ITU Events

ITU Regional Cybersecurity Forum for Europe and CIS

27 – 28 February 2020
Sofia, Bulgaria

Follow us on twitter: @ITU_EUR & @ITUMoscow
www.itu.int/go/EURCIS_CSForum20

ITU Regional Initiative for Europe on enhancing trust and confidence in the use of ICTs

ITU Regional Initiative for CIS on the development and regulation of infocommunication infrastructure to make cities and human settlements inclusive, safe, and resilient

POLICIES & STRATEGIES | CERTIFICATION FRAMEWORKS | DATA PROTECTION | SECURITY CHALLENGES | 5G, eSIM IoT, AI

Hosted and co-organized by:

REPUBLIC OF BULGARIA
State e-Government Agency

REPUBLIC OF BULGARIA
Ministry of Transport, Information Technology and Communications

ITU

Quantum Key Distribution in the Cold Reality of Cybersecurity

Arnaud Taddei

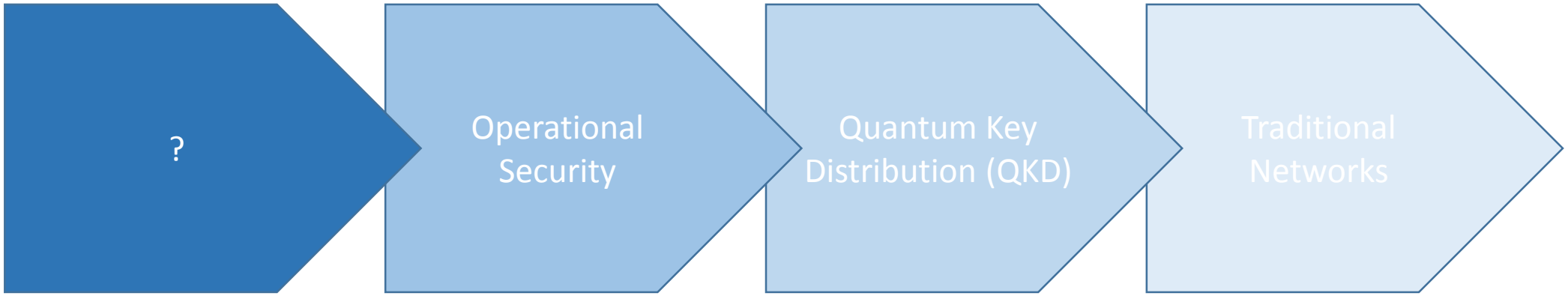
Technical Director, Standards and Architectures

Broadcom Inc.

