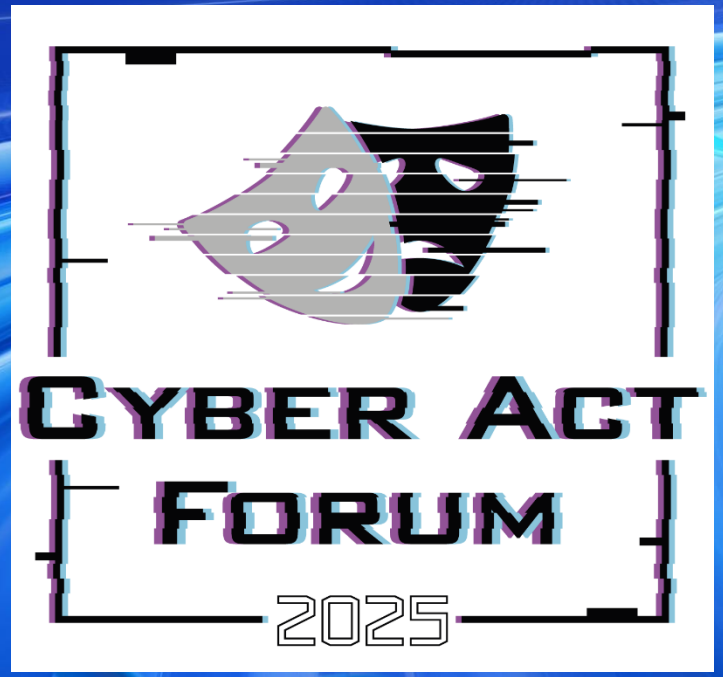
“Security in DNA, Trust through Transparency”

ZTE



Anticipating a More Secure and Intelligent Digital Era: AI, Security, and the Evolution Beyond 5G

Luca Bongiorni

Director of ZTE Italia’s Cybersecurity Lab

Security Evolution from 1G to 6G: A Brief Overview

ZTE

ZTE

Key Strategic Direction:

Evolution towards 6G

6G Security Evolution Drivers

Technical Requirements

Quantum Crisis

- Quantum computing could break traditional encryption in 10 to 20 years.
- 6G standards will be completed by 2030.
- 6G must include post-quantum cryptography (PQC) to stay secure.

AI Threats

- Communication and AI integration in 6G is an industry consensus.
- Ensuring AI security is the first priority.

Business Requirements

Immersive XR

Ultimate resolution, 10 Gbit/s, MTO latency < 20 ms, avoiding dizziness

Digital Twin

Virtual &Real Integration, Models Reliable & Credible

V2X

Vehicle-to-vehicle: 5 ms,
Vehicle-to-road: 100 ms,
Vehicle-to-cloud: seconds,

Network Requirements

Desert Search & Rescue

Deep Coverage, Meter-level Positioning

Ubiquitous Connection

Fishery
Animal Husbandry

Building Trustworthy Ubiquitous Connections to Meet Network Needs Everywhere

Wide-area coverage, crop monitoring, low cost, and automatic irrigation control system

Service Requirements

Massive Communications

Terminal Density: $10^6 km^2 \rightarrow 10^8 km^2$

Robot

Sensors detect surrounding environment, a large number of mobile robots, drones, and AGV are deployed

Environment Sensing

The closed-loop control determines the deterministic delay, the network has a reliability of 99.99%. It relies on the perception network

Evolution Requirements

From Out-of-band to In-band

Passive to Active

From Standardization to Customization

AI
Artificial Intelligence

Compute
Human↔Virtual↔Physical Interaction

Connectivity
Ubiquitous Connectivity

Sensing
Self-Sensing Network

Security
Proactive, Intrinsic, & Elastic Security

Security, as Indispensable Safety Gene of 6G Networks & Cornerstone for Ensuring the Stability, Reliability, Authenticity, & Credibility of 6G Networks.

