5G & 6G Security

Emrah Tomur

4th Industrial revolution

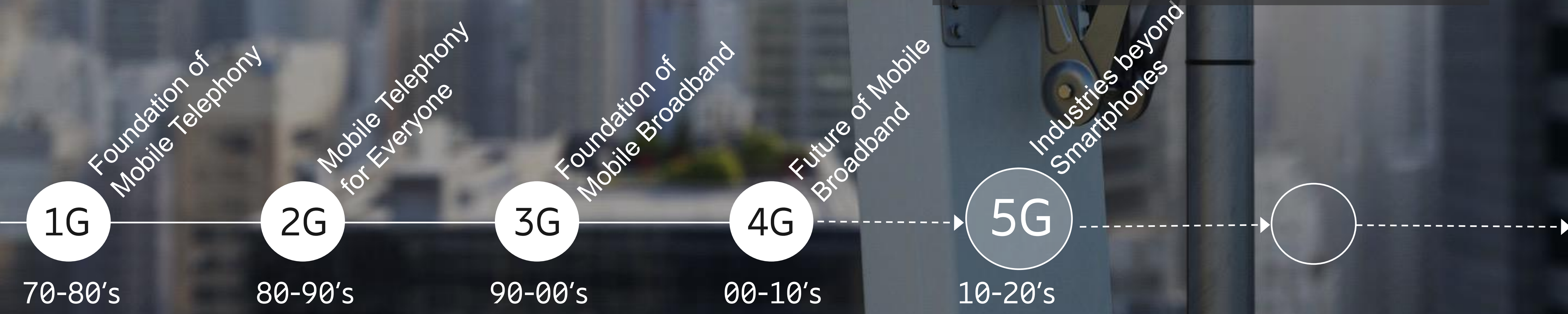
powered by 5G

Enriched Broadband Communications

Critical Machine Type Communications

Massive Machine Type Communications

10-100X End-user Data Rates	
5X Lower Latency	1000X Mobile Data Volumes
10-100X Connected Devices	10X Battery Life


1G
Foundation of Mobile Telephony
70-80's
2G
Mobile Telephony for Everyone
80-90's
3G
Foundation of Mobile Broadband
90-00's
4G
Future of Mobile Broadband
00-10's
5G
Industries beyond Smartphones
10-20's

Why is security so important in 5G?

Constantly evolving security threats

Critical infrastructure and increased business risks

Increasing regulatory requirements (e.g. GDPR)

New deployment scenarios and use-cases

Billions of new devices

Cloud-specific challenges

New business contexts → New attack vectors → New security & privacy approach

Service providers should offer enterprises a trust stack built on evolved telecom network security

Trusted business

Service providers to be trusted by customers and that enterprises can build trusted business together with them.

Trusted operations

Trusted operations of the network and all enterprise processes running on top of it

Trusted deployment

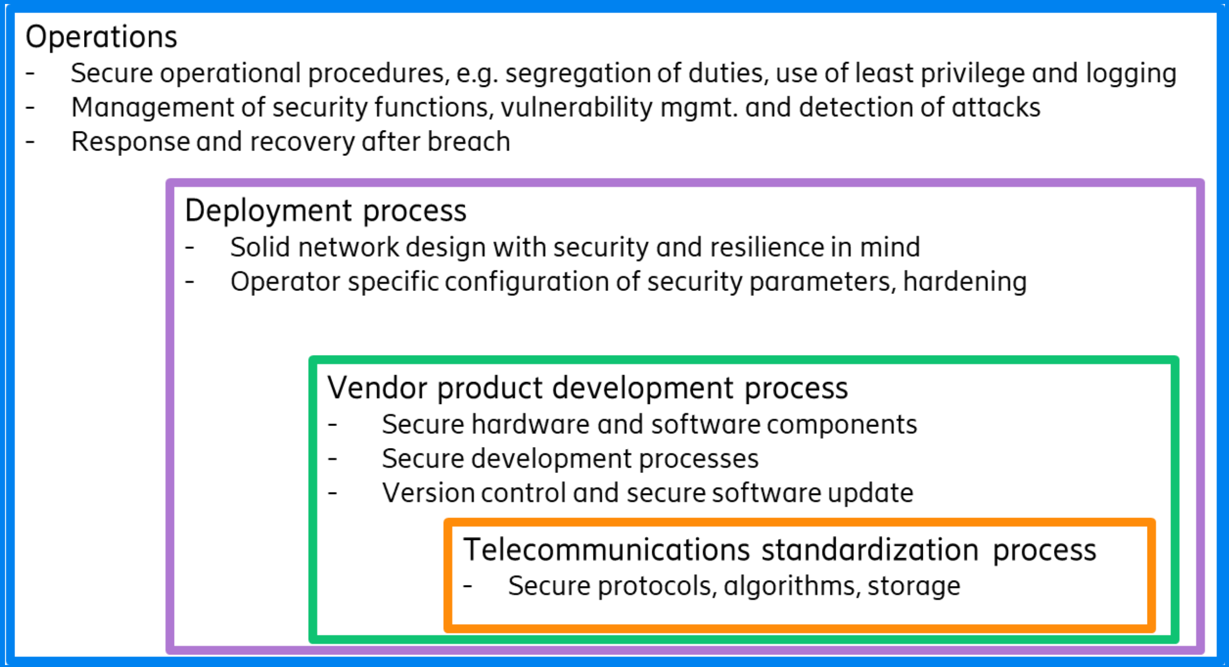
A trusted network architecture and configuration to fend off against the network and the devices that connect to it

Trusted HW & SW

Ensuring trust from the bottom with security & privacy functions, characteristics & HW/SW root of trust in every part of the network

Building trustworthiness in 5G

Operations – daily procedures, monitoring, response
Deployment –hardened architecture and configuration
Product development – robust design and development
Standardization – secure protocols and algorithms
Research – new security solutions



Operations
- Secure operational procedures, e.g. segregation of duties, use of least privilege and logging
- Management of security functions, vulnerability mgmt. and detection of attacks
- Response and recovery after breach

Deployment process
- Solid network design with security and resilience in mind
- Operator specific configuration of security parameters, hardening

Vendor product development process
- Secure hardware and software components
- Secure development processes
- Version control and secure software update

Telecommunications standardization process
- Secure protocols, algorithms, storage

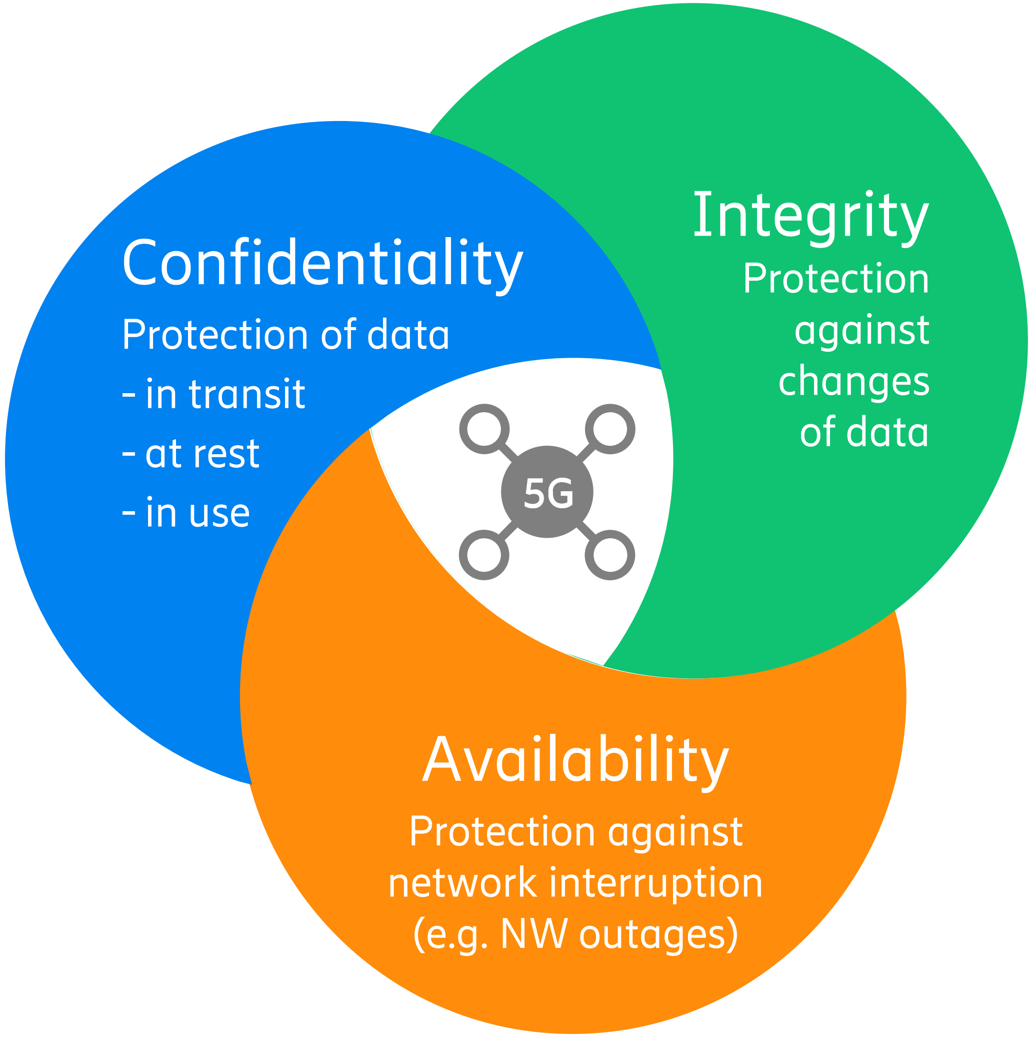
The mobile network assets

Information assets:

