DISCRETION

IST-SET-198 Research Symposium (RSY) on
"Quantum Technology for Defence and Security"

Disruptive Sdn seCuRE communicaTIons for eurOpean defeNse

EDIDP-CSAMN-SDN-2020 – SDN for defense use including the development of products and technologies

03/10/2023 (E1 session) ***Catarina Bastos***

Co-funded by the European Union

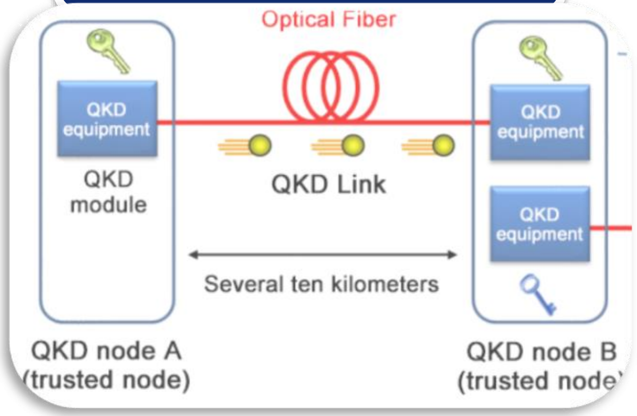
© Copyright DEIMOS

WHY QUANTUM KEY DISTRIBUTION?

QUANTUM COMPUTERS

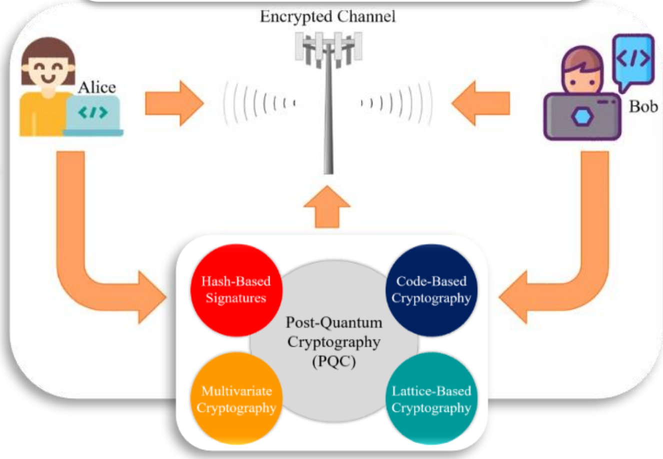
Can **break** commonly used cryptographic protocols

QUANTUM KEY DISTRIBUTION



- ✓ **Stronger and long-lived security** assurances;
  ⚠ *Need dedicated systems w/ physical limitations;*
- ✓ Better solution in **critical sectors** that require strong and lasting security.

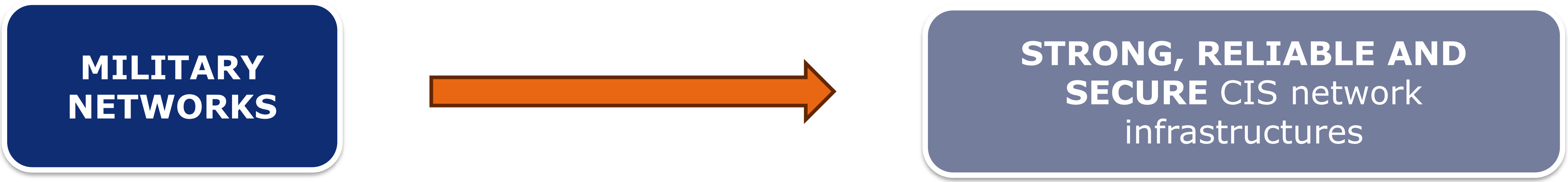
POST QUANTUM CRYPTO


Encrypted Channel
Alice
Bob
Hash-Based Signatures
Code-Based Cryptography
Post-Quantum Cryptography (PQC)
Multivariate Cryptography
Lattice-Based Cryptography

- ✓ **Low cost** and **easier** to implement;
- ✓ Better solution for **small and mobile devices**.

© Copyright DEIMOS

DISCRETION MOTIVATION



MILITARY NETWORKS

STRONG, RELIABLE AND SECURE CIS network infrastructures

❑ **SOFTWARE DEFINED NETWORKS (SDN):**

- ○ More agile, flexible, easier to manage and to re-configure, and to support interoperation among diverse networks.
- ○ ***Challenging***: tactical networking and sharing information in dynamical environment using SDN.
- ○ ***SDN Flexibility***: allows integration of disruptive technologies like **Quantum Key Distribution (QKD)**.

DISCRETION: quantum-enabled SDN architecture uniting under the same management the quantum and classical communications.

