Journal of Telecommunications and the Digital Economy

6G Fundamentals: Vision and Enabling Technologies

From 5G to 6G Trustworthy and Resilient Systems

David Soldani
University of New South Wales, Australia

Abstract: This article reviews the 6G global landscape and the most relevant private and public initiatives, with US$ billions of investments in next generation information and communication (ICT) systems and application services. Then, it presents the 3rd Generation Partnership Project (3GPP) technology roadmap towards 6G and 5G New Radio (NR) releases. This is followed by an introduction to the latest shift in paradigm "from Internet of Things (IoT) to Internet of Intelligence (IoI)", which paves the way towards 6G wireless. The new system is anticipated to provide pervasive connectivity to functions with the ability to represent knowledge, process knowledge, and make decisions, with or without human intervention. Beyond that, the paper discusses the new carrier frequency bands above 110 GHz; and innovative fundamental enabling technologies, such as integrated semantic communication and sensing, low earth orbiting satellites, quantum key distribution, post quantum cryptography, and distributed ledger technology; and portrays a network vision for 6G wireless, looking to 2030 and beyond. Conclusions are drawn on 6G prospects, the needs of security by design for 6G; as well as the potential of 6G for securely connecting pervasive intelligence and preserving privacy; and new research directions to cater for new use categories and requirements.

Keywords: 5G, B5G, 6G, Cyber Security, Privacy Protection

5G is Operational and Accelerating

The fifth generation of mobile communication system, denoted as 5G, is expanding over the world. The global 5G landscape was discussed in GSMA (2021a), in terms of assigned spectrum and live and planned 5G launches. As of Q4 2020, "new" spectrum specifically earmarked for 5G had been assigned in 38 markets. About 130 operators have already received spectrum across low (≤ 1GHz), mid (= 1-6 GHz) and high bands (≥ 6GHz); about 50 operators in low band, 100 operators in mid band (mostly exploited), and 40 operators in high band. More than 110 operators have planned to launch 5G, most of them in Asia Pacific and Europe. (For updates see gsmaintelligence.com.)

Today, 5G services are already available across East Asia and North America, and most new launches continue to be in Europe. We therefore expect to see significant connections growth across this region in 2022. China with its massive base and local device availability dominates the global 5G connections (230+ millions, at the time of writing), and China will still account for nearly half of the global consumer 5G connections, which the Global System for Mobile Communications Association (GSMA) forecasts to reach 1.8 billion by 2025 (GSMA, 2021a).

The 5G landscape briefly – in terms of announced 5G devices by form factor, 5G connections and 5G global adoption by 2025 – was captured in GSA (2021). According to the Global Mobile Suppliers Association (GSA), by mid-April 2021 we had more than 700 announced devices: 350+ smartphones, 130+ Fixed Wireless Access (FWA) Customer Premise Equipment (CPE) devices (indoor and outdoor), 90+ modules, 30+ modems, 30+ hotspots, 20+ notebooks and tablets, and 30+ other devices (including drones, TVs, vehicle OBUs, etc.).

The architecture of 5G is constantly evolving and will continue to evolve over the next decade until 6G is developed (Soldani *et al.*, 2018; Nokia, 2020; Ericsson, 2020; 5G Americas, 2021a). Whereas the first 5G release (Release 15) predominantly addressed the immediate needs of enhancing the mobile broadband experience (eMBB), the release of the 16th and 17th versions take 5G toward the full 5G vision, balancing the needs of mobile broadband operators with expansion into new markets, including vertical players. The second phase of 5G has been finalised in 3GPP with the anticipated release of the 16th version (Release 16) of the technical specifications (3GPP, 2020a). The 18th releases and beyond will focus on the definition of new use cases, study items (SI) and work items (WI) towards 6G, which is expected to be specified by 2030 (Soldani, 2021a). The 3GPP 5G to 6G high level roadmap is depicted in Figure 1.

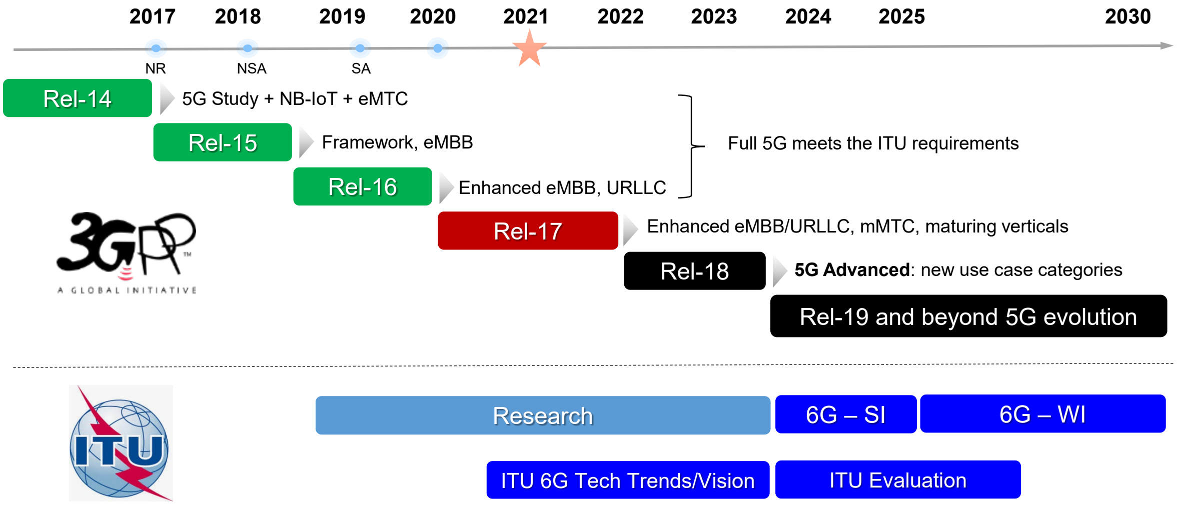


Figure 1. 3GPP 5G to 6G roadmap (Soldani, 2021a).

Release 16 forms the foundation for supporting Industrial IoT. It has an Ultra-Reliable Low-Latency Communications (URLLC) functionality with ability to achieve unprecedented levels of reliability, down to packet error rates of 10^{-6} ("six nines"). It boasts integration with IEEE Time-Sensitive Networking (TSN). It supports Private Networks, which are also known as Non-Public Networks (NPN), with both an NPN-specific authentication mechanism for User Equipment (UE) without a Universal Subscriber Identity Module (USIM) and an Authentication and Key Agreement (AKA) mechanism for the UE with a USIM card. It has a New Radio (NR) in Unlicensed (NR-U) spectrum in the 5 GHz and 6 GHz frequency bands, which may coexist with other systems such as IEEE 802.11 variants or LTE Licensed-Assisted Access (LAA). Vehicular communication ("V2X") features a *sidelink* for direct communication between devices.

Beyond this, Release 16 supports Full 5G System Resilience with security features for service-based interfaces (SBI), Transport Layer Security (TLS) and Token-based authorization (Auth2.0); Authentication and Key Management for Applications (AKMA), such as IoT over 5G; and Network Slice-Specific Authentication and Authorization (NSSAA). It also supports Wireless-Wireline Convergence (WWC) and Future Railway Mobile Communication System (FRMCS – Phase 2). The support extends to Network Automation Phase 2; Integrated Access & Backhaul (IAB), which adds support for wireless backhauling of base stations using the NR radio interface with larger bandwidths, for network densification without requiring fibre implementation in every base station; Device Power Saving; Mobility Enhancement, and Enhanced Massive MIMO with multiple Transmission and Reception Points (TRPs). Dynamic Spectrum Sharing (DSS) – already supported by Release 15 – will become Wideband New Radio DSS with Carrier Aggregation (CA) to enable a quicker NR deployment on existing LTE bands, with efficient pooling of the resources between LTE and NR, providing a path for NR and LTE to co-exist while also enabling a granular spectrum re-farming (3GPP, 2020a).

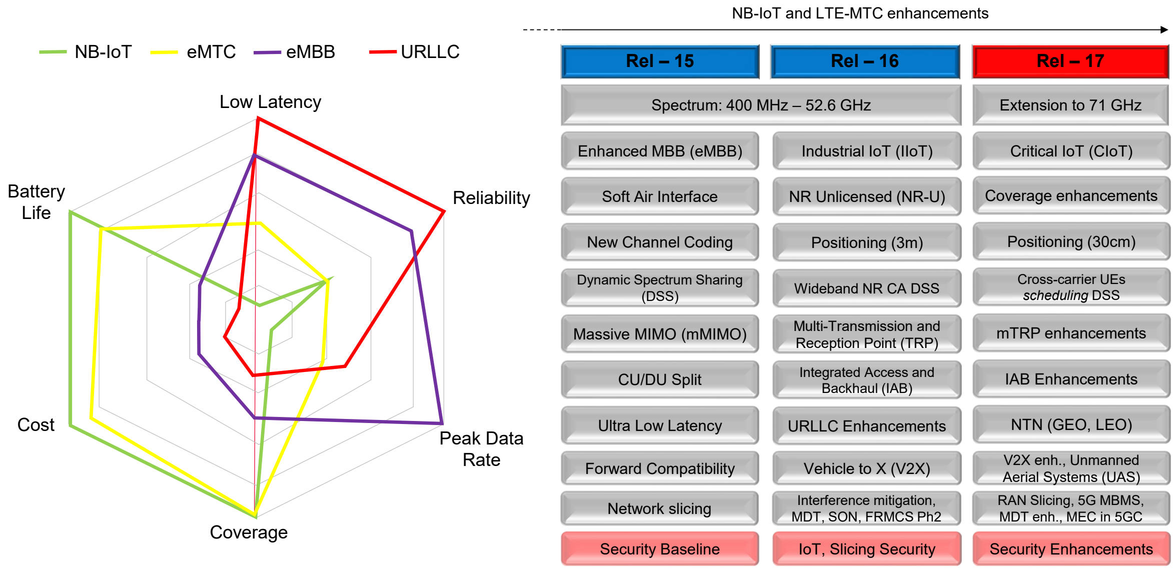
As regards Release 17, the features to be included in this version have been agreed to and are scheduled for completion by the end of 2021 (3GPP, 2020b). Release 17 targets an even wider ecosystem expansion, particularly Critical IoT (CIoT). It will support native Time Sensitive Communication (TSC); High-Accuracy Positioning (cm-level); Sidelink enhancement for public safety and pedestrians; Multimedia Broadcast Multicast Services (MBMS); Non-Terrestrial Networks (NTN), such as Geostationary Earth Orbiting (GEO) and Low Earth Orbiting (LEO) satellites; and FRMCS enhancements (FRMCS – Phase 3). Further support will be provided to Radio Access Network (RAN) Slicing; Network Automation enhancements; New Radio in the 52–71 GHz frequency range; Device Power Saving enhancements; Further enhanced MIMO; Multiple USIMs; Unmanned Aircraft Systems (UAS) and Multi-Access Edge

Computing (MEC), particularly suitable for delay-sensitive applications. This is illustrated in Figure 2 (3GPP, 2020b).

An NTN system is a network where spaceborne (i.e., GEO, MEO, LEO) or airborne (i.e., UAS and HAPS) vehicles behave either as a relay node or as a base station, thus distinguishing transparent (amplify and forward, or decode and forward) and non-transparent (with own radio resource management algorithms) satellite architectures. GEO satellites are at around 35,786 km altitude in synchronicity with the Earth's rotation. GEO beam footprint size ranges from 200 to 3500 km. MEO satellites circulate at an altitude varying from 7000 to 25000 km with a beam footprint size that ranges from 100 to 1000 km. LEO satellites move at an altitude from 300 to 1500 km, with a beam footprint size that ranges from 100 to 1000 km. LEO and MEO are also known as Non-GEO (NGSO) satellites and their motion around Earth varies from 1.5 to 10 hours (Rinaldi *et al.*, 2020; Lin *et al.*, 2021). The airborne category encompasses UAS platforms, which are typically placed at an altitude between 8 and 50 km and includes High Altitude Platform Systems (HAPS) at 20 km altitude. Like the GEO satellite, the UAS position can be kept fixed in the sky with respect to a given point on the ground. UAS beam footprint size ranges from 5 to 200 km. NTN terminal refers to either the 3GPP UE or a specific satellite terminal. Very small aperture terminals operate in the radio frequency of Ka-band (i.e., 30 GHz in the uplink and 20 GHz in the downlink), whereas handheld terminals operate in the S-band (i.e., 2 GHz) (3GPP, 2020b).