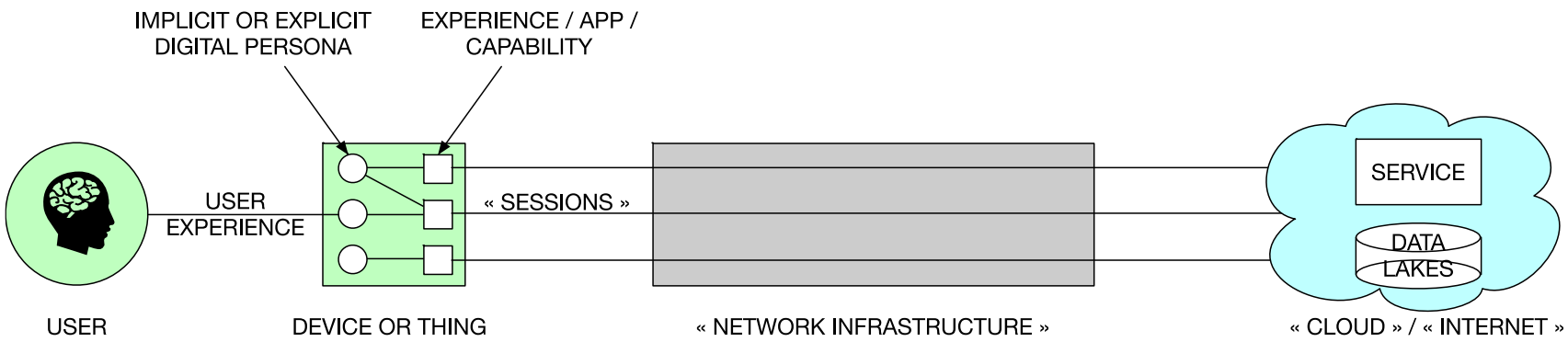
Arnaud Taddei

ITU-T SG17 WP3 Chairman, Co-Convenor long term strategy

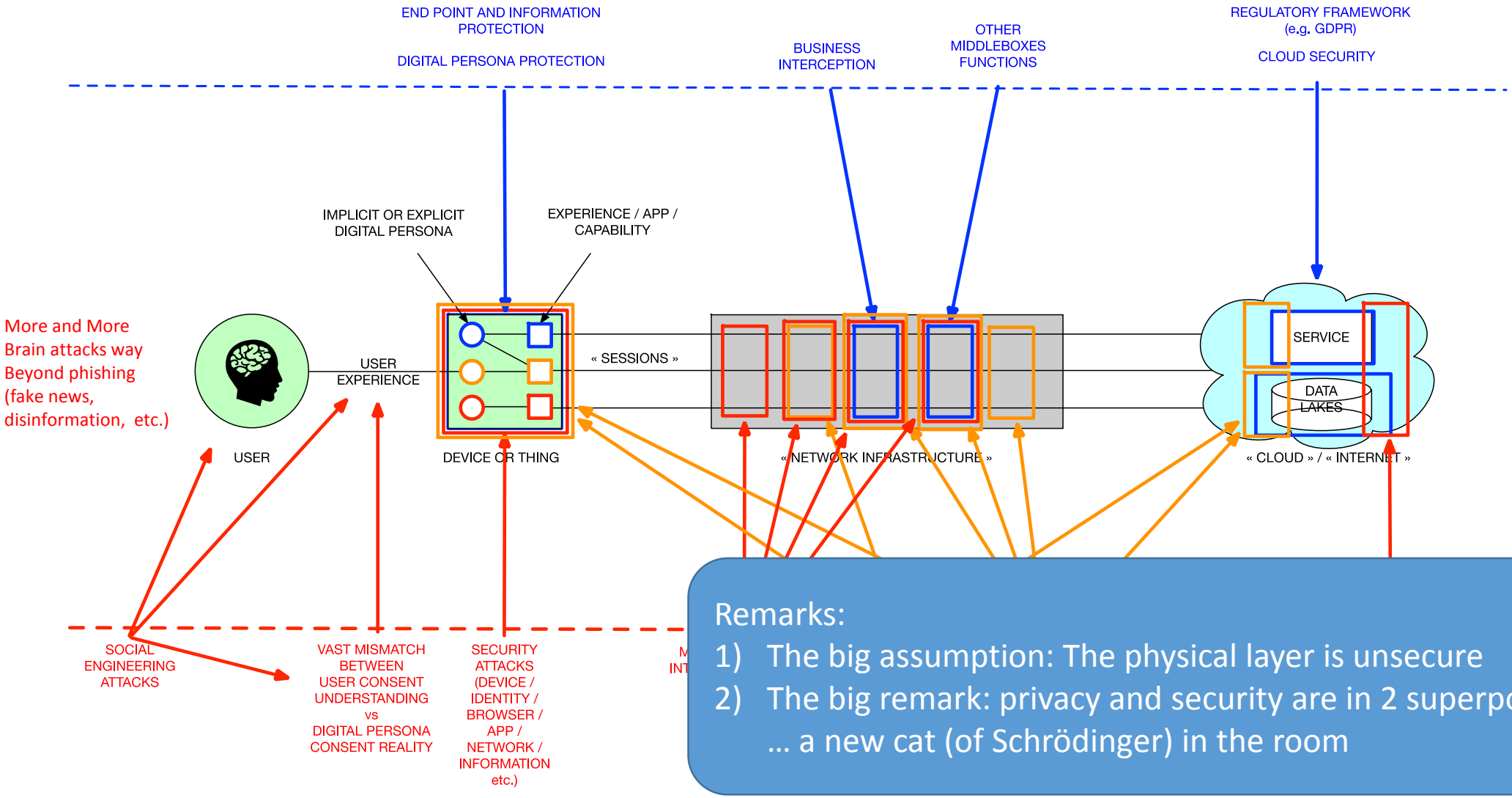
ITU-T TSAG Standardization Strategy Rapporteur



