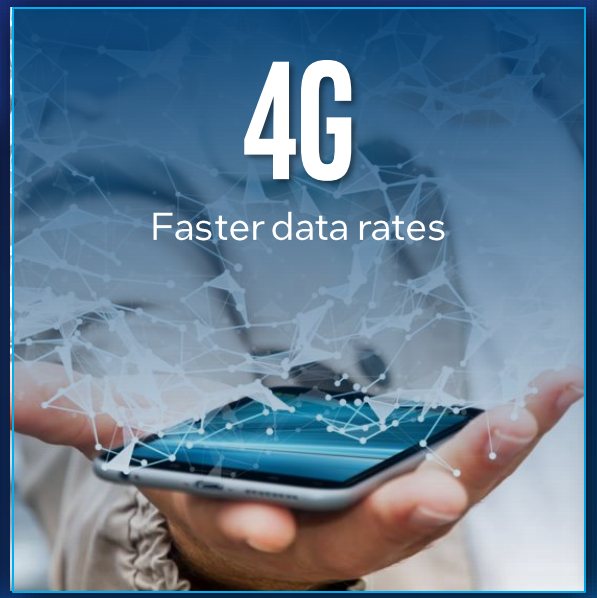
5G/6G Standards Update

November 17 2022

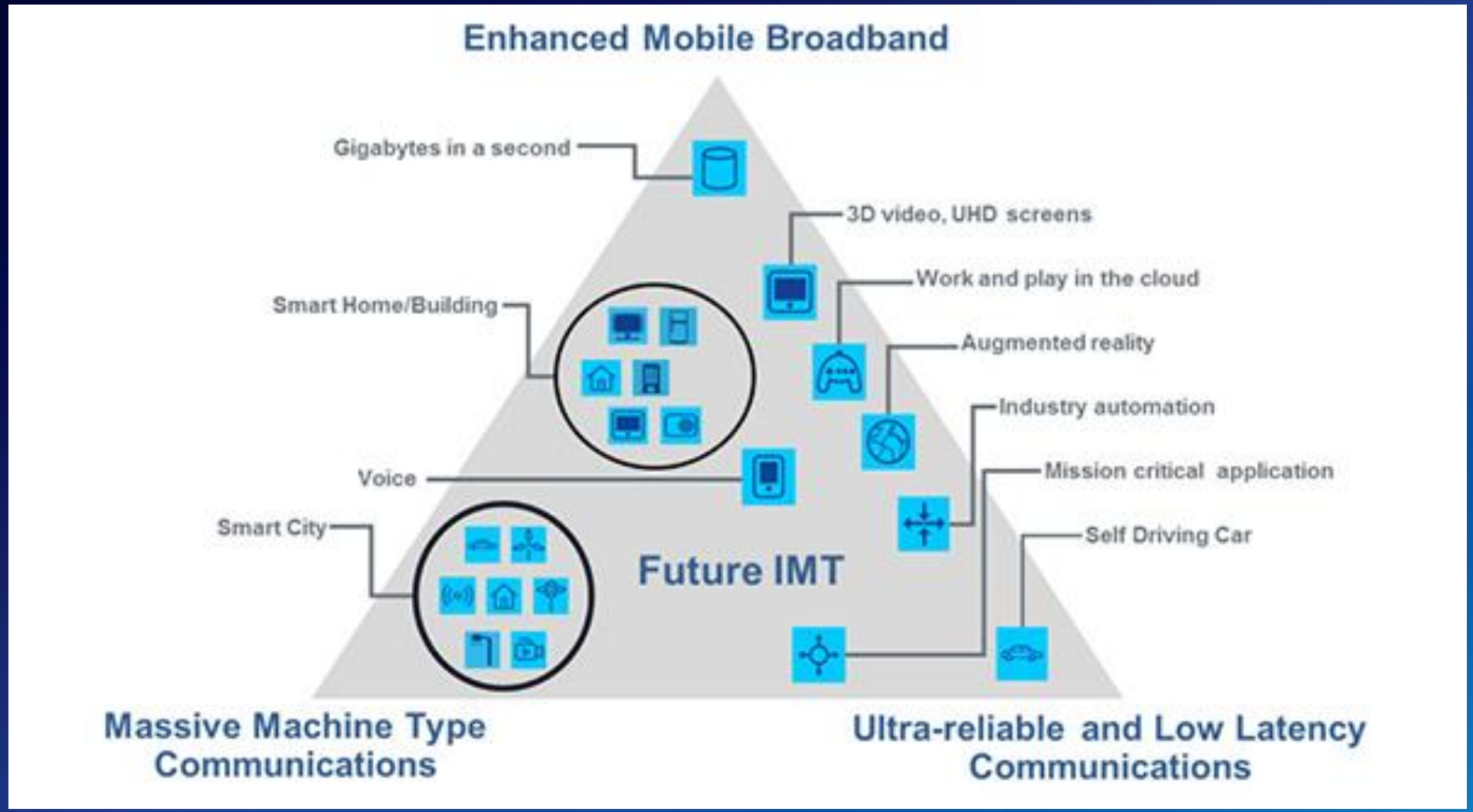
Claire Vishik

What is 5G?

- Provides higher speeds, greater capacity and lower latency
- Transforms infrastructure to be virtualized and software defined
- Distributes intelligence throughout the network

