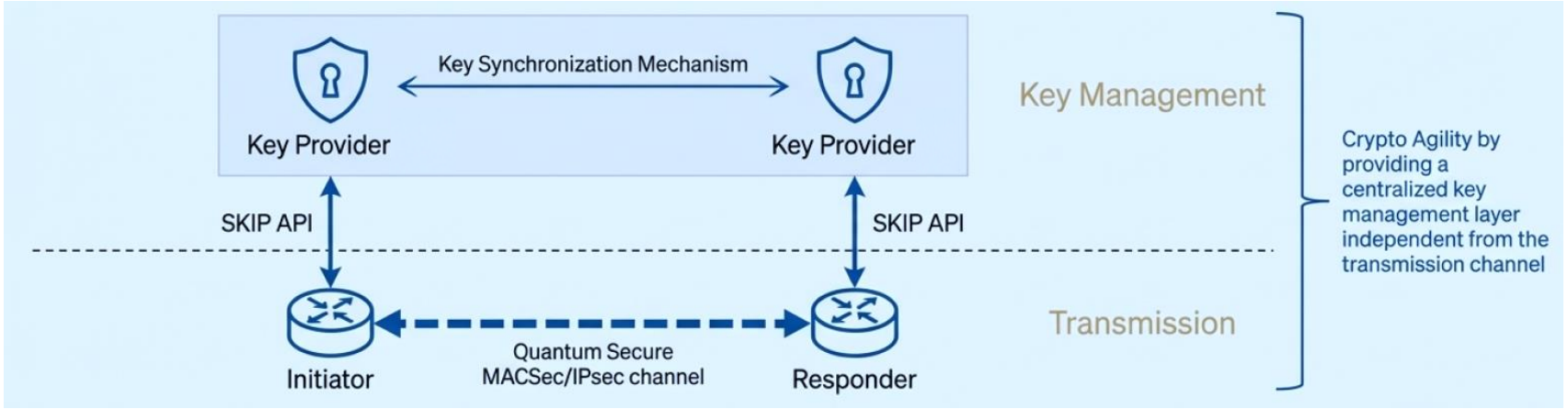
Stress-testing PQC performance in dynamic, resource-constrained tactical scenarios.

Experiment 3: Quantum Key Distribution Analysis

Evaluating the real-world viability and vulnerabilities of QKD as a fallback option.

Design for Agility & Resilience

How can we build a future-proof, resilient and secure communications infrastructure that can adapt to the uncertain and evolving threat landscape?



The concept

- The secure transmission layer (e.g. IP Sec VPN, MAC Sec) is agnostic to the key source. If the key provider is compromised or fails, it can be swapped with minimal disruption.

Key technologies

- MDI-QKD, DV-QKD, SKIP API, IKE2/IPSec
- ML-KEM-1024; BIKE-L5; Classic-McEliece-348864; FrodoKEM-1344-AES, BIKE-L1; BIKE-L

Design for Agility & Resilience

Outcomes

Key Providers (KPs) functionality and performance evaluation

- KPs entropy
- key rates

Evaluation of architectural approaches to the design of quantum resistant communication networks

Evaluation of benefits and challenges for QKD, including QKD vulnerabilities

The results of experiments will be used to

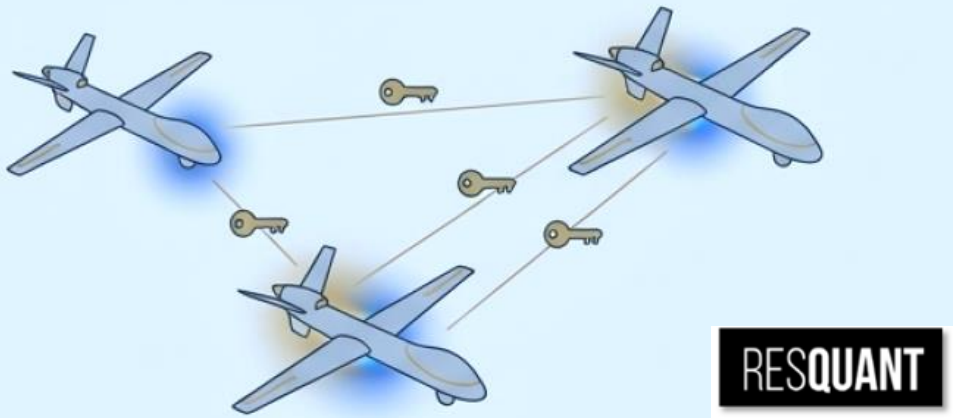
Define minimum requirements for crypto agility architecture in quantum resistant NATO networks