Narrow Band IoT (NB-IoT) and LTE-Machine Type Communication (MTC), i.e., broadband IoT, will be further enhanced in parallel and will coexist with the current and NR future 3GPP releases. Currently, the majority of cellular IoT connections still rely on 4G connectivity. This technology is likely to have a large market penetration by 2025, with massive-machine type communications, based on NB-IoT and LTE-MTC devices, predicted to constitute more than 40% of all cellular IoT connections. Broadband IoT will contribute nearly 34 of those percentage points. Critical-IoT with requirements on extremely low latency and ultra-high reliability will contribute only a small fraction to the total cellular IoT connections even in 2025 (5G Americas, 2021a).

The release of versions 16 and 17 will witness an expansion of the ecosystem that can take advantage of 5G. As depicted in Figure 2, it will do so by adding many features to provide the full range of functionality required by new industry segments. It will make 5G networks easier to deploy and operate end to end. As already described, Release 17 is currently anticipated to be finalized in the second quarter of 2022. However, the evolution of mobile communication technology will obviously not end with Release 17.



Rel – 15	Rel – 16	Rel – 17
Spectrum: 400 MHz – 52.6 GHz		Extension to 71 GHz
Enhanced MBB (eMBB)	Industrial IoT (IIoT)	Critical IoT (CIoT)
Soft Air Interface	NR Unlicensed (NR-U)	Coverage enhancements
New Channel Coding	Positioning (3m)	Positioning (30cm)
Dynamic Spectrum Sharing (DSS)	Wideband NR CA DSS	Cross-carrier UEs *scheduling* DSS
Massive MIMO (mMIMO)	Multi-Transmission and Reception Point (TRP)	mTRP enhancements
CU/DU Split	Integrated Access and Backhaul (IAB)	IAB Enhancements
Ultra Low Latency	URLLC Enhancements	NTN (GEO, LEO)
Forward Compatibility	Vehicle to X (V2X)	V2X enh., Unmanned Aerial Systems (UAS)
Network slicing	Interference mitigation, MDT, SON, FRMCS Ph2	RAN Slicing, 5G MBMS, MDT enh., MEC in 5GC
Security Baseline	IoT, Slicing Security	Security Enhancements

Figure 2. 3GPP R15, 16 and 17 supported spectrum and key features (Soldani, 2021a).

The evolution of 5G will continue in subsequent releases, and Release 18, denoted as *5G-Advanced* by 3GPP, will enhance its capabilities and extend the use cases to which it can be applied. However, as shown in Figure 1, at some stage, the wireless industry is expected to transit from 5G into 6G, that is, the *Sixth-Generation mobile communication system*.

At the time of writing, many use cases and related enabling technologies of 6G wireless are still under discussion, and it remains to be seen whether 6G will come along with a new air-interface or it will simply further enhance the 5G Advanced new radio. At this stage, 6G-related activities are primarily focusing on identifying the new problems and stakeholders' needs that, in turn, will drive the definition of a new set of technical requirements and features, which 6G wireless will need to support from day one. In parallel, as examined in the following sections, many joint research and innovation projects are currently focusing on fundamental technology components to cater for the needs of consumers and vertical sectors (5G Americas, 2021b).

6G Gains Momentum

While the deployment of next generation mobile communication systems still lies ahead on a time frame of ten or more years, many ongoing 6G programs and related investments provide a captivating prospect for significant acceleration of 6G studies. Industry and public organisations have already started investing in research and innovation (R&I) actions, to meet the requirements 6G will probably demand when it goes live around 2030 (Castro, 2021, 5G Americas, 2021b).

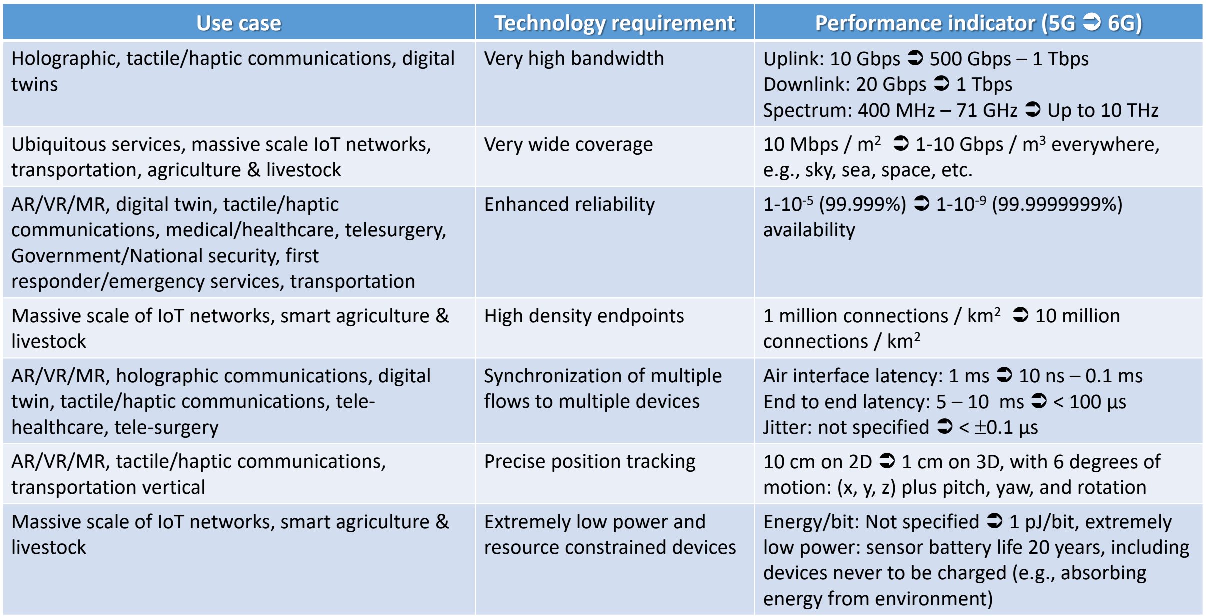
These include the usage scenarios promised in 5G networks but not achieved yet, and more advanced use cases that are emerging in the context of 6G systems. Examples of such emerging scenarios include communications at Terahertz, ubiquitous coverage (land, air, space, sea), holoportation, tactile/haptic communications, medical/health vertical, government/national security, imaging and sensing, public safety services, cyber-physical systems/manufacturing, and transportation. Examples of relevant use cases and consequent technology requirements are shown in Figure 3 (5G Americas, 2021b). For more information and other usage scenarios, towards 6G, the reader may refer to, for example, 6G Flagship (2021a) or 6GIC Vision (2021).

Specific international efforts by leading nations in the wireless cellular industry and relevant beyond 5G (B5G) and 6G initiatives and associated investments are illustrated in Figure 4.

In **Europe**, within the EU Horizon 2020 R&I framework program, three recent joint projects, focused on 6G development, have been announced, namely: Hexa-X, RISE-6G, and NEW-6G. The European Commission (EC), within the Smart Network and Service framework program, has proposed a €900 million budget to invest in 6G research, with particular attention to standardisation leadership and boosting 5G deployment (Castro, 2021).

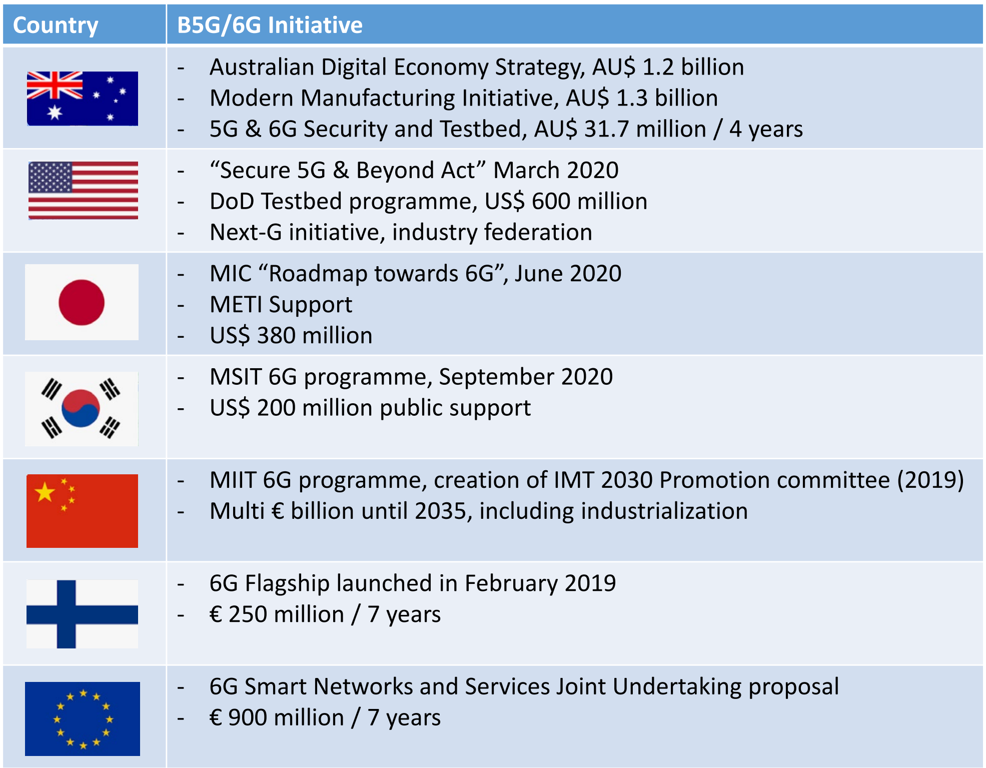
Beyond that, several countries have kicked off their own endeavours and allocated budget to conduct their own research. Australia, USA, UK, Europe, Japan, South Korea, and China are in the mix, and there is pressure on other nations to join the club.

In 2021, in **Australia**, the Federal Government has pledged AU$ 1.2 billion, investing in the settings, infrastructure, and incentives to grow Australia's digital economy. (The investment boosts the recently launched Modern Manufacturing Initiative (MMI), AU$ 1.3 billion.) New investments under the Digital Economy Strategy in Australia's cyber security, safety and trust include $31.7 million to secure their future connectivity using 5G and 6G mobile networks.



Use case	Technology requirement	Performance indicator (5G ➲ 6G)
Holographic, tactile/haptic communications, digital twins	Very high bandwidth	Uplink: 10 Gbps ➲ 500 Gbps – 1 Tbps Downlink: 20 Gbps ➲ 1 Tbps Spectrum: 400 MHz – 71 GHz ➲ Up to 10 THz
Ubiquitous services, massive scale IoT networks, transportation, agriculture & livestock	Very wide coverage	10 Mbps / m^2 ➲ 1-10 Gbps / m^3 everywhere, e.g., sky, sea, space, etc.
AR/VR/MR, digital twin, tactile/haptic communications, medical/healthcare, telesurgery, Government/National security, first responder/emergency services, transportation	Enhanced reliability	1-10^{-5} (99.999%) ➲ 1-10^{-9} (99.9999999%) availability
Massive scale of IoT networks, smart agriculture & livestock	High density endpoints	1 million connections / km^2 ➲ 10 million connections / km^2
AR/VR/MR, holographic communications, digital twin, tactile/haptic communications, tele-healthcare, tele-surgery	Synchronization of multiple flows to multiple devices	Air interface latency: 1 ms ➲ 10 ns – 0.1 ms End to end latency: 5 – 10 ms ➲ < 100 µs Jitter: not specified ➲ < ±0.1 µs
AR/VR/MR, tactile/haptic communications, transportation vertical	Precise position tracking	10 cm on 2D ➲ 1 cm on 3D, with 6 degrees of motion: (x, y, z) plus pitch, yaw, and rotation
Massive scale of IoT networks, smart agriculture & livestock	Extremely low power and resource constrained devices	Energy/bit: Not specified ➲ 1 pJ/bit, extremely low power: sensor battery life 20 years, including devices never to be charged (e.g., absorbing energy from environment)

Figure 3. Examples of use cases and corresponding technology requirements (5G Americas, 2021b).