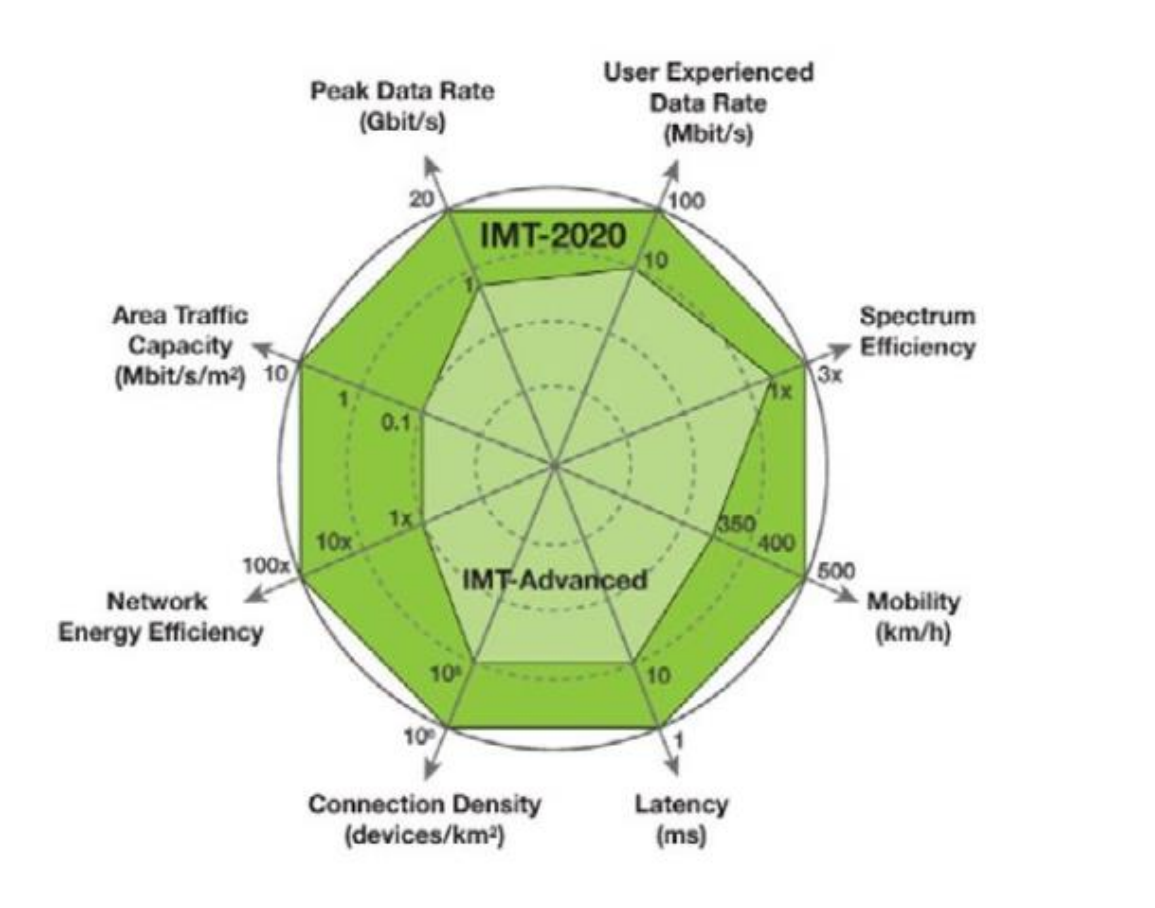


5G Use cases



From 5G roadmap - ITU

5G requirements



From: www.3gpp.org

5G Requirements (TR 38.913)

KPI	values
Peak data rate	20 Gbps for DL, 10 Gbps for UL
Peak SE	30 bps/Hz
Bandwidth	Up to ITU-R requirement
C-Plane Latency (IDLE->ACTIVE)	20 ms
U-Plane Latency	eMBB: 4 ms for DL, 4 ms for UL. URLLC: 1 ms for DL, 1 ms for UL
Reliability	Up to 1-10^-5 for X (FFS) bytes within 1 ms
Connection density	1 Million devices/km^2 in urban environment
Target mobility	500 km/h

Where Are We Today?

Rise of Machines

Billions of Smart Connected Devices

Industrial IoT

Smart Homes/Buildings

Smart Cities

Autonomous Vehicles

Massive Data with 5G & IoT

Autonomous Driving
1 GB/second

Smart Hospital
4000 GB/day

Connected Factory
1million GB/day

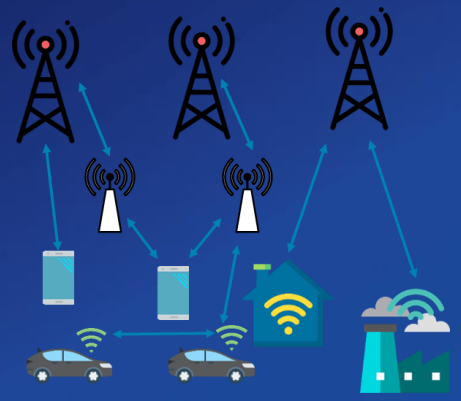
Source: Amalgamation of analyst data and Intel analysis.
And VNI Global Traffic Forecast. VNI stands for Visual Networking Index.

Growing Network Complexity

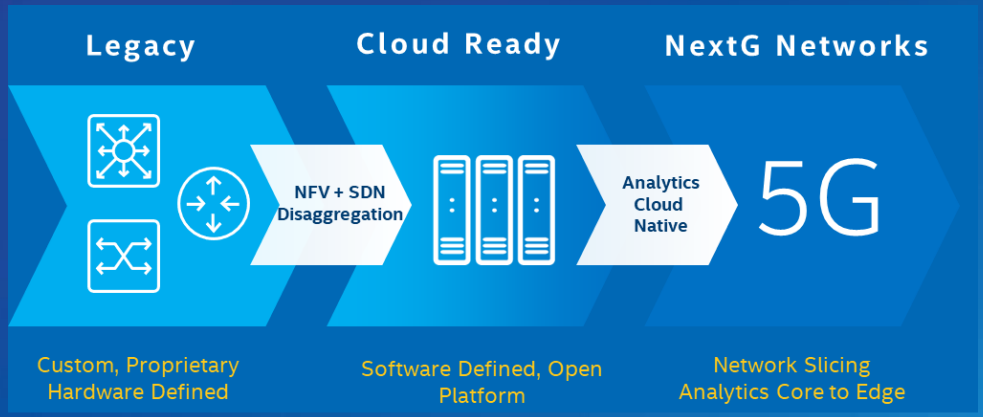
Large number of Bands & Band combinations

Ultra Dense Networks

Diverse links, traffic, services, cells, devices



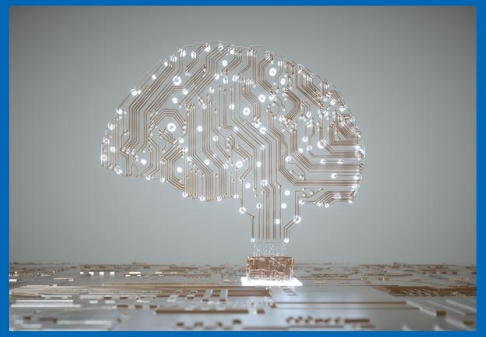
Cloudification of Network Infrastructure



Emerging Trends in Next G Networks

Growing Role of AI

Introduction of AI promises significant economic value

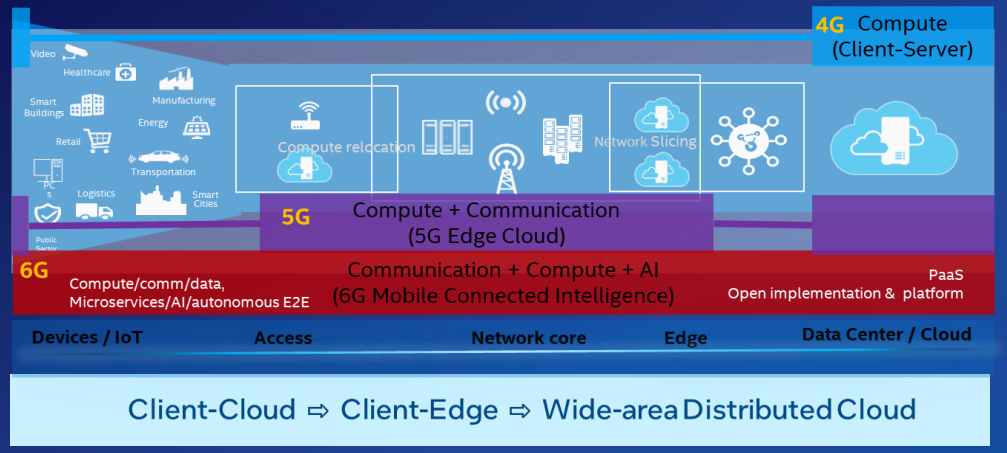


ABI predicts AI and 5G will contribute an economic impact of 17.9 Trillion USD by 2035!