Inform about the solutions already available on the market

The experiments on crypto agility and cyber resilience will be continued in relation to time-critical applications and specific operational deployments secured with quantum resistant cryptographic solutions

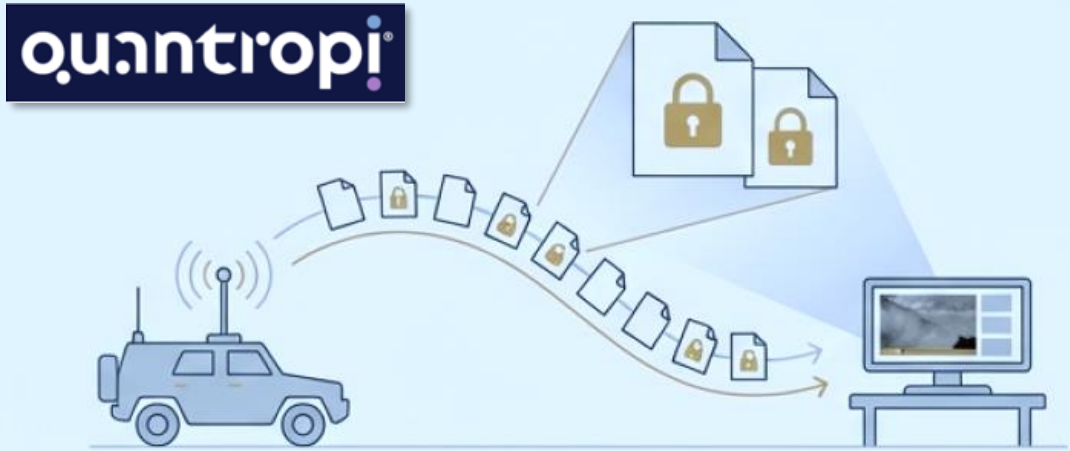
Secure mobile platforms

Scenario 1: Quantum-Secure Identification Friend or Foe (IFF)



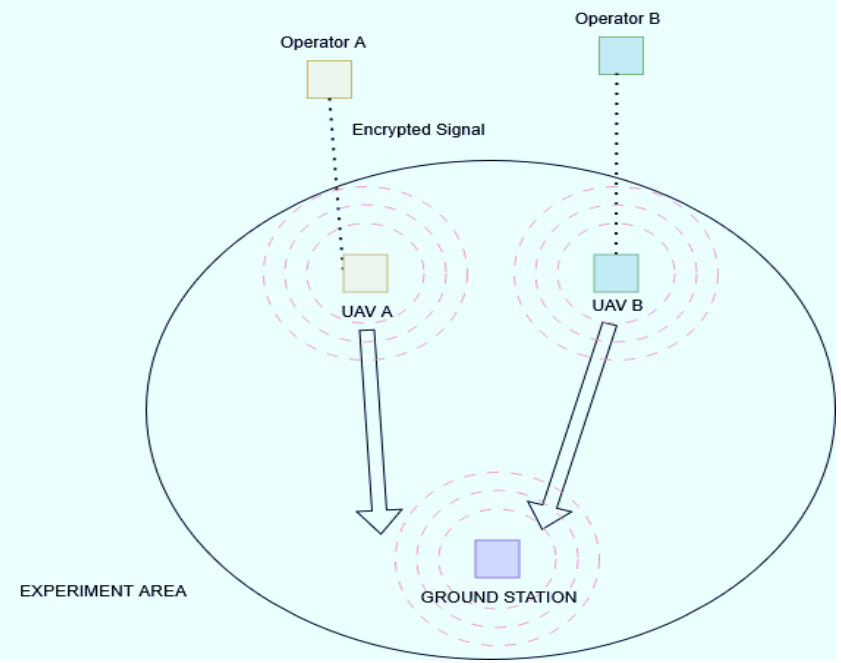
- **Objective:** Use quantum-secure algorithm to authenticate friendly UAVs and mitigate spoofing attacks
- **Setup**: 2 UAVs equipped with PQC-capable FPGA accelerators, directional antennas
- **Challenge**: Computational overhead, energy limitations, mobility, communications

