



6G Fundamentals: Vision & Enabling Technologies

Towards Trustworthy Solutions & Resilient Systems

Author: [David Soldani](#)



Published by 6GWorld, 15 June 2021

Link: <https://www.6gworld.com/latest-research/6g-fundamentals-vision-and-enabling-technologies/>

Reference number: 6GW02

6G Gains Momentum

While the next generation of mobile connectivity still lies roughly a decade ahead, the number of 6G initiatives ongoing globally, and corresponding investments provide an intriguing prospect for the future. Public and private sectors have already started investing in research and innovation (R&I) actions to tackle requirements that 6G will probably demand when it reaches commercial reality around 2030 ([Castro, 2021](#), [5G Americas, 2021b](#)).

These include use cases promised in 5G networks but not yet realised, and more advanced scenarios that are emerging in the context of next generation/6G networks such as Terahertz frequencies, holoportation, tactile/haptic communications, ubiquitous services (land, air, space, sea), medical/health services, government/national security, imaging and sensing, first responder/emergency services, cyber-physical systems/manufacturing, and transportation services. Some examples of relevant use cases and corresponding technology requirements are shown in Figure 1 ([5G Americas, 2021b](#)). For more information and other usage scenarios towards 6G, the reader may refer to, e.g., ([6G Flagship, 2021a](#), [6GIC Vision, 2021](#)).

Specific international efforts by leading nations in the wireless cellular industry and relevant Beyond 5G (B5G) and 6G initiatives and related investments are illustrated in Figure 2.

In **Europe**, within the EU Horizon 2020 R&I framework programme, three recent joint projects focused on 6G development have been announced: Hexa-X, RISE-6G, and NEW-6G. The European Commission (EC), within the Smart Network and Service framework programme, 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 a budget to carry out their own research. Australia, China, Finland, Japan, South Korea, UK and the USA are in the mix, and there is pressure on other nations to join the club.

In 2021, in **Australia**, the Federal Government published the Digital Economy Strategy for a modern and digital economy to drive Australia's future prosperity, towards a leading digital economy and society by 2030. The 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 (99.999999%) availability
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 1. Examples of use cases and corresponding technology requirements (5G Americas, 2021b).

A 'Secure-G' Connectivity Test Lab, co-designed with industry, will enable businesses to test measures, protocols, standards, and software that underpin transparent and secure 5G connectivity. Through the 6G security and development program, the Australian Government will undertake foundational research into the security requirements of 6G and future connectivity technologies. This will ensure Australia stays ahead of the curve by ensuring technologies are developed with security in mind from the ground up and help to shape international future connectivity standards in a way that aligns with the government's values and expectations around security (Australian Government, 2021).

In **North America**, Next G activities are primarily centred upon academia with additional efforts from agencies of the US government and Standards Developing Organizations (SDOs) (5G Americas, 2021b). In October 2020, the industry Alliance for Telecommunications Industry Solutions (ATIS) launched the Next G Alliance (NGA), an initiative aiming to lay 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 founding 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).








Country	B5G/6G Initiative
	<ul style="list-style-type: none"> - 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
	<ul style="list-style-type: none"> - "Secure 5G & Beyond Act" March 2020 - DoD Testbed programme, US\$ 600 million - Next-G initiative, industry federation
	<ul style="list-style-type: none"> - MIC "Roadmap towards 6G", June 2020 - METI Support - US\$ 380 million
	<ul style="list-style-type: none"> - MSIT 6G programme, September 2020 - US\$ 200 million public support
	<ul style="list-style-type: none"> - MIIT 6G programme, creation of IMT 2030 Promotion committee (2019) - Multi € billion until 2035, including industrialization
	<ul style="list-style-type: none"> - 6G Flagship launched in February 2019 - € 250 million / 7 years
	<ul style="list-style-type: none"> - 6G Smart Networks and Services Joint Undertaking proposal - € 900 million / 7 years

Figure 2. Examples of Beyond 5G (B5G) and 6G initiatives ongoing globally (Castro, 2021).

On April 18th 2018, the Academy of **Finland** selected the University of Oulu to lead a new national research program on 6G. The 6G Flagship initiative consists of five collaboration partners, including Aalto University, Business Oulu, Nokia, Oulu University of Applied Sciences, and VTT Technical Research Centre of Finland Ltd. Two additional company co-creators include Keysight Technologies and InterDigital. In June 2019 ETRI (Korea) signed an MOU with the University of Oulu, as did Japan's Beyond 5G Promotion Consortium in June 2021. The total budget for the 2020-30 Flagship program is €250+ million ([5G Americas, 2021b](#)).