DISCRETION OBJECTIVES

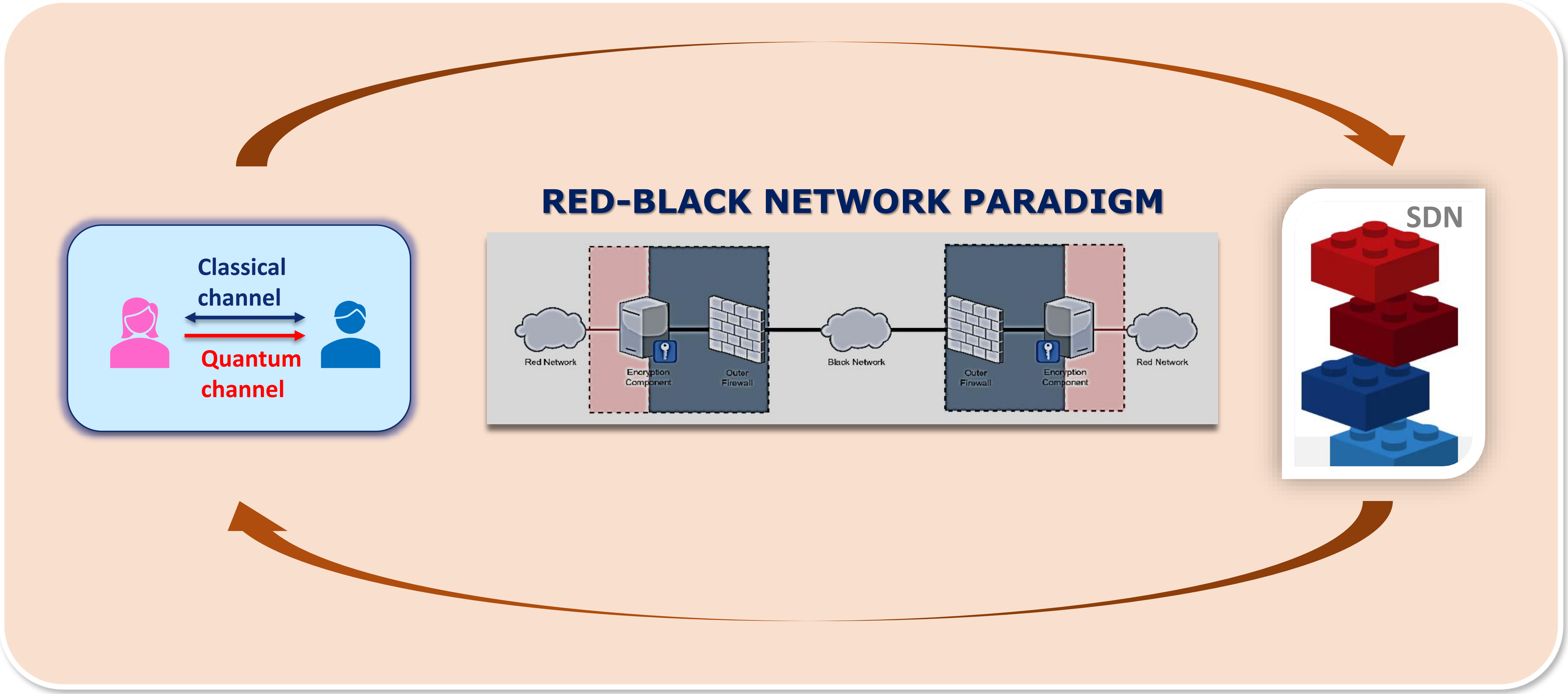
DISCRETION

- ❑ Design and propose an architecture of an SDN for secure communication which can evolve in time according to Member States operational needs and ambition;
- ❑ Introduce quantum technologies in Europe as a mechanism for secure share of information between Member States Defence;
- ❑ Development of HW + SW for distribution of keys and also for generation of keys (using QKD) for military applications;
- ❑ Support PESCO project EU Cyber Academia and Innovation Hub;

DISCRETION objectives aligned with relevant technological building blocks for Cyber Defence:

- ○ Explore similarities and differences between cyber operations and electronic warfare, including SDN;
- ○ Quantum computing and cryptography with cyber implications.