Traditional Network
Typical experience



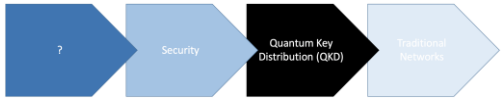
Traditional Network - Cold reality



Remarks:

1) The big assumption: The physical layer is unsecure
2) The big remark: privacy and security are in 2 superposition states … a new cat (of Schrödinger) in the room

A Quantum Map



Quantum Phyiscs
➔ Entanglement

Quantum Computing

Quantum Communication

Quantum Metrology

Can resolve many new problem classes (NP completele, support AI, find new materials, …)

Can break Shor's algorithm ➔ QDay

Quantum Key Distribution (QKD)

Quantum Random Number Generation (QRNG)

Quantum Information Networks (QIN)

Quantum Clocks
Quantum Sensors
…

Quantum Clouds
Quantum Simulation
NP Complete Pbs
Etc.

Quantum Resistance

Quantum Safe Cryptography (QSC)

Physics

Mathematics

Quantum Key Distribution (QKD)

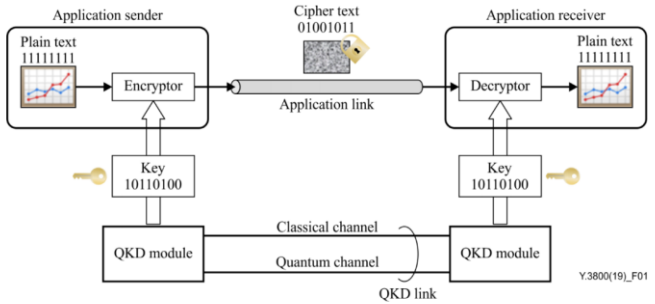


Figure 1 – Configuration example of QKD use for securing a P-to-P application link

Ensures physical layer to be secure
New technology with new characteristics
First time:

- A resource needs to be produced
- A resource is consumed
- A resource is perishable