On November 20th 2019, **Japan** announced a stimulus pack of \$2 billion to support industry research on 6G technologies with a timeline of 2020-2030. On January 22 2020, the Japanese government announced plans to develop a comprehensive 6G strategy. A 6G panel was created to discuss and analyse technology developments and use cases. The panel included private sector representatives and university researchers. On April 2020, 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 two percent at present ([5G Americas, 2021b](#)). As noted above, during 2021 Japan also created a connection with Finland's 6G Flagship.

In August 2020, **South Korea's** Ministry of Science & ICT (MSIT) announced US\$170 million of public support in investments for 6G research and development for the five years from 2021 to 2026. According to the Korean strategy, during that first phase the MSIT will concentrate on building high-risk 6G core technology, "not covered by private investment," in global cooperation. Their goals are to: reach 1 Tbps data rate; achieve 0.1 ms wireless latency (below 5ms wired latency); expand the connectivity range to 10 km from the ground; apply artificial intelligence to the entire network; and embed security by design from the ground up. The government plans to roll out additional pilot projects that include some of the use cases expected for 6G, like smart factories, smart cities, and autonomous vehicles. Nevertheless, the program also seeks to go beyond these use cases and create technologies such as 6G satellites ([Castro, 2021](#)).

On November 7th 2019, **China** officially launched research and development for its 6G mobile networks. The Ministry of Science and Technology set up two working groups. The first group consists of government agencies responsible for promoting 6G research and development. The second group, known as the "China 6G Wireless Technology Task Force" consists of vendors, operators, Chinese Research Agencies and Chinese universities. Their purpose is to form a panel tasked with laying out the development of 6G and proving its scientific feasibility. The Chinese Government has committed more than \$30 billion towards 5G R&D over five years, and 6G may receive similar investments ([5G Americas, 2021b](#)).

6G Network Architecture Vision

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 ranges from 1000 to 5000 times higher in machines than in humans. Hence, *the intelligence must be centralised*, which also reduces the cost of the device of any form factor ([GSA, 2021](#)). As illustrated in Figure 3, 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 5-10ms for dependable *remote control* of a

connected device, or exchange *haptic feedback*, with no cyber sickness, between two peer entities ([Soldani & Innocenti, 2019](#)). Hence, *all intelligent functions must be placed at the network edge*, i.e., close to the device or end user.

3. Machine Learning, in the sense of pattern recognition algorithms, have many flaws, limitations, and bias. Hence, *machine learning (ML) must meet machine reasoning (MR)*. A possible reference architecture to achieve this goal is shown in Figure 4.
4. It is an imperative to improve efficiency and productivity for Green House Gas (GHG) reduction. Hence, digitisation 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*, which is only feasible if we make technology safe, secure, dependable, accountable, and protecting 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; merging digital, virtual, and physical worlds; new business opportunities; and the *wireless* technology evolution towards 6G were discussed ([6G Symposium, 2021](#)).

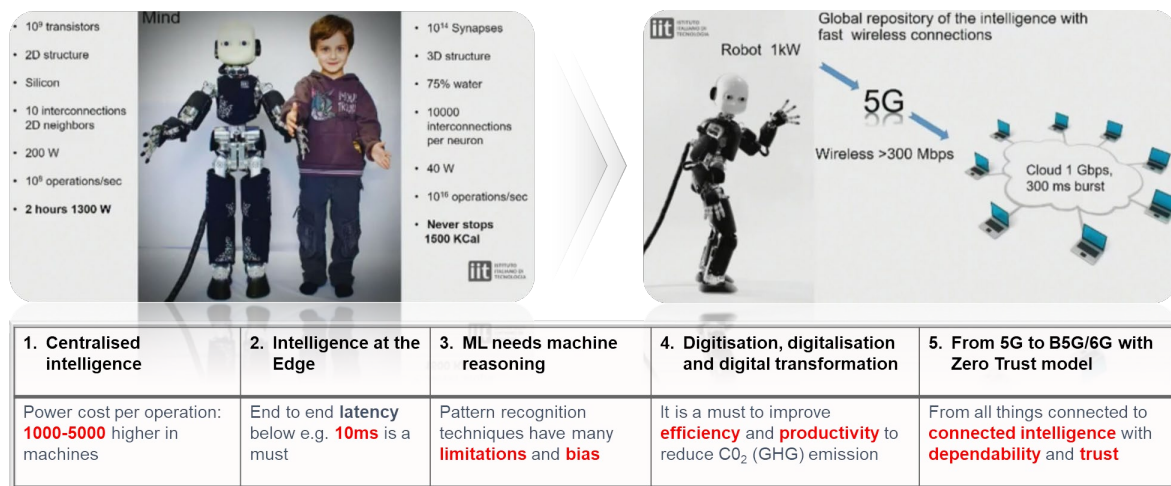


Figure 3. Examples of societal challenges and necessary corrective actions ([Soldani, 2021b](#)).