Scenario 2: Quantum-Secure Video over Tactical Radio

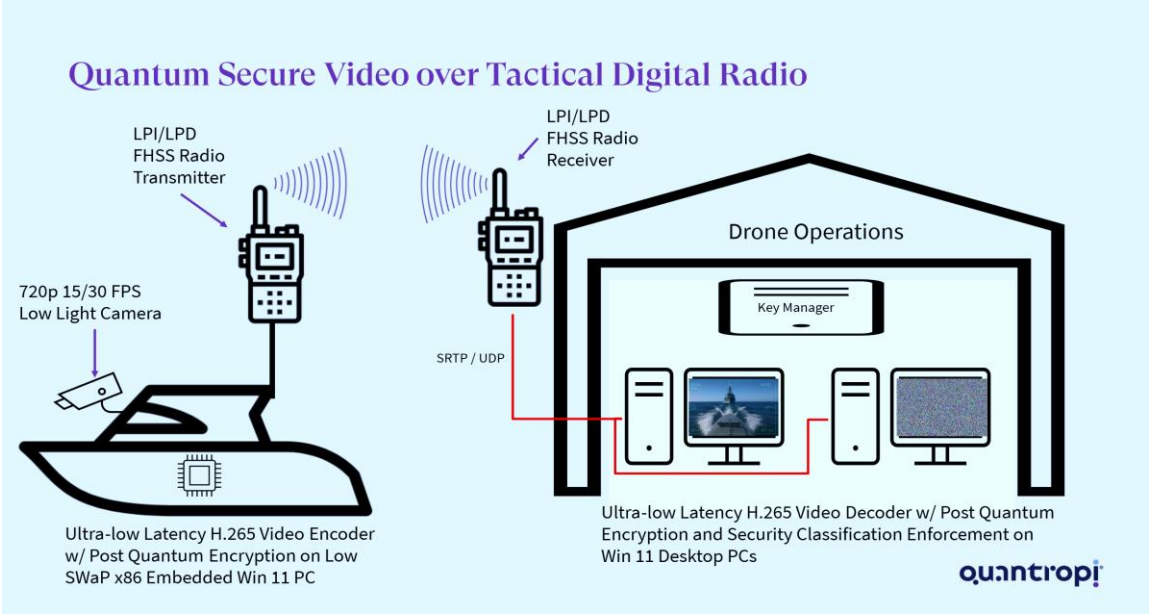


- **Objective:** Showcase feasibility and performance of PQC for encrypting high bandwidth video streams over RF links
- **Setup**: Mobile platform with camera, CNR, operation workstation
- **Challenge**: To obtain very small latency enabling to control the unmanned platform