Security Recognized as a Core Element of 6G by Major Organizations Worldwide

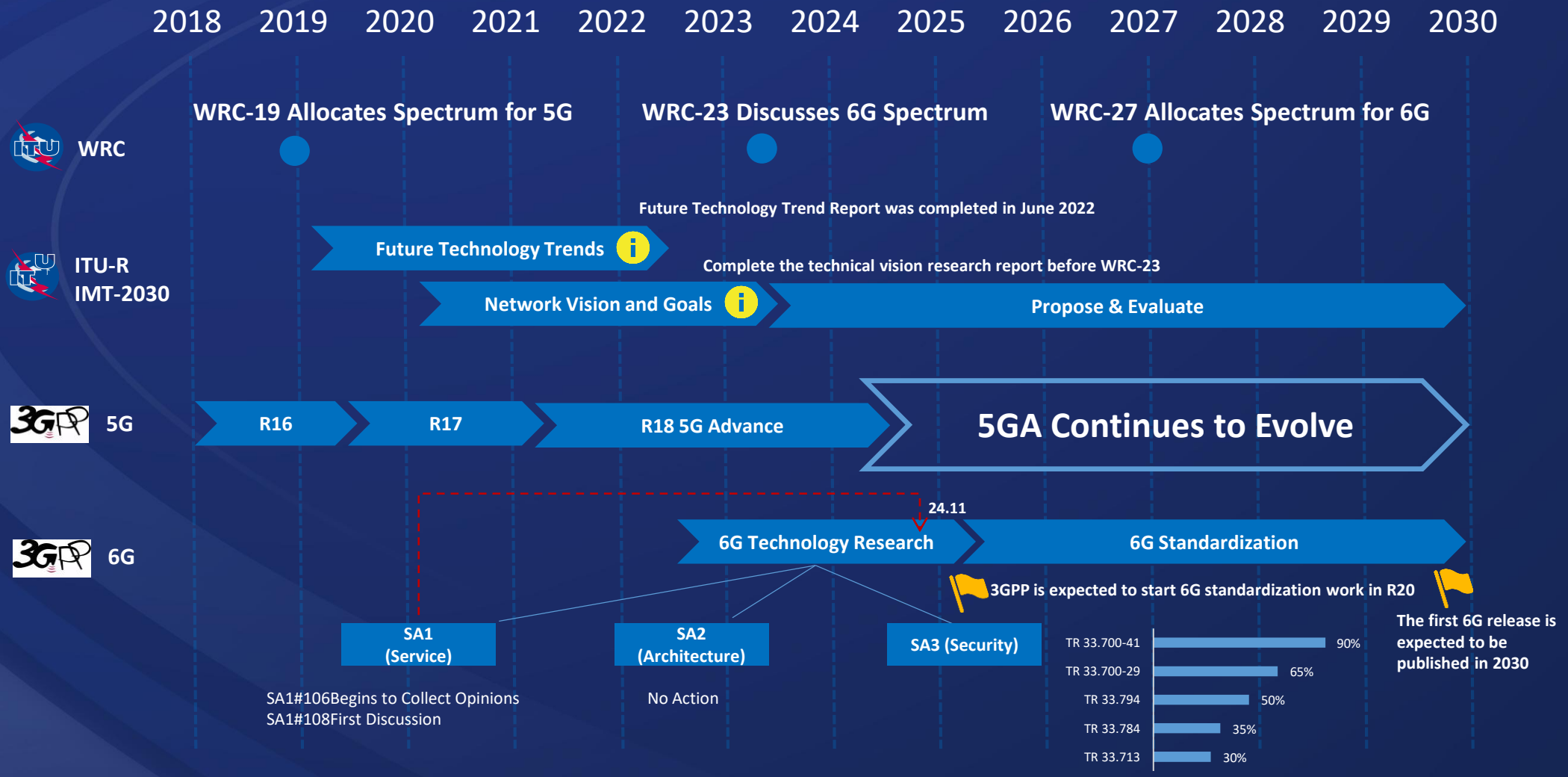
Puneet Jain

3GPP SA
3GPP SA Chair

	Security	AI	Immersive Communication	Energy Efficiency Sustainability	Ubiquitous Connectivity	Perception	Smart Living	Native VoNR	FWA-FWC	LPWA	Northbound API	Healthcare	Autonomous Driving	Positioning	Backward Compatibility
GSMA	√	√	√	√				√							
NGMN	√	√	√	√	√	√	√	√			√	√		√	√
5GAA	√	√	√	√	√	√					√		√	√	
5G-ACIA	√	√	√	√		√					√				√
5G-MAG	√	√	√	√	√	√	√								
GSOA	√				√									√	
TCCA	√	√			√										√
WBA	√	√				√									
B5GPC	√	√	√	√	√	√	√					√	√	√	
6GForum	√	√	√	√	√	√	√					√	√	√	
IMT-2030	√	√	√	√	√	√	√							√	
B6GA	√	√	√	√	√	√	√	√	√	√	√	√		√	√
NextGA	√	√	√	√	√	√	√		√	√		√		√	
6GSNS	√	√	√	√	√	√	√					√		√	
ITU	√	√	√	√	√	√	√					√		√	