- **Data in transit:** data sent over the network.
  - **User data**: content
  - **Control signaling**: information exchange between involved points of network controlling and terminating user data sessions
  - **Management traffic**: information exchange that manages network elements in a network
- **Data at rest:** data stored on a computer or storage system, data centers and clouds
- **Data in use:** data in memory currently used by a computer processor

Other assets:

- Systems and application providing services to users
- Frequency spectra


Confidentiality
Protection of data
- in transit
- at rest
- in use
Integrity
Protection against changes of data
Availability
Protection against network interruption (e.g. NW outages)
5G

Most common issues resulting in security breach or incident

Security policy not enforced or monitored

Lack of hardening

Insecure configuration of the network

Current operational procedures prone for mistakes

Lack of visibility, control and continuous monitoring

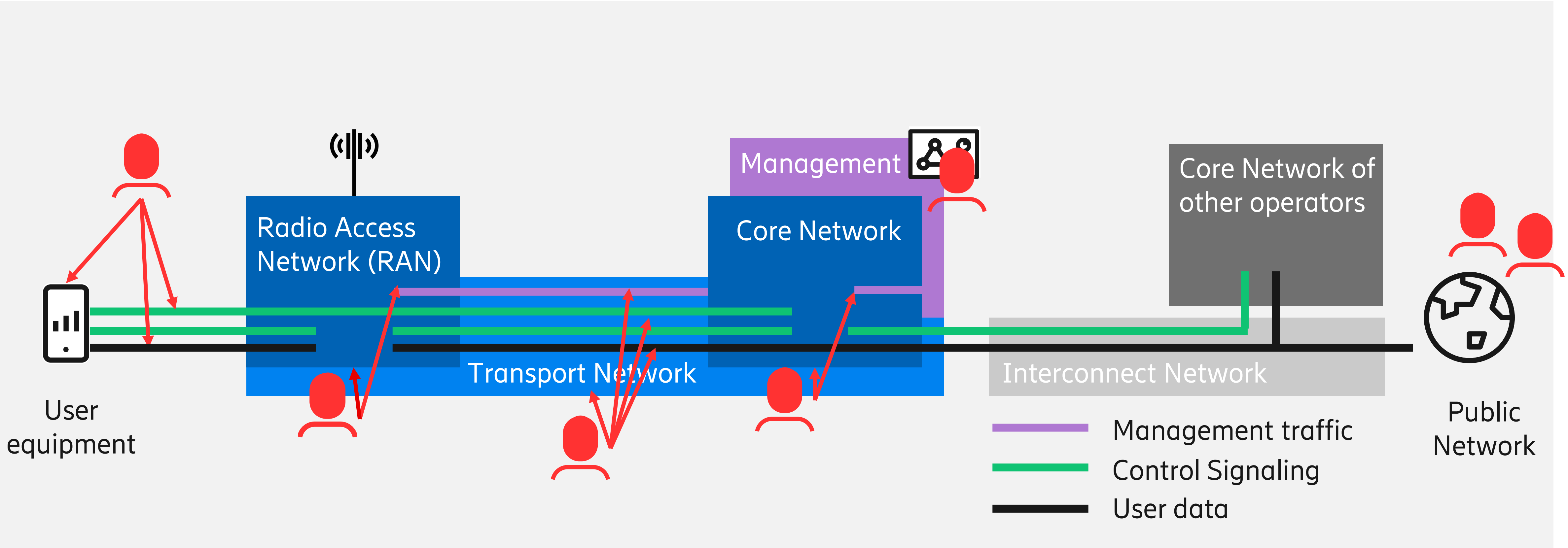
Threat actors & Attacker motivations

- A number of threat actors exist
  - Organized cyber criminals
  - Nation states
  - Hacktivists, e.g. “Anonymous”
  - Terrorists
  - Insiders
- Attacker motivations
  - Money
  - Information and data
  - Sabotage

Mobile network attack vectors

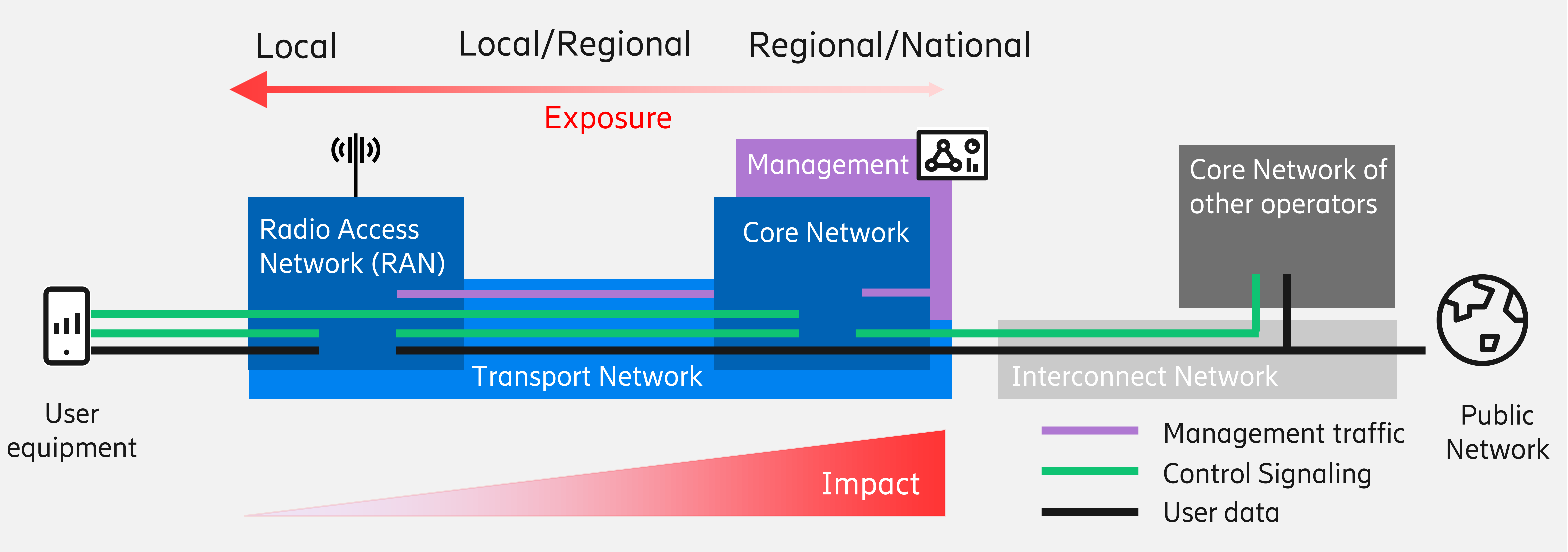
- Eavesdropping
- Denial of Service (DoS)
- Software manipulation/malware
- Man-in-the-Middle
- Physical attack
- Insider attack
  - Intentional
  - Unintentional

Examples of common attacks



Risk for intrusion across the network

- Threats
  - Nodes/Data centers closer to the RAN are more exposed physically
  - Network between nodes/data centers are also exposed to attacks
- Network impact lower further out toward the RAN

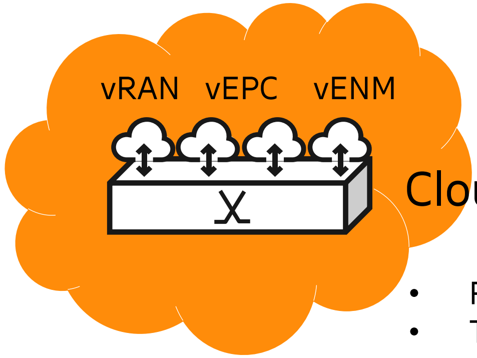


Virtualization & cloud security

New attack vectors and trust relations requires additional security

- SW decoupled from dedicated HW
- Other organization is managing the infrastructure
- Yet another organization may share the same HW

Virtual nodes

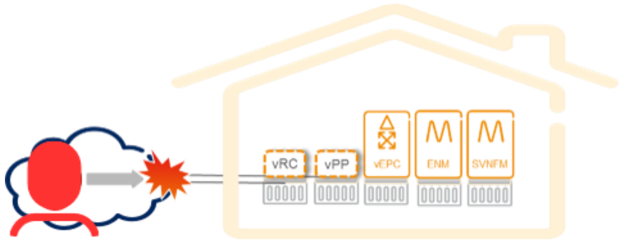


vRAN vEPC vENM

Cloud infrastructure

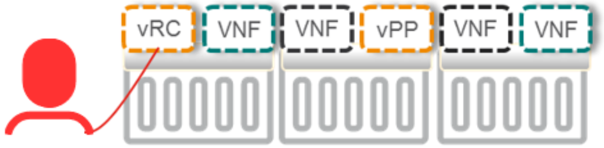
- Root of trust tied to HW?
- Trusted anchors tied to HW?

