



Francisco Fontes

Senior Technology Consultant · Altice Labs, S.A.



QKD Networks and 6G

Innovation for the Connected Future

Company at a Glance

75+ years of telecom innovation

500+ experts based in Aveiro, Portugal

Altice Group's dedicated innovation and R&D hub

Market Position

Leading telecom innovator in Portugal with global operator deployments

Trusted partner with proven expertise across fixed, mobile and digital networks

End-to-end portfolio spanning **Fixed Networks, 5G, Cloud, IoT and AI**

Innovation Focus

Telecom innovation & R&D:
5G/6G, FTTH, OLT & ONT

Advanced digital platforms:
OSS/BSS, AI & cloud-native

Strong European R&D network:
EU projects, universities & research

5G Lab validation
solutions tested before market launch

Quantum Keys Distribution Networks (QKDN)

Network infrastructure that securely distributes cryptographic keys between users using quantum key distribution, enabling the detection of eavesdropping and enhancing communications security against both current and future quantum-enabled attacks

Quantum Technologies

Quantum technologies exploit the laws of quantum mechanics to process information, communicate securely, and measure the physical world beyond classical limits.



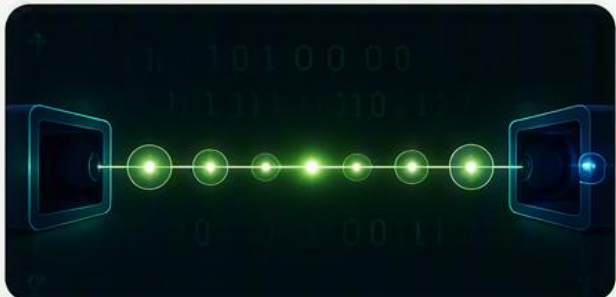
Quantum Computing



Leverages **superposition** and **entanglement** to perform computations in fundamentally new ways, enabling major speedups for selected optimization, simulation, and cryptographic problems.



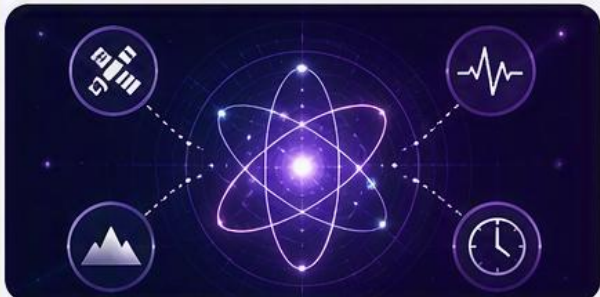
Quantum Communications



Exploits quantum properties of light and matter to provide **ultra-secure** information exchange, detect eavesdropping, and enable future quantum networking and **Quantum Internet** applications.



Quantum Sensing



Harnesses quantum phenomena to measure physical parameters with **unprecedented accuracy and sensitivity**, supporting advanced navigation, imaging, detection, and monitoring applications.

Foundational Quantum Phenomena



Superposition

A quantum system can exist in multiple states simultaneously.



Entanglement

Quantum systems become correlated and linked, no matter the distance.



Interference

Quantum waves can constructively or destructively interfere.



Tunneling

Particles can pass through barriers that are impossible to cross classically.



Coherence

Quantum states can maintain well-defined phase relationships.



Duality

Quantum entities exhibit both wave-like and particle-like behavior.

Preparing for the Quantum Threat (Q-Day)

The transition to quantum-safe security is urgent.



1. THE THREAT

When quantum computers becomes powerful enough to, in practical time, break widely used public-key cryptography, e.g., RSA, Diffie-Hellman, and Elliptic Curve Cryptography



compromising the confidentiality and authenticity of today's digital communications

2. TIMELINE: Q-DAY

Expected to happen between

2029 – 2038

most likely around the

early-to-mid 2030s



3. ACT NOW

Before Q-Day, "harvest now, decrypt later" attacks are happening, making the transition to other mechanisms an urgent priority for governments, enterprises, and critical infrastructures



Capture now and store, **decrypting** when a cryptographically relevant quantum computer exists to efficiently perform the task

HOW "HARVEST NOW, DECRYPT LATER" WORKS



Encrypted data is transmitted today using public-key cryptography



Attackers intercept and harvest the encrypted data now



Data is stored for future decryption



When a powerful enough quantum computer exists (Q-Day)...