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](#)).

This is precisely what was already envisioned in ([Soldani & Manzalini, 2015](#)), where the authors presented the blueprint of an AI-native operating system for the first time and, particularly, the services on top expected in the 2020 to 2030 time frame. Figure 5 is exactly inspired by the architecture that the authors published at that time, looking at 5G and beyond, with the possibility of integrating the 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. These centralised computing platforms would be 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 characterise the 6G system ([5GPPP Technology Board, 2021](#)).

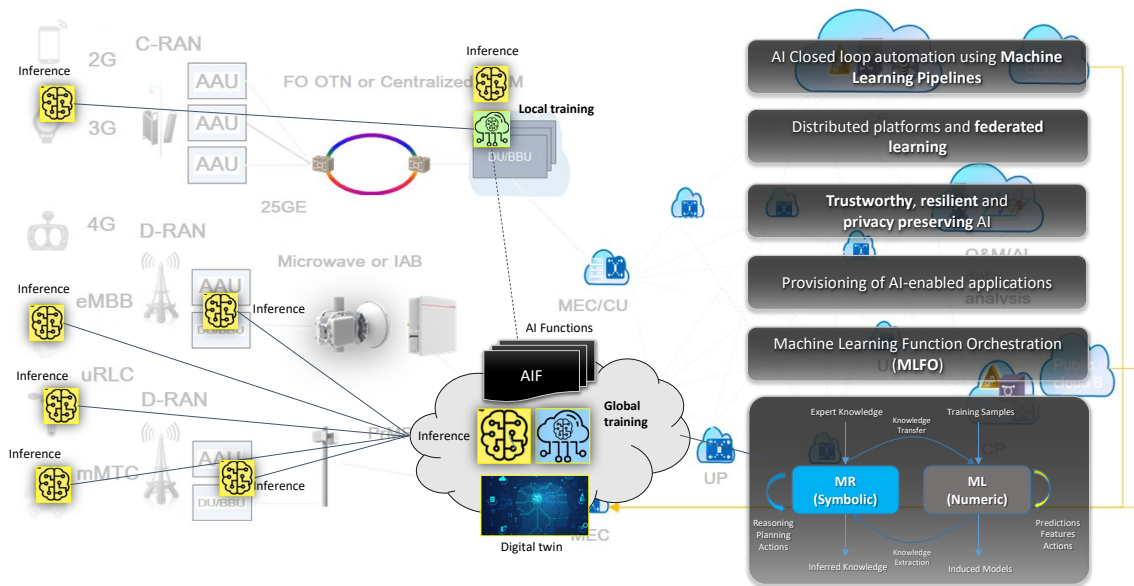


Figure 4. Examples of how Machine Learning (ML) may meet Machine Reasoning (MR) (Soldani, 2021b).

The 6G wireless architecture will be shaped by five key constituents (Tong & Zhu, 2021), as illustrated in Figure 5: *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 the 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 any sort of sensor, is expected to lead to significant advances in 6G wireless technology. Higher frequency bands allow very fine resolutions in all physical dimensions: Range, angle, and Doppler shift (6GIC Vision, 2021).

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 for external customers (AlaaS). Examples of such services could include AI-enabled high precision localisation and end user mobility trends, etc. Quantum (Q) key distribution technology can be deployed for the fibre-optic link between the Neural Centre and the Neural Edge. The IaaS, PaaS and AlaaS, borrowed from cloud services, could very well coexist as they 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, from offline AI to real-time AI (Soldani & Manzalini, 2015; Tong & Zhu, 2021).