Country	B5G/6G Initiative
🇦🇺	- Australian Digital Economy Strategy, AU$ 1.2 billion - Modern Manufacturing Initiative, AU$ 1.3 billion - 5G & 6G Security and Testbed, AU$ 31.7 million / 4 years
🇺🇸	- “Secure 5G & Beyond Act” March 2020 - DoD Testbed programme, US$ 600 million - Next-G initiative, industry federation
🇯🇵	- MIC “Roadmap towards 6G”, June 2020 - METI Support - US$ 380 million
🇰🇷	- MSIT 6G programme, September 2020 - US$ 200 million public support
🇨🇳	- MIIT 6G programme, creation of IMT 2030 Promotion committee (2019) - Multi € billion until 2035, including industrialization
🇫🇮	- 6G Flagship launched in February 2019 - € 250 million / 7 years
🇪🇺	- 6G Smart Networks and Services Joint Undertaking proposal - € 900 million / 7 years

Figure 4. Examples of Beyond 5G (B5G) and 6G initiatives ongoing globally (Castro, 2021).

The Australia Government will build a joint 'Secure-G' Connectivity Test Lab with industry, which will enable the involved organisations to verify protocols, compliance with standards, and quality of software towards a transparent and secure 5G connectivity. Beyond that, the Government will invest in 6G security to address the security requirements of 6G and future connectivity technologies. This will make Australia become a global leader in cyber space, ensuring that 6G technologies are secure by design and help shape international security standards in alignment with Australia’s national interest (Australian Government, 2021).

In **North America**, Next G activities are primarily centred around academia with additional efforts from agencies of the US government and Standards Developing Organizations (SDOs) (5G Americas, 2021b). In 2020, the industry Alliance for Telecommunications Industry Solutions (ATIS) launched the Next G Alliance (NGA), an initiative aiming to lay out the foundations of 6G in North America, and issued a call-for-action urging the United States to promote 6G leadership. The group currently has 48 founders and contributing members, including some tech. giants like Google, Apple, Microsoft, Facebook, Samsung, Ericsson, Nokia, Qualcomm, and most of the major carriers in the U.S. and Canada. The first initiative outcome – a common roadmap to 6G – is expected to be delivered by the end of 2021 (ATIS, 2021).

In 2018, in **Finland**, the University of Oulu started leading a national research program on 6G. The 6G Flagship initiative consists of five collaboration partners, including Aalto University, Nokia and VTT (5G Americas, 2021b).

In 2019, **Japan** announced a stimulus pack of $2 billion to support industry research on 6G technologies with a timeline of 2020-2030. In 2020, the Japanese government announced plans to develop a 6G strategy with private sector representatives and university researchers. The Beyond 5G Promotion Consortium includes the University of Tokyo, along with major Japanese telecom players such as Rakuten Mobile, Nippon Telegraph & Telephone, NTT Docomo, KDDI and SoftBank Corp, which aims at commercialising 6G services in the 2030s. During the same year, the Japan communications ministry unveiled ambitious goals under its "Beyond 5G" strategy, seeking to capture a 30% global market share for base stations and other infrastructure, up from just 2% at the time of writing (5G Americas, 2021b).

In 2021, Japan's Beyond 5G Promotion Consortium has signed an agreement with Finnish group 6G Flagship. The initiative follows a $4.5 billion commitment by Japan and the U.S. toward the development of next-generation communications technology (Hirose, 2021).

In 2020, in **South Korea**, the Ministry of Science & ICT (MSIT) announced US$170 million of public support for investments in 6G research and development for five years. The targets are to reach 1 Tbps data rate; achieve 0.1 ms wireless latency (below 5ms wired latency); expand connectivity from ground to 10 km in space; apply artificial intelligence to the entire network; and provide security by design, end to end. The use cases in focus are smart factories, smart cities, and autonomous vehicles. Non-terrestrial networks, such as 6G satellites, will be among the key fundamental enabling technologies that will be investigated (Castro, 2021).

In **China**, the Chinese Government has invested more than $30 billion towards 5G R&D over five years, and 6G is expected to receive comparable investments (5G Americas, 2021b). In 2019, two working groups were set up. The first team are government agencies responsible for promoting 6G research and development. The second group, called the "China 6G Wireless Technology Task Force", consists of vendors, operators, China Research Agencies and Chinese universities, tasked with laying out the development of 6G and proving its scientific feasibility. Beyond that, in 2020, China launched a satellite containing experimental 6G technologies. The Tianyan-5 Satellite, sent up with 13 other satellites, will test Terahertz (THz) communications in what the BBC described as a "world first" test of 6G technology in space (Tonkin, 2020).

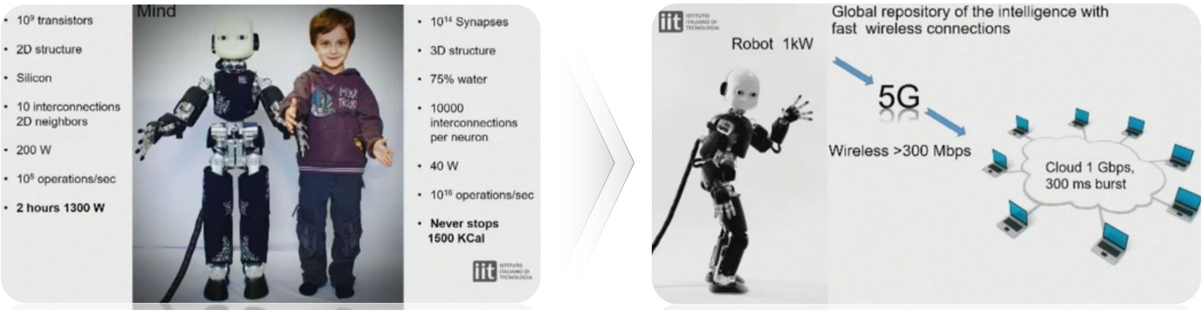
6G Network Architecture Vision

Based on the following evidence, the author's vision is that, by 2030, *all intelligence will be connected following a defence-in-depth strategy – augmented by a zero-trust model – through digital twinning, using B5G/6G wireless, and machine reasoning will meet machine learning at the edge.*

The following societal challenges and necessities are the main source of inspiration for the formulation of this vision (Soldani, 2021b):

1. The power cost per operation is from 1000 to 5000 higher in machines than in humans. Hence, *the intelligence must be centralized*, which also reduces the cost of the device of any form factor (GSA, 2021). As illustrated in Figure 5, our brain corresponds to a lamp of 40 W and can perform 10^{16} operations per second, while one of the most advanced humanoid platforms, produced and named *iCub* by the Italian Institute of Technology (iit), requires 200 W to perform 10^{8} operations. This means that a boy after eating a chocolate would keep moving for 1 week and iCub, with an equivalent amount of energy in kWh, would run out of power in 2 hours.
2. The two-way, end-to-end latency must be below 5-10 ms for dependable *remote control* of a connected device, or to exchange *haptic feedback* with no cyber sickness, between two peer entities (Soldani & Innocenti, 2019). Hence, *all intelligent functions must be placed at the Edge*: i.e., close to the device or end user.
3. Machine Learning, i.e., pattern recognition algorithms, have many flaws, limitations and biases. Hence, *machine learning (ML) must meet machine reasoning (MR)*, and a possible reference architecture to achieve this goal is shown in Figure 6.
4. It is an imperative to improve efficiency and productivity to reduce Green House Gas (GHG) emission (CO_2). Hence, digitization and digital transformation is a must, and currently one of the most valuable approaches is *digital twinning*. (A digital twin is a virtual representation that serves as the real-time digital counterpart of a physical object or process.)
5. We are currently witnessing a paradigm shift from "all things connected" to "connected intelligence" and that is only feasible if we make technology safe, secure, and protective of privacy. Hence, a *new mobile communication system (B5G/6G) is required that supports security by design, based on a Zero Trust model.*

In May 2021, similar views were presented at the recent 6G Symposium on "Shaping Industry & Society Beyond 5G", where use cases; emerging digital, virtual, and physical worlds, bringing new business opportunities; and the *wireless* technology evolution towards 6G were discussed (6G Symposium, 2021).



1. Centralized intelligence	2. Intelligence at the Edge	3. ML needs machine reasoning	4. Digitisation, digitalisation and digital transformation	5. From 5G to B5G/6G with Zero Trust model
Power cost per operation: **1000-5000** higher in machines	End to end **latency** below e.g. **10ms** is a must	Pattern recognition techniques have many **limitations** and **bias**	It is a must to improve **efficiency** and **productivity** to reduce CO_2 (GHG) emission	From all things connected to **connected intelligence** with **dependability** and **trust**

Figure 5. Examples of societal challenges and necessary corrective actions (Soldani, 2021b).

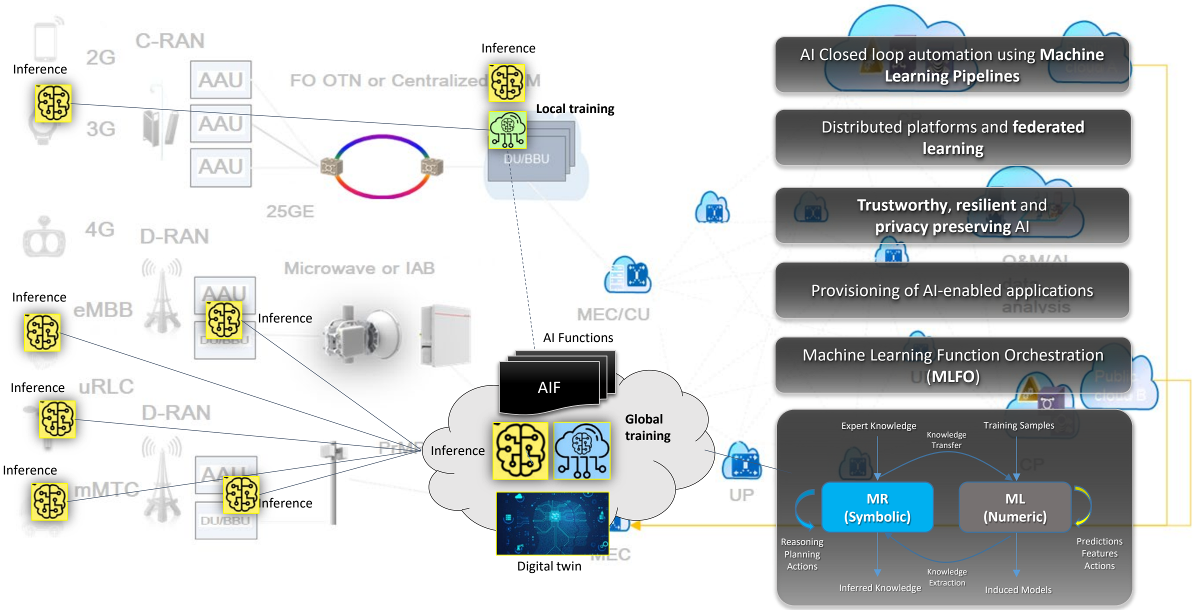


Figure 6. Examples of how Machine Learning (ML) may meet Machine Reasoning (MR) (Soldani, 2021b).

In short, 6G wireless aims at bridging the “physical world” and the “cyber world”; it is about a new paradigm shift: from *connected people and things* (information world) to *connected intelligence* (intelligent world). 6G wireless is the technology to deliver artificial intelligence to everyone, anywhere and at any time (Tong & Zhu, 2021, Soldani, 2021e).

This is precisely what was already envisioned in Soldani & Manzalini (2015), where the authors presented a blueprint of an AI native operating system for the first time and, particularly, the services on top expected in the horizon 2020 and 2030. Figure 7 is identically inspired by the architecture the authors published at that time, looking at 5G and beyond. It also included the possibility of integrating sensing and communication capabilities of access nodes together with intelligent functions pervasively distributed at the edge of the network, as well as with centralised computing platforms. The latter is responsible for the control of all connected functions, as well as the orchestration, not only of virtual network functions or virtual slice instances, but also the placement of nodes of different machine learning pipelines, which will unquestionably characterize the 6G system (5GPPP Technology Board, 2021).