...the data is decrypted, compromising confidentiality and authenticity

SOLUTIONS: BUILD QUANTUM-SAFE TODAY



1. PQC (POST QUANTUM CRYPTOGRAPHY)

Use cryptographic algorithms that are believed to be secure against quantum attacks.



Software-based solution



Deployable across existing systems



Protects data in transit and at rest



2. QKD (QUANTUM KEY DISTRIBUTION)

Use quantum properties of light to generate and share encryption keys with provable security.



Detects eavesdropping in real time



Provides keys for symmetric encryption



Ideal for high-security communications



The transition to quantum-safe cryptography is not optional—start today to protect tomorrow.

Post Quantum Cryptography (PQC)

Building Quantum-resilient security

THE CHALLENGE

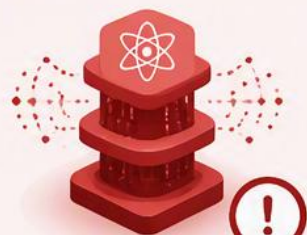
Today's Public-Key Cryptography

Relies on math problems that standard computers find very hard to solve.



Quantum Threat

A large quantum computer running Shor's algorithm can solve these problems quickly.



THE SOLUTION: POST-QUANTUM CRYPTOGRAPHY



Replaces vulnerable algorithms with **quantum-resistant** alternatives.



Based on hard mathematical problems believed to remain secure even for quantum computers.



Post-quantum algorithms run on **regular, classical computers**.



Enables **crypto-agility**, allowing systems to smoothly transition to new cryptographic standards.

Key PQC Algorithms



ML-KEM

(Module-Lattice-Based Key-Encapsulation Mechanism)
Used for secure key exchange and data confidentiality.



ML-DSA

Used for digital signatures, authentication, and checking data integrity.



SLH-DSA

Used for digital signatures, authentication, and checking data integrity.

SEAMLESS INTEGRATION WITH TODAY'S INFRASTRUCTURE



TLS / HTTPS



VPNs



5G Networks



PKI



Enterprise Applications

Can be **integrated into existing systems** including TLS, VPNs, 5G networks, PKI, and enterprise applications.



A CRITICAL CYBERSECURITY PRIORITY

Migration to post-quantum cryptography is essential—well before the arrival of cryptographically relevant quantum computers.

TODAY



Q-DAY



Migration needed well before Q-Day

Quantum Keys Distribution (QKD)

Secure distribution of cryptographic keys, based in quantum communications



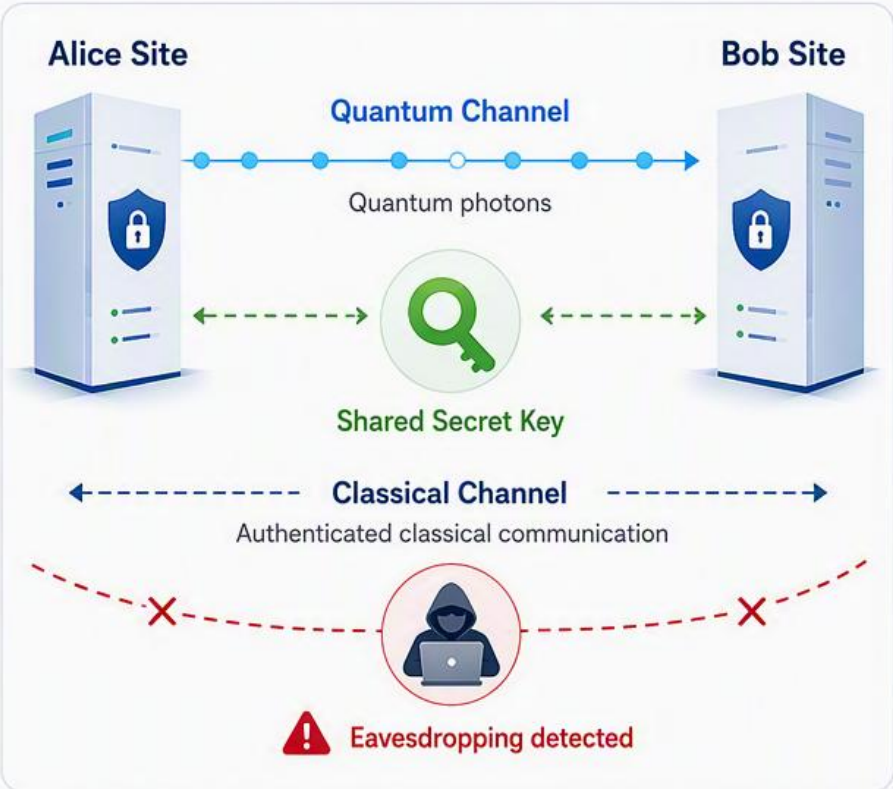
Shared Secret Key
Two parties establish a shared cryptographic key