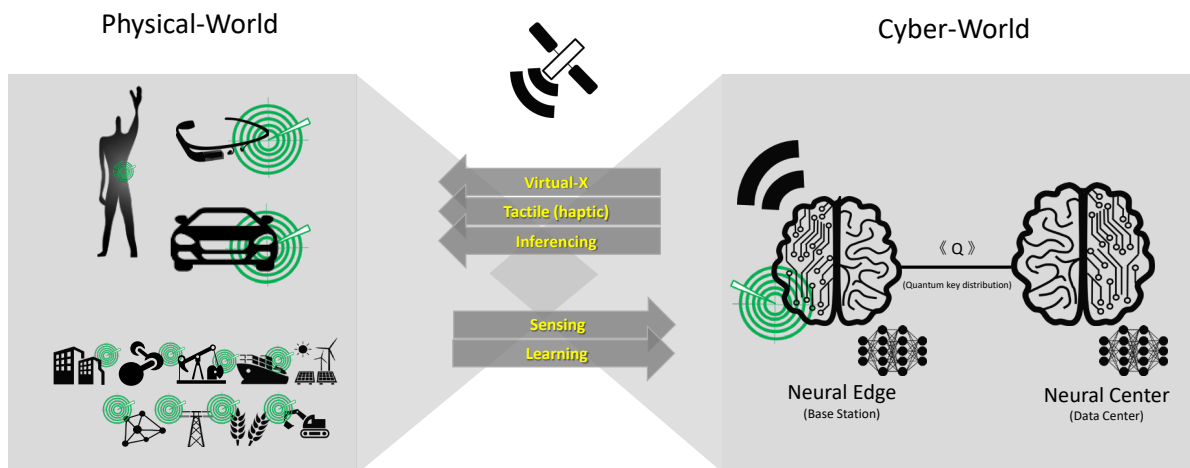


Figure 5. 6G Wireless network architecture vision (Tong & Zhu, 2021).

Non-Terrestrial Networks (NTN) are an integral part of the 6G wireless system, and a massive LEO satellite constellation will integrate traditional and non-traditional networks aiming at ultimately full earth coverage, combining different fronthaul, backhaul, and midhaul approaches. For example, 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 6, which is an improved version of what authors presented in (Yaacoub, 2020).

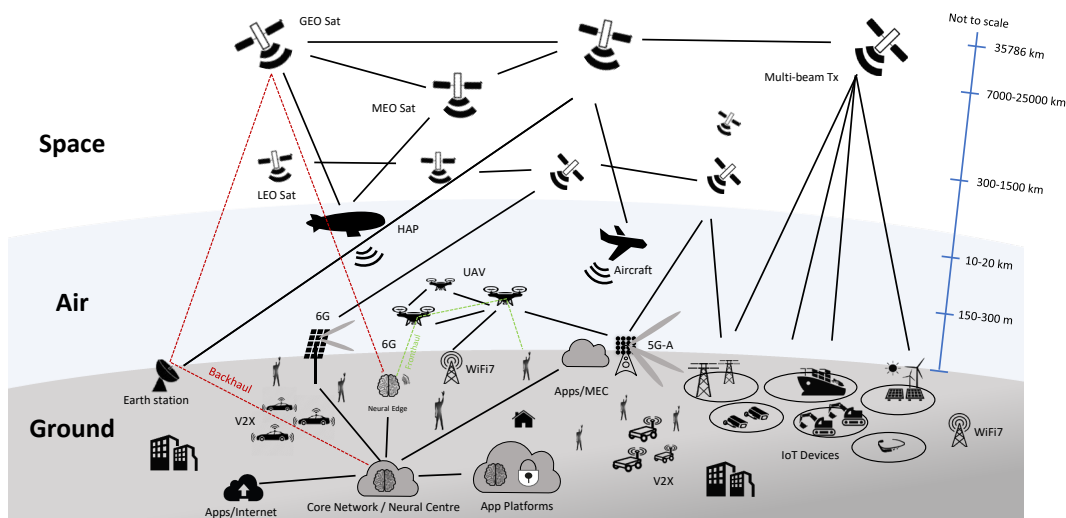


Figure 6. Examples of fronthaul (in red) and backhaul (in green) approaches towards ubiquitous connectivity.

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 and satisfy the related technology requirements collected in Figure 1. This paper anticipates five essential technology enablers that will be necessary to fulfill the needs of the next generation system and 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 7.

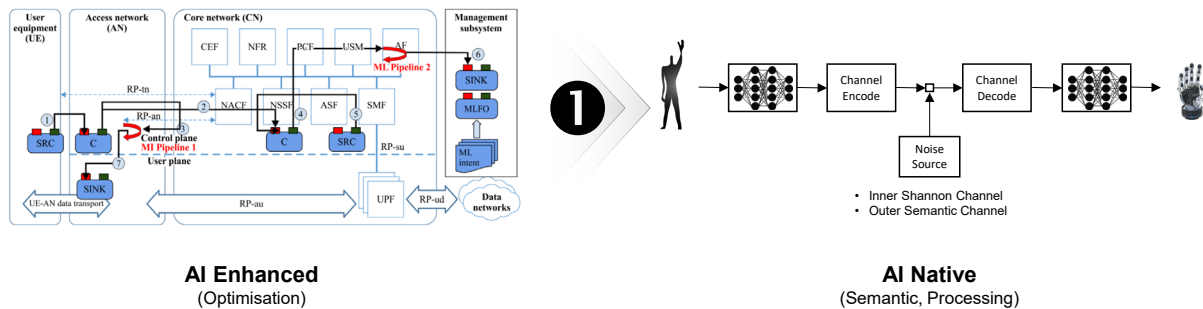


Figure 7. From AI enhanced networks to AI native communication systems (Soldani, 2021b).