Source: 5G & AI: The Foundations for the next Societal & Business Leap, ABI Research & Intel

Autonomy for Devices & Networks

Evolving Network Infrastructure



Merging of Physical & Digital Worlds

Extended Reality

Immersive Media

Digital Twins

6G Technology Objectives – Intel Vision

5G, 5G-Advanced, and 6G Standards

5G – 3GPP Releases 15-16-17

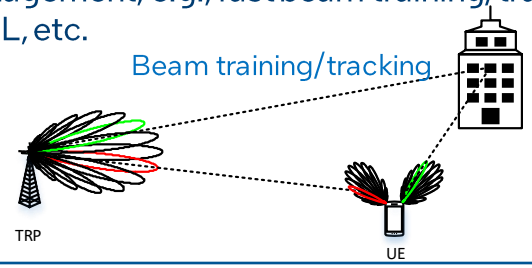
Rel-15 5G Basic Capabilities

Support of higher & wider frequency band

- Rel-15 supports up to 52.6 GHz (sub-1GHz, sub-6 GHz, above 6 GHz)
  - Much wider BW available in 24.5-39 GHz bands, e.g., ~1 GHz
- Support of wider BW per component carrier
  - Up to 400 MHz in Rel-15 (note: LTE supports up to 20 MHz per CC)
  - Reduced overhead to support wideband operation
  - Facilitate efficient implementation to support wideband operation

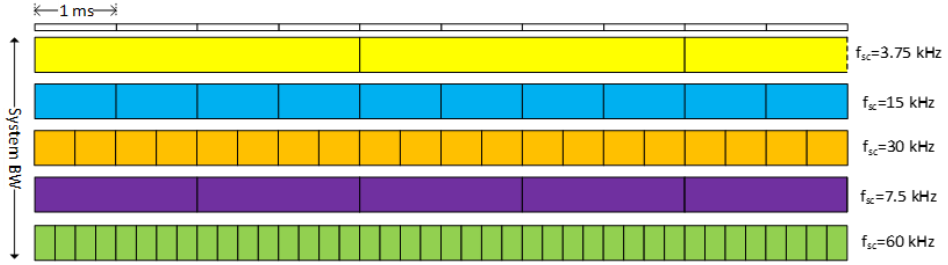
Enhanced multi-antenna techniques

- Massive MIMO, 3D Beamforming
- Enhanced channel status feedback, MIMO layer mapping, precoding, etc.
- Improved beam management, e.g., fast beam training/tracking, decoupled DL and UL, etc.



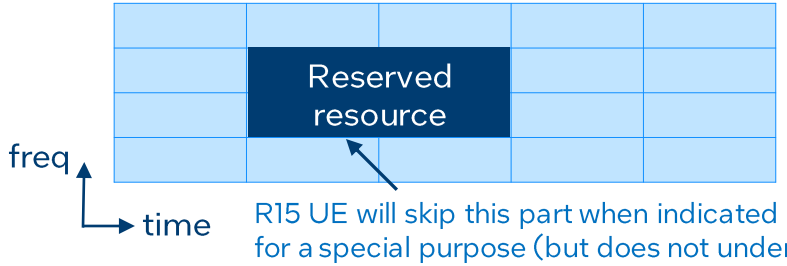
Scalable numerology

- Support multiple numerologies (subcarrier spacing, CP, slot length) with scaling (LTE: 15 kHz subcarrier spacing only for MBB)
- Performance improvement by selecting best numerologies for different deployment scenarios; facilitate forward compatible design



Forward Compatibility

- Allow future evolution while minimally sacrificing efficiency
- Ex) support of reserved resources, scalable numerologies, block-wise flexible time/freq resource allocation for different use cases and different numerologies, network slicing, etc.



R15 UE will skip this part when indicated by gNB in the future for a special purpose (but does not understand the content)

Rel-15 5G NR Radio Link Feature Examples

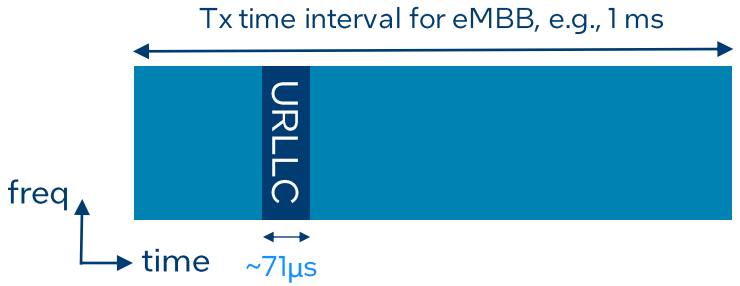
Advanced Channel Coding Schemes

- LDPC for data and Polar coding for control (for eMBB)
  - Efficient support of very high peak rates and lower latency
  - Better performance, esp. for small packets.
- TBD for URLLC and mMTC

Code	Data rate	Area	Throughput/Area
LTE turbo code	1.67 Gbps	2.004 mm^2 @45nm	0.81
802.11n LDPC code	3 Gbps	0.81 mm^2 @45nm	3.70
Polar Code with List L=16	0.46 Gbps	7.47 mm^2 @90nm	0.061

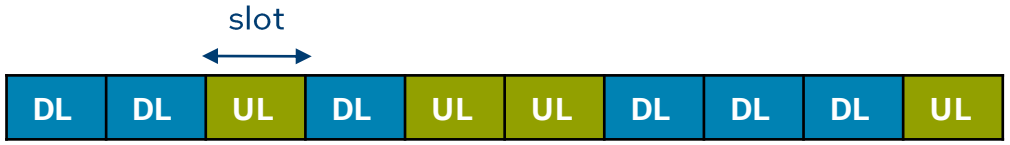
Support for low latency & high reliability

- Support 1 ms end-to-end delay, e.g., via 1-symbol Tx time interval
- Support for ultra-reliable transmission, e.g., 10^{-5} packet error rate, e.g., via packet duplication from multiple transmission points.



Support for dynamic TDD

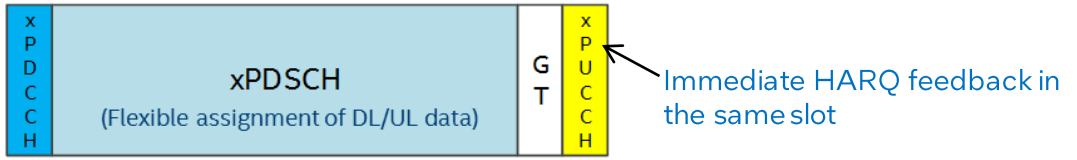
- Support of dynamic chance of DL/UL direction
  - More flexible usage of DL and UL resources
  - Performance improvement for both network and UE
- Cross-link interference handling is a key challenge