Security by Physics
Security guaranteed by quantum mechanics



Eavesdropping Detection
Any interception attempt is immediately detectable





EuroQCI
Europe-wide quantum communications infrastructure



IberianQCI
Interconnecting Portugal and Spain



PTQCI (Portugal)
4 connected quantum sites

 **Altice Labs**

 SDN design and implementation of PTQCI

 Participant in IberianQCI



Quantum-safe key exchange



Eavesdropping detection

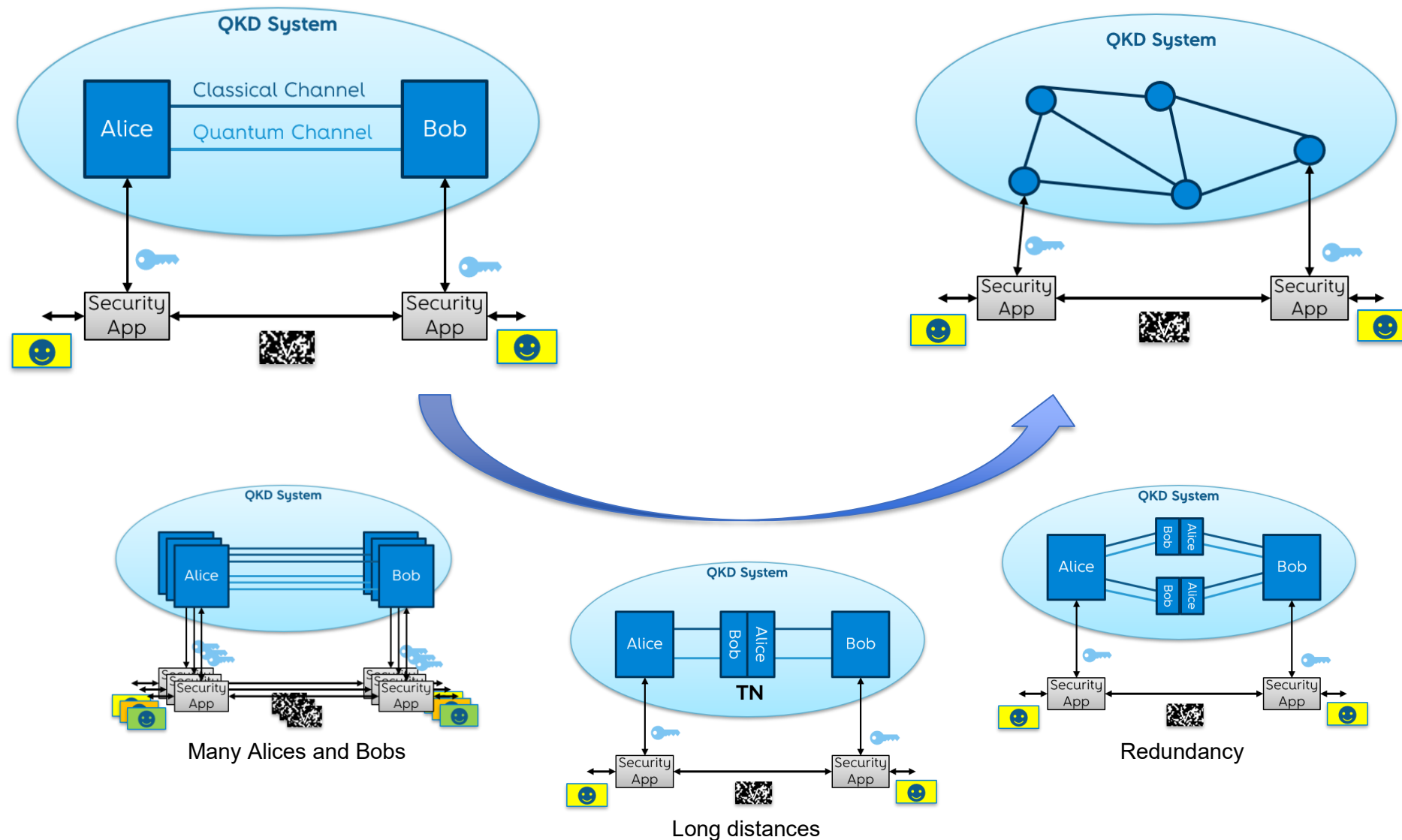


Quantum communication infrastructure

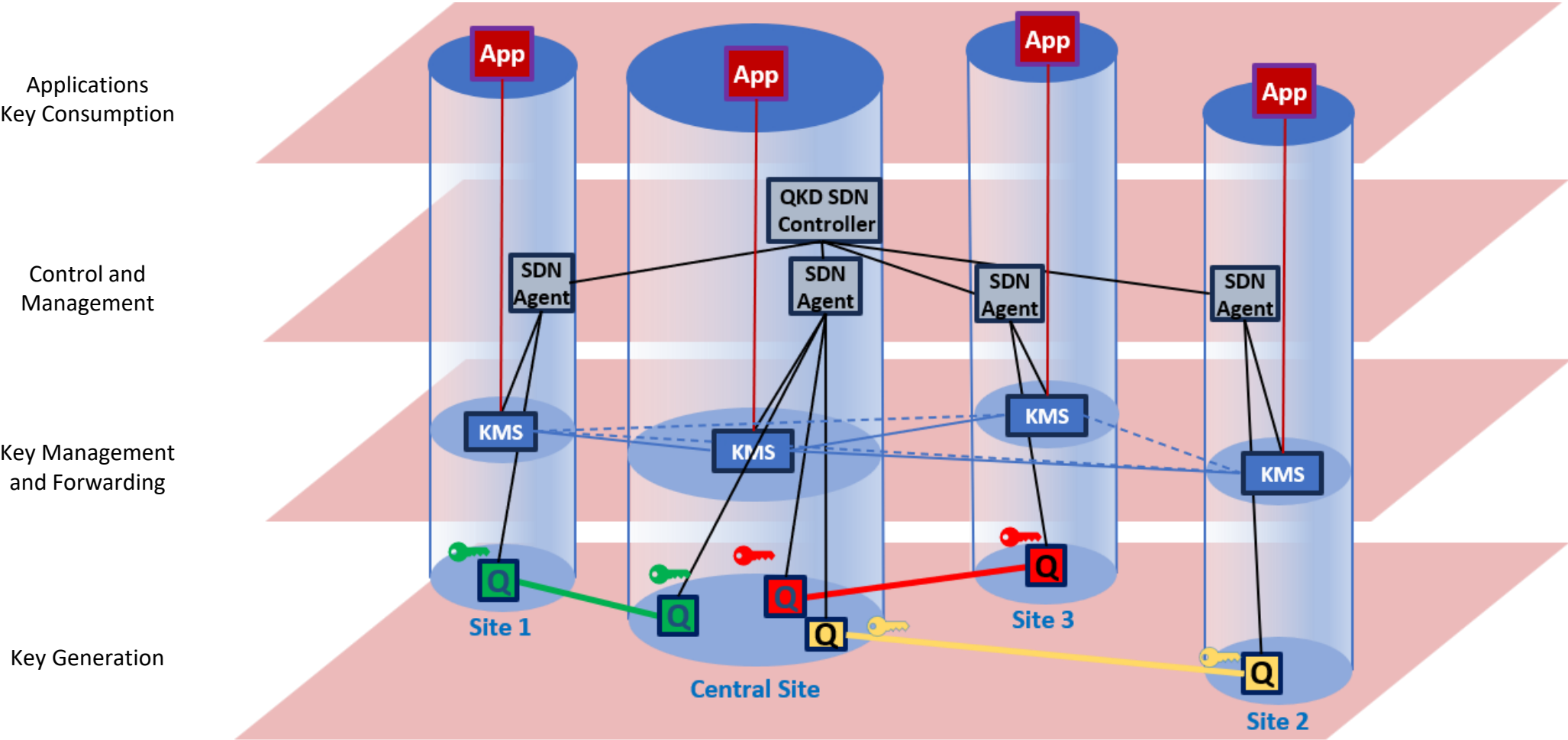


Connectivity from Portugal to Europe