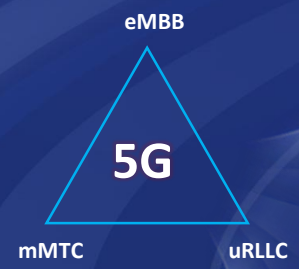
According to the 3GPP SA Chair, security has been unanimously recognized by all 15 global 6G standards and pre-research organizations as the top priority—even ahead of AI—demonstrating the industry's broad consensus on the paramount importance of 6G security.

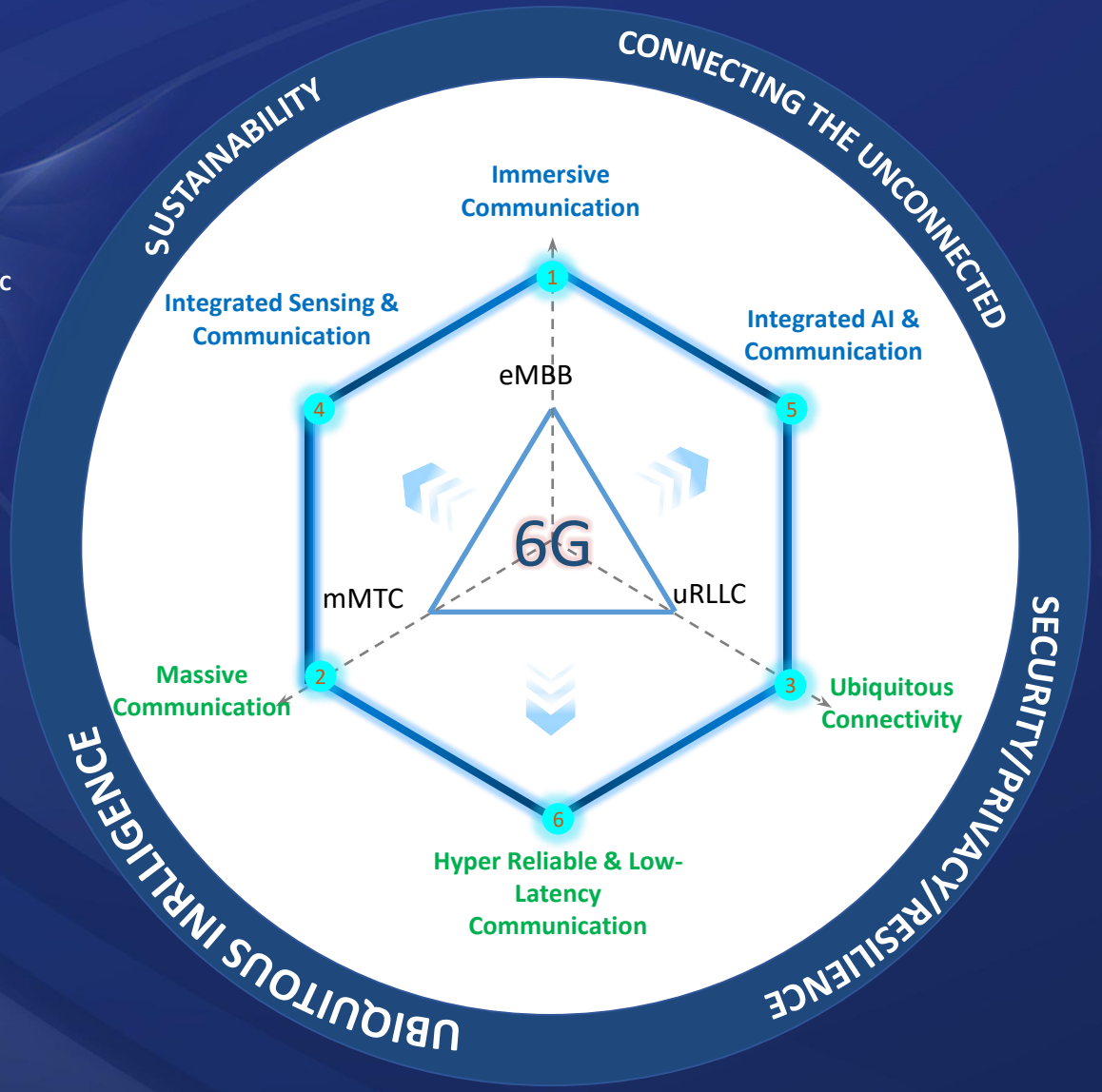
6G Standard Progression



3GPP SA1 officially started the research on 6G requirements in August 2024, other working groups are expected to start the formulation of 6G-related standards in 2025.