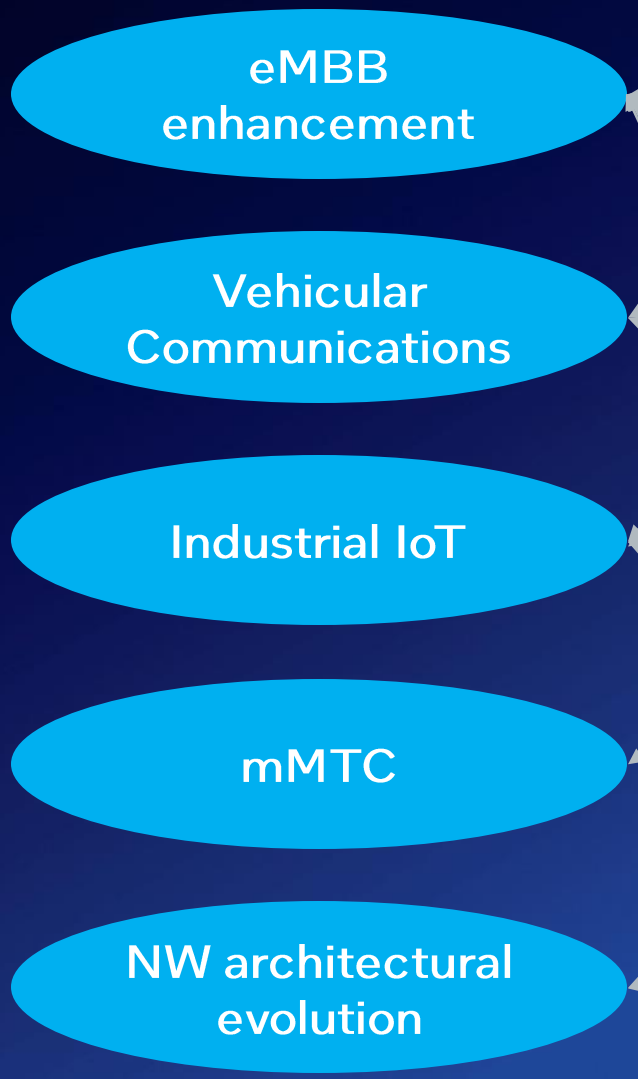
Can dynamically change DL/UL direction every slot

Self-contained slot structure

- Immediate HARQ feedback in the same slot as data
- Performance benefits in latency and throughput
- Cleaner design by eliminating HARQ reTx related restrictions → Facilitate forward compatible NR design
- Good for operation in unlicensed spectrum by mitigating complication from LBT requirement in shared spectrum.



Rel-16 5G Enhancements



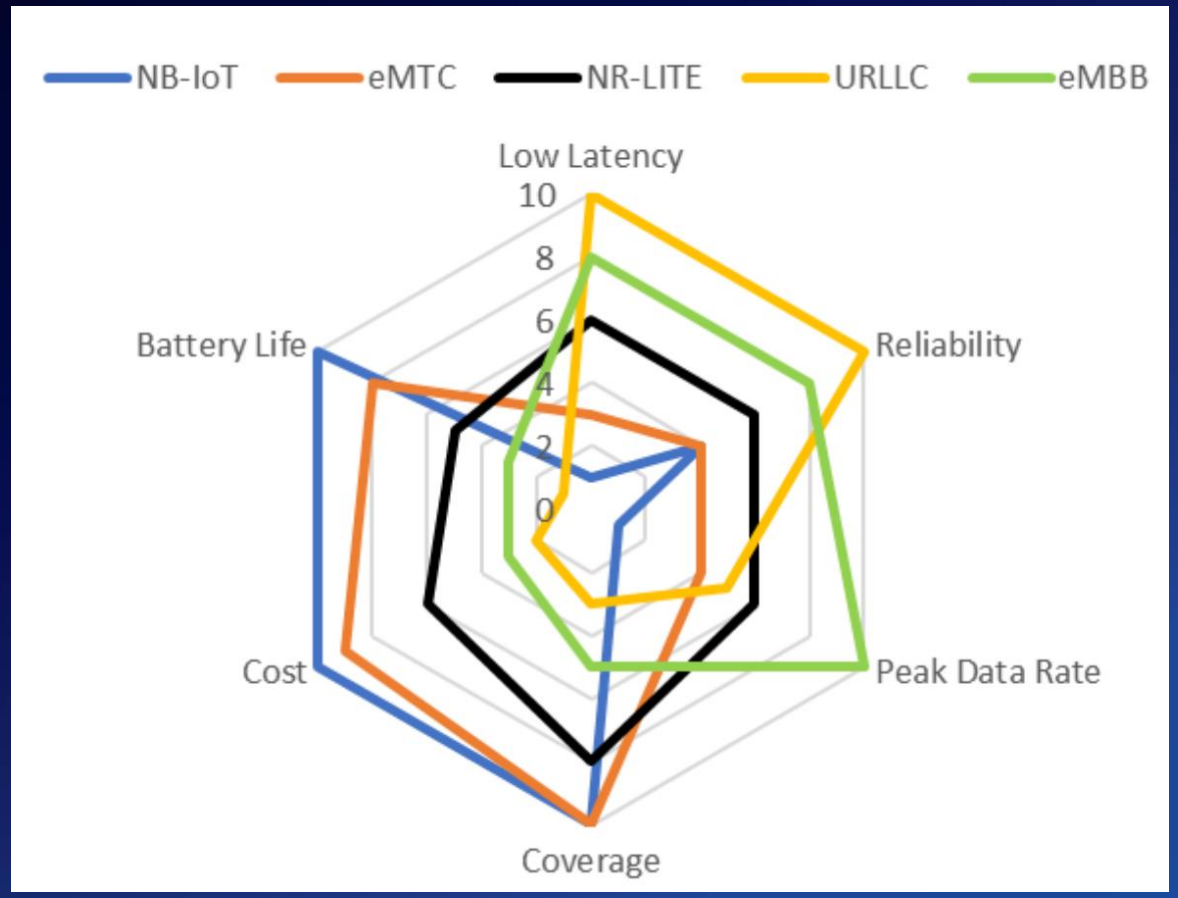
NR Rel-16 Study/Work Items
NR beyond 52.6 GHz study (regulation, use case, requirements)
Mobility enhancement
Positioning support
NR Unlicensed
MIMO enhancement
LTE-M / NB-IOT enhancement
NR V2X
2-step RACH
UE power saving
Physical Layer enh. for URLLC
Industrial IOT (L2/L3)
DC and CA enhancements, RF Spectrum Enhancements
Integrated Access Backhaul (IAB)
Remote interference management (RIM) and cross link interference (CLI)
Solutions evaluation for Non-Terrestrial Network (NTN)
Optimisations on UE radio capability signalling
SON/MDT

Rel-16: URLLC / IIoT Enhancements

Rel-16 enhancements to improve the operation efficiency & new use cases

- Higher network spectral efficiency while satisfying stringent requirements
- Enhanced intra- and inter-UE multiplexing between services with different QoS requirements (e.g., eMBB and URLLC, etc.)
- Enable support of Wireless Ethernet and Time Sensitive Networking (TSN)

Rel-17: RedCap Device
(Reduced Capability Device)