From QKD to QDK Networks and QKD Services



PTQCI QKD Network



6G

ITU-R IMT-2030

Next generation mobile communication system,
natively incorporating AI as a new architecture plane,
seamlessly integrating communications, computing, sensing, and intelligence,
to enable autonomous, intent-driven services across terrestrial, aerial, and space domains

Trends of IMT-2030 /6G (1)

Motivation and societal considerations

1. Inclusivity
2. Ubiquitous connectivity
3. Sustainability
4. Innovation
5. Enhanced security and resilience
6. Standardization and interoperability
7. Interworking

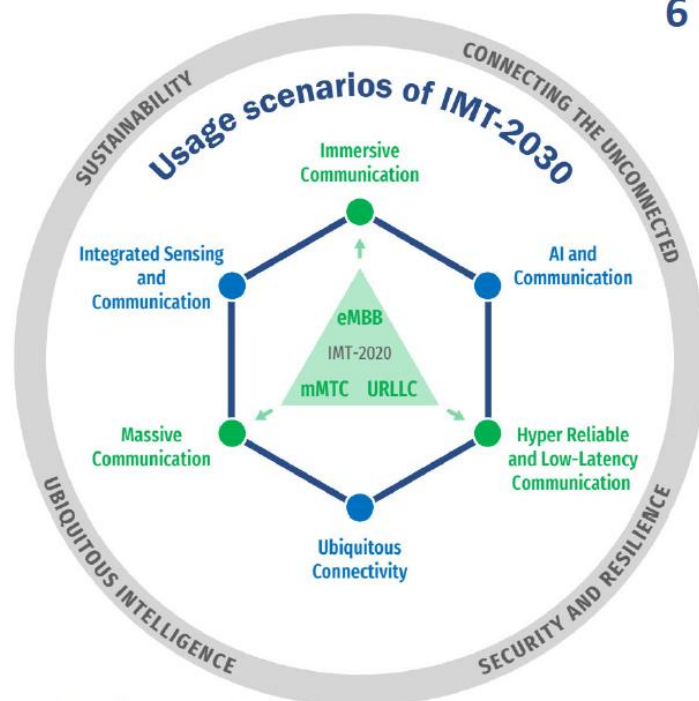
User and application trends

- Ubiquitous
 - Intelligence
 - Computing
 - Connectivity
- Integration of Sensing And Communication
- Sustainability
- Immersive multimedia and multi-sensory interactions
- Smart industrial applications
- Digital health and well-being
- Digital twin and virtual world

(1) ITU-R M.2160-0 (11/2023)

6G Usage scenarios and Capabilities (1)

Usage scenarios



So called "Wheel diagram"

6 Usage scenarios

Extension from IMT-2020 (5G)

eMBB → Immersive Communication

mMTC → Massive Communication

URLLC → HURLLC (Hyper Reliable & Low-Latency Communication)