- External attack/intrusion
  - – Protection of traffic and access



- Cross VNF attacks
  - + Environment correctly set-up
  - + Protection of keys and SW

- Insider attack/intrusion
  - + Additional authentication and different levels of authorization
  - Trust required



Security defined by 3GPP

Air interface

- Mutual authentication (User Equipment – Core NW)
- Integrity protected control signaling (mandatory)
- Encrypted User and Control signaling traffic (option to enable)
- 5G Standalone - Integrity protected user traffic (option to enable)*
- 5G Standalone - Enhanced Subscriber Privacy
  - Concealing the SUPI (IMSI)

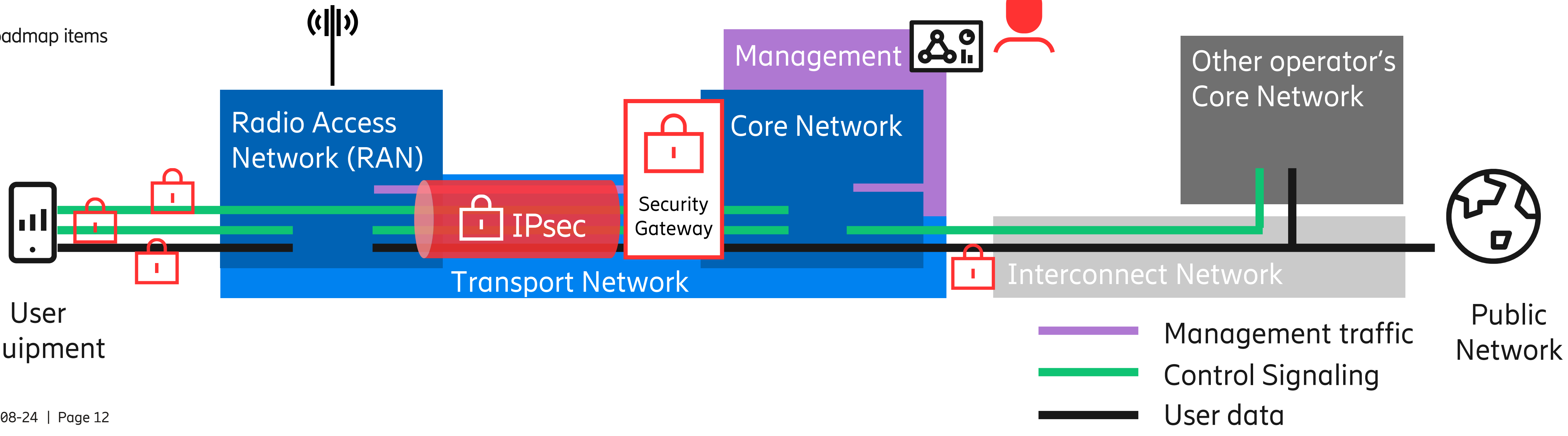
Interconnect Network

- 5G Standalone - protection of application data over the roaming interface

Transport Network

- IPsec
  - Mutual authentication (Radio Node – SEG, option to enable)
  - Encrypted and integrity protected traffic, all or parts (option to enable)
- DTLS (5G Standalone, (gNB – 5GC, gNB-DU – gNB CU))*
  - Mutual control signaling authentication (option to enable)
  - Encrypted and integrity protected control signaling traffic (option to enable)

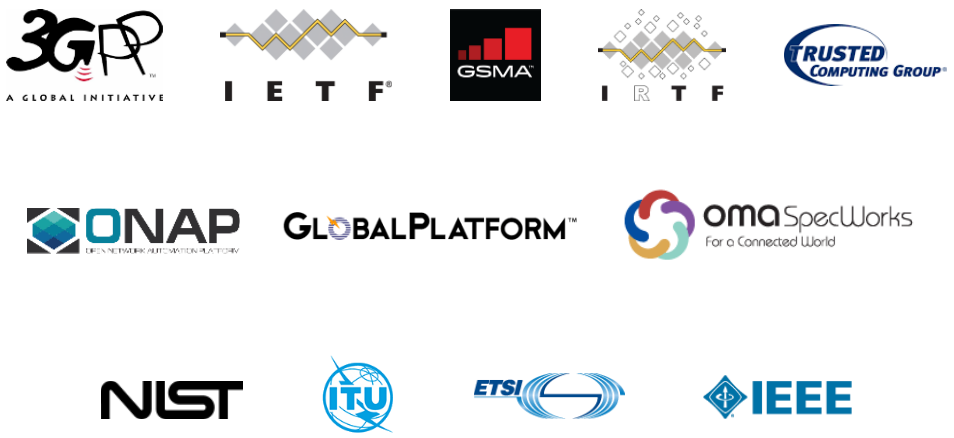
(Blue text = new with 5G/3GPP Rel. 15)



* Roadmap items

5G security standardization

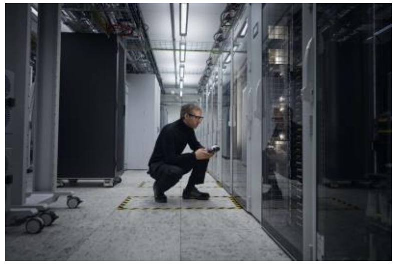
Ericsson drives security standardization for mobile networks in all the most-relevant organizations, and participates or monitors the rest



3GPP defines the 5G mobile network system

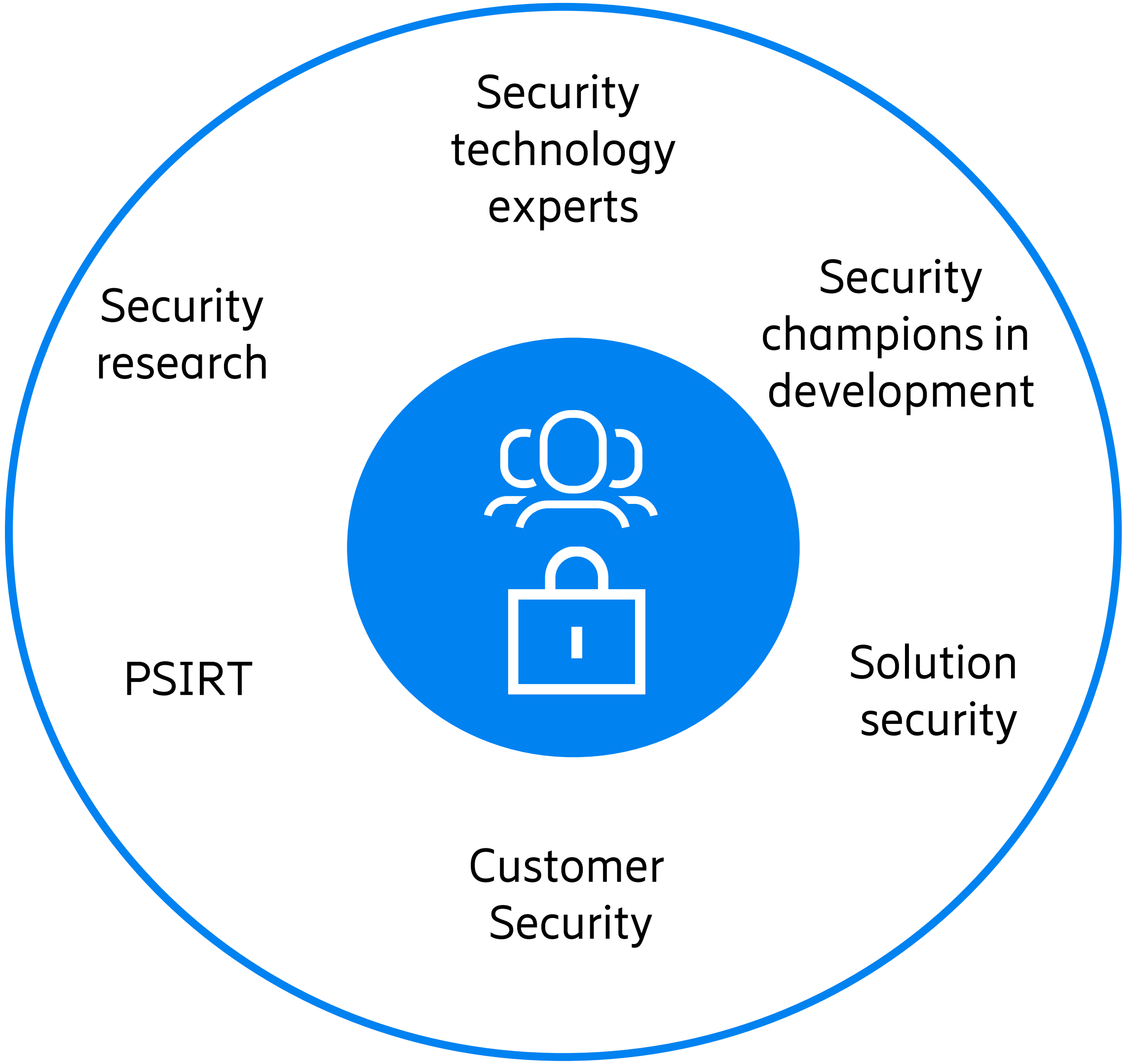
- 3GPP (the 3rd Generation Partnership Project) unites telecommunications standard development organizations around the world (i.e., ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, and TTC).
- It is the de-facto organization that develops technical specifications for mobile networks (i.e., 2G, 3G, 4G, and 5G)
- Its technical specifications are published as so-called "Releases", each of which provides a set of functionalities that are stable at a given point and can be implemented
- 3GPP Release 15 delivered the first 5G technical specifications

Safeguarding the network



Security operations & management	Adaptive & automated security to manage dynamic environment	Ericsson Security Manager with threat mgmt. (ESM)
Secure platforms & applications	Ensuring end-to-end security architecture	Security products and functions
Secure products	Privacy and security built-in to products by design	Secure product development (SRM)
Secure approach	Consistent security practices appropriate to the new context	3GPP security standards as foundation