The 6G wireless architecture will be shaped by five key constituents (Tong & Zhu, 2021), as illustrated in Figure 7: *virtual-X*, *tactile*, *inferencing*, *sensing*, and *learning*. AI will be the dominant service and application (5GPPP Technology Board, 2021). The primary spectrum will be millimetre and terahertz waves, which lie at the far end of the infrared band, just before the start of the microwave band (6G Flagship, 2021b). This will allow us to apply wireless sensing capabilities and 6G wireless will operate as a sensor network (6G Flagship, 2020a). The network and devices can perform real-time (RT) sensing, which will be the fabric to link the physical world and the cyber world (6GIC Vision, 2021).

The primary service will be virtual reality (VR) for everything. The virtual-X channel will allow access to digital content in the cyber world; the augmented tactile channel will carry haptic feedback, as the augmented neural system for the physical world (Soldani & Innocenti, 2019); and the inference channel will exchange services between the AI engine and the end user.

From the physical world to the digital world, the primary applications are sensing and collecting big data for machine learning (ML). New compression technologies and novel approaches will be required to train the neural networks (Soldani & Illingworth, 2020). The integration of sensing with communication capabilities in the mmWave/THz multiband radio heads, operating above 110 GHz, as well as in other connected devices, of any form factor (such as cameras and sensors), is expected to lead to significant advances in 6G wireless technology. Higher frequency bands allow the system to sense objects with very fine resolutions, in all physical dimensions: range, angle, and Doppler shift (6GIC Vision, 2021).

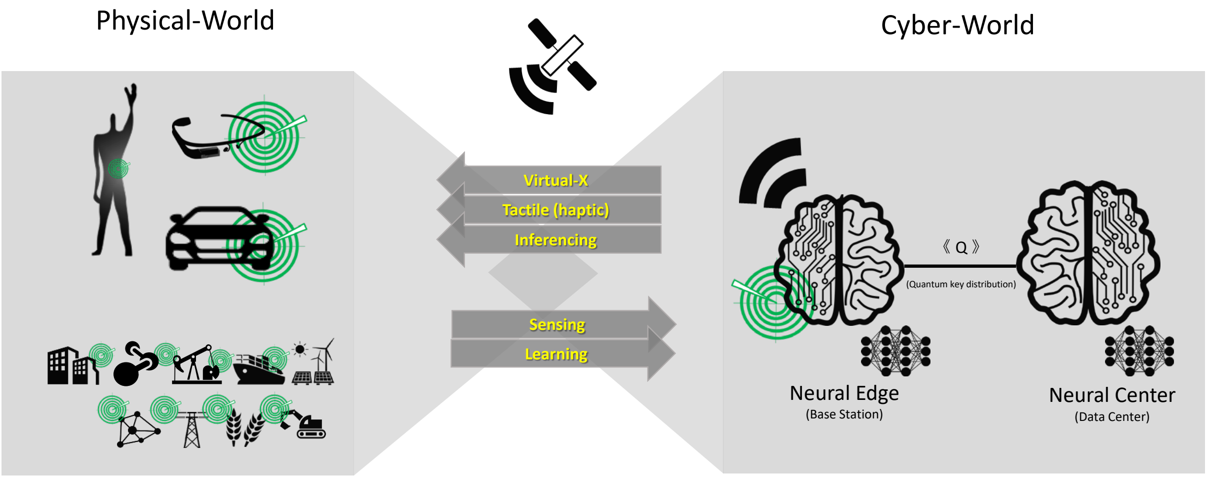


Figure 7. 6G Wireless network architecture vision (Tong & Zhu, 2021, Soldani, 2021e).

On the network side, we have the 6G Base Station (BS) node, at the Deep Edge, and 6G Neural Edge, at the Edge. Edge Nodes will have capabilities for AI resource runtime scheduling and orchestration (IaaS) and AI workflow/data runtime scheduling and orchestration (PaaS). The Edge Node will be mostly used for local ML, so the classical Point of Presence (PoP) at the edge will become the Neural Edge, and the BS will become the Deep Neural Node. Neural Centres (Cloud with Global AI capabilities) provide AI services to external customers (AIaaS). Examples of such services could include AI-enabled high precision localisation and end user mobility trends, etc. Quantum Key Distribution (QKD) can be deployed for the fibre-optic link between the Neural Centre and the Neural Edge (GSMA, 2021b). IaaS, PaaS and AIaaS, borrowed from cloud services, could very well coexist as they would cover diversified AI service requirements from very different sectors. AI services that run on this advanced infrastructure will bring many advantages: from global AI to local AI, form offline AI to real-time AI (Soldani & Manzalini, 2015; Tong & Zhu, 2021).

Non-terrestrial networks are an integral part of the 6G wireless system, and a massive LEO satellite constellation will bridge traditional and non-traditional networks aiming at full planet coverage, eventually, by combining different fronthaul, backhaul, and midhaul techniques. For instance, satellite or fibre may form the backhaul, whereas the multi-hop could be part of the fronthaul, in conjunction with the 6G terrestrial nodes, used for direct access, as depicted in Figure 8, which is an improved version of what the authors presented in Yaacoub & Alouini (2020).

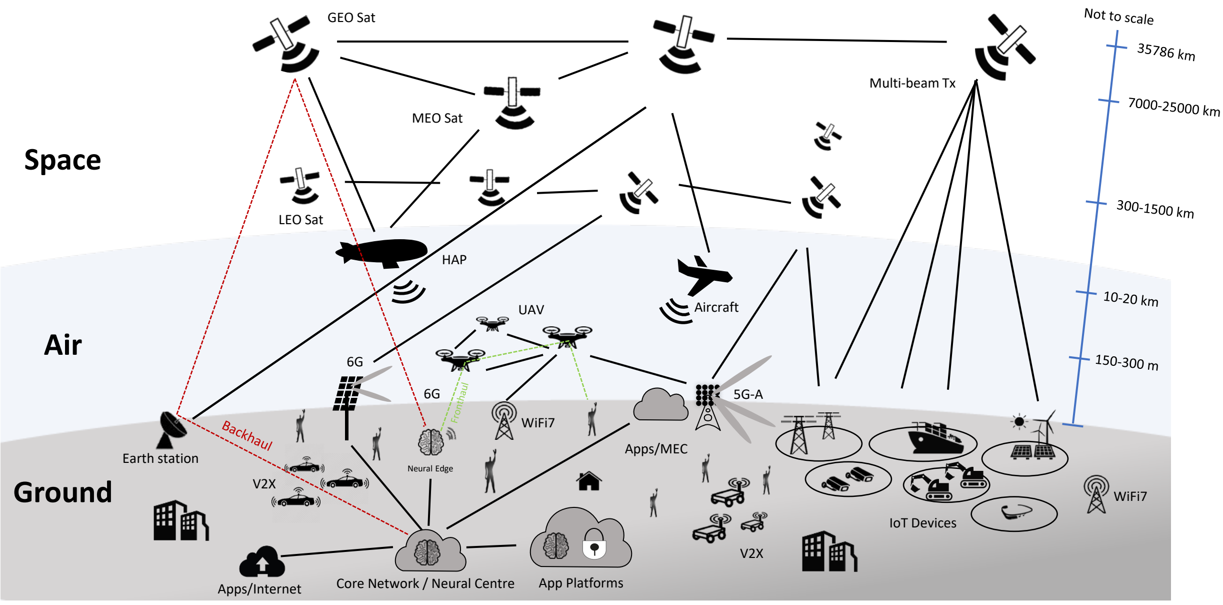


Figure 8. Examples of fronthaul (in red) and backhaul (in green) approaches towards ubiquitous connectivity.

6G Fundamental Enabling Technologies

This section provides examples of concrete technical approaches or solutions to cater for the usage scenarios and use cases introduced in the previous sections while satisfying the related technology requirements collected in Figure 3.

This paper anticipates five essential technology enablers that will be necessary to fulfill the needs of the next generation system to realise the fundamental shift in paradigm *from the internet of things to the internet of intelligence*, the latter being defined as functions with the ability to represent knowledge, process knowledge and make decisions (Soldani, 2021b).

Artificial Intelligence at the network edge

The first shift in paradigm is about going *from an artificial intelligence enhanced network*, which is the 5G system today and its future releases, to an *AI native communication platform*, as shown in Figure 9.

A unified, logical architecture for ML for future networks, including 5G, has been already defined by the ITU-T Focus Group (FG) -ML5G (Soldani & Illingworth, 2020). The FG-ML5G proposes a logical *ML pipeline*, i.e., a set of logical entities (each with specific functionalities) that can be combined to form an *analytics function*. Each functionality in the ML pipeline is defined as a *ML Pipeline node*, e.g., source, collector, pre-processor, model, policy, distributor, or sink. In particular:

- A ***source*** (src) is a node that *generates data* that can be used as input for the ML function; it could be a UE, session management function (SMF), access and mobility management function (AMF) or any other entity in the network, including an application function (AF).
- A ***collector*** (C) is a node responsible for *collecting data* from the src: e.g., it may use the radio resource control (RRC) protocol to configure UE, acting as a src; or vendor specific operations, administration and maintenance (OAM) protocols to configure an AMF or AF acting as a src.
- A ***pre-processor*** (PP) is a node responsible for *cleaning data, aggregating data or performing any other pre-processing* needed for the data so that it is in a suitable form for the ML model to consume it.
- A ***model*** (M) is an *ML model*, e.g., a prediction function. (Model training is required to be done in a *sandbox* – a domain internal to the network operator in which ML models can be trained, verified and their effects on the network studied – using training data.)
- A ***policy*** (P) is a node that provides a *control* for an operator to put a *mechanism* into place to minimise impacts on a live network, so that the operation is not impacted, e.g., to safeguard the sanity of the network.
- A ***distributor*** (D) is a node responsible for identifying the sinks and *distributing the ML output to the corresponding sinks*; it may use RRC protocol to configure a UE acting as a sink.
- A ***sink*** (S) is the *target node* of the ML output, on which it takes action (*inference*), e.g., a UE adjusting its measurement periodicity based on ML output.

Chaining is the process of connecting ML functions or nodes together to form a complete ML pipeline. The chain itself is declared by the network operator (NOP) in the use case specification, i.e., in the *intent* – a declarative mechanism used for specifying the ML use case

– and its technology-specific implementation in the network is done by the *ML function orchestrator* (MLFO).

The MLFO utilises the constraints (e.g., timing constraints for prediction) defined in the intent to determine the *placement and chaining of ML functions*. Also, the MLFO monitors and manages the ML pipeline nodes in the system and the model, and performs all necessary tasks, including *model reselection*, when the performance falls below a predefined threshold.

An *ML application* can be realised by instantiating logical entities of the ML pipeline with specific roles (e.g., src, collector, sink) and distributing these entities among network functions (NFs) specific to the technology, e.g., virtual network functions (VNFs), based on the related requirements of the logical entities (e.g., a traffic classifier that needs to be fed with data summaries every *X* ms) and capabilities of the node (e.g., computing power at the edge).

In addition to supporting the concept of ML pipeline by design, 6G Wireless is expected to incorporate *outer semantic channels* (Tong & Zhu, 2021), starting precisely from the initial Shannon and Weaver's categorization, which was inspired by Nikola Tesla — who stated, in 1926: "When wireless is perfectly applied, the whole Earth will be converted into a huge brain" (Tesla Universe, n.d.).

The communication through the *inner Shannon channel*, studied and optimised for more than 60 years, could be augmented by an outer channel that models how the human brain processes signals, sensed from the environment, and takes actions. Our brain acquires knowledge from experience, and, in *real time* (RT), i.e., instantaneously, takes complex decisions, without thinking or hesitating, and performs extremely complicated tasks with a sustainable energy consumption (Soldani, 2021b).