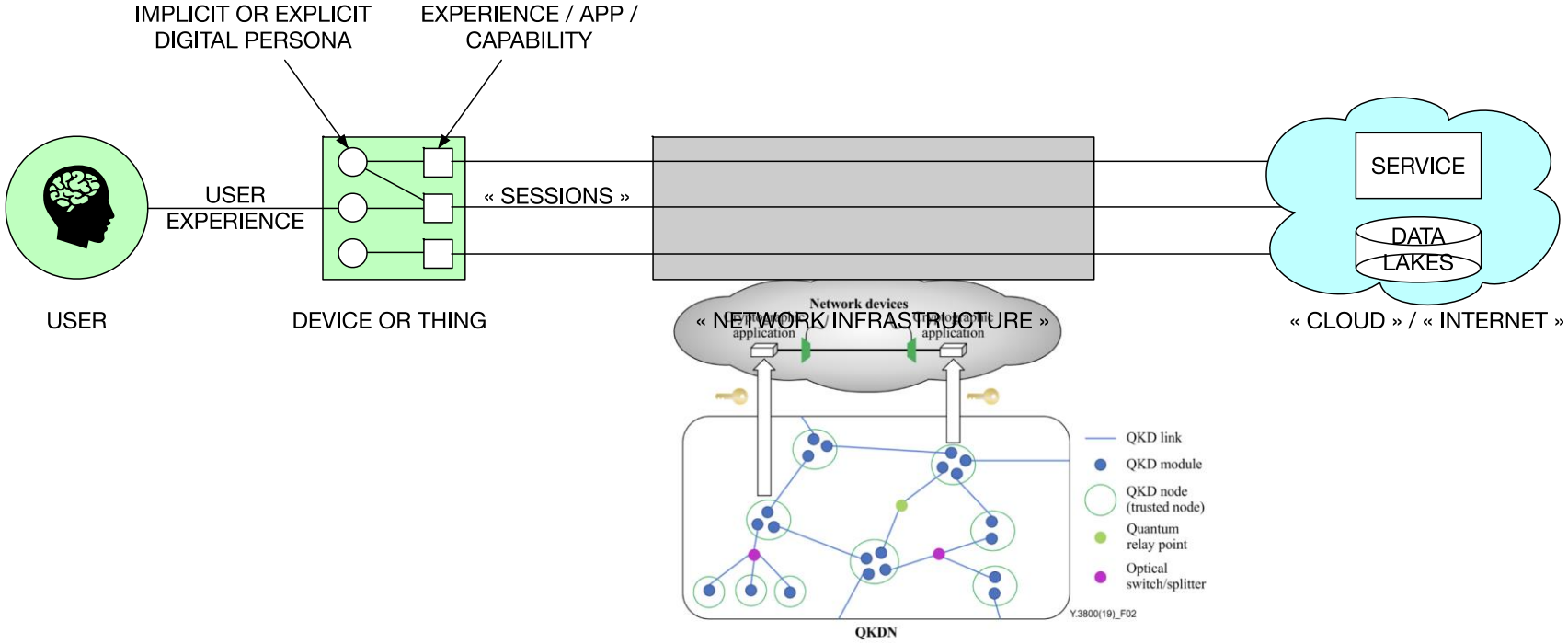


Figure 2 – Illustration of QKDN concepts and their relation to a user network

Science Fiction? NO!

Non exhaustive list – Beyond Data Center to Data Center, dozens of use cases

Country/Region	Research	Industry	Infrastructure - Ground	Infrastructure - Space	Projects/Programs	Comments
China	Yes	Yes	Beijing-Shanghai, etc.	Satellite Micius	Many	
EU	Yes	Yes	Yes	Planned (Thales Espace)	OpenQKD	Will prioritize institutional customers (Hospitals, etc.)
US	Yes	Yes (QAI)	Yes	?	?	
Canada	Yes	Yes	?	Planned (Honneywell)	?	
Japan	Yes	Yes	Yes	?	?	
UK	Yes	Yes	Yes	?	?	
Spain	Yes	?	Yes	?	?	SDN QKD
Switzerland	Yes	Yes	Yes	?	?	Banking Sector as commercial customers

Standardization:

- ITU-T SG13-SG17, FG-QIT4N
- ETSI ETSI ISG QKD, ETSI TC Cyber QSC
- ISO ISO/IEC JTC 1/SC27
- IRTF Quantum Internet Research Group (QIRG)

But who guards the guards?

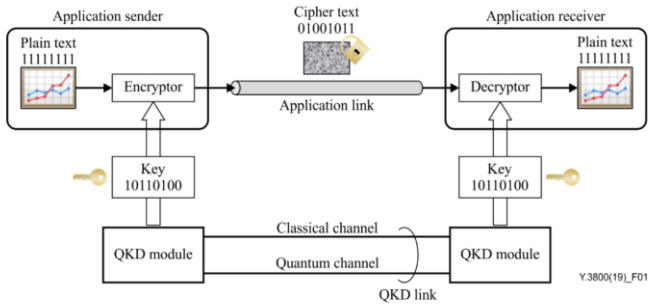


Figure 1 – Configuration example of QKD use for securing a P-to-P application link