Security through the lifecycle



Security technology experts

Security champions in development

Solution security

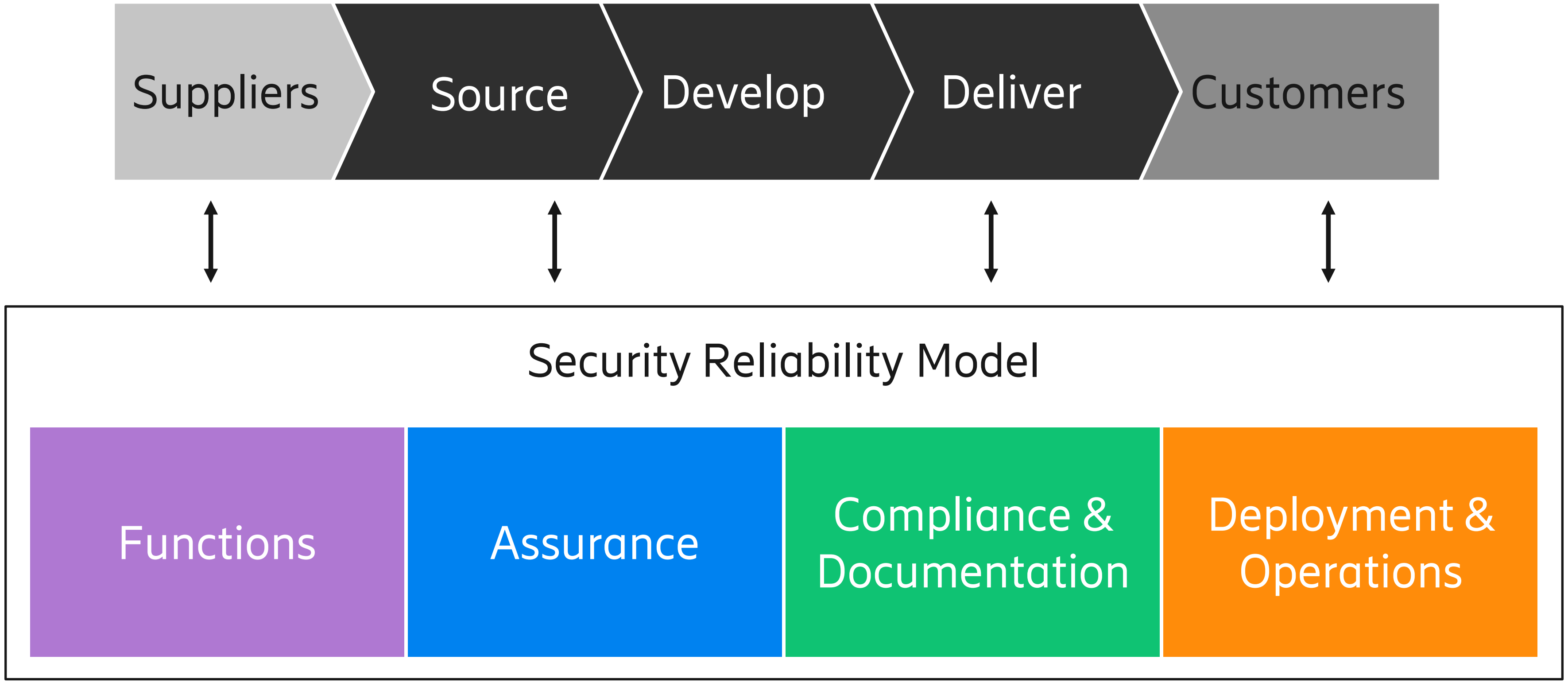
Customer Security

PSIRT

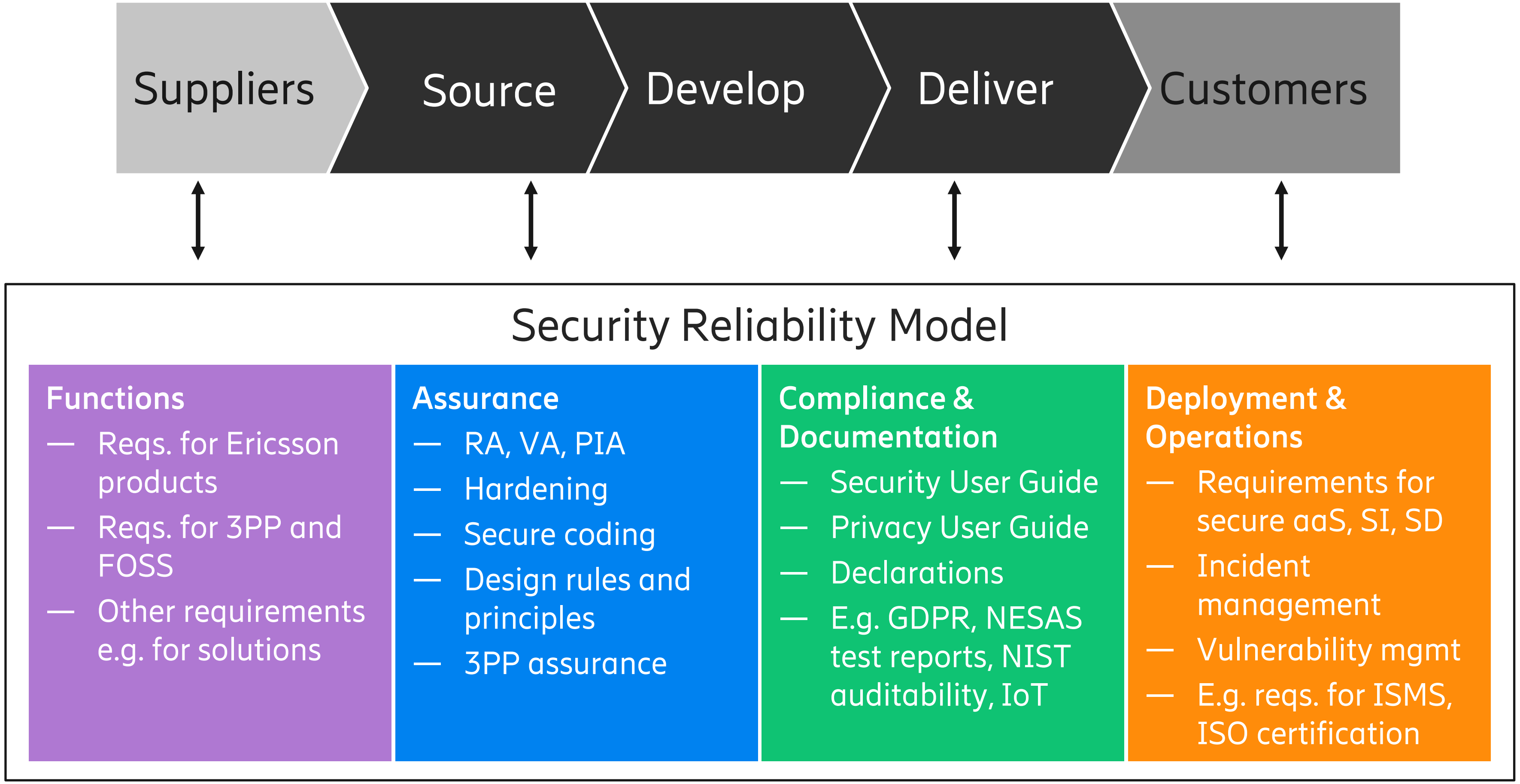
Security research

Secure products

Security Reliability Model: The Ericsson framework for securing products and solutions



Security Reliability Model: The Ericsson framework for securing products and solutions



Security Reliability Model

Functions

- Reqs. for Ericsson products
- Reqs. for 3PP and FOSS
- Other requirements e.g. for solutions

Assurance

- RA, VA, PIA
- Hardening
- Secure coding
- Design rules and principles
- 3PP assurance

Compliance & Documentation

- Security User Guide
- Privacy User Guide
- Declarations
- E.g. GDPR, NESAS test reports, NIST auditability, IoT

Deployment & Operations

- Requirements for secure aaS, SI, SD
- Incident management
- Vulnerability mgmt
- E.g. reqs. for ISMS, ISO certification

Important pillars to secure 5G

Defense in depth to meet common threats

- Security by design
- Ericsson offers in-built security controls on all levels

Network security depends on CSP policy & configuration

- IPsec/Security Gateways, Firewalls and NW/node configuration
- Unique users with least privileges
- Education of staff

Strengthen the safeguard by security management

- Maintained hardening
- Security policy management
- Quick discovery and recovery in case of an intrusion or attack

3GPP standard security improvements introduced in 5G Release 15

Subscriber authentication

Enhanced subscriber privacy

SBA security and interconnect

Integrity protection of user plane

Protection of RAN-CN interfaces (transport)

3GPP standard security improvements introduced in 5G Release 15

Subscriber authentication

- Authentication terminated in HPLMN
- Non SIM card based authentication (useful for IoT devices)

Enhanced subscriber privacy

- Mechanism for encrypting long term subscriber identifiers
- Long term subscriber identifiers no longer used for paging

SBA security and interconnect

- Support of TLS and OAuth 2.0 mandatory on all network functions
- Application layer security enablers between operators

Integrity protection of user plane

- Integrity protection of user plane mandatory on UE and gNB
- Use is optional and under the control of the operator

Protection of RAN-CN interfaces (transport)

- IPsec support mandatory on gNB side
- DTLS over SCTP support mandatory in addition to IPsec

Main drivers and corresponding challenges

towards 6G era

Trustworthiness

Trusted communication and computing for industry and society relying on critical information

Sustainable world

Communication and network as part of and enabler for sustainable development

Simplified life

Massive use of AI across systems for optimal assistance and efficiency

Application demands

Extended and new services requiring extreme connectivity performance

Some technology trends

Hardware
Generic HW acceleration, metamaterials, future devices

Cloud
Continued cloudification for cost/efficiency, also in RAN, adapted implementation/standard, programmability