New

Ubiquitous Connectivity

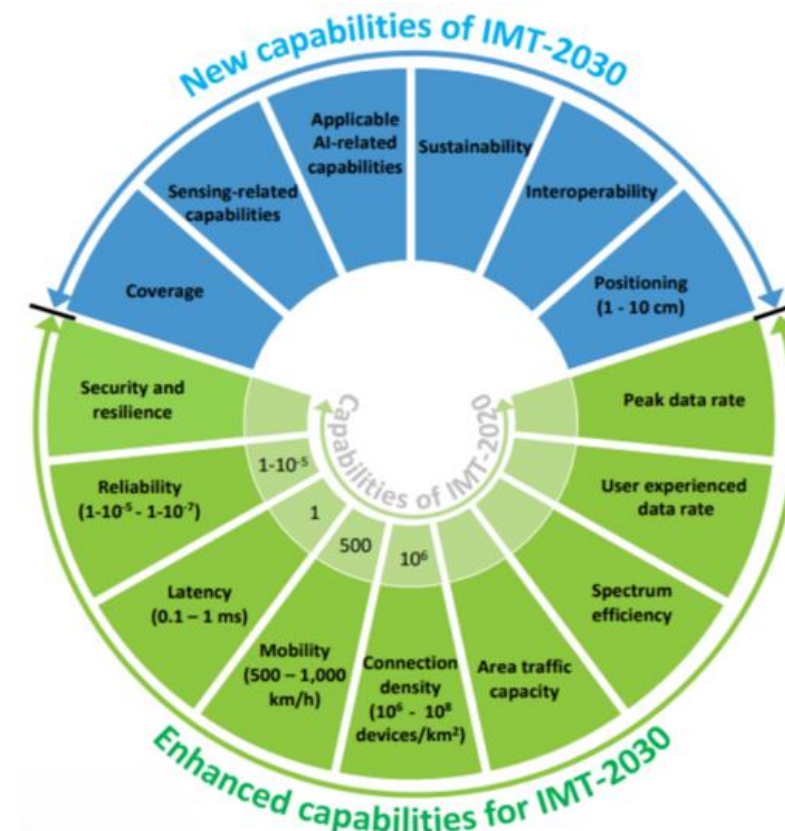
AI and Communication

Integrated Sensing and Communication

4 Overarching aspects:

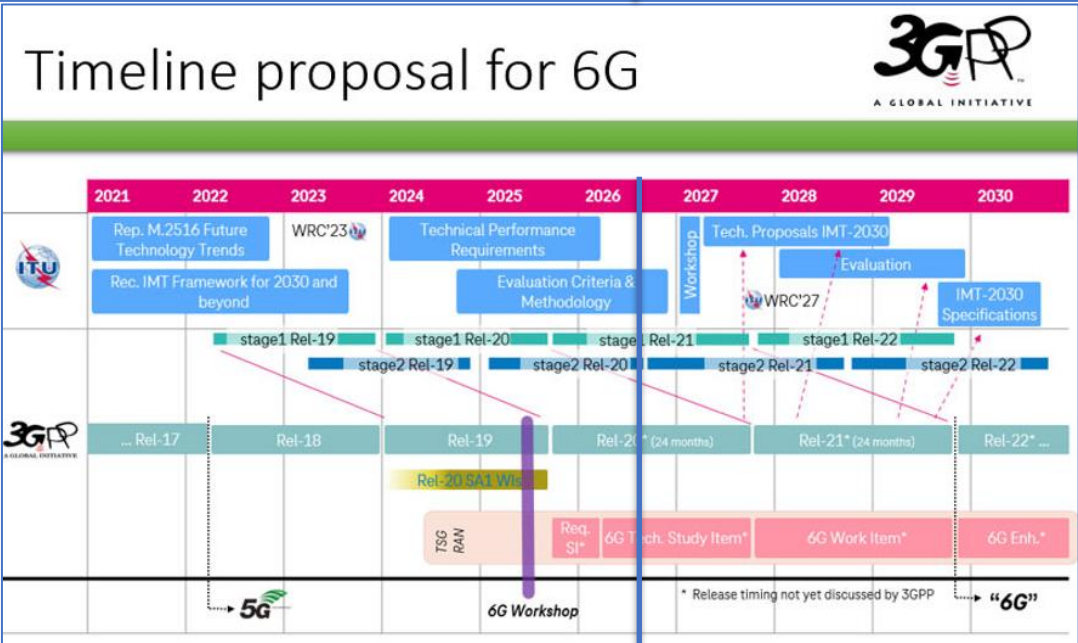
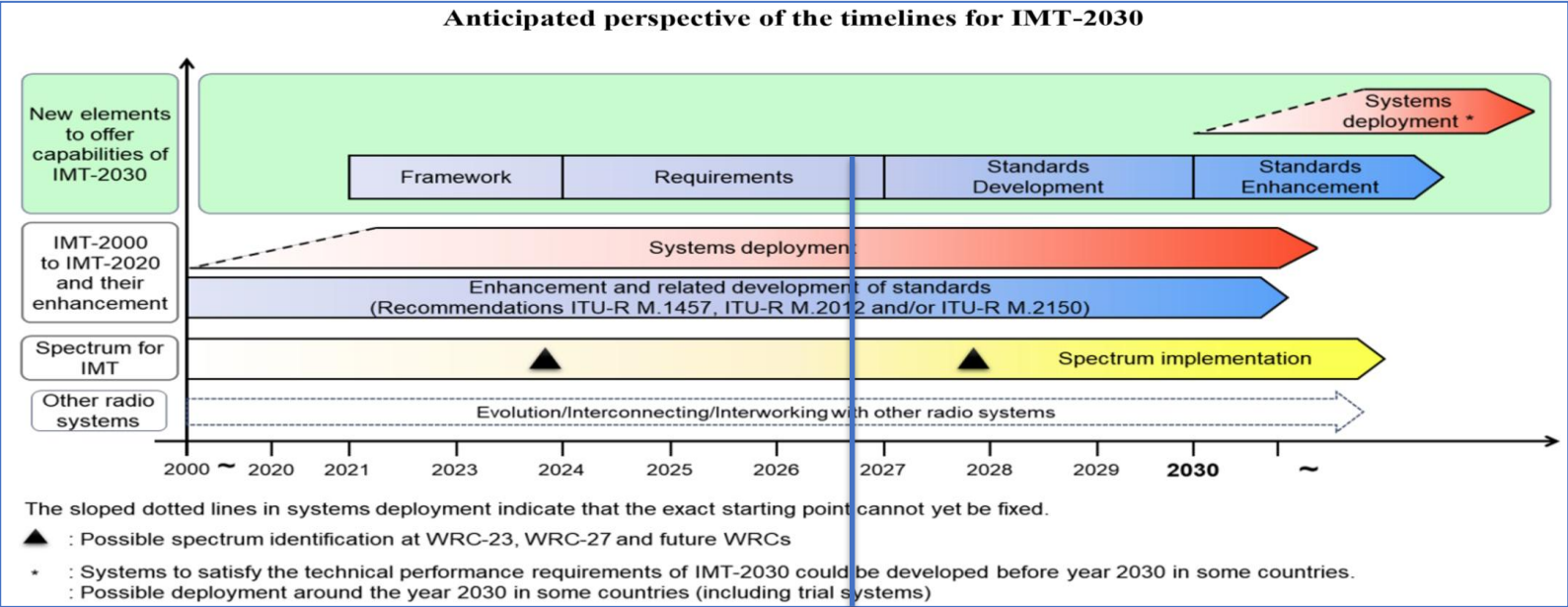
act as design principles commonly applicable to all usage scenarios

Sustainability, Connecting the unconnected,
Ubiquitous intelligence, Security/resilience



(1) ITU-R M.2160-0 (11/2023)

6G Timeline: ITU-R and 3GPP



As for 5G and IMT-2020, 3GPP will develop candidate technologies for IMT-2030 (6G)

6G: What seems to be definitive

Most likely an evolved standalone core (6GC) with support for cloud-continuum

- Built directly on top of the cloud-native, Service-Based Architecture (SBA) developed for 5G

New AI plane: AI-Native (not AI-assisted)

- Intent-Driven and zero-touch operation
- Agentic Networks

Cloud-native, distributed architecture

Improved quantum-safe security (6G will face the Q-Day!) and resiliency

Continuity of 5G-NR basic principles (no NOMA)

- Signal, modulation, and channel coding will remain

Integrated Sensing And Communications (ISAC)

Multi-RAT

More spectrum, in FR3/7-15GHz

(1) <https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci>

“

Quantum and 6G will shape communications for the 30s decade



Obrigado.

Questões e contactos

fontes@alticelabs.com

wireless-meeting.com