DISCRETION: SYMBIOTIC SOLUTION



Classical channel

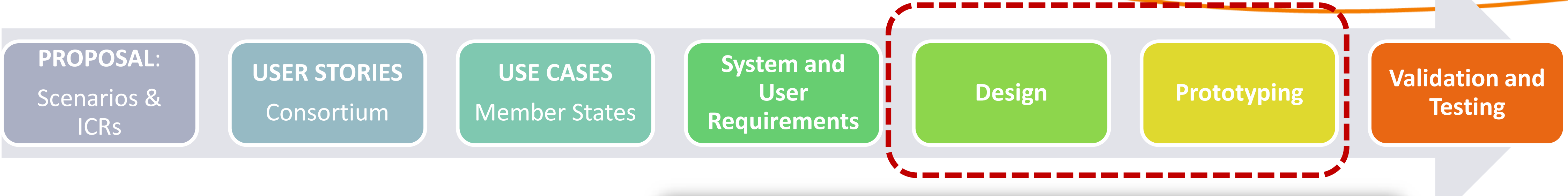
Quantum channel

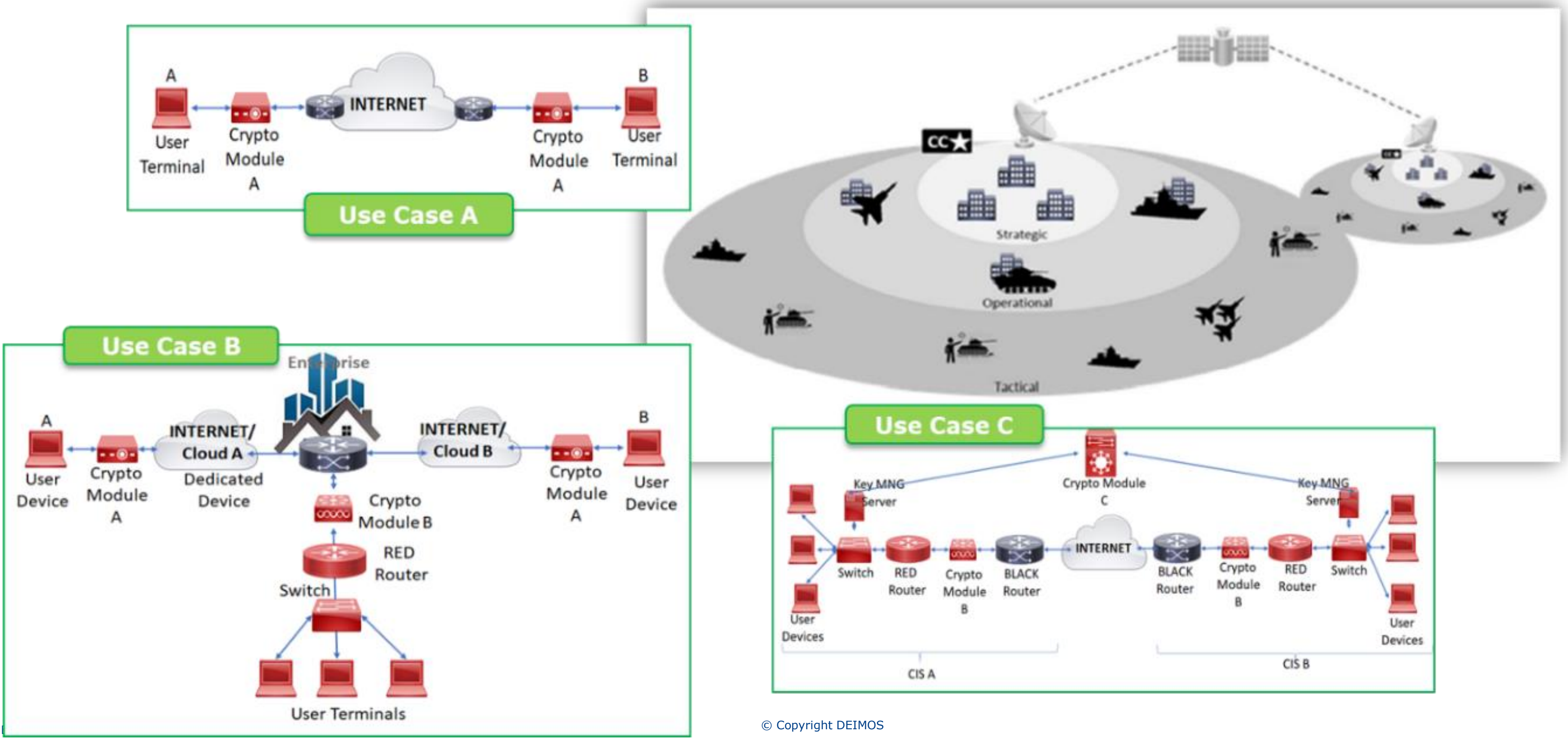
RED-BLACK NETWORK PARADIGM

SDN

© Copyright DEIMOS

DISCRETION WORKFLOW, SCENARIOS AND USE CASES

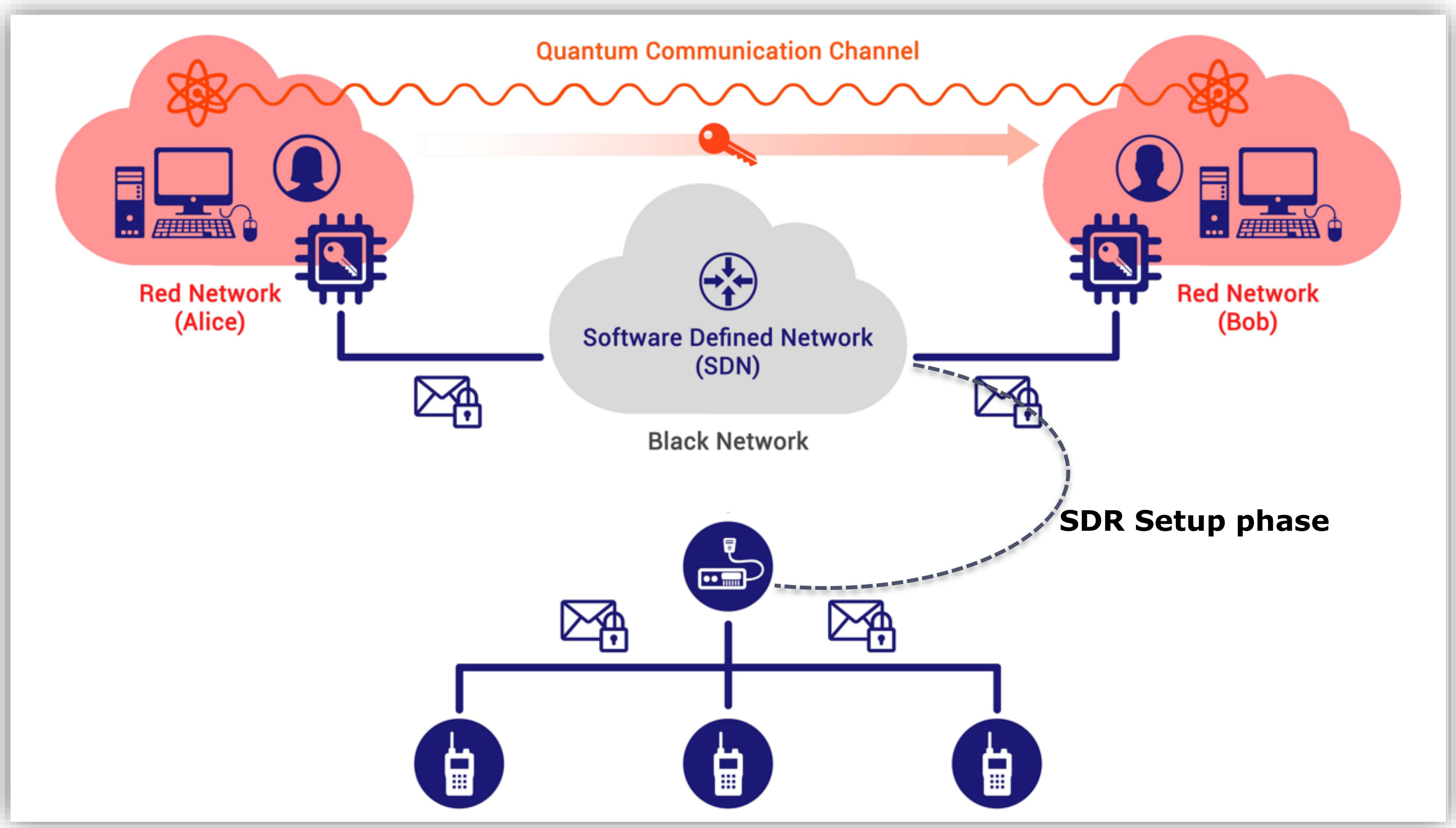




© Copyright DEIMOS

SDN ARCHITECTURE IN RED-BLACK NETWORK DEPLOYMENTS

Military scenarios pose an additional challenge for operation across different security perimeters



QKD Control and associated channels, **QKD nodes** have been tagged as red network elements:

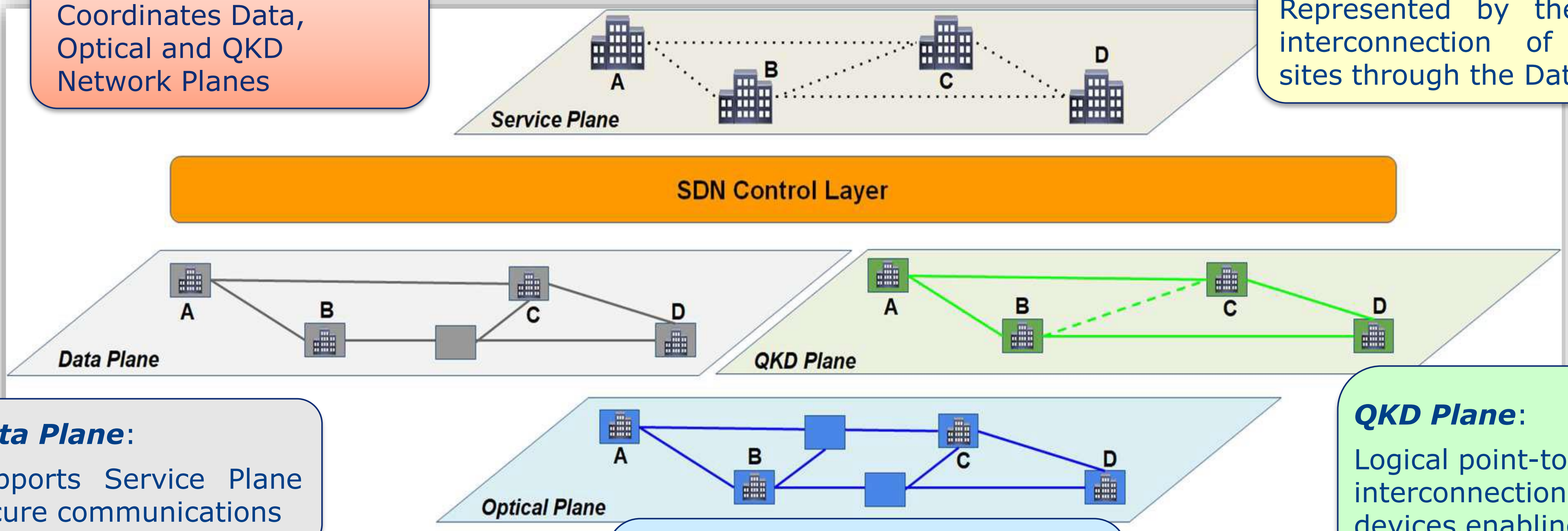
- ❑ Separate QKD plane for the black network
- ❑ Isolation between, Service Plane SDN Apps and SDN-QKD introduces constraints to network automation and programmability of the black network.
- ❑ Ongoing analysis of existent trade-offs to provide an ample degree of **programmability without compromising security.**
- ❑ **SDR interacts with DISCRETION system in the setup phase.**

© Copyright DEIMOS

SOFTWARE DEFINED NETWORK

SDN Control Plane: Coordinates Data, Optical and QKD Network Planes

Service Plane: Represented by the logical interconnection of military sites through the Data Plane



Data Plane: Supports Service Plane secure communications

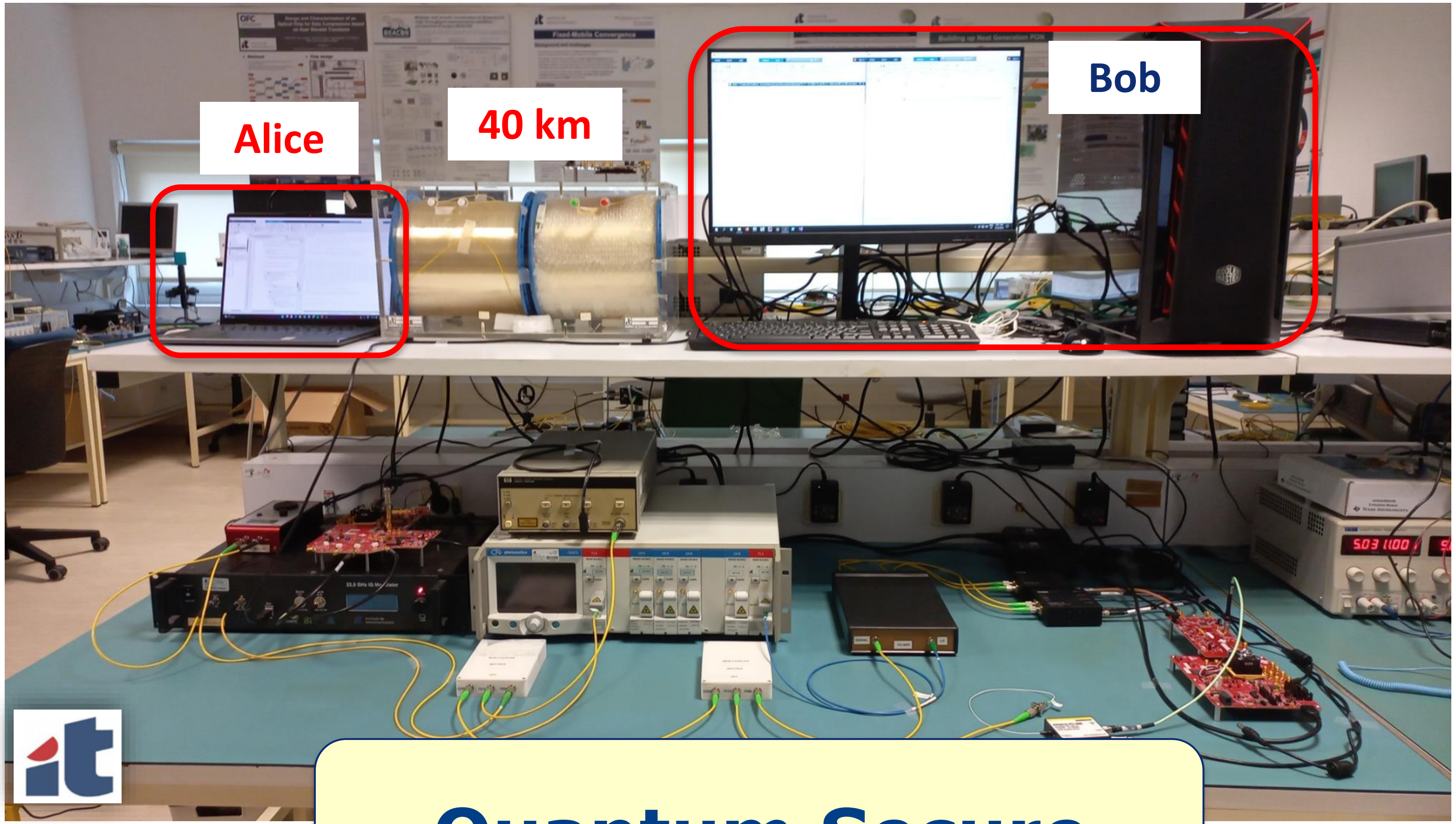
Optical Plane:

- supports QKD Plane
- serves the optical connectivity among QKD devices

QKD Plane: Logical point-to-point interconnection of QKD devices enabling the generation of symmetric quantum keys

CONTINUOUS VARIABLE - QUANTUM KEY DISTRIBUTION NODES

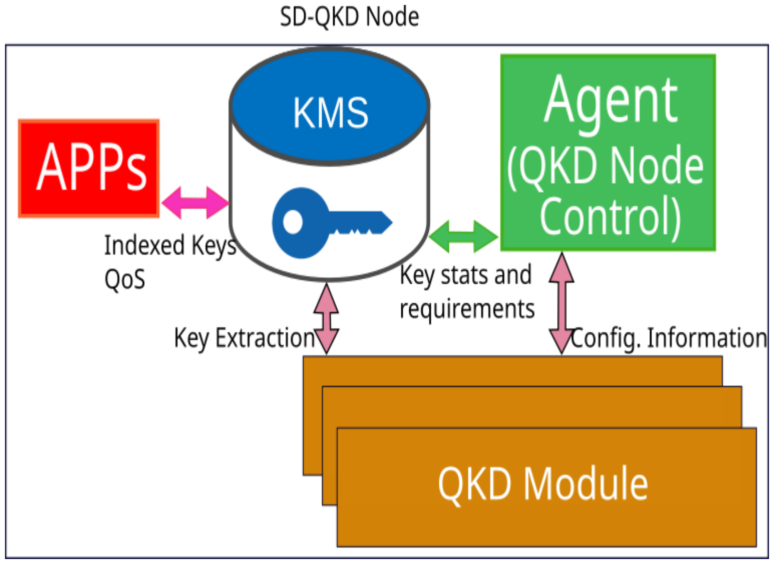
❑ **Based on technology already developed in the Lab:**



Quantum Secure

ETSI GS QKD 015

QKD node: set of QKD modules that implement hardware, firmware supporting the CV-QKD technology.