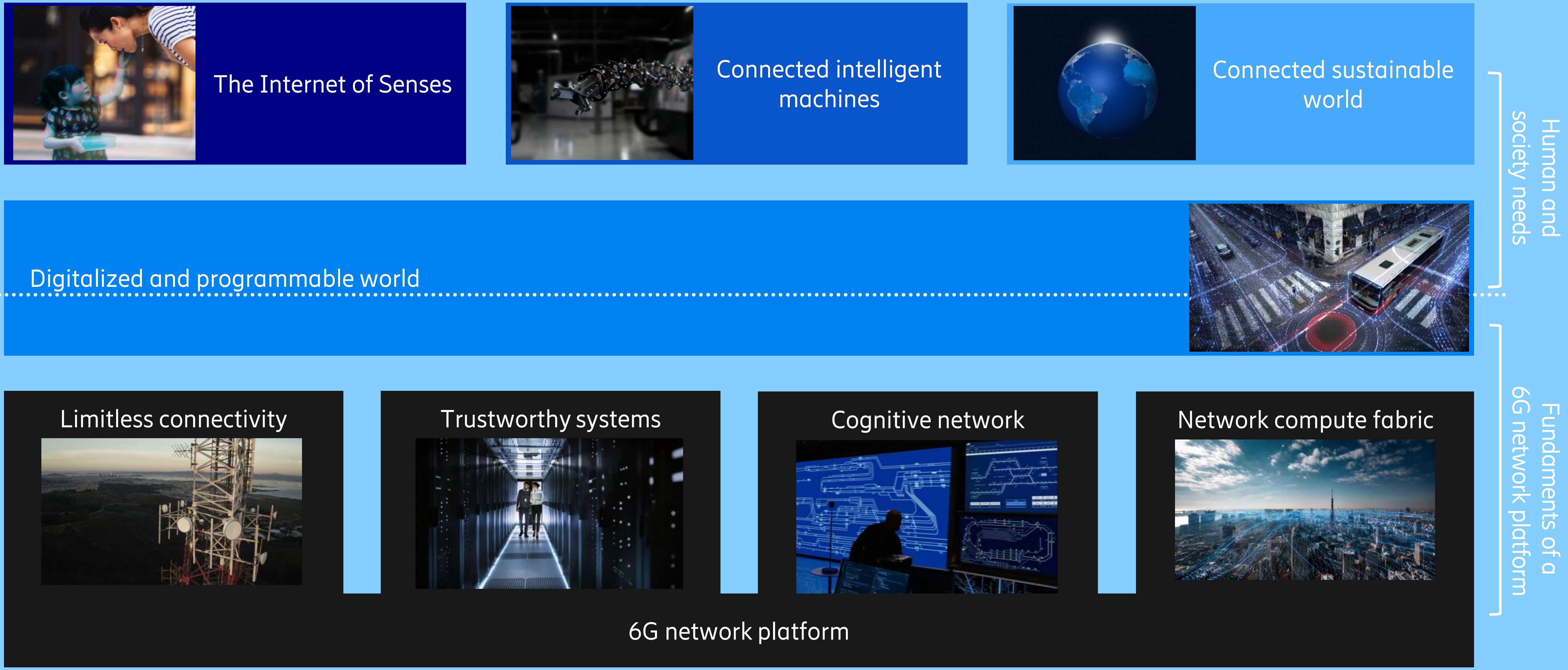
Open source
Higher reliance on open source components

Continuous evolution
Fast evolution of underlying tools and development (DevOps) at a higher pace

Integrated AI
Widespread use of AI for automation and cost-efficiency in cognitive and data-driven networks

Internet evolution
Distributed resilient services, evolving multi-path tailorable transport and security

2030 scenarios



The Internet of Senses

Connected intelligent machines

Connected sustainable world

Digitalized and programmable world

Limitless connectivity

Trustworthy systems

Cognitive network

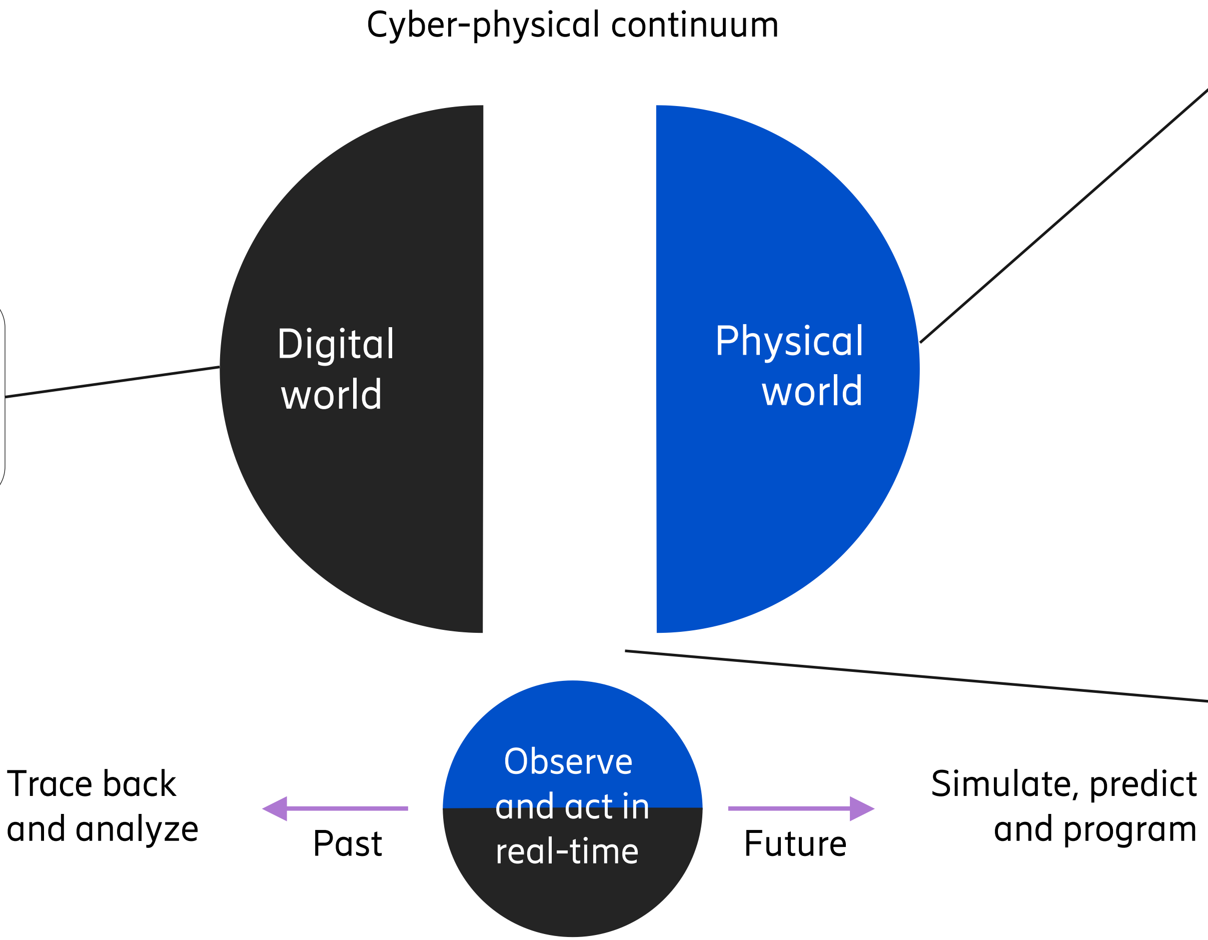
Network compute fabric

6G network platform

Human and society needs

Fundaments of a 6G network platform

Connecting a cyber-physical world



Countless sensors embedded in physical world send data to update the digital representation in real time

Actuators in the real world carry out functions that is programmed in the digital representation

The network platform provides intelligence, ever-present connectivity, and full synchronization in a cyber-physical continuum

A safer and more sustainable world

- Massive amounts of small zero-energy sensors and actuators of various rates
- Joint communication and sensing
- Real time and very low latency
- Secure and reliable communication

A personal concierge cloud

- Security, privacy, processing in cloud
- Automatic personalization of surroundings
- Personal intent management

A more authentic communication between people

- Advancements in devices (AR glasses, contact lenses, haptics…)
- High bandwidth and cell density (when used at scale)
- Edge compute and spatial mapping

6G Use-case examples

Use-case scenarios enabled by the network platform

The Internet of Senses

Telepresence

Merged reality game/work

Immersive sports

Connected Intelligent Machines

AI partners

Interacting robots

Flexible manufacturing

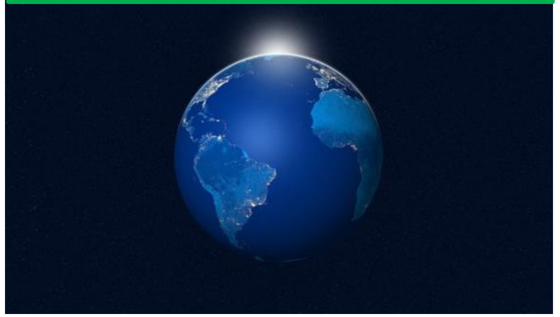
Digitalized & programmable physical world

Interactive 4D map

Precision healthcare

Sensor infrastructure web

Connected sustainable world



E-health for all

Earth monitor

Autonomous supply chains

Internet of senses

Telepresence

Experience cyber-physical objects with all senses, blurring the line between physical and digital world

Immersive physical experience of the world away from you through interaction in the digital world

Immersive sports

Accurately capture live sport events and enable local AI assisted 3D rendering close to the audience allowing remote 360º experience from any point-of-view on the field

Merged reality game/ work

Enable massive merged reality gaming on-the-move, interacting digitally with many other users and physical and digital objects

Connected intelligent machines

Separate parts of the digital world are merged through the physical network

AI partners

Autonomous systems and robots assist and collaborate with human colleagues to solve simple or complicated tasks

Interacting robots

Massive number of autonomous robots can interact and self-organize to collaborate to solve complex tasks

Flexible manufacturing

Highly flexible and configurable factories enable high-throughput of AI assisted custom-made products

Digitalized & programmable physical world

Precision healthcare

Implanted, injected, ingested or topical sensors provide accurate sensor data through a local data hub to ensure utmost patient security and privacy

Interactive 4D map

Optimized design and management of cities and utilities using real-time digital twin

The physical and the digital worlds are synchronized with sensor/actuator data

Sensor infrastructure web

Widely distributed sensors can provide accurate real-time sensor data which is as reliable as on-board sensor data

Connected sustainable world

E-health for all

Provide cost-effective video/XR doctor’s consultations remotely to everyone (rural/impoverished/etc.)