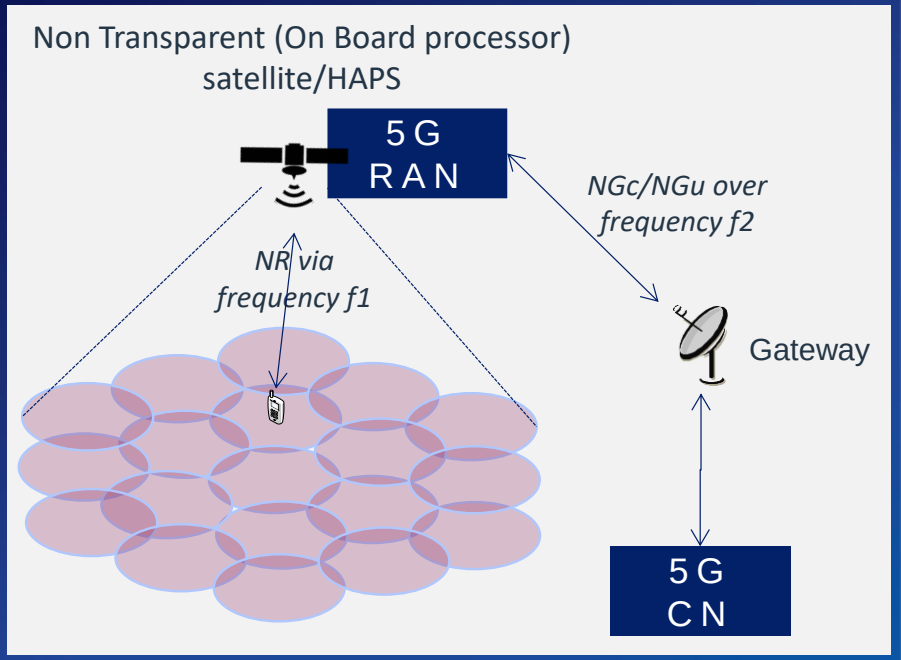
*RP-190831, Nokia

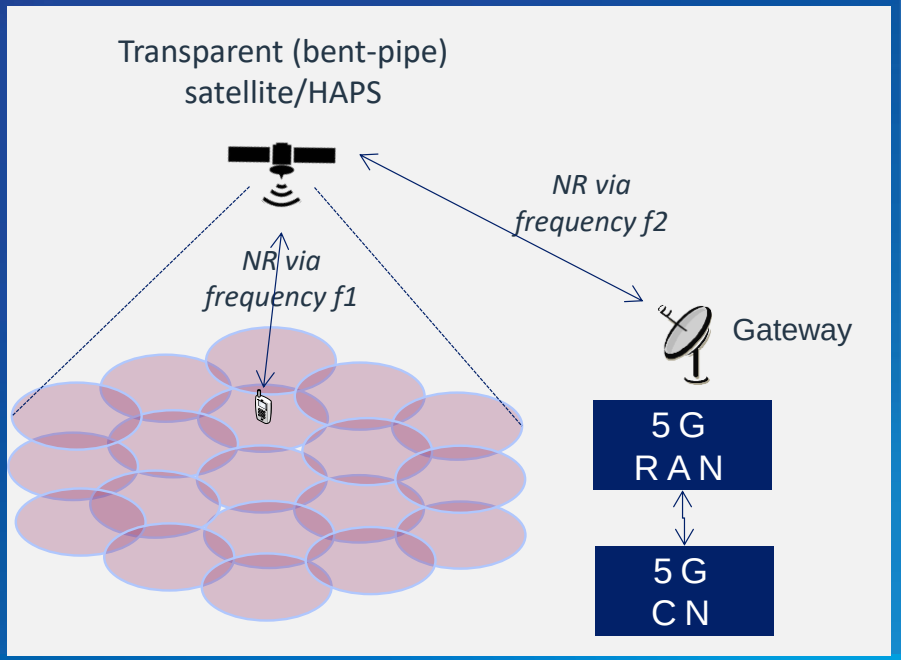
- Reduction of device complexity, size, minimum bandwidth, Rx/Tx antennas, and power consumption
- Various use cases between LPWA (Low-Power-Wide-Area) and eMBB/URLLC such as industrial wireless sensor, video surveillance, wearable
- Improve coverage due to loss of complexity reduction
- UE power consumption reduction to offer multi-year battery lifetime (e.g. for industrial WSN – Wireless Sensor Network)

Rel-17: NTN

(Non-Terrestrial Network; a.k.a. Satellite Comm.)

- Ubiquitous radio access service via satellite (GEO - Geosynchronous Equatorial Orbit and LEO - Low-Earth Orbit) and HAPS (High Altitude Platforms) using 5G NR
- ATG (Air to Ground) by leveraging solutions for satellite communications
- Both 3GPP power class 3 (smartphone) and VSAT (Very Small Aperture Terminal)
- S-band (2GHz carrier frequency) and Ka-band (20/30GHz for DL/UL)
- Technical challenges on large round trip delay, large Doppler shift, large cell size

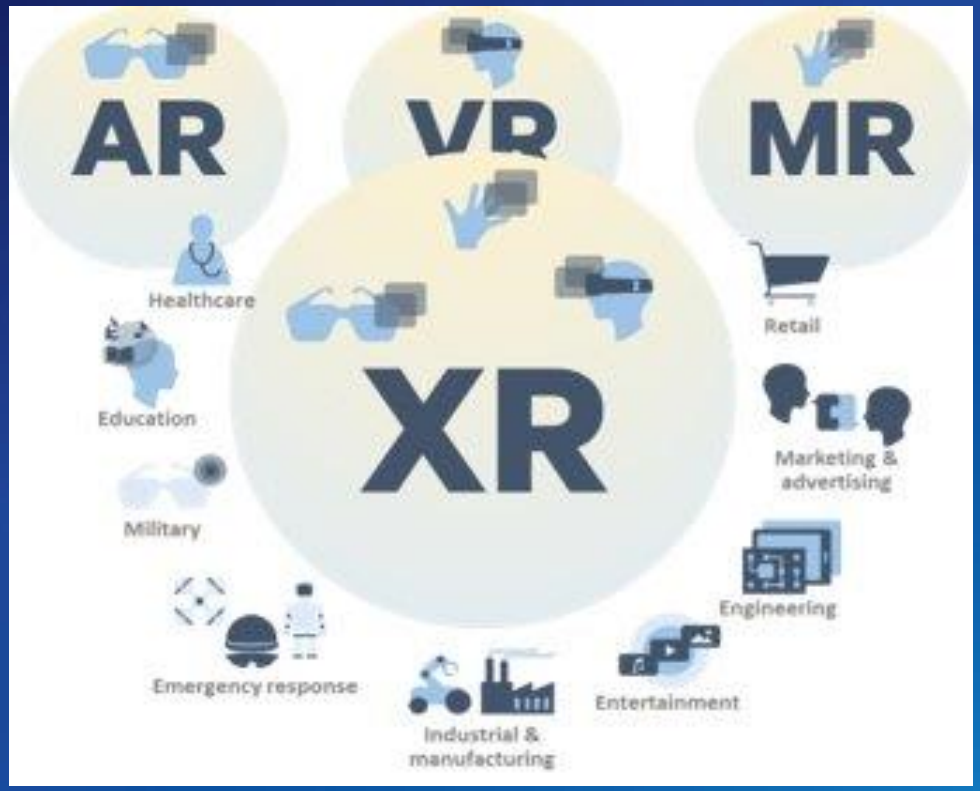




5G-Advanced – 3GPP Releases 18-19

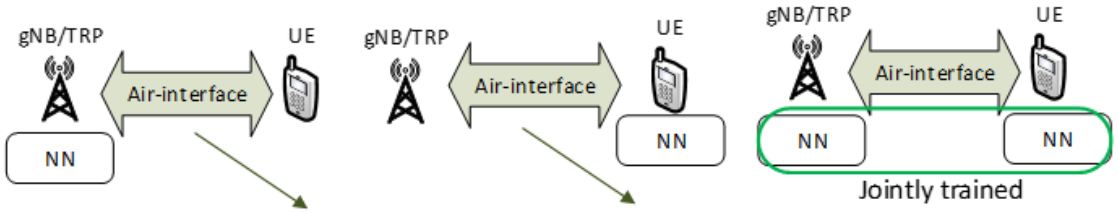
Rel-18: Study on XR (Extended Reality)