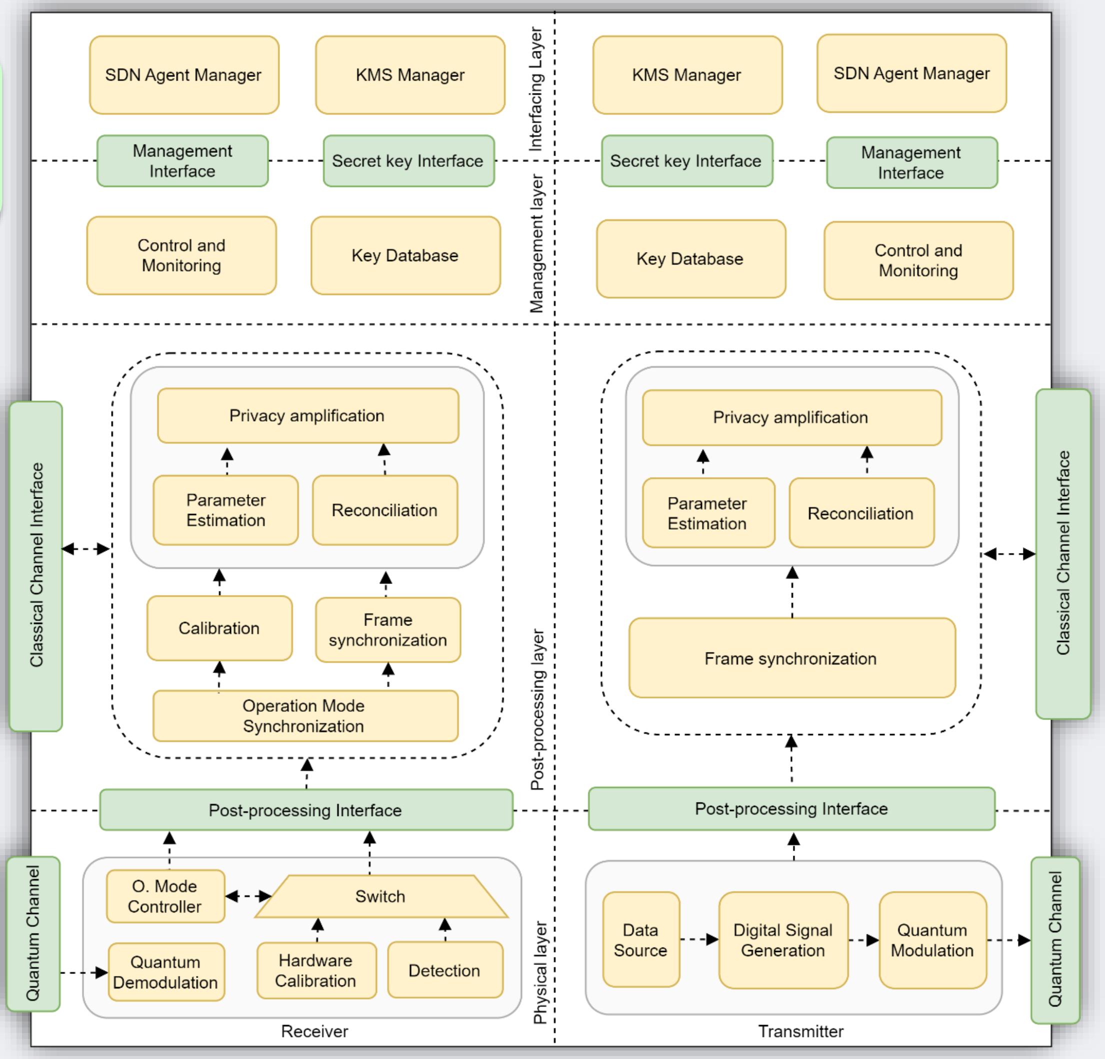
© Copyright DEIMOS

QUANTUM KEY DISTRIBUTION ARCHITECTURE

Management Layer

Post-Processing Layer

Physical Layer



CYBER SITUATIONAL AWARENESS

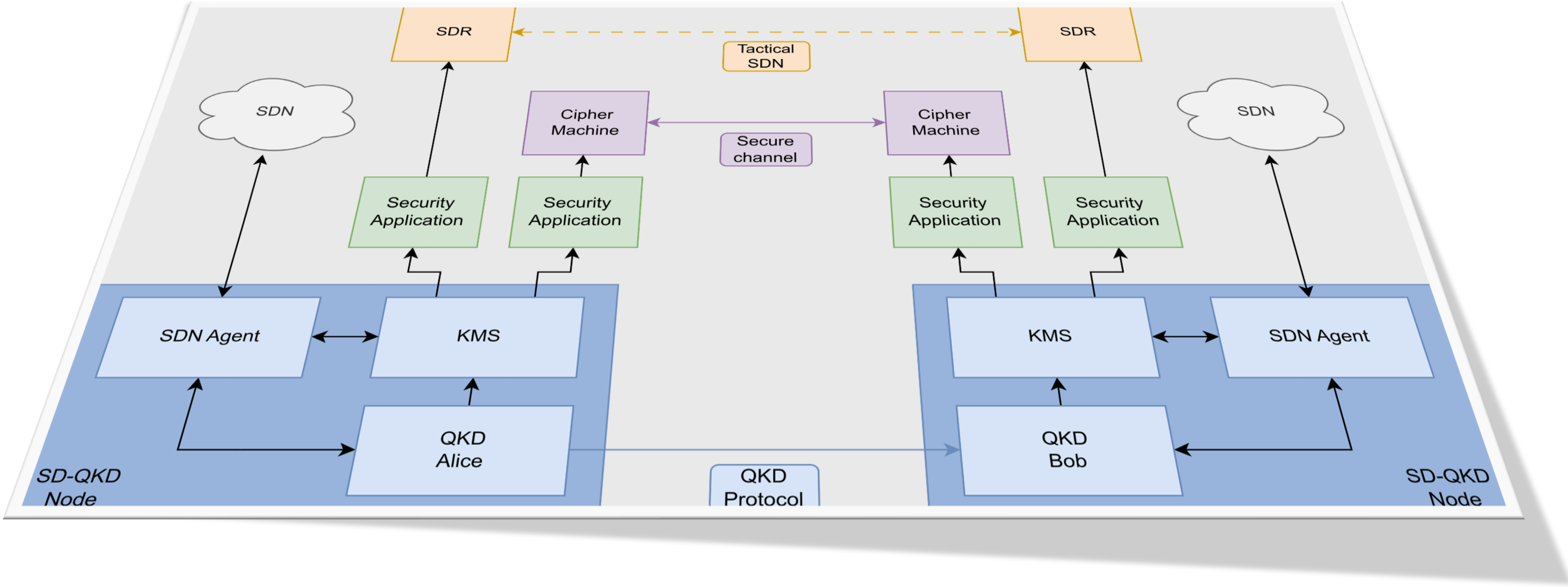
Through cipher machines for data protection

- ❑ **Network segregation,** enabling real-time data protection with hardened and customized systems**;**
- ❑ Using key material provided by **a Key Management System (KMS)** integrating the SD-QKD plane and pre-shared keys;
- ❑ **Strict Red-black architecture of the military networks** providing the required level of security and segregation.

GNS
Gabinete Nacional de Segurança
4003
Com a colaboração de:
TÉCNICO LISBOA
inesc id lisboa
it Instituto de Telecomunicações