Population level health monitoring and disease prevention using ubiquitous sensors

Using networks to enable a sustainable transformation

Earth monitor

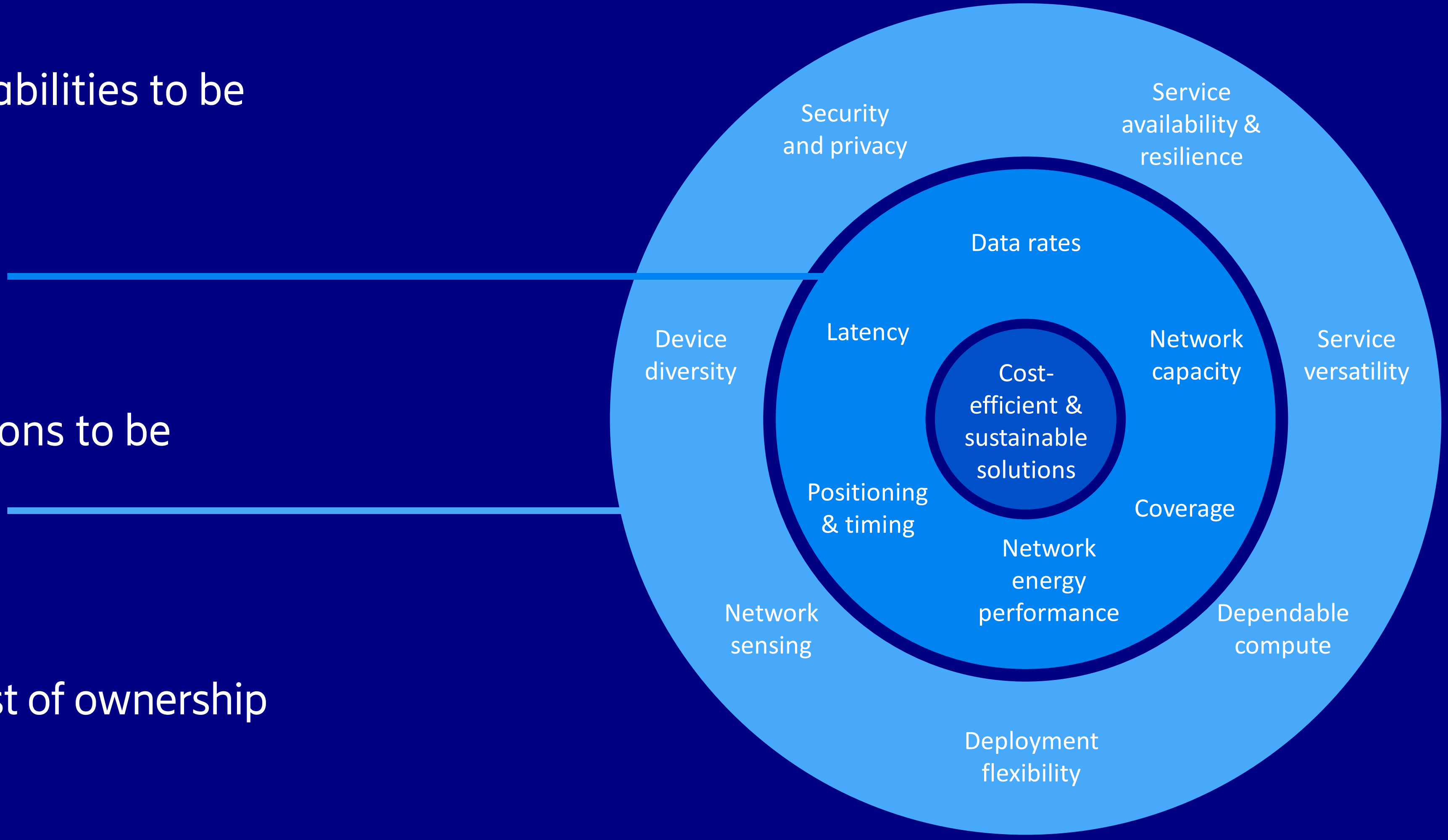
Global integration of sensors for system-critical environmental indicators, e.g., for pollution, flora, fauna, natural disasters, etc.

Autonomous supply chain

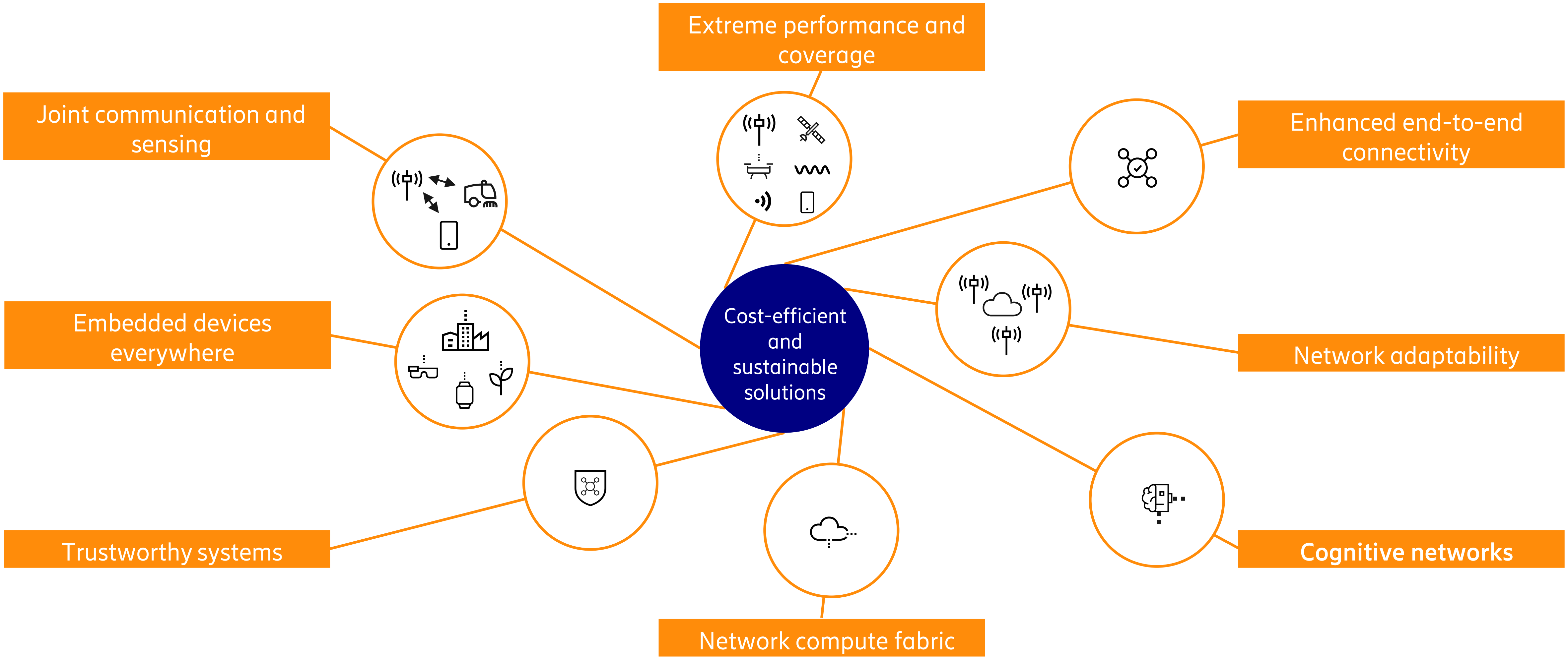
Automizing and optimizing the full supply chain using AI and global coverage: through ordering, sourcing, manufacturing, delivery, recycling etc.