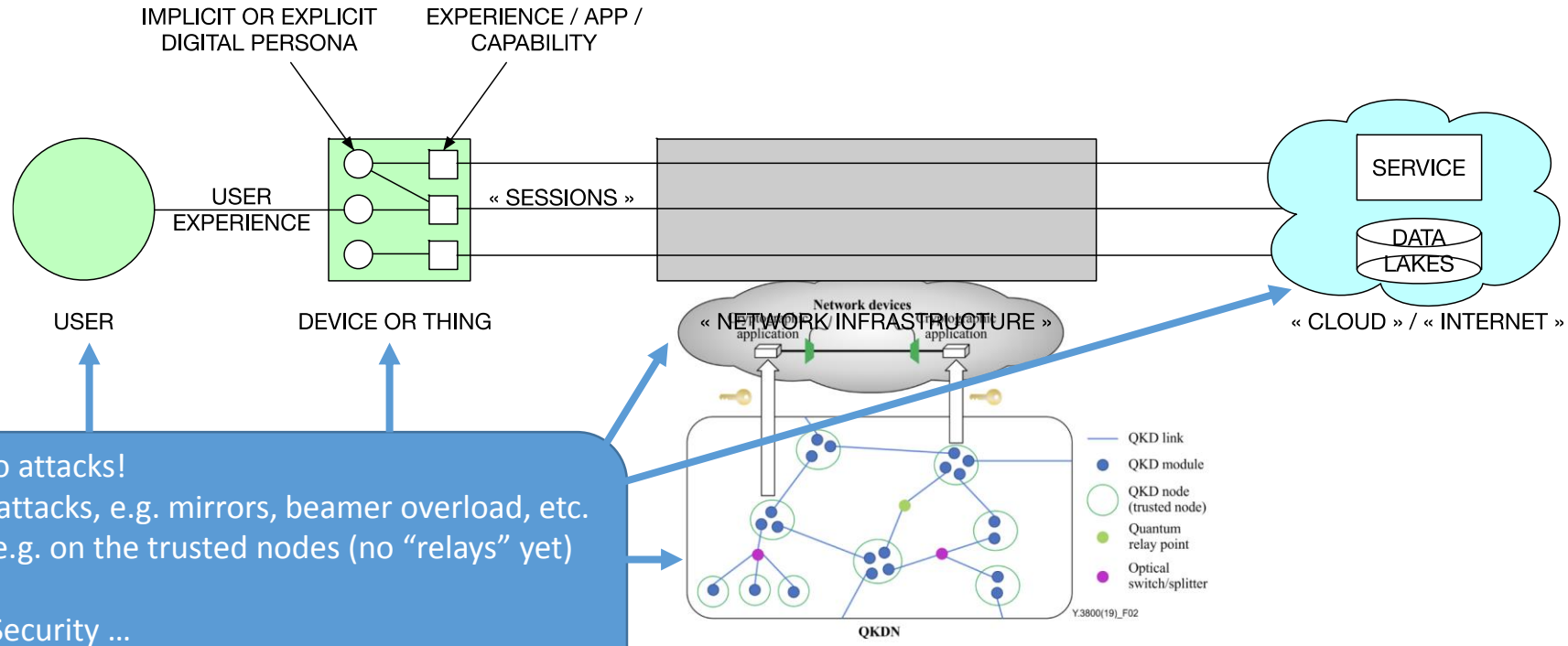


Figure 2 – Illustration of QKDN concepts and their relation to a user network

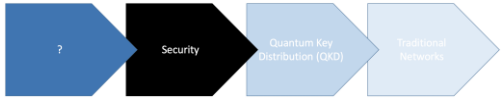
QKD not immune to attacks!

- Physics can do attacks, e.g. mirrors, beamer overload, etc.
- Cyber attacks, e.g. on the trusted nodes (no “relays” yet)

Need Operational Security …

But where is it defined?