6G Core Security Capability





Business Security

Ensure the process **security** of typical 6G services and application scenarios such as communication services, sensing services, intelligent services, and computing services.

Infrastructure Security

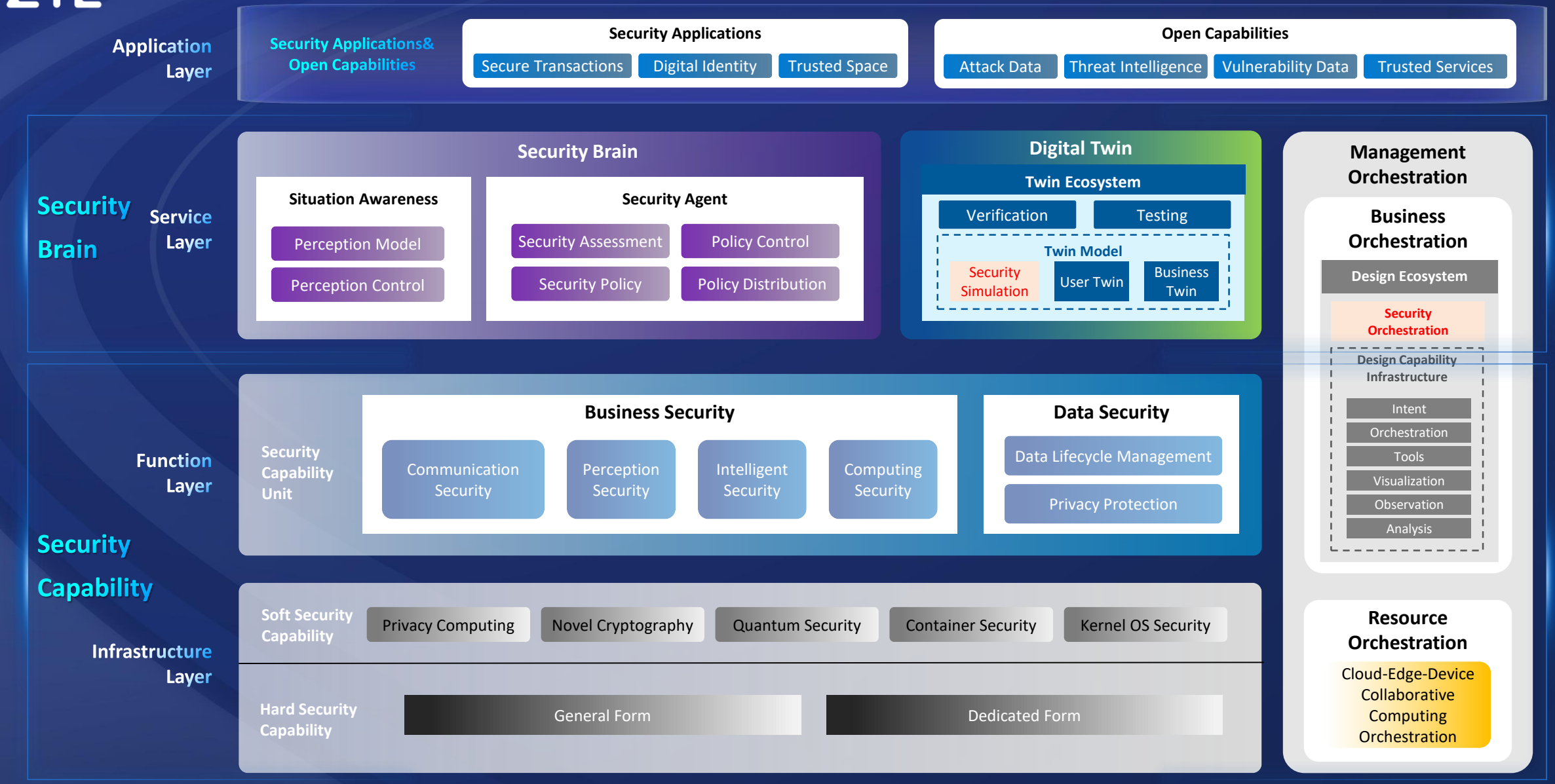
Ensure the security of infrastructure such as IT facilities, links, and communication network elements, with the ability to resist internal and external attacks and achieve **resilient** recovery

Data Security

Ensure the full lifecycle security and **privacy** protection of user data, service data, and network data.