Needed capabilities

- Inner ring of classical capabilities to be enhanced in networks
  - Stretching 5G
- Outer ring of new dimensions to be addressed by networks
- Sustainability and total cost of ownership at the core



Technology areas



Cost-efficient and sustainable solutions

Extreme performance and coverage

Joint communication and sensing

Enhanced end-to-end connectivity

Embedded devices everywhere

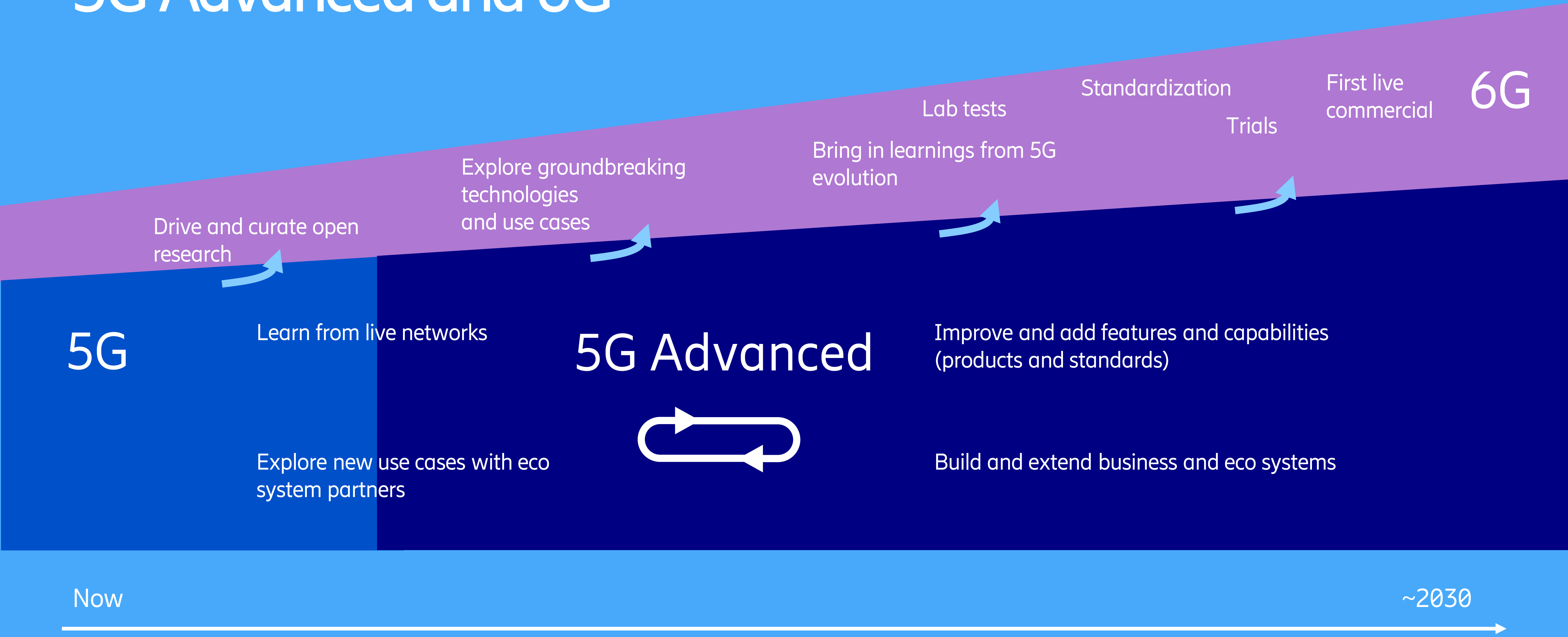
Network adaptability

Trustworthy systems

Cognitive networks

Network compute fabric

Evolution and long-term horizon 5G Advanced and 6G



6G

First live commercial

Standardization

Trials

Lab tests

Bring in learnings from 5G evolution

Explore groundbreaking technologies and use cases

Drive and curate open research

5G

Learn from live networks

Explore new use cases with eco system partners

5G Advanced

Improve and add features and capabilities (products and standards)

Build and extend business and eco systems

Now

~2030

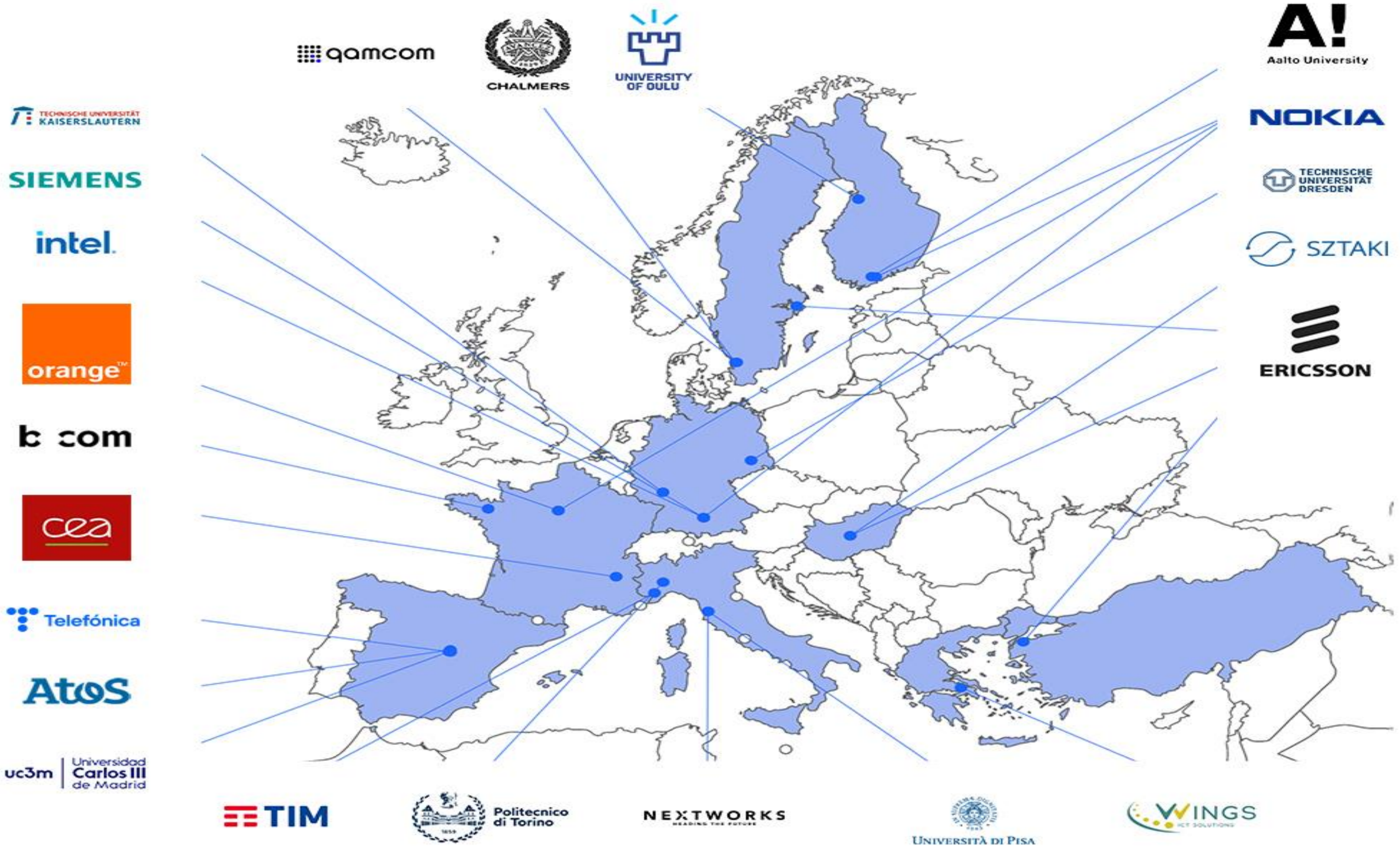
Security Aspects in 6G

- New use cases ask for improvements in security requirements or even put new ones
- Multiple players in eco-system and different kinds of data – different requirements
  - Massive, pervasive deployments of unattended and untrusted devices
  - Data flows: Provenance, real-time, AI applications
  - Trust fabrics: multi-domain, focused on attestation
- AI-specific threats
- AI use by attackers

6G Threat Landscape

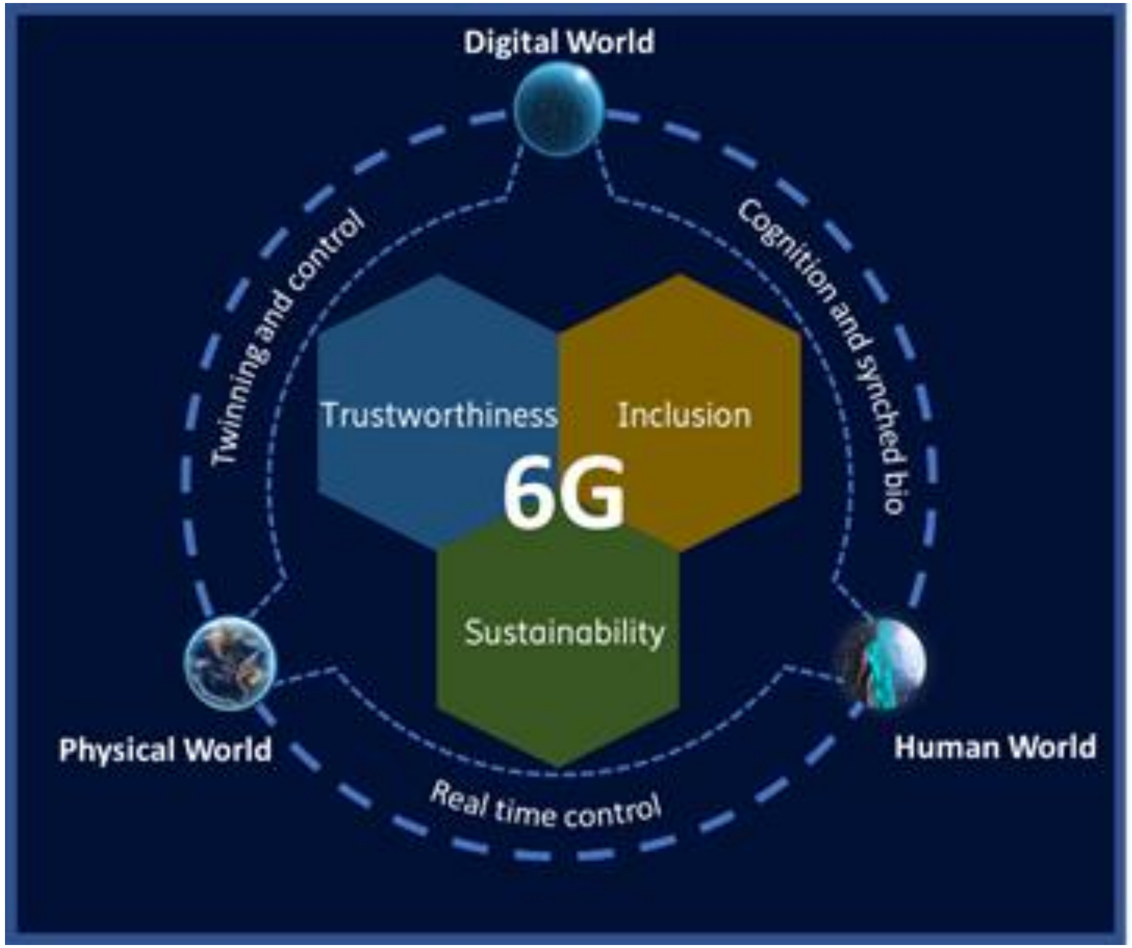
- Residual risks in today’s networks
  - Implications of generalized virtualization
  - Amplification of complexity and automation
  - Increasing use of third-party elements
- New potential risks
  - Number and diversity of end-user devices
  - Heterogeneity of network structures
  - New stakeholders for providing service
- Evolution of the attack ecosystem
  - Extended ground for distributed patterns
  - Growing economic return for miscreants