- XR/CG application awareness in the RAN
- Power saving techniques for UEs engaged in XR/CG services
- Capacity improvements for delivery of XR/CG services



Rel-18: Study on AI/ML for Air Interface

- Establish AI-ML framework, model, terminology and description
- Evaluation methodology, KPIs (overhead, inference/training complexity, robustness), SLS or LLS evaluations
- Specifications impact

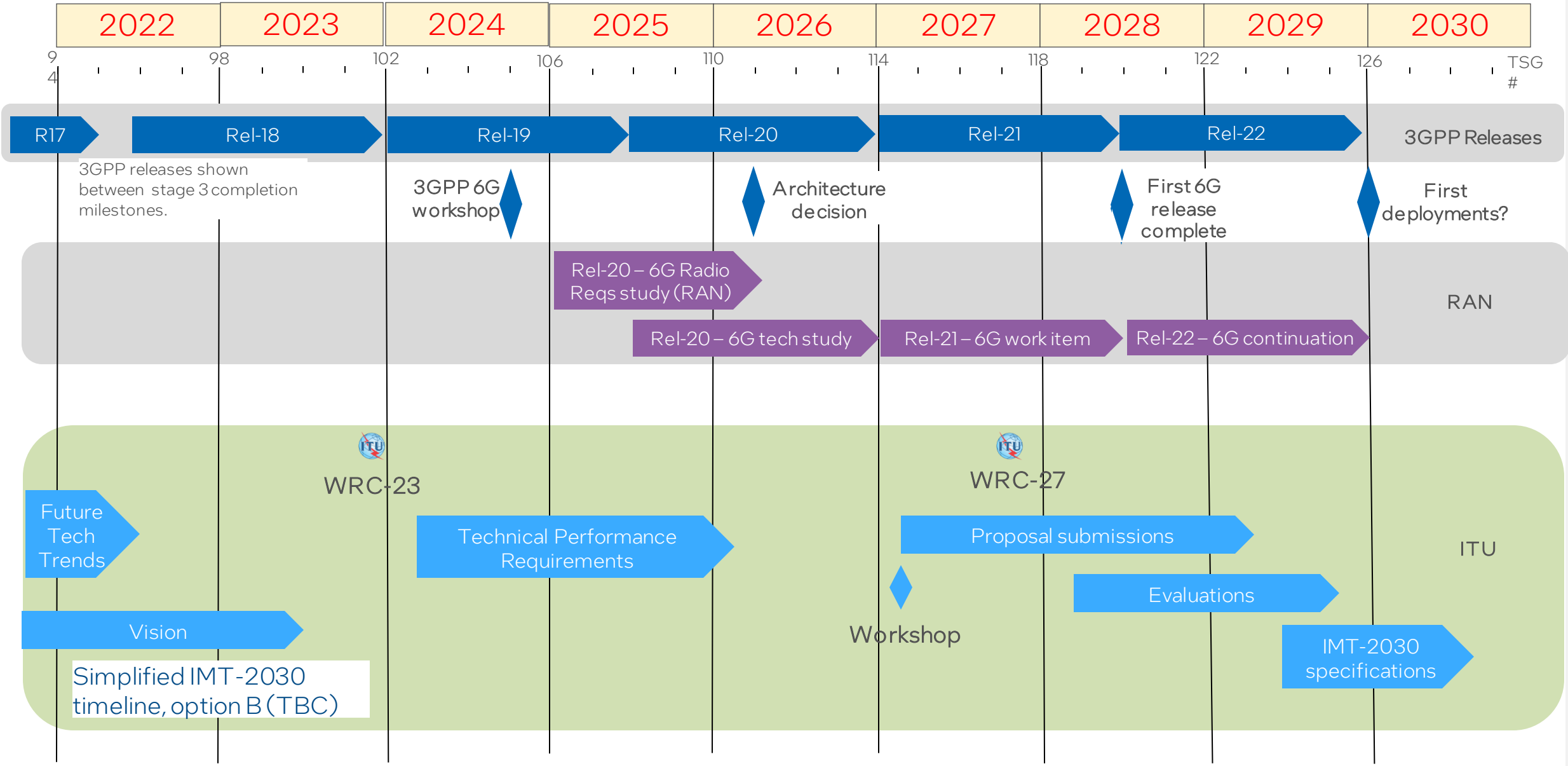


Rel-18/19 time-frame

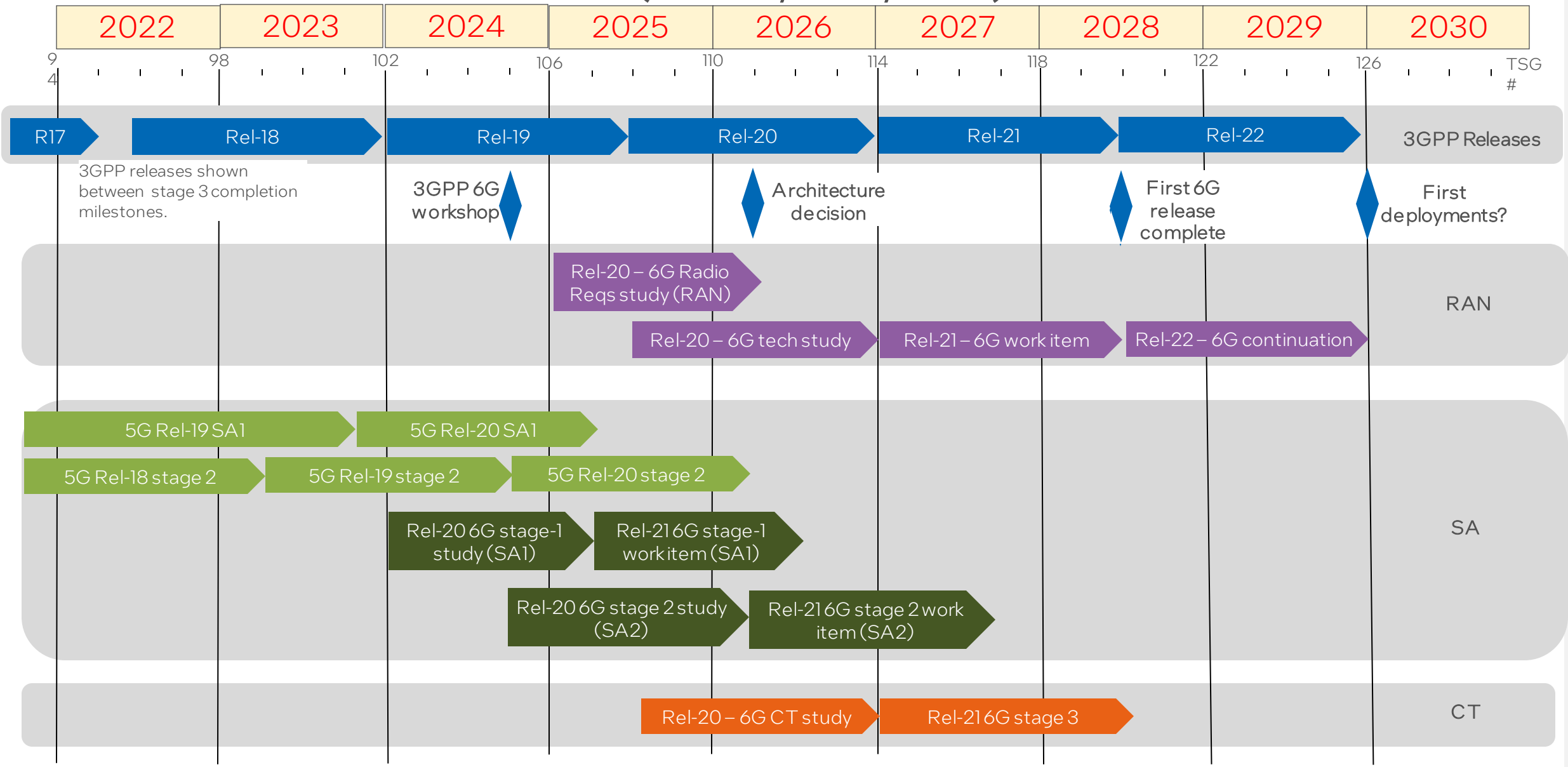
	Single-sided mode @ NW only	Single-sided mode @ UE only	2-sided model @{NW, UE}
No specification impact	Purely implementation	Purely implementation	NA
+ specification impact + basic level	Signaling assistance for model management	Signaling assistance for model management	Signaling assistance + offline model
++ specification impact + advanced level	NA	Model download + signaling assistance	Model download + signaling assistance