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 an *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.
- A **collector** (C) is a node responsible for *collecting data* from the src.
- A **pre-processor** (PP), is a node responsible for *cleaning data, aggregating data or performing any other pre-processing* needed for the ML model to consume them.
- A **model** (M) is an *ML model*, e.g. a prediction function.
- A **policy** (P) is a node that provides a *control* for an operator to put a *mechanism* to minimise impacts into place on a live network, so that operation is not impacted.
- A **distributor** (D) is a node responsible for identifying the sinks and *distributing the ML output to the corresponding sinks*.
- A **sink** (S) is the *target node* of the ML output, on which it takes action (*inference*).

Chaining is the process of connecting ML functions or nodes together to form the 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. It also 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 categorisation, 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".

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*, 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 exploitable and explainable meanings to be derived from an unlimited amount of sanitised information (i.e., data) ([Calvanese & Barbarossa, 2021](#)).

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](#)).

Combined Sensing and Communication

The second paradigm shift is about going *from an information-centric approach of bits and bytes to uplink and downlink sensing*, with sensing capabilities imbued in the devices and in access points (radio heads), denoted as *Neural Edges* in Figure 5 and Figure 6), operating at very high frequencies in millimetre waves (mmW) and Terahertz (THz) spectrum, and using very large contiguous and/or detached bandwidths (of several GHz).

The definition of the THz band seems to vary in the literature, although the ITU definition of the tremendously high frequency (THF) region holds that the scientific definition of the *THz band* is from 0.3 THz to 3 THz.

In ([6G Flagship, 2021b](#)), authors call the higher end of the extremely high frequency (EHF) band the *upper mmW band* or *region*. This band covers frequencies of 100–300 GHz, and it will most likely be the most interesting band in the coming years for the research of new radio communication systems. The region provides a much larger portion of spectrum than the *lower mmW region* (30–100 GHz). As already discussed, the latter has already been adopted extensively by many standards, including 3GPP 5G NR, IEEE 802.11, and other wireless technologies which, at these frequencies, are unable to support terabit per second (Tbps) radio links.

The capability of 6G wireless link transmission is expected to be improved by at least 10–100 times that of 5G to achieve a Tbps target and to support the throughput demands of data-rate-intensive applications, such as the ones reported in Figure 1. In addition to improving the *spectral efficiency*, 6G wireless is anticipated to widen the supported frequency bandwidths and operate at a variety of carrier frequencies by exploiting the above spectrum and transmitting 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 frequencies 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 $10\ \mu\text{m}$, 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 the most important application of 6G. Integrating sensing functions with the base stations (BSs) of already-installed networks is an effective technical way of building a 6G sensing network (see Figure 6). The 6G wireless sensing capabilities can be applied to any critical infrastructure, such as transport, utilities, ports, datacentres etc., by using the infrastructure deployed close to critical points to sense the status and dynamics of traffic, fluids, gas, etc. and then share this data to realise an intelligent system with little or no human intervention.

From the terminal device’s perspective, the sensing skill could be obtained using methods that make use of various sensors such as touch panels, camera, infrared, or gyroscopes already embedded in devices, which allow them to sense the situation and context of the surrounding environment. The results are then made available on the network via a wireless connection ([6G Flagship, 2021b](#)).

Sensing is the basic means of intelligence and an important part of future 6G networks and devices. We will have full capability to sense the environment and context, like radar or lidar systems today, and therefore extract a lot of information in addition to the classical channel quality indicators and radio resource measurements. By integrating this information with other sources of data, images, or anything that can be captured by other devices we can, thus, make it possible to offer Sensing as a Service ([Soldani, 2021b](#)).

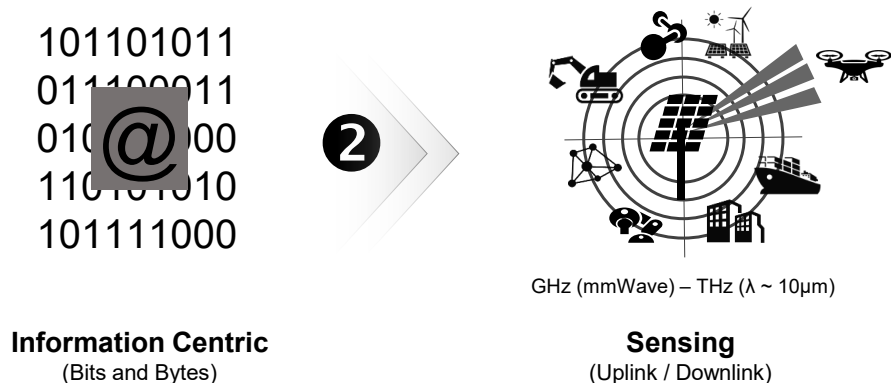


Figure 8. From information centric to integrated sensing and communication ([Soldani, 2021b](#)).