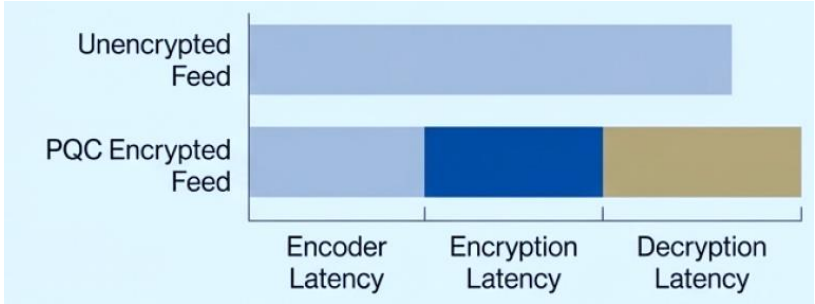
Secure mobile platforms



- **Metrics**
  - Total authentication time, data link latency, computation time
  - Throughput
  - Resilience, protocol disruptions based on SNR and BER
- Solutions tested
  - ML-DSA, Falcon



- **Metrics**

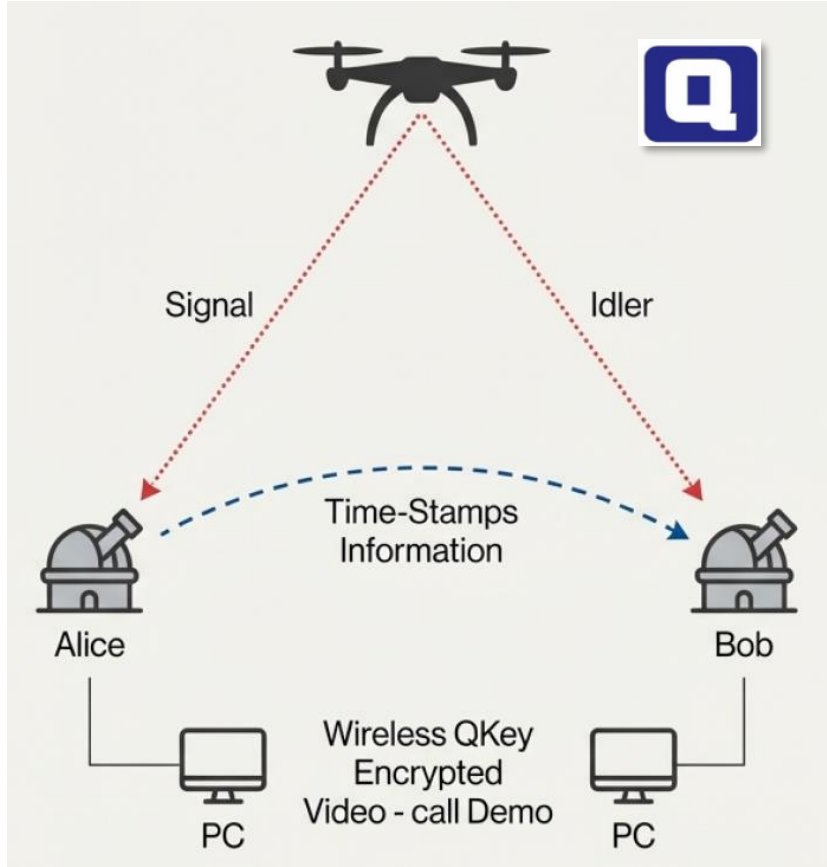


- **Solutions tested:** PQC – ML-KEM, ML-DSA; Symmetric Encryption – QEEP 1024 bit