Mimicking how our brain works, an AI native 6G wireless system could support semantic communication capabilities by design. A goal-oriented and semantic communication may be enabled by the broad adoption of deep neural networks (DNN), which allow the derivation of exploitable and explainable meanings from an unlimited amount of sanitised information (data) (Calvanese Strinati & Barbarossa, 2021).

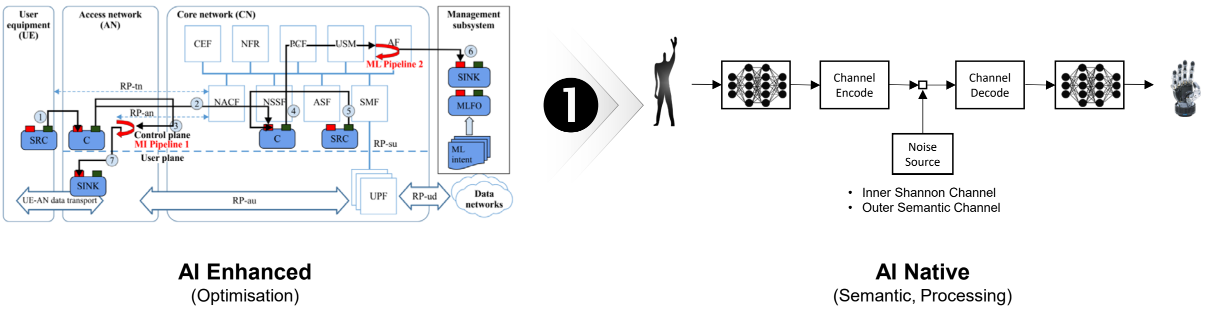


Figure 9. From AI enhanced networks to AI native communication systems (Soldani, 2021b).

The design and effective control and management of new generation wireless networks may be achieved with a massive exploitation of generative pre-trained transformer platforms (GTP) (Tong & Zhu, 2021, Soldani, 2021e).

Combined sensing and communication

The second shift in paradigm is about going *from an information centric approach of bits and bytes to uplink and downlink sensing*, with sensing capabilities embedded in devices and access points (radio heads), denoted as *Neural Edges* in Figure 7 and Figure 8, operating at very high frequencies (millimetre waves and THz communications) and using very large contiguous and/or non-contiguous (detached) bandwidths (of several GHz).

Several definitions of the THz band may be found in the literature, although the ITU definition of the *tremendously high frequency* (THF) region states that the *THz band* is from 0.3 THz to 3 THz (6G Flagship, 2021b).

In 6G Flagship (2021b), the authors call the higher end of the extremely high frequency (EHF) band the *upper mmW band* or *region*. The band covers frequencies of 100–300 GHz, and that will likely be among the most interesting bands in coming years for the design of new-found radio communication systems. This region provides a much larger slice of spectrum than the *lower mmW region* (30–100 GHz). As discussed earlier, the latter has already been adopted extensively by many standardisation organisations, e.g., 3GPP 5G NR, IEEE 802.11, and other wireless technologies, which, at these frequencies, are unable to provide Tbps radio speeds.

The capability of 6G wireless link transmission is expected to improve by at least 10–100 fold, above that of 5G, to achieve the very high band target and to support the throughput demands of data-rate-intensive services, such as those reported in Figure 3. In addition to improving *spectral efficiency*, 6G wireless is anticipated to widen the supported frequency bandwidths, operate at a variety of carrier frequencies, and transmit at minimal transmission power. Going to the upper mmW band (100–300 GHz), and, in the future, also to the THz band (>300 GHz), network throughput and resource sharing among users could be pushed far beyond that of the current 5G systems, especially in densely populated areas. 6G wireless communication at Terahertz can be used to create powerful links that act as if optical fibres were installed, while connecting satellites or connecting the ground and satellites (6G Flagship, 2021b).

The upper mmW or THz band, with wavelength (λ) around 10 μm, has both the potential for *extremely high-rate communications* and *sensing networks*, in which network infrastructures and devices, of any form factor, are equipped with sensing capabilities (6G Flagship, 2020a).

Sensing is the fundamental enabling technology for *connected intelligence*, which is perhaps the most important application of 6G. Integrating sensing functions with the base stations on already installed networks is a viable way of constructing a 6G sensing network, as shown in Figure 8. The 6G sensing capabilities can be deployed on any critical infrastructure, such as transport, water, gas, ports, electricity, datacentres, close to important points to determine the status and dynamics of traffic, fluids, gas, etc. and then process these data to realise a system able to make decisions, with little or no human intervention (6G Flagship, 2021b).

From the terminal's perspective, the sensing capability could be exploited using methods that make use of various sensor types, such as touch panels, camera, infrared, or gyroscope to smart devices, which allow them to sense the situation and context of the surrounding environment. The results can then be transferred to other parts of the network via a wireless connection (6G Flagship, 2021b).

In short, sensing is a basic means of intelligence and an important part of future 6G networks and devices. We will have full capability of sensing the environment, context, like the radar or lidar systems today, and therefore can extract extensive information, in addition to the classical channel quality indicator (CQI) and other radio measurements, and integrate this information with other sources of data, images, or anything that can be captured by other devices, and thus make it possible to offer Sensing as a Service (Soldani, 2021b).

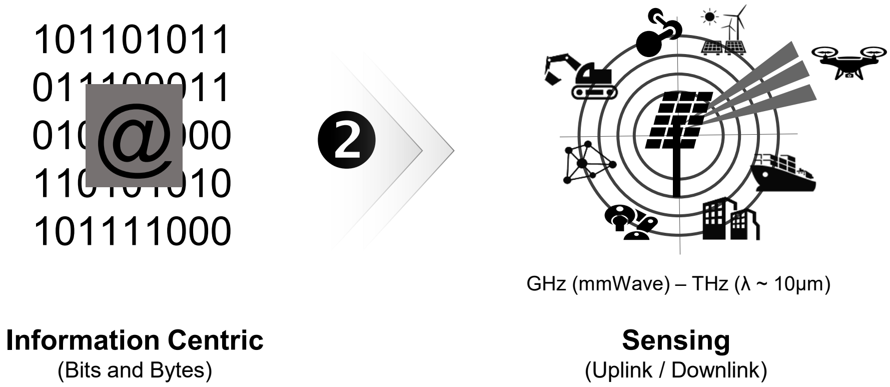


Figure 10. From information centric to integrated sensing and communication (Soldani, 2021b).

Space, air and extreme ground connectivity

The next generation of communication systems is expected to provide *ubiquitous services* in new remote areas not previously served at all (e.g., remote areas, outer space and across entire oceans). Such communication services will create a seamless unified connectivity framework consisting of *terrestrial* (ground-based and marine), *airborne* (satellites, balloons, drones, etc.) and *space based* (LEO/MEO/GEO satellite constellations) networks (see Figure 8).

NTN systems are likely to be an integral part of the *access* network to 6G services and *backhaul* of next generation information and communication systems. The uniqueness of NTNs is in their capability to offer wide area coverage by providing connectivity over regions (e.g., rural areas, vessels, aeroplanes) that are expensive or difficult to reach with terrestrial networks. Therefore, the NTN represents a coverage extension for the terrestrial network in a world market where the demand for different services is growing steadily, due to the ever-increasing number of devices connected to the Internet (Rinaldi *et al.*, 2020; Lin *et al.*, 2021).

Moreover, LEO satellite constellations may be deployed to provide *ultra-low latency services*, optimally down to 1 to 3 ms, between two or more devices in communication. This is because the length of the satellite radio link, end to end, would be shorter than the orthodromic surface distance that would be required to connect the two peer entities by deploying fibre on ground. As illustrated in Figure 11, for example, from London to Shanghai the orthodromic distance is ~10,000 km and that would be reduced to about 1,500 km if the two entities were connected via LEO satellites (Tong & Zhu, 2021, Soldani, 2021e).

When THz communication is used on LEO communications, *beam steering* is required, even for a fixed station to facilitate installation, and its development will be important in the future.

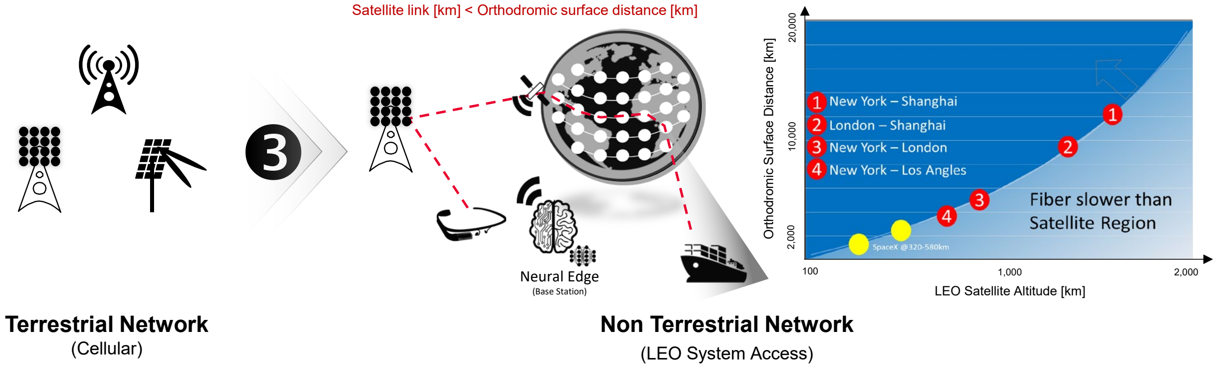


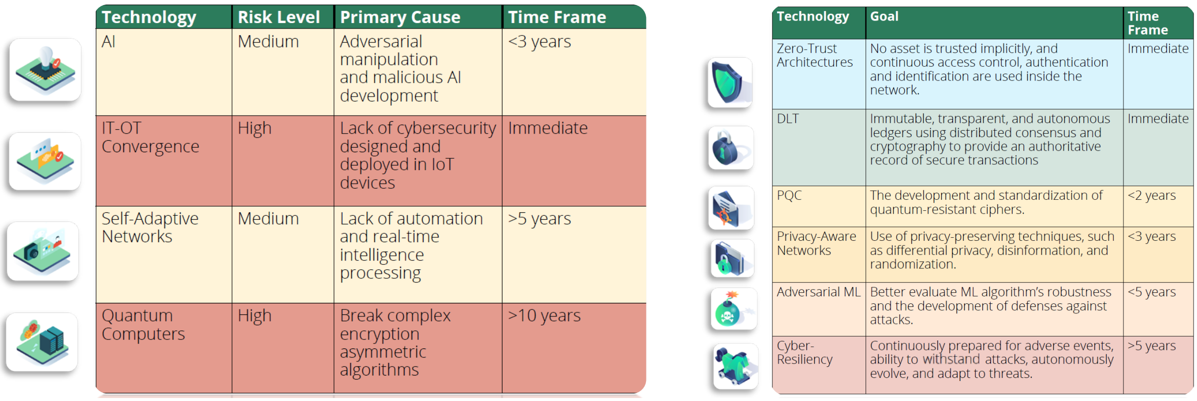
Figure 11. From cellular networks to integrated terrestrial and non-terrestrial infrastructures (Soldani, 2021b).

Privacy preservation, security controls and assurance

The fourth shift in paradigm is about cyber security and privacy protection, in general: *6G wireless is projected to be secure by design*, which is more than a security enhanced system, as is the case today for 5G with respect to 4G (Soldani *et al.*, 2018; 5G Americas, 2020).

Although it is currently difficult to envision pre-emptive security controls – as 6G wireless has not been agreed and specified by any standardisation development organization(SDO) yet – it is important to recognise the fact that a preliminary analysis of the potential threats can be done by simply examining the *risk exposure of the proposed 6G technologies*, as, with any new technology, new threats will emerge that need to be mitigated, in addition to any existing threats that will be carried over from past generation networks (Menting, 2021).

A comprehensive list of potential risks and new threats inherent in the design, development and implementation of 6G wireless communications was discussed in Menting (2021), along with possible security controls, measures and necessary efforts to remediate for the potential weaknesses. A summary of the potential threats, vulnerabilities and corresponding security mechanisms is depicted in Figure 12 (see also ENISA, 2020).