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, such as outer space and across entire oceans. Such communication services will create a seamless integrated connectivity framework consisting of *terrestrial* (land-based and marine), *airborne* (pseudo satellites, aircraft, balloons, drones, etc.) and *space based* (LEO/MEO/GEO satellite constellations) infrastructures (see Figure 6).

A Geostationary Earth Orbiting (GEO) satellite has a circular and equatorial orbit around Earth at 35,786 km altitude and the orbital period is equal to the Earth rotation period. The GEO appears fixed in the sky to the ground observers. GEO beam footprint size ranges from 200 to 3,500 km. A Medium Earth Orbiting (MEO) satellite has a circular orbit around Earth at an altitude varying from 7,000 to 25,000 km. MEO beam footprint size ranges from 100 to 1,000 km. A Low Earth Orbiting (LEO) satellite has a circular orbit around Earth at an

altitude between 300 to 1500 km, with a beam footprint size that ranges from 100 to 1,000 km. LEO and MEO are also known as Non-GEO (NGSO) satellites for their motion around Earth with a lower period than the Earth rotation time; in fact, it varies from 1.5 to 10 hours (Rinaldi et al., 2020; Lin et al., 2021).

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. The airborne category encompasses UAS platforms (Unmanned Aerial Systems, essentially drones), which are typically placed at an altitude between 8 and 50km and include High Altitude Platform Systems (HAPS) at 20km altitude or more. Like the GEO satellite, the UAS position can be kept fixed in the sky relative to a given point on the ground. UAS beam footprint size ranges from 5 to 200 km.

In 5G, an NTN terminal refers to either the 3GPP user equipment 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 radio frequency of S-band (i.e., 2 GHz) (3GPP, 2020b; Soldani, 2021a; Soldani, 2021c).

NTN systems will be an integral part of the *access* network to 6G services and *backhaul* of next generation information and communication systems, able to satisfy the demands of anywhere and anytime service availability, continuity, and scalability over wide areas. The uniqueness of NTN is in their capability to offer wide area coverage by providing connectivity over regions (e.g., rural areas, vessels, airplanes) 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*, down to 1-3ms, between two or more devices in communication. This is because the length of 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 9, for example, from London to Shanghai the orthodromic distance is ~10,000km and that would reduce to about 1,500 km, if the two entities were connected via LEO satellites (Tong & Zhu, 2021).

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.

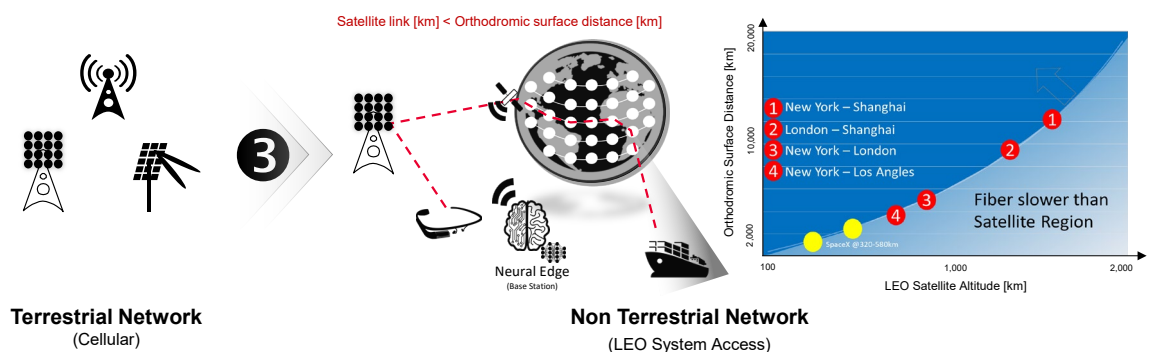


Figure 9. From cellular networks to integrated terrestrial and non-terrestrial infrastructures (Soldani, 2021b).

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 it is the case for 5G today compared 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 standards 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 to potential vulnerabilities in the design, development, and implementation of 6G wireless communications was discussed in ([Menting, 2021](#)), along with possible security control 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 10 (see also [ENISA, 2020](#)).