Currently, the 6G security research in the industry is quite fragmented. Starting from the widely recognized overall goals and framework for 6G defined by ITU-R, the key security capabilities for 6G can be identified as: 6G service security, infrastructure security, and data security.

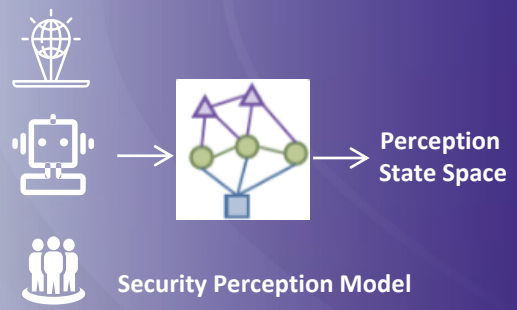
Preliminary Considerations on ZTE 6G Security Architecture



The overall architecture is divided into four layers, with the core focus on the Security Brain and Security Capabilities.

Security Brain: One of the Core of 6G Security Architecture

Situational Awareness Engine



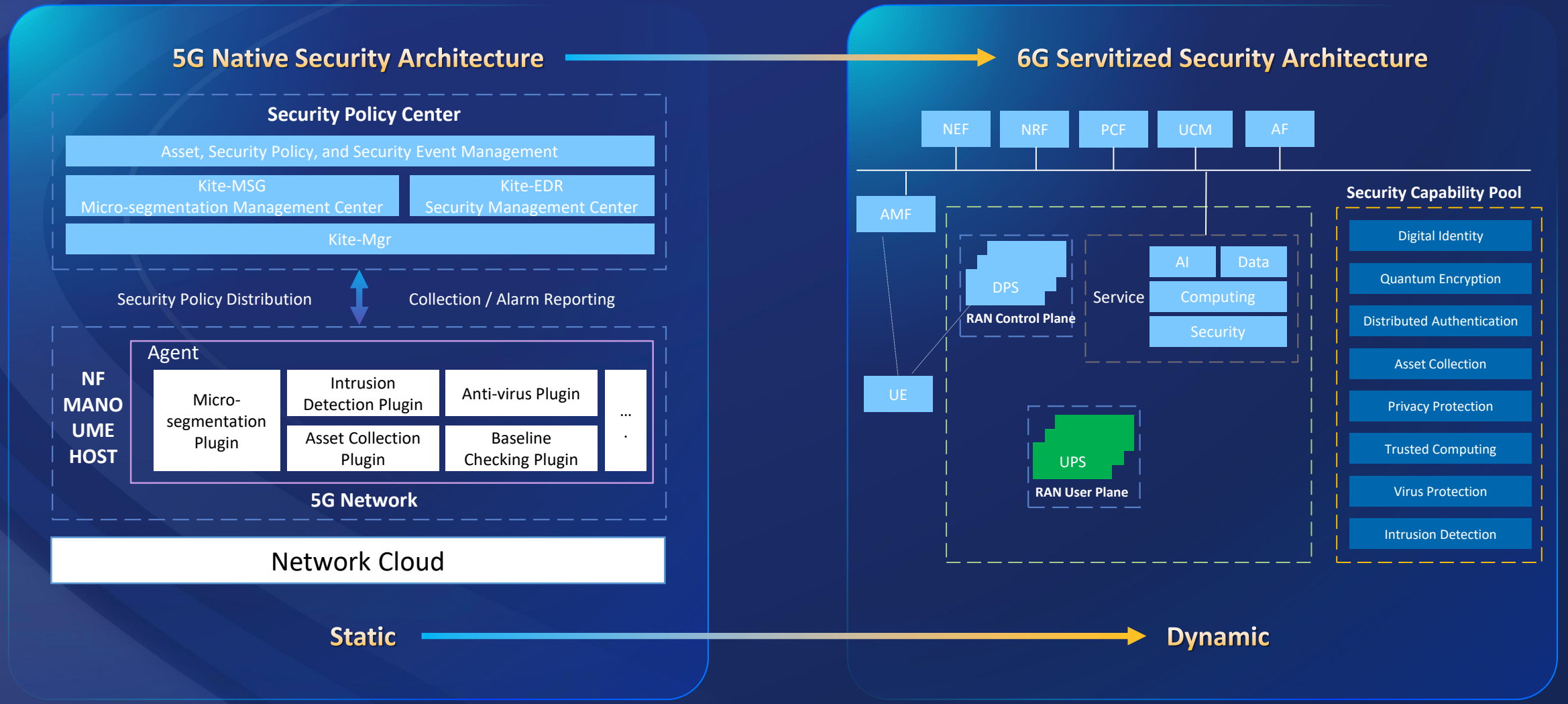
Security Intelligence Center

Security as a Service Capabilities

- Quantum Encryption
- Digital Identity
- Physical Layer Security
- Trusted Computing
- Privacy Protection
- Distributed Authentication

AI serves as the foundational element for 6G development, and the Security Brain is the centralized embodiment of AI-powered 6G security. The 6G security architecture has been built centered on the Security Brain.

Security as a Service: One of the Core of 6G Security Architecture



Servitization of security capabilities is integrated with AI, computing, and data services. Through flexible orchestration, security capabilities can be deployed and scaled on demand to meet diverse security requirements.

Post-Quantum Cryptography: Milestones and Future Horizons

1994

Peter Shor proposes Shor's algorithm, demonstrating ***quantum computers' ability to break RSA and ECC***, igniting interest in quantum-resistant cryptography.