Technology	Risk Level	Primary Cause	Time Frame
AI	Medium	Adversarial manipulation and malicious AI development	<3 years
IT-OT Convergence	High	Lack of cybersecurity designed and deployed in IoT devices	Immediate
Self-Adaptive Networks	Medium	Lack of automation and real-time intelligence processing	>5 years
Quantum Computers	High	Break complex encryption asymmetric algorithms	>10 years

Technology	Goal	Time Frame
Zero-Trust Architectures	No asset is trusted implicitly, and continuous access control, authentication and identification are used inside the network.	Immediate
DLT	Immutable, transparent, and autonomous ledgers using distributed consensus and cryptography to provide an authoritative record of secure transactions	Immediate
PQC	The development and standardization of quantum-resistant ciphers.	<2 years
Privacy-Aware Networks	Use of privacy-preserving techniques, such as differential privacy, disinformation, and randomization.	<3 years
Adversarial ML	Better evaluate ML algorithm's robustness and the development of defenses against attacks.	<5 years
Cyber-Resiliency	Continuously prepared for adverse events, ability to withstand attacks, autonomously evolve, and adapt to threats.	>5 years

Figure 12. Potential threats and novel events, and corresponding security measures (Menting, 2021).

To shift from a *security enhanced network to a security by design system*, 6G needs to integrate security at the heart of the infrastructure and instil the whole network end-to-end with a defence-in-depth strategy, augmented by a Zero Trust model (Soldani, 2020), with the ability to cope with different situations and unexpected events in extreme conditions. Also, the standardization process for 6G must provide new mechanisms for security control, security assurance and privacy preservation (Soldani, 2021d), as shown in Figure 13.

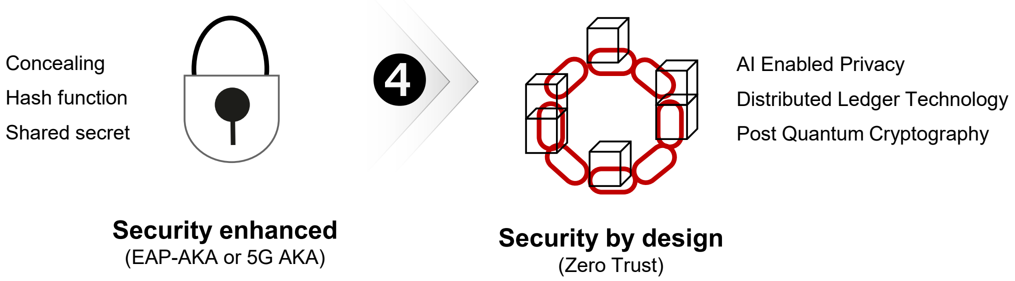


Figure 13. From security enhanced networks to security by design systems (Soldani, 2021b).

Privacy preservation

In 5G, the Extensible Authentication Protocol—Authentication and Key Agreement (EAP-AKA), and 5G Authentication and Key Agreement (5G AKA) – used for Non-3GPP and 3GPP authorized access, respectively – procedures support the *mutual authentication* between the UE and the network, based on a secret (shared) master key (***K***) in the Universal Integrated Circuit Card (UICC), better known as Universal Subscriber Identity Module (USIM), and the Authentication Credential Repository and Processing Function (ARPF). The user's privacy is preserved by concealing the globally unique 5G Subscription Permanent Identifier (SUPI), which can be either in the format of International Mobile Subscriber Identity (IMSI) or presented as a Network Access Identifier (NAI) (3GPP, 2021).

The EAP supports both *primary authentication* (implemented during initial registration, for example, when a terminal is turned on for the first time during a call or session) and *secondary authentication* (executed for authorisation during the set-up of user plane connections, for example, to surf the web or to establish a voice over IP call). The secondary authentication allows the operator to delegate the authorisation to a third party; it is meant for authentication between UE and external data networks (EDN), residing outside the operator's domain. (A similar service was also possible in 4G, but it is now integrated in the 5G architecture.) This mechanism allows an independent authentication and authorization, e.g., using 5G *network slicing*, before the UE may connect to that external network using EAP to request secondary authentication by, e.g., a private network, such as a campus network, in the case of MEC deployment (3GPP, 2021).

As summarised in Figure 14, on the side of the 5G Core Network (5GC), the key element that effectively performs authentication with the UE is Authentication Server Function (AUSF). The AUSF utilises services of Unified Data Management (UDM) and ARPF, which are responsible for hosting the functions related to subscribers' data management and for selecting authentication methods and computing data and keying material that AUSF needs to do its job.

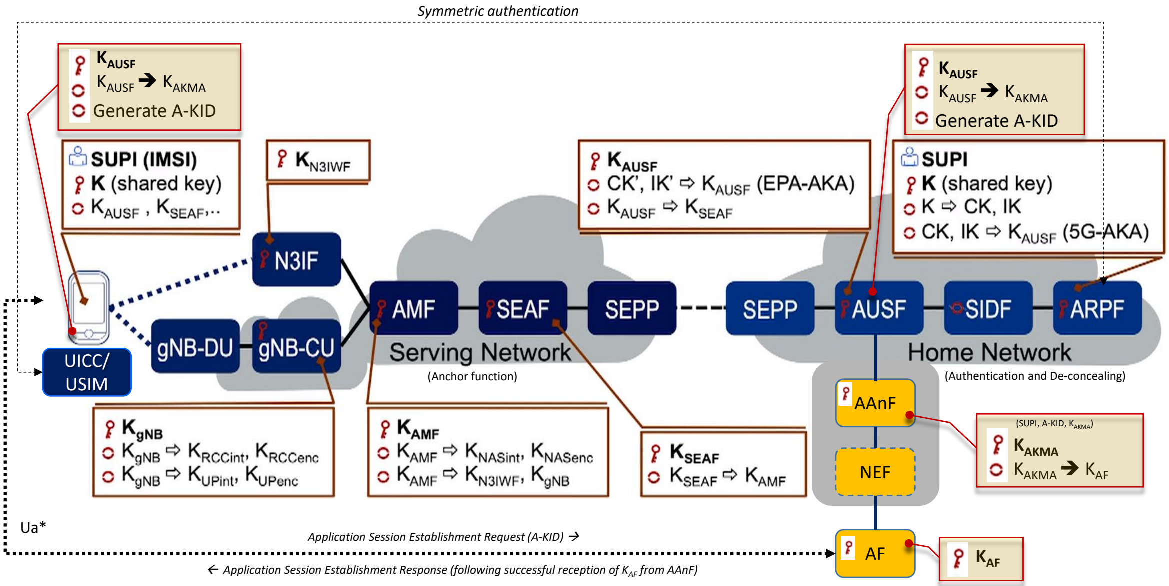

Symmetric authentication
K_{AUSF}
K_{AUSF} → K_{AKMA}
Generate A-KID
SUPI (IMSI)
K (shared key)
K_{AUSF} , K_{SEAF},..
K_{N3IWF}
N3IF
UICC/ USIM
gNB-DU
gNB-CU
AMF
SEAF
SEPP
Serving Network
(Anchor function)
K_{AUSF}
CK', IK' ⇨ K_{AUSF} (EPA-AKA)
K_{AUSF} ⇨ K_{SEAF}
SEPP
AUSF
SIDF
ARPF
Home Network
(Authentication and De-concealing)
K_{AUSF}
K_{AUSF} → K_{AKMA}
Generate A-KID
SUPI
K (shared key)
K ⇨ CK, IK
CK, IK ⇨ K_{AUSF} (5G-AKA)
K_{gNB}
K_{gNB} ⇨ K_{RCCint}, K_{RCCenc}
K_{gNB} ⇨ K_{UPint}, K_{UPenc}
K_{AMF}
K_{AMF} ⇨ K_{NASint}, K_{NASenc}
K_{AMF} ⇨ K_{N3IWF}, K_{gNB}
K_{SEAF}
K_{SEAF} ⇨ K_{AMF}
AAnF
NEF
(SUPI, A-KID, K_{AKMA})
K_{AKMA}
K_{AKMA} → K_{AF}
Ua*
Application Session Establishment Request (A-KID) →
AF
K_{AF}
← Application Session Establishment Response (following successful reception of K_{AF} from AAnF)

Figure 14. Key generation hierarchy in 5G, improved version of what was shown in Stuhlfauth (2020).

Concurrently, Subscriber Identifier De-concealing Function (SIDF) derives the Subscription Permanent Identifier (SUPI) from the Subscription Concealed Identifier (SUCI). In 5G, this all happens in the Home Network (HN) core, which was not the case on earlier core network platforms (3GPP, 2021).

In the 5G system, SUCI is a *privacy preserving identifier* containing the hidden SUPI. The UE generates a SUCI using a protection scheme with the public key of the HN that was securely provisioned to the USIM during the subscriber registration.

Only the Mobile Subscriber Identification Number (MSIN), part of the SUPI, gets concealed by the protection scheme, while the home network identifier MCC/MNC – the first three digits represent the Mobile Country Code (MCC) and the next two to three bits form the Mobile Network Code (MNC), identifying the network operator – gets transmitted in plaintext (3GPP, 2021).

The subscriber identification mechanism allows the identification of a UE on the radio path by means of the SUCI. This mechanism is usually invoked by the Serving Network (SN) by sending an Identifier (ID) Request to the UE, when the UE is not identifiable by means of a temporary identity. The UE then responds with the Identifier Response, containing the SUCI. Additionally, if the UE sends a Registration Request message of type "initial registration" to a mobile network for which it does not already have a 5G Globally Unique Temporary User Equipment Identity (5G-GUTI), then the UE includes a SUCI with the Registration Request.

On the side of the serving network, the key function is 5G Security Anchor Function (SEAF) that stores the anchor key ($\boldsymbol{K_{SEAF}}$) provided by the AUSF of the home network. Keys for more than one security context can then be derived from the $\boldsymbol{K_{SEAF}}$, without the need of a new authentication run, *regardless of the access network technology used by the UE*. In 5G, the home network always oversees the authentication, instead of the visiting/roaming network, as done in 4G or earlier system generations (3GPP, 2021).

Moreover, in 5G mobile systems, another authentication framework is the Authentication and Key Management for Applications (AKMA), where subscriber credentials can be used for authentication and key management of 3rd party applications and IoT traffic (ENISA, 2021).

As 5G networks evolve, it is expected that there will be increased reliance on AI enabled smart applications requiring situational, context-aware, and customized privacy solutions. Hence, the 5G privacy preserving approach may not be well suited for future wireless applications, due to a diverse and complex set of novel privacy challenges (6G Flagship, 2020c).

One potential solution is the use of *pairs of deep neural networks,* which can be trained with differential privacy, a formal privacy framework that limits the likelihood that queries of *personal identifiable information* (PII) – sensitive data that can include, e.g., the full name of a person, his or her social security number, driver's license, financial information, medical records, etc. – could identify a real data subject (Beaulieu-Jones *et al.*, 2019).

Also, *Distributed Ledger Technologies* (DTL), such as *blockchain*, may be an enabler for data integrity – beyond Hash Functions, used in 5G and other traditional communication systems

– and the use of trustless computing between stakeholders, as well as presenting a privacy protection ability across the network (WBGTIL, 2021). For example, blockchain offers privacy-protection data sharing mechanisms, can optimize access control, provide key characteristics, such as data integrity, traceability and monitoring, and ensure an efficient accountability mechanism, among other aspects, for Machine Type Communications in 6G (6G Flagship, 2020c).

The concepts related to *Federated Learning* (FL), as exemplified in Figure 6, are also active topics in the research community for ensuring privacy protection. FL is a distributed machine learning technique that allows model training for large amounts of data generated locally and the required modelling is done by each individual learner in the federation. Instead of sending a raw training dataset, each individual learner transmits their local model to an "aggregator" to build a global model. This method can provide solutions to vital challenges of data privacy, data ownership and data locality as it follows the approach of "bringing the code to the data, instead of the data to the code" (6G Flagship, 2020c).

Furthermore, 6G wireless is expected to be *privacy-aware*, supporting privacy-preserving techniques, such as, for instance, *differential privacy, disinformation and randomization* (Menting, 2021).