QKD Analysis

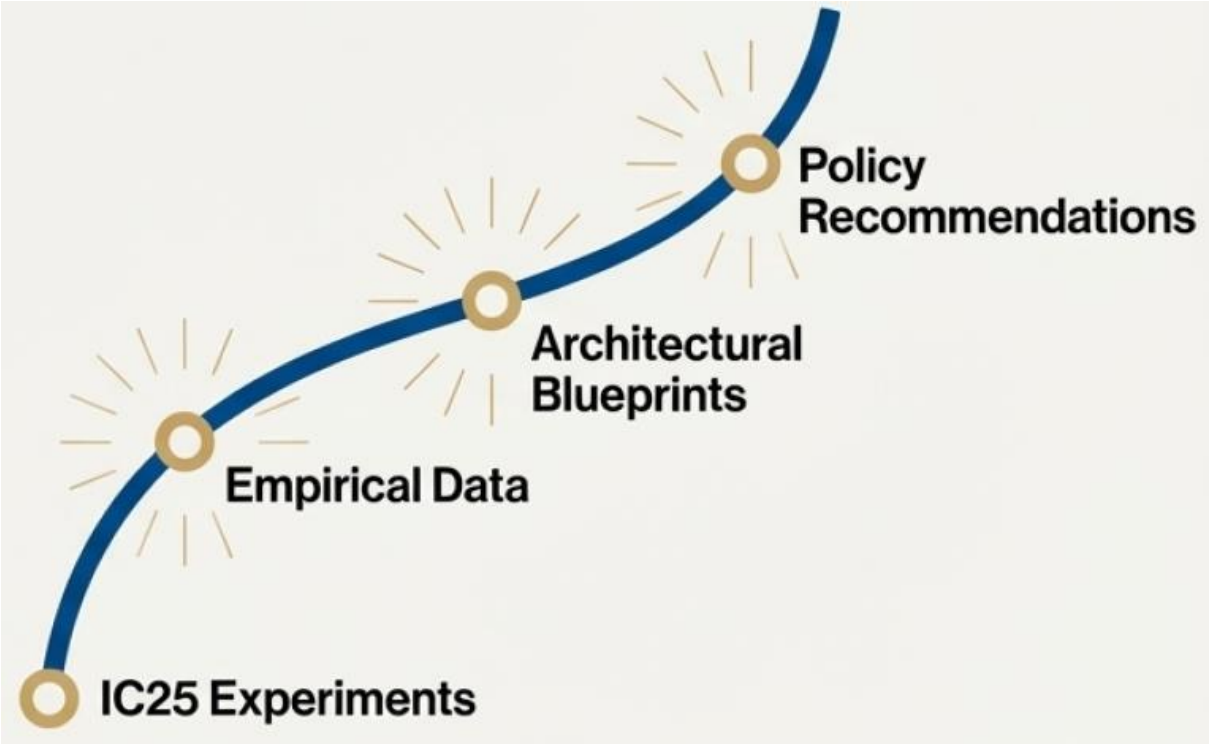
How viable are QKD systems for mobile secure communication networks, and what are their potential vulnerabilities?

- **Objective1:** Evaluate the performance and atmospheric resilience of an open-space QKD channel (BBM-92) to provide quantum secure video call encryption
- **Setup**: Drone equipped with an entangled photon source (EPS), two ground stations (Alice and Bob), the time tagging processing unit and two clients consuming the keys to encrypt a video channel using AES-256
- **Challenges**: Maintaining precise laser alignment between ground stations, mobility, vibrations and limited stability of drones in flight, sensitivity to atmospheric conditions