6G – 3GPP Release 20 and onwards

6G – 3GPP + ITU timelines

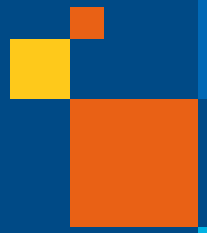


6G timeline for 3GPP (RAN/SA/CT)



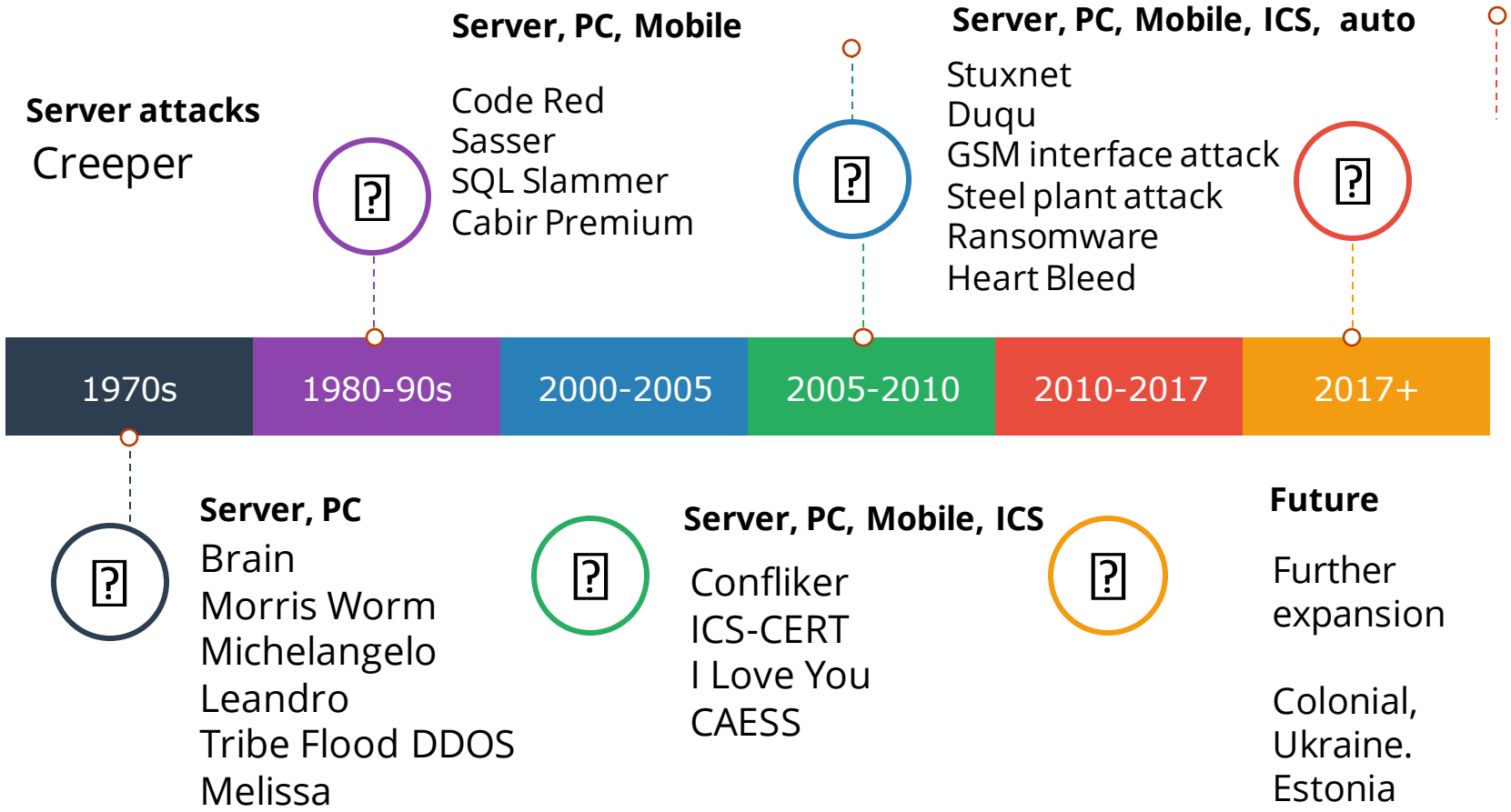
Colours: 3GPP | 5G SA | 6G SA | 6G CT | 6G RAN