© Copyright DEIMOS

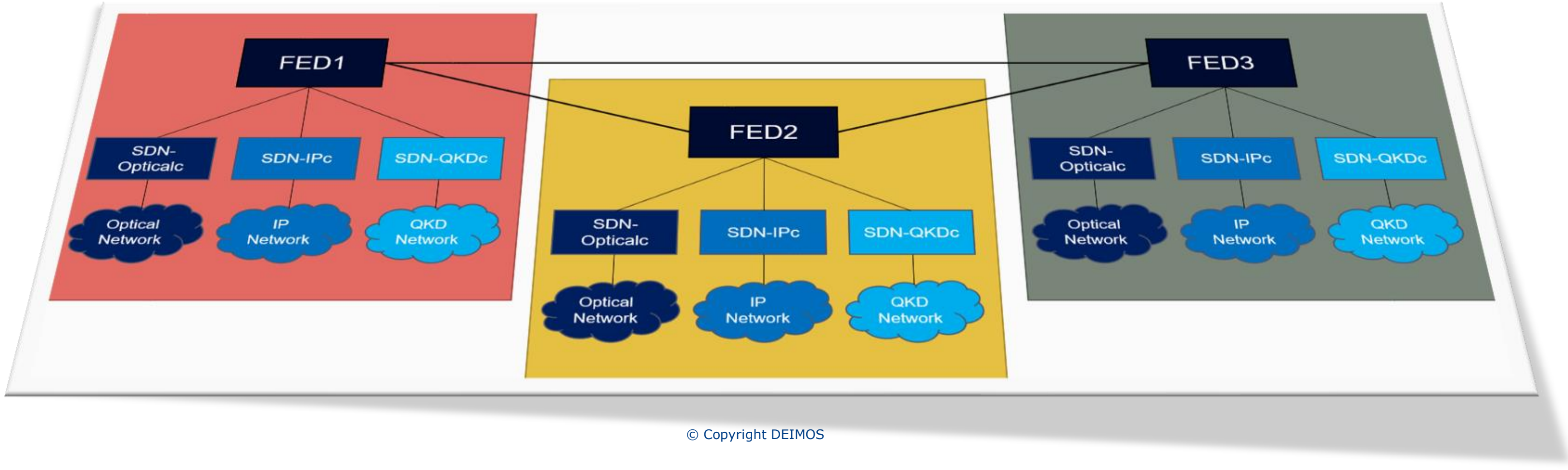
DISCRETION: PRELIMINARY DESIGN



© Copyright DEIMOS

FEDERATED HIERARCHICAL SDN ARCHITECTURE

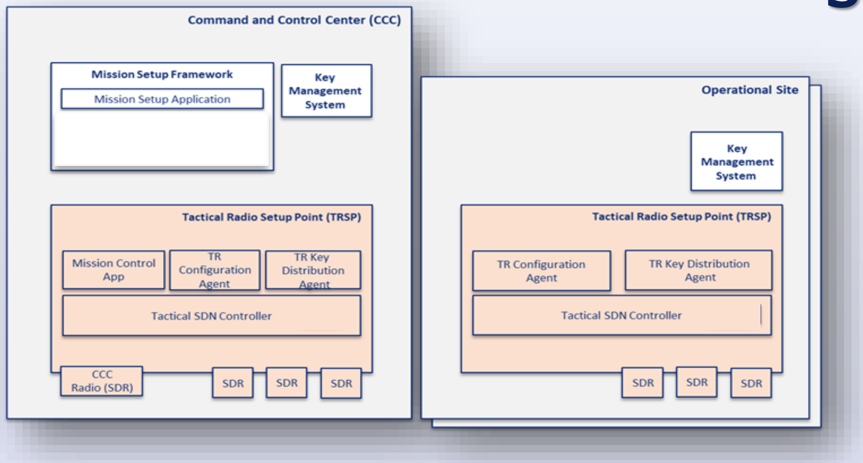
- ❑ **Inter-domain federated Architecture:**
  - o Network sovereignty on each administrative domain (e.g. country)
  - o Communications established according to previously agreed SLAs allowing the different members of a coalition to share information and network resources without losing control over their own networks.
- ❑ **Intra-(administrative) domain hierarchical SDN architecture**
  - o Easier control of each domain when it is provided by a specialized controller,
  - o Greater adaptability in multi-provider scenarios
  - o High available and scalable solution through distributed Domain Level Controllers.



© Copyright DEIMOS

TACTICAL SDN: SDN-SDR INTEROPERABILITY

Setup

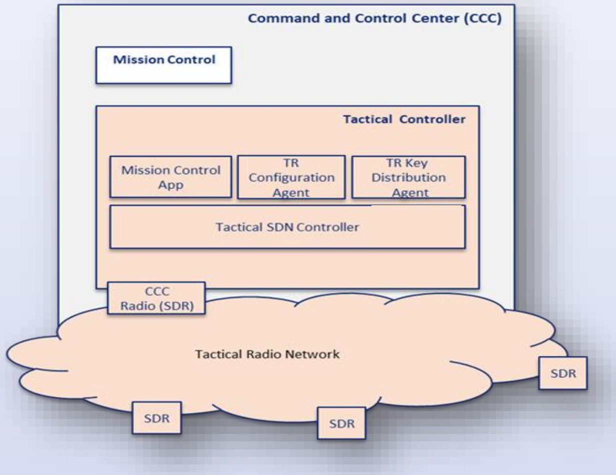


- ✓ Connected to the **Operational SDN**
- ✓ Using **DISCRETION system for Key distribution** and remote SDR configuration
- ✓ SDRs physically connected to the network

Use Case 1: Mission Setup

- Actions for the setup scenario
- Deployment of the configuration
- Distribution of Cryptographic keyset

Mission



- ✓ **Tactical,** on the field, no guaranteed connection to operational network
- ✓ **Control plane** at the Command and Control Centre (CCC), or a SDN hierarchy culminating at the CCC.

Use Case 2: Data-based SDR control

- Closing a control loop,
- Starting with situational awareness data,
- Triggering a decision,
- Enforcing it to the SDRs

Use Case 3: Tactical key management

Managing the security of the tactical network:

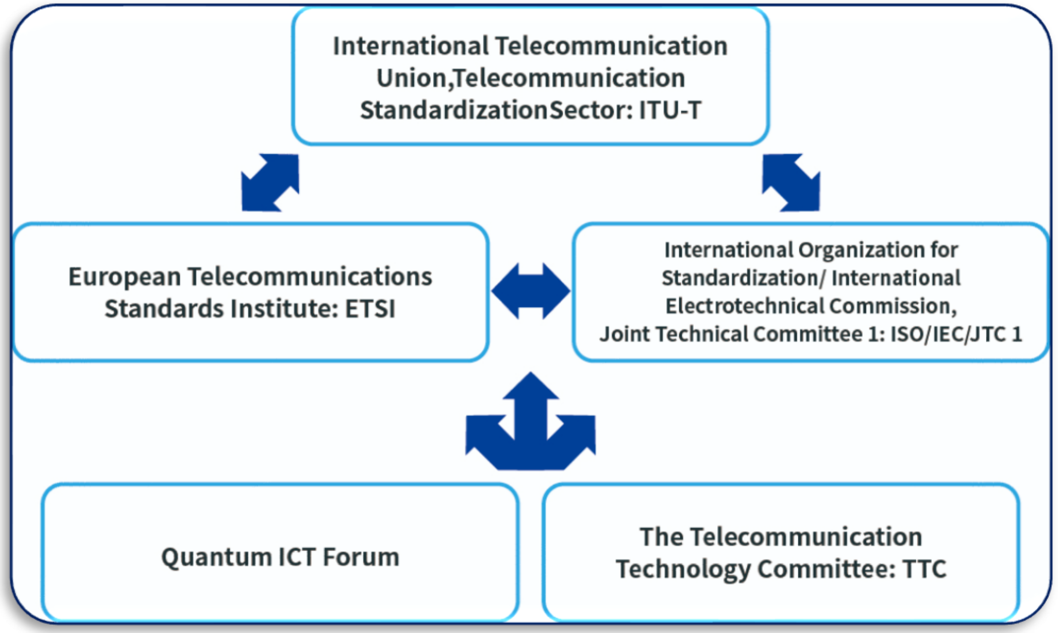
- forcing key rotation,
- redefining groups

© Copyright DEIMOS

SECURE STANDARDS IN DISCRETION

Why a strict evaluation for each standard?