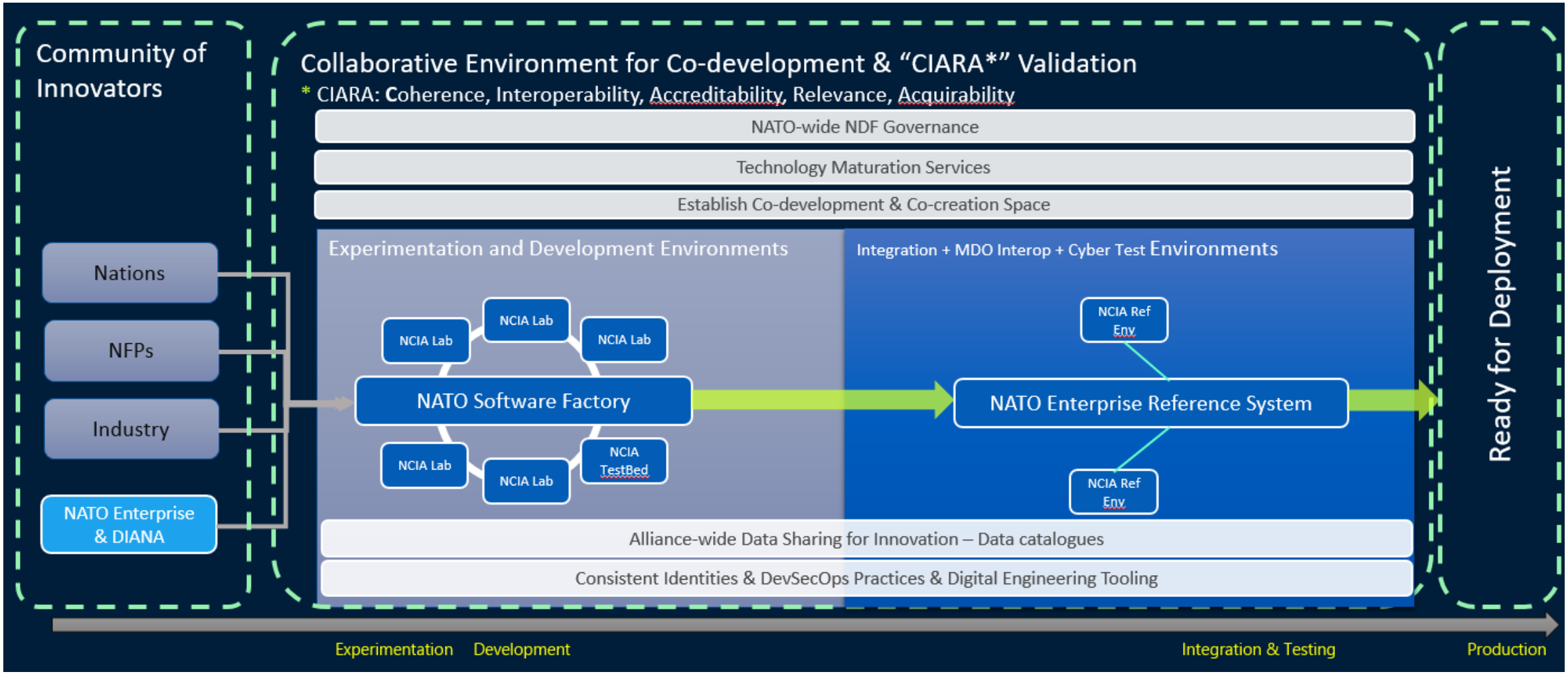
- **Objective 2**: Perform a successful side-channel attack (SCA) on a UAV-based mobile QKD system, effectively extracting a quantum-generated key
- **Setup 2** : Adversarial setup - n antennas, each dedicated to a single photon detector (SPD), an analog-to-digital converter (ADC) and a reinforcement learning algorithm
- **Challenges 2**: Full key reconstruction

Next steps



- Report strategic outcomes
  - Influence NATO Policy
  - De-risk future NATO systems
  - Engage with Allies
  - Accelerate innovation
- Continue exploration of quantum technologies within Innovation Continuum 26 topics:
  - *Audacious Training*
  - *Atlantic Antisubmarine Warfare*
  - *Counter Unmanned Systems (C-Uxs)*
  - *Joint Targeting*

NATO Digital Foundry (NDF)



Launching on Dec. 10th in The Hague!

… or join us!

- ✓Internships:
  - ❑https://www.ncia.nato.int/careers/young-professionals
- ✓Master's thesis:
  - ❑E-mail us
- ✓NATO IST-219 RTG on Quantum Technologies Vulnerabilities
  - ❑ Join as member
  - ❑ Contribute: submit a paper to Symposium/Lecture Series
- ✓International Conference on Military Communications and Information Systems (ICMCIS)
  - ❑ https://icmcis.eu/
  - ❑ 12-13 May 2026, Bath, UK
- ✓MILCOM
  - ❑ www.milcom.org,
  - ❑ 12-16 Oct 2026, Bethesda, MD, USA

Contact us

E-mail joanna.sliwa@ncia.nato.int;

Phone konrad.wrona@ncia.nato.int