Operational Security – The Sad Status



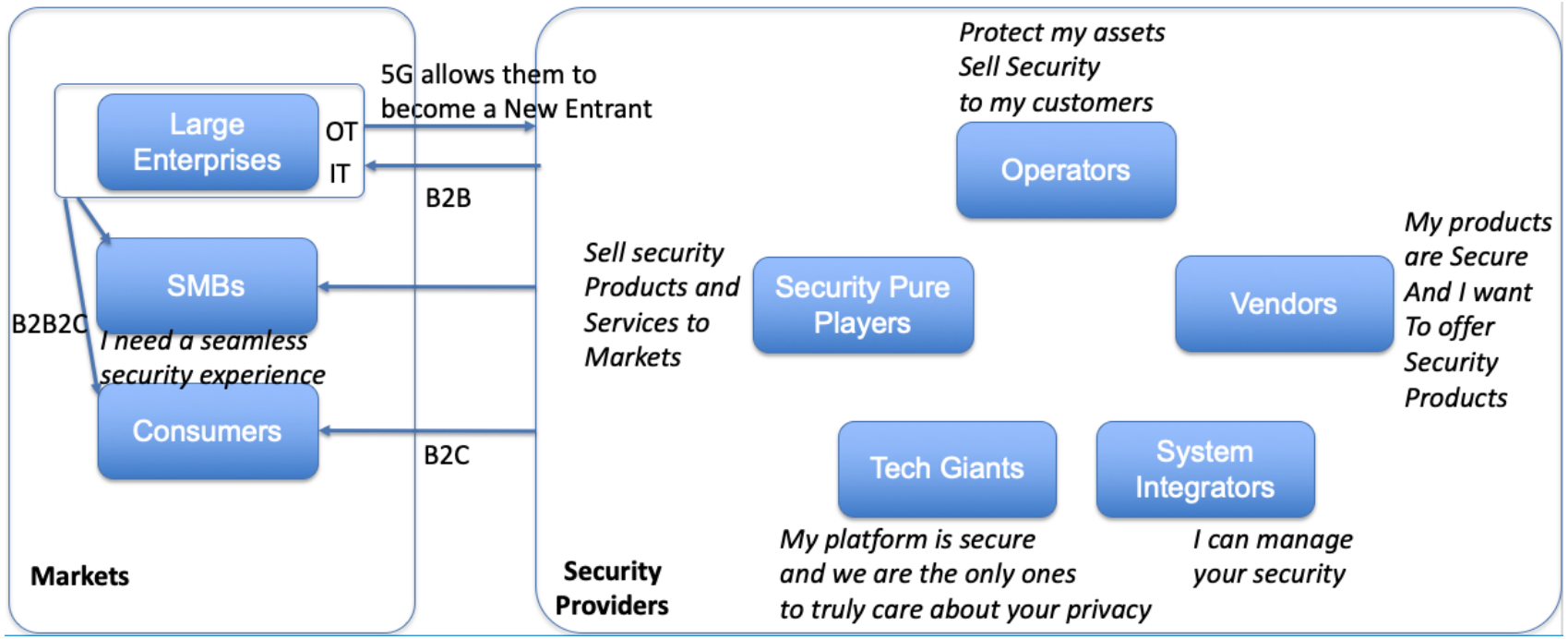
Operational Security Layer	Nature of the layer	Ideal Status	Real Status
Security Services (Cyber Defence Centers, SoCs, CERT, CSIRT, assessment, pentests, etc.)	**People** Doing the cyber security services	- Professionalisation - Easy access to manpower	- Vocational at best - Gross lack of manpower - CDC definition nascent (X.framcdc)
Playbooks	**Knowledge** Human and Machine readable recipes	- JSON based playbooks - Shareable	- Inexistent, gap (OASIS CACAO now)
Security Stack	**Security Products** Endpoint Security, Network Centric Security, …	- Formal overall architecture - Orchestratable - Integratable - Simple	- Inexistent, gap (OASIS, ITU) - Overly complicated stack - Industry consolidations needed - Encryption != security
Asset to Protect	**Architecture to Protect** Networks, Devices, Data Centers, IoTs, Verticals, People	- Secure by design allows orchestrator - Attack surface minimized	- Secure by Design != Secure - Gigantic attack surface with 5G, IoT, Verticalization, etc.

An unsaid Babel Tower

Difficulties inside and between each of the main constituencies

- Governments
- Industry
- Academia
- Civil Society

Example: Industry Babel Tower



Thank You

NOTE: I could have taken any other emerging topic than Quantum and arrived to the same conclusion!