Protection of network interfaces

In 5G, the implementation of the radio access network may be split or disaggregated, where the RAN is separated into Distributed Units (DU) and Central Units (CU). The CU performs security functions (cryptography), it terminates the Access Stratum (AS) security protocols and is typically deployed in sites with restricted access to maintenance personnel. Together, DU and CU form the gNB (Soldani, 2021c), as shown in Figure 15.

In 5G, at the radio interface, the signalling and user plane traffic is encrypted using a 128-bits cypher key (256-bits after 3GPP Release 17) and information integrity is provided using a Hash Function. (The user plane integrity at the radio interface is only supported by the NR.) However, in 5G, only the Non-Access Stratum (NAS) protocol – end-to-end direct transfer signalling, i.e., control plane traffic between the UE and Access and Mobility Function (AMF) – is encrypted with integrity protection, using $\boldsymbol{K_{NASint}}$, $\boldsymbol{K_{NASenc}}$ (see Figure 14 and Figure 15).

Since the traffic transmitted through F1 and E1 interfaces (Figure 15) may carry sensitive data, the 3GPP security assurance specifications (3GPP, 2021) require compulsory confidentiality, integrity and replay protection for signalling messages at F1 (F1-C) and E1 interface (E1-C and E1-U), while making it optional for user plane traffic at F1 interface (F1-U). For both F1 and E1 interfaces, the support of IPSec ESP protocol (IETF RFC 4303) and IKEv2 certificate-based authentication (TS 33.310) is mandatory. The user plane traffic at F1 interface (F1-U) may be safeguarded differently, including setting integrity and/or encryption off/on (ENISA, 2021).

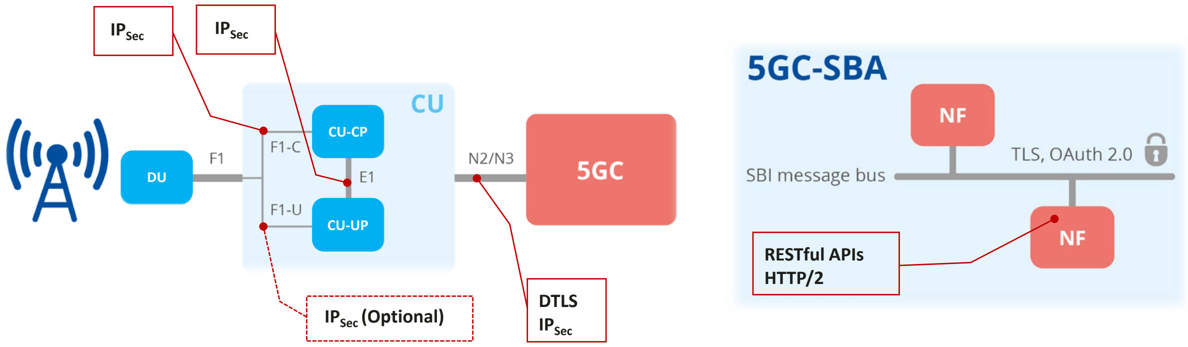


Figure 15. Protection of interfaces/virtual functions in 5G, improved version of what shown in ENISA (2021).

Interfaces N2 and N3 (also shown in Figure 15) are interfaces that connect 5G-RAN with AMF and User Plane Function (UPF), respectively. The support of IPsec ESP and IKEv2 certificate-based authentication is required for both interfaces. In addition, 3GPP (2021) demands the support of DTLS (RFC 6083) together with IPSec, which hides network topology. Particularly, the IPSec tunnel, between the gNB and 5GC, may be implemented using a Security Gateway (SEG) at both sides, to terminate the connection between the two elements (ENISA, 2021).

The 5GC Service Based Architecture (SBA) is based on virtual network functions (VNF) that support several micro-services, which can be exposed to other network entities. These VNFs offer their micro-services through Service Based Interfaces (SBIs), using HTTP/2 and RESTful APIs (3GPP, 2021).

From the security perspective, the network functions (NFs) must support client and server *certificates* and TLS, which needs to be implemented for transport protection, whilst NDS/IP may be integrated in the protocol stack for safeguarding the network layer (ENISA, 2021). Overall, the Network Repository Function (NRF) plays the role of an *authorization server* that provides access tokens to other network functions in communication, which need to exchange messages safely between them. Mutual authentication between these network functions is compulsory. For example, the mutual authentication of NF-NRF takes place during the discovery, registration and access token request procedures. (The authentication function depends on the supported protocol. If that is TLS, then the authentication provided by TLS would be used.) The authorization is based on the OAuth 2.0 framework (RFC 6749).

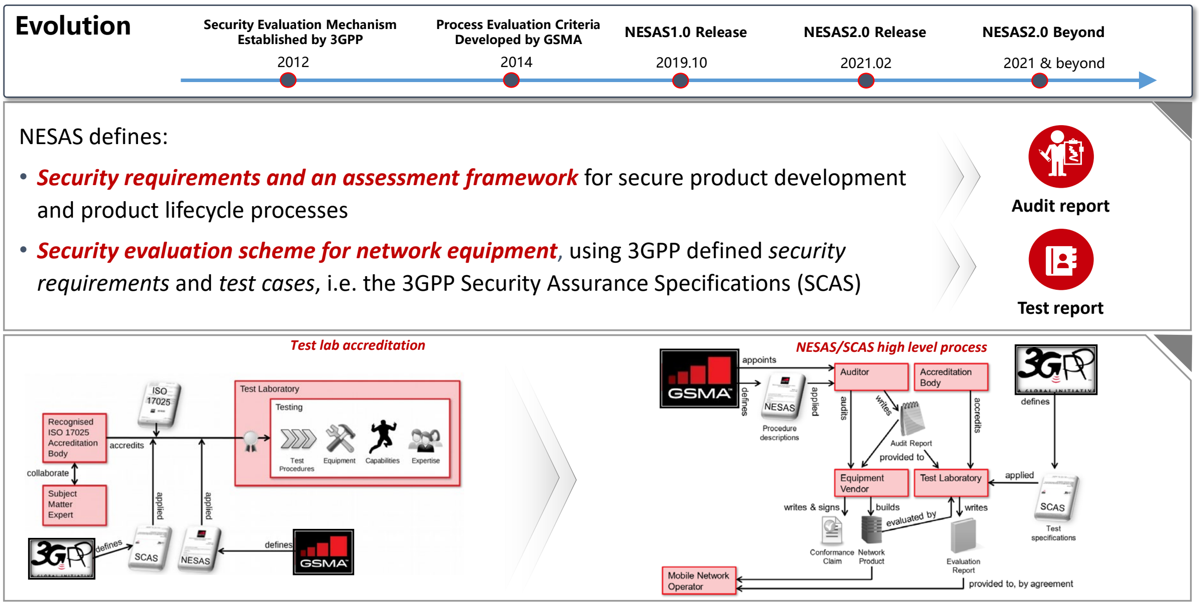
The *5G security architecture, features and protocols simply enhance the mechanisms that constitute the 4G security posture, and 6G is expected to go well beyond that* (Soldani, 2021f).

For example, as shown in Figure 12, 6G wireless is expected to support, but not be limited to, the following security controls and assurance mechanisms (Menting, 2021; Soldani, 2020):

- **Zero-Trust architecture (ZTA)**: not a single asset is trusted implicitly, and continuous access control, authentication and identification are used inside the network.
- **Distributed Ledger Technology (DLT)**: immutable, transparent, and autonomous ledgers using distributed consensus and cryptography to provide an authoritative record of secure transactions.
- **Post Quantum Cryptography (PQC)**: creating quantum-resistant ciphers that future quantum computers cannot crack.
- **Adversarial ML**: better evaluate ML algorithm's robustness and the development of defences against attacks.
- **Cyber-Resiliency**: continuous detection and appropriate response to adverse events, ability to withstand attacks, autonomously evolve, and adapt to threats.

Security assurance

The GSMA network element security assurance scheme (NESAS), jointly defined by 3GPP and GSMA, provides an industry-wide security assurance framework to facilitate improvements in security levels across the mobile industry (GSMA, 2020).


Evolution
Security Evaluation Mechanism Established by 3GPP
2012
Process Evaluation Criteria Developed by GSMA
2014
NESAS1.0 Release
2019.10
NESAS2.0 Release
2021.02
NESAS2.0 Beyond
2021 & beyond

NESAS defines:

- ***Security requirements and an assessment framework*** for secure product development and product lifecycle processes
- ***Security evaluation scheme for network equipment***, using 3GPP defined *security requirements* and *test cases*, i.e. the 3GPP Security Assurance Specifications (SCAS)

Figure 16. GSMA NESAS and 3GPP SCAS methodologies and milestones (Soldani, 2021d).

The NESAS defines security requirements based on 3GPP technical specifications and an assessment framework for secure product development and product lifecycle processes; and a security evaluation scheme for network equipment using the 3GPP-defined security specifications and test cases, i.e., 3GPP security assurance specifications (SCAS).

- **NESAS Development and Lifecycle Assessment Methodology** — defines audit and assessment process for vendor development and product lifecycle process under the GSMA NESAS.

- **NESAS Development and Lifecycle Security Requirements** — defines security requirements for vendor development and product lifecycle process under the GSMA NESAS.

The NESAS is focused on the vendor aspects of the supply chain, and thus provides a security assurance framework to improve security levels across all mobile industry, because it has been developed and will progress, as the ICT will evolve, following well established practices and schemes that provide trustworthy security assurance (Soldani, 2021d).

Industry players, governments, security agencies and regulators are recommended to adopt the GSMA NESAS for testing and evaluating telecoms equipment of current and future generations. The NESAS is a customized, authoritative, unified, efficient and constantly evolving security assurance scheme for the mobile industry and could be a part of *certification & accreditation processes* against a fixed set of security standards and policies for current 5G and future 6G network security authorization in any country (Soldani, 2021d).

Ultimately, to realise the above vision of 6G information and network security will require collaboration among all key stakeholders. All parties in the industry chain need to take their own security responsibilities, to mitigate the related cyber security risks (Soldani, 2021d):

- **Suppliers** must prioritize cyber security sufficiently (e.g., respect laws, regulations, standards, certify their products, and ensure quality in their supply chains).
- **Telco operators** are responsible for assessing risks and taking appropriate measures to ensure compliance, security and resilience of their networks.
- **Service providers and customers** are responsible for the implementation, deployment, support and activation of all appropriate security mechanisms of service applications and information (data).
- **Regulators** are responsible for guaranteeing that telco providers take appropriate measures to safeguard the general security and resilience of their networks and services.
- **Governments** have the responsibility of taking the necessary measures to ensure the protection of the national security interests and the enforcement of conformance programs and independent product testing and certification.
- **Standardization development organizations** must ensure that there are proper specifications and standards for security assurance and best practices in place, such as the GSMA NESAS.

Prosumer centric systems

The last, but not the least, critical shift in paradigm is that we are moving *from an operator centric system*, which is essentially a generic pipe of bits, *to something truly centred on the end user*.

The end user is expected to become a true *prosumer*, meaning that subscribers will be able not only to consume content and information, but also create content and substance and share that, making it available to communities of people and cyber entities, connecting to and exploiting 6G services (Soldani, 2021b).

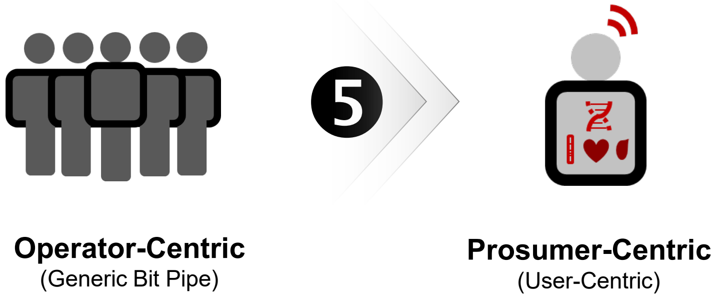


Figure 17. From generic bit-pipe networks to prosumer-centric systems (Soldani, 2021b).