Initial Point

2016

PQC Standardization Launched

NIST ***initiates a global call for quantum-resistant algorithms,*** marking the start of a collaborative effort to standardize PQC.

2022

1st PQC Standards Announced

NIST ***standardizes four algorithms*** (CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON, SPHINCS+), paving the way for practical PQC deployment.

2025-2030

Widespread Adoption and Integration

PQC algorithms will be integrated into protocols like TLS, VPNs, and blockchain, with industries like finance and healthcare leading adoption to secure data against quantum threats.

The threat landscape is keeping evolving....

RISK	Impact	Urgency
Quantum computers threaten to shatter current encryption	Banking, communications, national infrastructure, even cryptography,	This disruption is not hypothetical; It's a visible horizon

The advent of quantum computing poses a significant risk to current cryptographic systems, threatening global data security and privacy.

6G: Building the Infrastructure Base for AI World

ZTE

People, Things→People, Things, Agents

Connectivity→Connectivity,Sensing, Computing

Communication→Distributed Intelligence

Internet of Everyhing→Intelligent Internet of All Everything

Sensing

Multidimentional, Real-time

Connectivity

Diverse, Ubiquitous

Intelligence

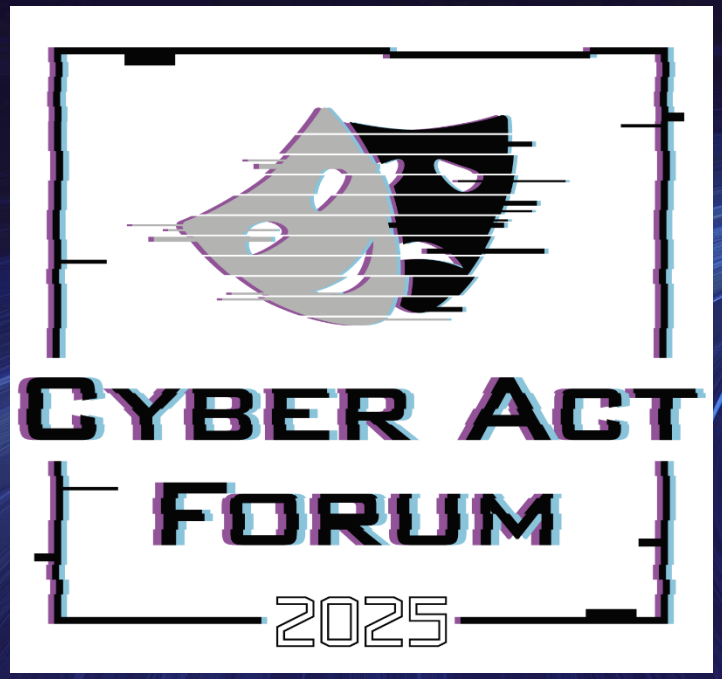
Native, Collaborative

6G

Seamless evolution

THANKS

ZTE



ZTE Cyber Security Lab

Security in DNA,

Trust through Transparency