5G Security and Resilience



intel®

Reach of cyberattacks is expanding



A broad field: cybersecurity

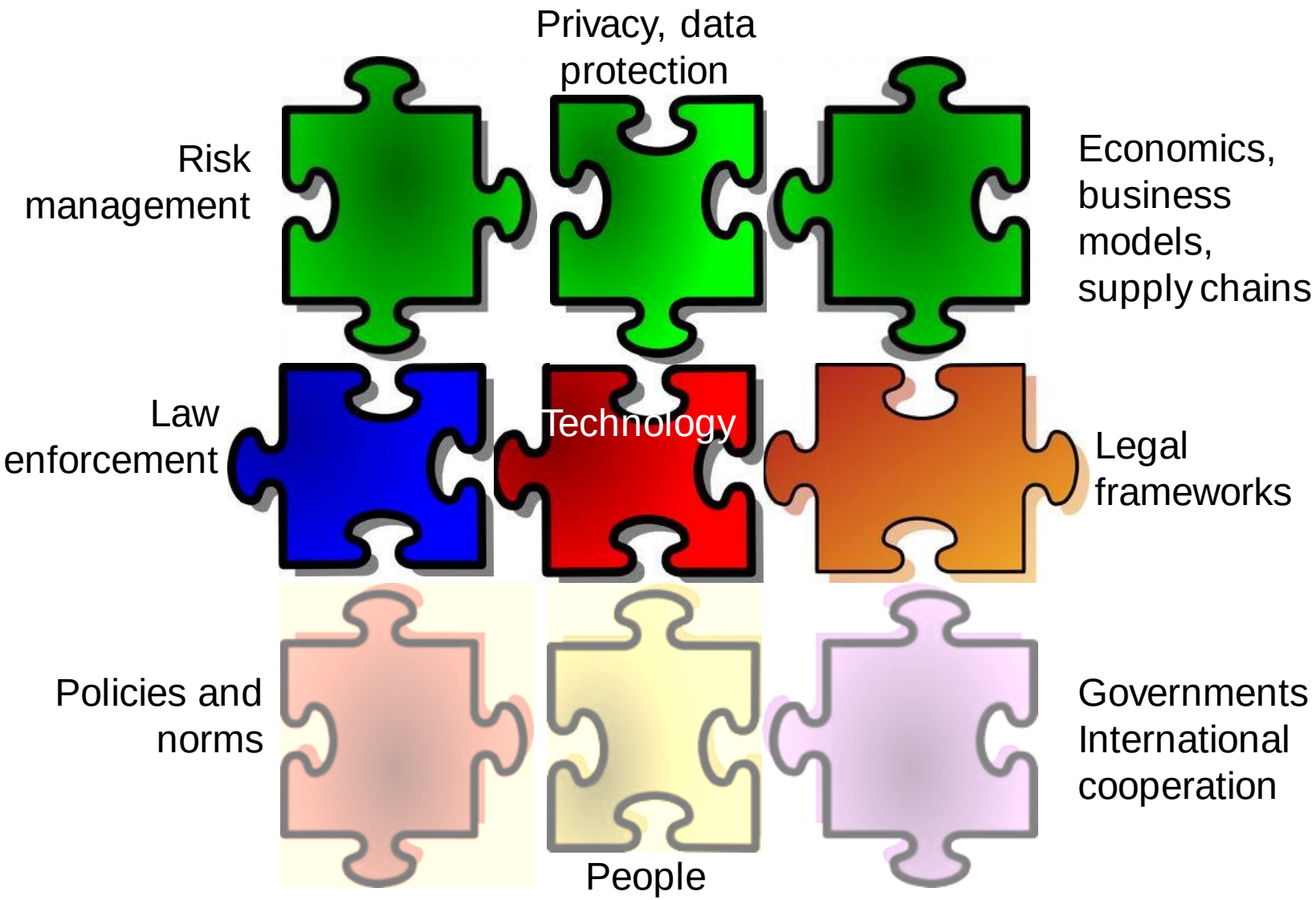
Complex space requiring collaboration of a multi-disciplinary global community for success

Narrow Definition	Broad Definition
Activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected...	Strategy, policy, and standards for security of and operations in cyberspace. Includes international engagement, incident response policies, law enforcement, information assurance, diplomacy, and other areas fundamental for security and stability of the global information infrastructure…

http://niccs.us-cert.gov/glossary#letter_c

National Initiative for Cybersecurity Careers & Studies

Some components of cybersecurity



Threat/protection balance for 5G

- A number of protective features
- Lessons learned from legacy networks

- As always, new technologies inherit some legacy security/privacy issues and new issues are discovered as these new technologies are deployed.
  - Overall, a good start for 5G

Applicable classes of threats (examples)

- Remote access exploitation/abuse
- Malicious code
- Information leakage
- Hardware/software manipulation
- Network intrusions
- Spectrum sensing
- Compromised supply chain
- Attacks on virtualization
- Attacks on signaling
- Traffic sniffing and manipulations
- And many more

Threat classes (ENISA 5G threat analysis)

- VULNERABILITY GROUPS FOR CORE NETWORK
- VULNERABILITY GROUPS FOR NETWORK SLICING
- VULNERABILITY GROUPS FOR RADIO ACCESS NETWORK
- VULNERABILITY GROUPS FOR NETWORK FUNCTION VIRTUALIZATION - MANO
- VULNERABILITY GROUPS FOR SOFTWARE DEFINED NETWORKS
- VULNERABILITY GROUPS FOR MULTI-ACCESS EDGE COMPUTING
- VULNERABILITY GROUPS FOR SECURITY ARCHITECTURE
- VULNERABILITY GROUPS FOR PHYSICAL INFRASTRUCTURE
- VULNERABILITY GROUPS FOR IMPLEMENTATION OPTIONS
- VULNERABILITY GROUPS FOR PROCESSES

Threat areas: illustration

Detailed threat landscapes include hundreds of attacks, most not specific to 5G.

Some of the key threat classes (Based on CAPEC):

Manipulation of network configuration /data forging	**Threat**	**Assets**
Routing tables manipulation	Route Disabling - (582), Contradictory Destinations in Traffic Routing Schemes - (481)	SDN, NFV, MANO
Falsification of configuration data	Manipulating Writeable Configuration Files - (75)	RAN, RAT
DNS manipulation	DNS Cache Poisoning - (142), DNS Domain Seizure - (585)	Security configuration data
Manipulation of access network and radio technology configuration data	Manipulating Writeable Configuration Files - (75)	
Exploitation of misconfigured or poorly configured systems/networks	Exploiting Incorrectly Configured Access Control Security Levels - (180)	

Threat areas II

Denial of service	Threats	Assets
Distributed denial of service (DDoS)	Flooding - (125), Traffic Injection - (594)	SDN, NFV
Amplification attacks	Flooding - (125), Amplification - (490)	MEC
MAC layer attacks	Man in the Middle Attack - (94)	CLOUD
Jamming of the network radio	Jamming - (601)	
Authentication traffic spikes	Authentication Abuse - (114), Traffic Injection - (594)	

Source: MITRE and EU Spider at https://spider-h2020.eu/

Threat agents

In order to address threats, threat agents need to be understood.

- Cyber criminals
- Insider (own, third parties)
- Nation states
- Hacktivists
- Cyber-fighters
- Cyber-terrorists
- Corporations
- Script kiddies

(ENISA, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks)

5G protective features

- Inter-operator security
  - Inter-operator security in 5G is provided by security proxy servers, which are essentially an evolution of 2G, 3G, and 4G signaling firewalls
- Security and privacy support
  - 5G networks use the home network public key for asymmetric encryption
- Primary authentication
  - Network and devices are mutually authenticated
- Secondary authentication
  - Data transmission networks outside the mobile operator domain, such as Wi-Fi calling, undergo secondary authentication.
- Key hierarchy
  - 5G employs key separation limiting the damage if a part of the infrastructure is compromised.

Protective features (continued)

- Radio network protection
  - In the base station (gNB) in 5G, the data processing module (Central Unit, or CU) and the radio module (Distributed Unit, or DU) are separated. The CU and DU interact via a secure interface preventing the attacker from breaching the operator's network, even if gaining access to the radio module
- Network slicing
  - Each slice is allocated its own resources (bandwidth, service quality, and so on) and has unique security policies. In theory, a compromise of any one slice should not impact the other slices or the network as a whole.

  - Source: GSMA

Protective technologies & processes available

- Secure configuration
- Software hardening
- Hardware root of trust
- Resilient supply chain
- Secure hardware and software development process


intel