Conclusions

The next generation of information and communication systems, denoted as 6G wireless, will enable the shift *from the Internet of Things to the Internet of Intelligence*, the latter defined as functions with the capability of representing knowledge and an ability to process knowledge and take decisions: *6G wireless will be the nervous system of the global digital economy*.

6G wireless is expected to be *secure by design*; connect intelligence, being AI native and prosumer centric; support a variety of new usage scenarios; and, consequently, cater for more stringent technology requirements than earlier mobile communication systems; by enhancing the performance of 5G wireless by a factor of tenfold or more, in terms of, but not be limited to, the following metrics: supported spectrum and bandwidth; coverage; reliability; latency; density of endpoints; synchronization of multiple flows to and from multiple *collaborative* devices; location and position tracking; and energy and resources consumption; amid other performance indicators. Also, new security control measures, security assurance schemes and privacy preservation approaches will form a core part of the 6G wireless posture.

Many 6G development initiatives are ongoing globally and the investments in R&I provide a fascinating prospect for our future. In Australia, EU, the UK, China, the US, South Korea and Japan, public and private sectors have already started investing US$ billions in R&I actions to tackle the technology requirements that 6G will demand, when it matures around 2030.

To realise the compelling vision of 6G wireless presented in this work requires *close cooperation and collaboration within all stakeholders and regions, globally*, even more than usual; as well as the *integration of satellite associations, alliances of vertical sectors, with the standardization development organizations*, such as the 3GPP, responsible for the technical specification of 6G wireless.

It also requires an ecosystem of public and private players and a multi-disciplinary approach to ensure that: a) all assets that form part of 6G systems are *interoperable* and *compliant* with *standardised security evaluation criteria*, such as the GSMA/3GPP NESAS (GSMA, 2020), for security authorisation in the country, where the system is deployed; and b) even the smallest and most insignificant asset within the end-to-end supply chain must support a *minimal set of approved security, safety and privacy requirements*.

References

3GPP. (2020a). 3GPP Release 16 Description. Retrieved from https://www.3gpp.org/release-16

3GPP. (2020b). 3GPP Release 17 Description. Retrieved from https://www.3gpp.org/release-17

3GPP. (2021). Security architecture and procedures for 5G System, TS 33.501, April 2021. Retrieved from https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169

5G Americas. (2020). Security Considerations for the 5G Era. Retrieved from https://www.5gamericas.org/wp-content/uploads/2020/07/Security-Considerations-for-the-5G-Era-2020-WP-Lossless.pdf

5G Americas. (2021a). The 5G Evolution: 3GPP Releases 16 and 17. Retrieved from https://www.5gamericas.org/wp-content/uploads/2021/01/InDesign-3GPP-Rel-16-17-2021.pdf

5G Americas. (2021b). Mobile Communications Beyond 2020 – The Evolution of 5G Towards Next G. Retrieved from https://www.5gamericas.org/wp-content/uploads/2020/12/Future-Networks-2020-InDesign-PDF.pdf

5GPPP Technology Board. (2021). AI and ML – Enablers for Beyond 5G Networks. Retrieved from https://5g-ppp.eu/wp-content/uploads/2021/05/AI-MLforNetworks-v1-0.pdf

6G Flagship. (2020a). 6G white paper on localization and sensing. 6G Research Vision, No. 12. Retrieved from http://jultika.oulu.fi/files/isbn9789526226743.pdf

6G Flagship. (2020b). White paper on 6G networking. 6G Research Visions, No. 6. Retrieved from http://jultika.oulu.fi/files/isbn9789526226842.pdf

6G Flagship. (2020c). 6G White Paper: Research Challenges for Trust, Security and Privacy. 6G Research Visions, No. 9. Retrieved from http://jultika.oulu.fi/files/isbn9789526226804.pdf

6G Flagship. (2021a). Discover how 6G will change our lives. *6G White Papers*. Retrieved from https://www.oulu.fi/6gflagship/6g-white-papers

6G Flagship. (2021b). White paper on RF enabling 6G – Opportunities and challenges from technology to spectrum. *6G Research Visions, No. 13*. Retrieved from http://jultika.oulu.fi/files/isbn9789526228419.pdf

6G Innovation Centre. (2021). 6G wireless: a new strategic vision. 5GIC Strategy Advisory Board. Retrieved from https://www.surrey.ac.uk/sites/default/files/2020-11/6g-wireless-a-new-strategic-vision-paper.pdf

6G Symposium. (2021). What 6G is and isn't: vision, key performance indicators, services and requirements. Retrieved from https://youtu.be/fFVoHMdaqrY

ATIS. (2021). Next Generation Alliance. ATIS initiative. Retrieved from https://nextgalliance.org/

Australian Government. (2021). Australia's Digital Economy Strategy. Retrieved from https://digitaleconomy.pmc.gov.au/

Beaulieu-Jones, B. K., Wu, Z. S., Williams, K., Lee, R., Bhavnani, S. P., Byrd, J. B., Casey, S., Greene, C. S. (2019). Privacy-Preserving Generative Deep Neural Networks Support Clinical Data Sharing. Open Access. Retrieved from https://www.ahajournals.org/doi/10.1161/CIRCOUTCOMES.118.005122

Calvanese Strinati, E. & Barbarossa, S. (2021). 6G networks: Beyond Shannon towards semantic and goal-oriented communications. *Computer Networks*, *190*. https://doi.org/10.1016/j.comnet.2021.107930

Castro, C. (2021). 6G Gains momentum with initiatives launched across the world. *6G World Exclusive*. Retrieved from https://www.6gworld.com/exclusives/6g-gains-momentum-with-initiatives-launched-across-the-world/

ENISA. (2020). 5G Supplement — To the Guideline on Security Measures under the EECC. Retrieved from https://www.enisa.europa.eu/publications/5g-supplement-security-measures-under-eecc

ENISA. (2021). Security in 5G Specifications — Controls in 3GPP Security Specifications (5G SA). Retrieved from https://www.enisa.europa.eu/news/enisa-news/cybersecurity-for-5g-enisa-releases-report-on-security-controls-in-3gpp

Ericsson. (2020). 5G evolution: 3GPP releases 16 & 17 overview. Retrieved from https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/5g-nr-evolution

GSA. (2021). 5G Market Snapshot: April 2021 — Member Report. Retrieved from https://gsacom.com/paper/5g-market-snapshot-april-2021-member-report/#:~:text=By%20mid%2DApril%202021%20435,could%20be%20used%20for%205G)

GSMA. (2020). Network Equipment Security Assurance Scheme (NESAS) – Enhancing trust in global mobile networks. Retrieved from https://www.gsma.com/security/network-equipment-security-assurance-scheme/

GSMA. (2021a). Global 5G Landscape (Q4 2020). Retrieved from https://assets.foleon.com/eu-west-2/uploads-7e3kk3/4816/global_5g_report.628d99ec2a01.pdf

GSMA. (2021b). Quantum Computing, Networking and Security. IG.11. Version 1.0. Retrieved from https://www.gsma.com/newsroom/wp-content/uploads//IG-11-Quantum-Computing-Networking-and-Security.pdf

Lin, X., Rommer, S., Euler, S., Yavuz, E. A, & Karlsson, R. S. (2021). 5G from Space: An Overview of 3GPP Non-Terrestrial Networks. *Eprint arXiv:2103.09156*. Retrieved from https://arxiv.org/ftp/arxiv/papers/2103/2103.09156.pdf

Menting, M. (2021). Conceptualizing Security in a 6G World. ABI Research. 6G World White Paper. Retrieved from https://www.6gworld.com/conceptualizing-security-in-a-6g-world-3/

Hirose, Y. (2021). Japan teams up with Finland on 6G development. Nikkei ASIA. Retrieved from https://asia.nikkei.com/Business/Telecommunication/Japan-teams-up-with-Finland-on-6G-development

Nokia. (2020). 5G Releases 16 and 17 in 3GPP – Nokia White Paper. Retrieved from https://gsacom.com/paper/5g-releases-16-and-17-in-3gpp-nokia-white-paper/

Rinaldi, F., Määttänen, H. L., Torsner, J., Pizzi, S., Andreev, S., Iera, A., Koucheryavy, Y., & Araniti, G. (2020). Non-Terrestrial Networks in 5G & Beyond: A Survey. *IEEE Access*, *8*, 165178–165200. https://doi.org/10.1109/ACCESS.2020.3022981

Soldani, D. (2020). On Australia's Cyber and Critical Technology International Engagement Strategy Towards 6G – How Australia may become a leader in Cyberspace. *Journal of Telecommunications and the Digital Economy*, *8*(4), 127–158. https://doi.org/10.18080/jtde.v8n4.340

Soldani, D. (2021a). 5G evolution, 6G vision, security controls and assurance. Webinar at AISA 2021. Retrieved from https://youtu.be/S9215UdnJs4

Soldani, D. (2021b). 5G, 5.5G and 6G Fundamentals. Webinar at the University of Sydney Business School. Retrieved from https://youtu.be/2jfgIScLDgw

Soldani, D. (2021c). Radio Access Network Evolution. IEEE Public Lecture. Retrieved from https://youtu.be/2yKXSZAINmI

Soldani, D. (2021d). 5G Security. *Cyber Defense eMagazine*, February 2021. Retrieved from https://cyberdefensemagazine.tradepub.com/free/w_cyba111/prgm.cgi

Soldani, D. (2021e). 6G Fundamentals: Vision & Enabling Technologies. *6GWorld Research Paper Ref: 6GW02*, 6G World, June. Retrieved from https://www.6gworld.com/latest-research/6g-fundamentals-vision-and-enabling-technologies/

Soldani, D. (2021f). From Security-Enhanced 5G Networks to Security-by-Design 6G Systems: Towards Trustworthy and Resilient Information and Communication Systems. *Cyber Defense eMagazine – August 2021 Edition*. Retrieved from https://www.yumpu.com/en/document/read/65794079/cyber-defense-emagazine-august-edition-for-2021

Soldani, D., & Illingworth, S. A. (2020). 5G AI-Enabled Automation. *Wiley 5G Ref: The Essential 5G reference Online*, Wiley & Sons, May. https://doi.org/10.1002/9781119471509.w5GRef225

Soldani, D., & Manzalini, A. (2015). Horizon 2020 and Beyond: On the 5G Operating System for a True Digital Society. *IEEE Vehicular Technology Magazine*, *10*(1), 32–42. https://doi.org/10.1109/MVT.2014.2380581

Soldani, D., & Innocenti, M. (2019). 5G Communication Systems and Connected Healthcare. *Chapter 7, Wiley Online Library*. Wiley & Sons. Retrieved from https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119515579.ch7

Soldani, D., Shore, M., Mitchell, J., & Gregory, M. (2018). The 4G to 5G Network Architecture Evolution in Australia. *Journal of Telecommunications and the Digital Economy*, *6*(4). https://doi.org/10.18080/jtde.v6n4.161

Stuhlfauth, R. (2020). 5G Security Aspects. Rohde & Swartz webinar, May 2020. Retrieved from https://www.rohde-schwarz.com/us/knowledge-center/videos/5g-security-aspects-video-detailpage_251220-638752.html

Tesla Universe. (n.d.). Nikola Tesla Quote #38. Retrieved from https://teslauniverse.com/nikola-tesla/quotes/38

Tong, W., & Zhu, P. (Eds). (2021). *6G: The Next Horizon From Connected People and Things to Connected Intelligence*. Cambridge: Cambridge University Press. https://doi.org/10.1017/9781108989817

Tonkin, C. (2020). China launched a 6G satellite – so what? The next 'next generation' might be just around the corner. ACS Information Age. Retrieved from https://ia.acs.org.au/article/2020/china-launched-a-6g-satellite---so-what-.html

World Bank Group Technology Innovation Lab. (2021). Blockchain Interoperability. White Paper. Retrieved from https://documents.worldbank.org/en/publication/documents-reports/documentdetail/373781615365676101/blockchain-interoperability

Yaacoub, E., & Alouini, M. S. (2020). A Key 6G Challenge and Opportunity—Connecting the Base of the Pyramid: A Survey on Rural Connectivity. *Proceedings of the IEEE*, *108*(4), 533–582. https://doi.org/10.1109/JPROC.2020.2976703