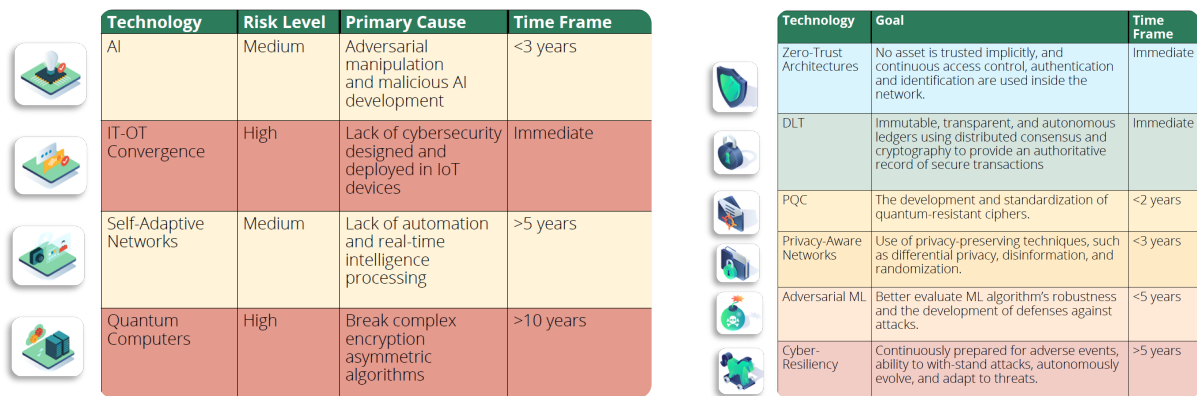


Figure 10. Potential threats and novel events, and corresponding security measures ([Menting, 2021](#)).

In short, 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 instill the whole network end-to-end with a defence-in-depth strategy, augmented by a Zero-Trust model ([Soldani, 2020](#)), with ability to cope with different situations and unexpected events in extreme conditions. Also, the standardisation process for 6G must provide new mechanisms for security control, security assurance and privacy preservation ([Soldani, 2021d](#)), as shown in Figure 11.

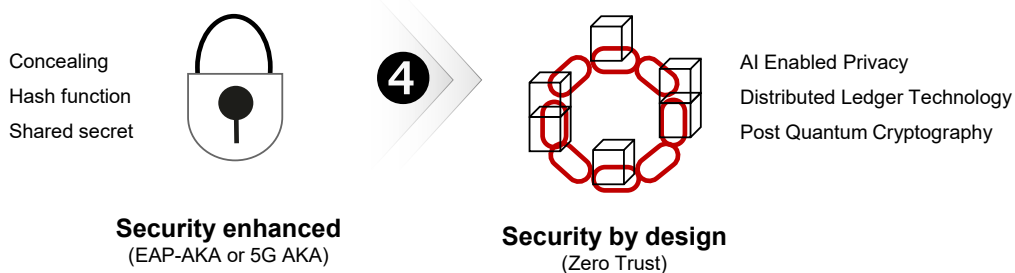


Figure 11. From security enhanced networks to security by design systems ([Soldani, 2021b](#)).

Privacy Protection

As 5G networks evolve, it is expected that there will be increased reliance on AI-enabled smart applications requiring situational, context-aware, and customised 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, 2019](#)).

Also, *Distributed Ledger Technologies* (DLT), such as *blockchain*, may be an enabler for data integrity – beyond Hash Functions used in 5G and other traditional communication systems – use of trustless computing between stakeholders, as well as presenting privacy protection mechanisms in the network. For example, blockchain offers privacy protected data sharing mechanisms, can optimise the 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](#)).

Concepts related to *Federated Learning* (FL), as exemplified in Figure 4, 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 locally on its generated source 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 *differential privacy, disinformation, and randomisation* ([Menting, 2021](#)).

Protection of Network Interfaces

Overall, the 5G security architecture, features and protocols simply enhance the mechanisms that constitute the 4G security posture, while 6G is expected to go well beyond that ([ENISA, 2021](#); [3GPP 2021](#); [5G Americas, 2021a](#)).

For example, as shown in Figure 10, 6G wireless is expected to support, but not be limited to, the following security controls and assurance mechanisms ([Menting, 2021](#); [Soldani, 2020](#)):

- **Zero-Trust Architectures (ZTA):** Not a single asset is trusted implicitly, and continuous access control, authentication and identification are used inside the network.
- **Distributed Ledger Technologies (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 algorithms’ robustness and the development of defenses against attacks.
- **Cyber-Resilience:** Continuous detection and appropriate response to adverse events, ability to withstand attacks, autonomously evolve, and adapt to threats.

Security Assurance

The Global System for Mobile Communications Association (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](#)).