- ❑ **Inter-Domain (red-black) is limited, and data cannot simply flow between boundaries.**
  - ○ Breaks some assumptions of standards
  - ○ May leak metadata across boundaries
  - ○ Cross-domain requires heavy filtering or Data-Diodes



International Telecommunication Union,Telecommunication StandardizationSector: ITU-T

European Telecommunications Standards Institute: ETSI

International Organization for Standardization/ International Electrotechnical Commission, Joint Technical Committee 1: ISO/IEC/JTC 1

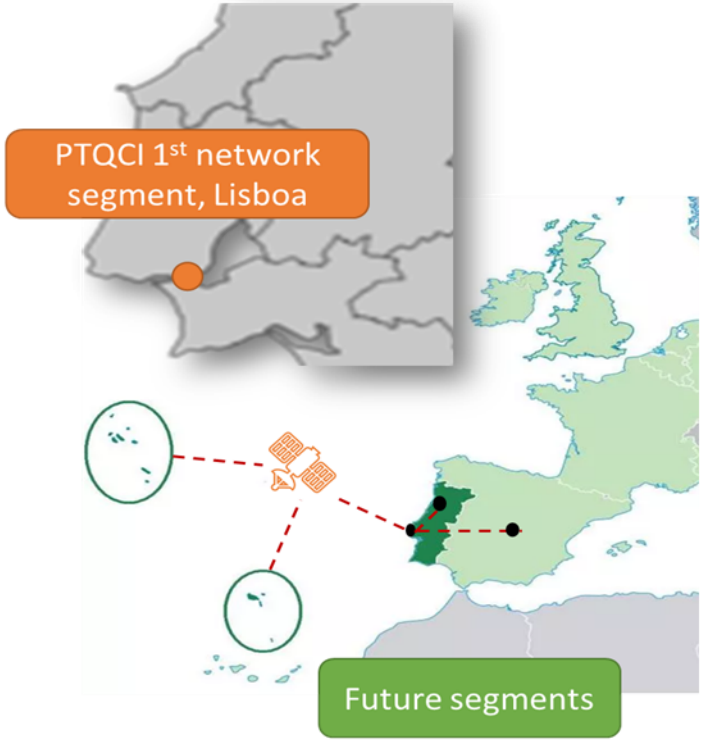
Quantum ICT Forum

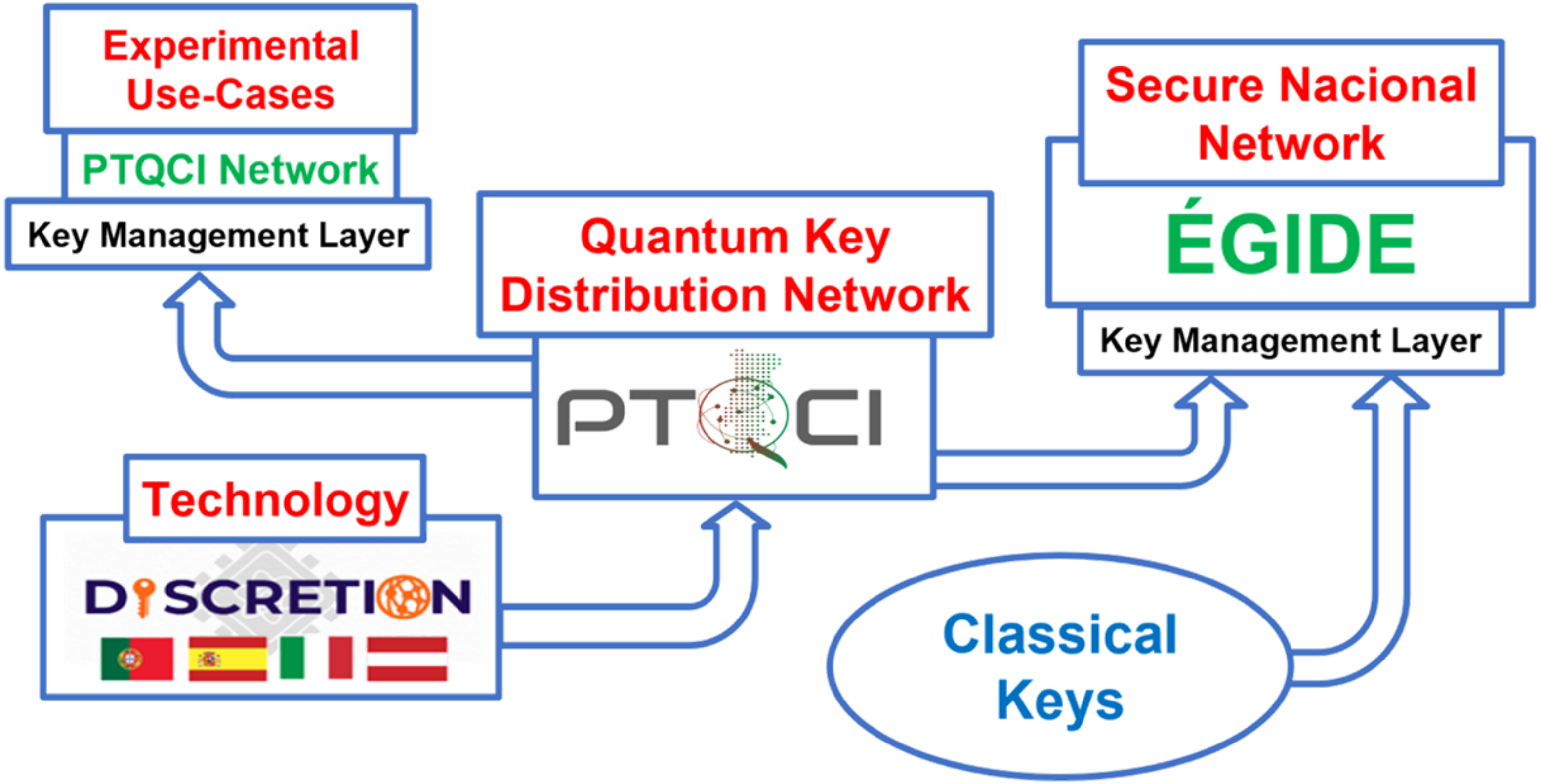
The Telecommunication Technology Committee: TTC

© Copyright DEIMOS

PORTUGUESE QUANTUM COMMUNICATION INFRASTRUCTURE

- ❑ **DISCRETION technology will be integrated in the 1st segment of PTQCI**





THANK YOU

https://discretion-eu.com/

*Trademarks **"Elecnor Deimos"**, **"Deimos"** and the logo of **Deimos (Elecnor Group)** encompass Elecnor Group’s companies of Aerospace, Technology and Information Systems: **Deimos Space S.L.U**. (Tres Cantos, Madrid, Spain), **Deimos Engineering and Systems S.L.U.** (Puertollano,Ciudad Real, Spain), **Deimos Engenharia S.A.** (Lisbon, Portugal), **Deimos Space UK Ltd.** (Harwell, Oxford, United Kingdom), **Deimos Space S.R.L.** (Bucharest, Romania).*

© Copyright DEIMOS