The flagship project Hexa – X
The joint European initiative to shape 6G



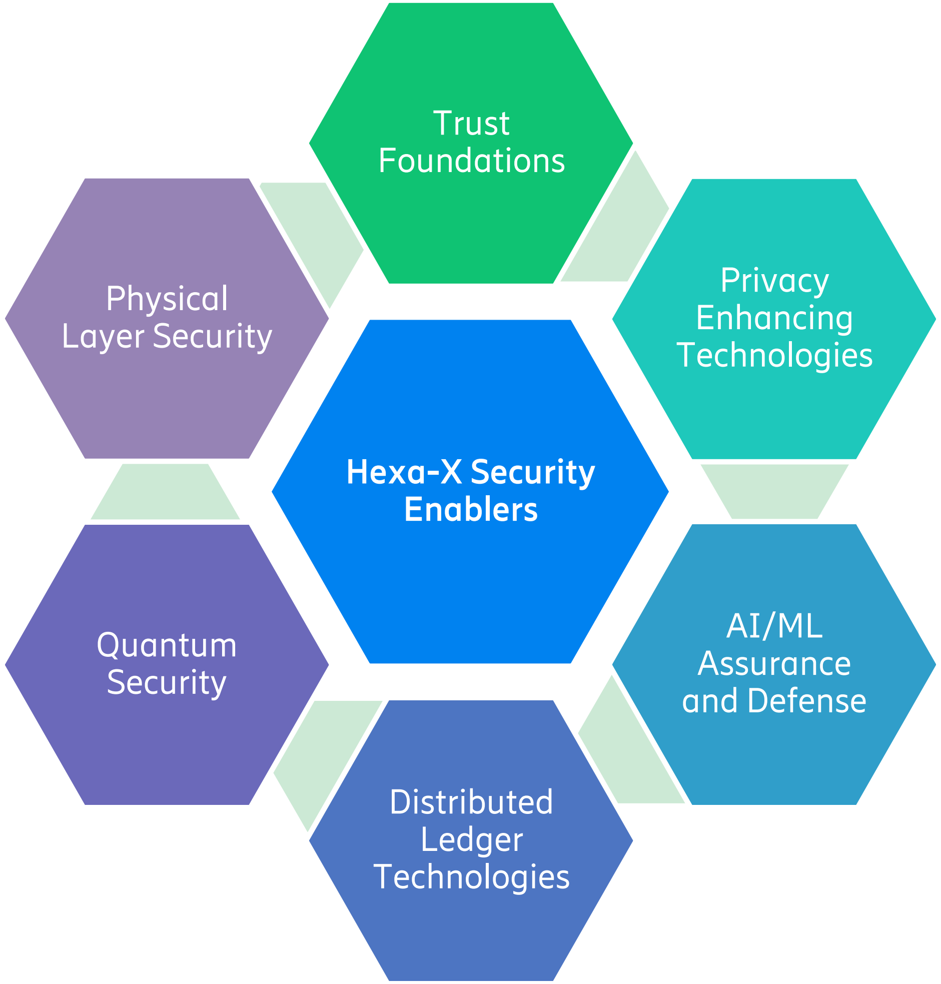
Hexa-X Vision

- The vision revolves around interactions between three worlds:
  - a human world of our senses, bodies, intelligence, and values;
  - a digital world of information, communication and computing;
  - a physical world of objects, organisms and processes
- The vision has three core values:
  - trustworthiness for 6G as a backbone of society;
  - inclusiveness for 6G to be available for everyone and everywhere;
  - sustainability for 6G to play the largest role possible towards a global development



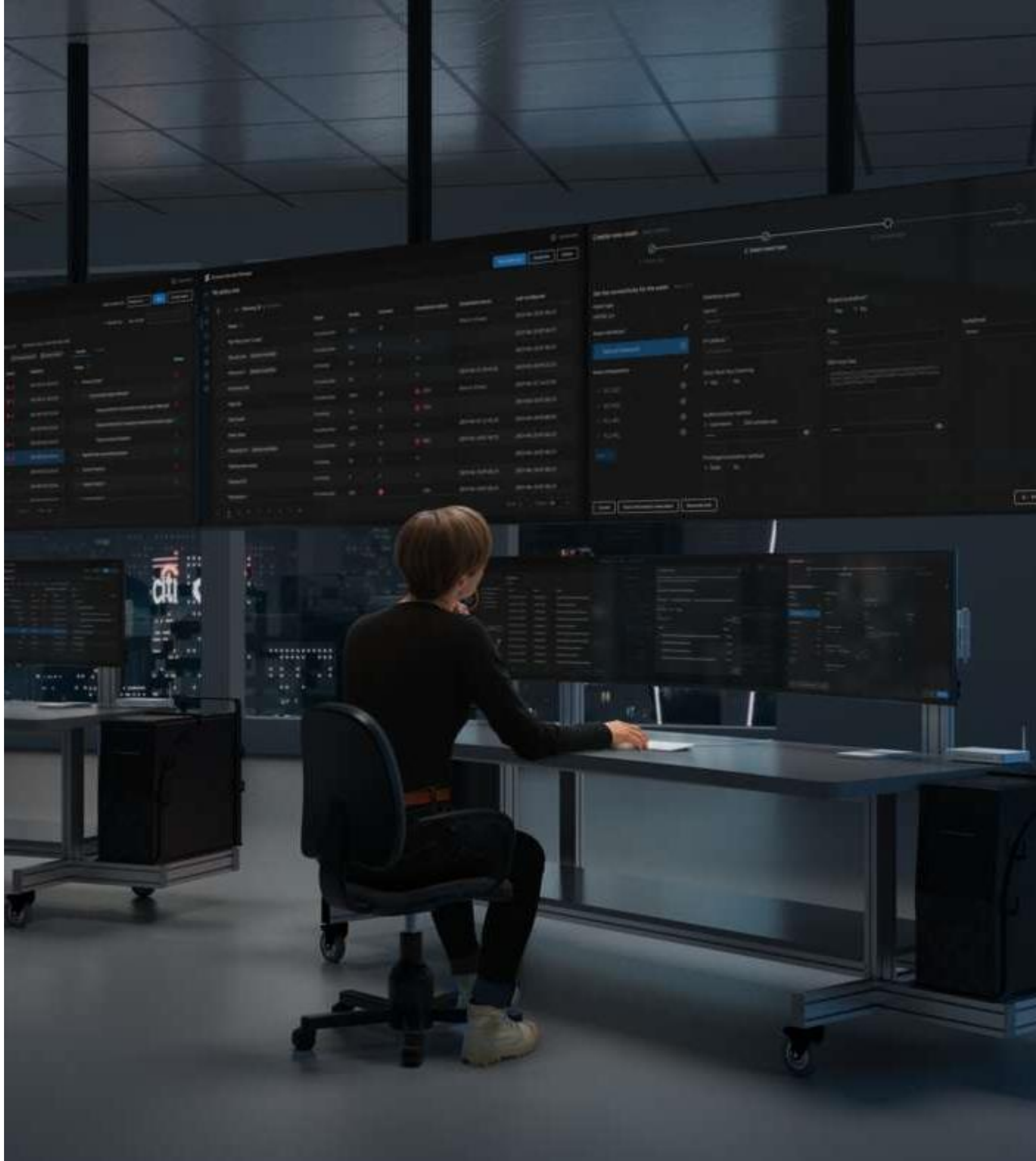
Security, Privacy, and Trust in Hexa-X

- Security, Privacy, and Trust are the main focus areas for Trustworthiness
- Several key security enablers are identified to address security challenges


Trust Foundations
Physical Layer Security
Privacy Enhancing Technologies
Hexa-X Security Enablers
Quantum Security
AI/ML Assurance and Defense
Distributed Ledger Technologies

Potential Security Technologies for 6G

- Trust foundations
  - Confidential computing
  - Secure identities
  - Attestation technologies
- Privacy enhancement
  - Differential privacy
  - Homomorphic encryption
  - Secure multi party computations
- AI/ML assurance and defense
  - Collaborative AI/ML
  - Intelligent monitoring
  - AI in software development



Potential Security Technologies for 6G

- Distributed ledgers
  - Support for AI data integrity
  - Smart contract applications
- Quantum security
  - Quantum key distribution
  - Post-quantum cryptography
- Physical layer security
  - Node authentication
  - Integrity
  - Confidentiality