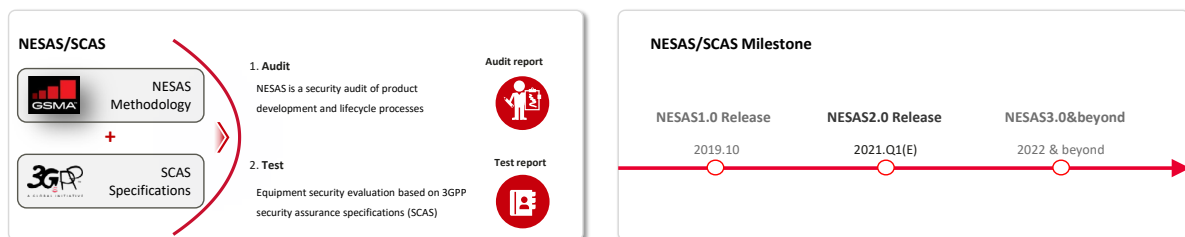


Figure 12. GSMA NESAS and 3GPP SCAS methodologies and milestones ([Soldani, 2021d](#)).

The NESAS defines security requirements based on 3GPP technical specifications and an assessment framework for secure product development and product lifecycle processes; and 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 customised, 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 authorisation 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 value chain need to take their own security responsibilities, to mitigate the related cyber security risks ([Soldani, 2021d](#)):

- **Suppliers** must prioritise 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 to take the necessary measures to ensure the protection of national security interests and the enforcement of conformance programs and independent product testing and certification.
- **Standardisation development organisations** 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 nothing else than a generic pipe of bits, *to something really centred around the end user*.

The end user is expected to become a real *prosumer*, which means that the end user will not only be able to consume content, information, but also he or she will have the ability to generate content and share that, making it available to various communities of people and cyber entities by connecting and exploiting 6G services ([Soldani, 2021b](#)).

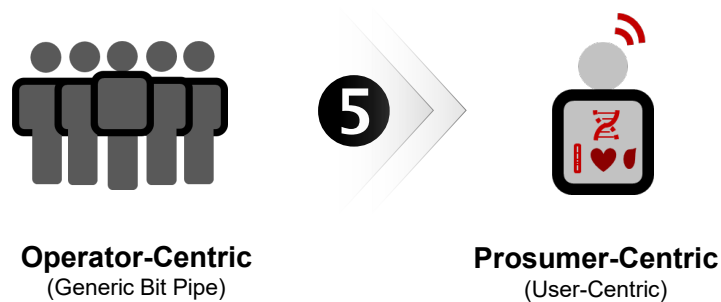


Figure 13. From generic bit-pipe networks to prosumer-centric systems ([Soldani, 2021b](#)).

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 capable of representing knowledge, able 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 ten or more times in terms of (but not limited to) the following metrics: Supported spectrum and bandwidth; coverage; reliability; latency; density of endpoints; synchronisation of multiple flows to and from multiple *collaborative* devices; location and position tracking; and energy and resource 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.

As we speak, many 6G 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 the tackle technology requirements that 6G will demand for, when it comes alive around 2030.

To realise the compelling vision of 6G wireless presented in this work, a *tight cooperation and collaboration among all regions and stakeholders, globally*, is necessary more than ever before; as well as the *integration of satellite associations, and alliances of vertical sectors, with the standardisation development organizations*, such as the 3GPP, liable for the technical specification of 6G wireless.

Also, it requires an ecosystem of public and private players and a multi-disciplinary approach to ensure that: a) all assets that will form part of 6G systems are *interoperable* and comply 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 supports the *minimal set of approved security, safety and privacy requirements*.

Biography



David Soldani received a Master of Science (M.Sc.) degree in Engineering with full marks and *magna cum laude approbatur* from the University of Florence, Italy, in 1994; and a Doctor of Science (D.Sc.) degree in Technology with *distinction* from Helsinki University of Technology, Finland, in 2006. In 2014, 2016 and 2018 he was appointed Visiting Professor, Industry Professor, and Adjunct Professor at University of Surrey, UK, University of Technology Sydney (UTS), Australia, and University of New South Wales (UNSW), respectively.

D. Soldani is currently at Huawei Technologies and, since 2018, he has been serving as Chief Technology Officer (CTO) and Cyber Security Officer (CSO) within the ASIA Pacific Region, and, since 2020, as Chairman of the IMDA 5G task force, in Singapore. Prior to that he was Head of 5G Technology, e2e, Global, at Nokia; and Head of Central Research Institute (CRI) and VP Strategic Research and Innovation in Europe, at Huawei European Research Centre (ERC).

David can be reached online at <https://www.linkedin.com/in/dr-david-soldani/>

References

- 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 Consideration 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/fFVoHMDaqY>
- 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. Elsevier B.V. *Computer Networks*. Retrieved from www.elsevier.com/locate/comnet
- 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 EEC. Retrieved from: <https://www.enisa.europa.eu/publications/5g-supplement-security-measures-under-eec>
- 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>
- GSA. (2021). 5G Market – Snapshot April 2021. Retrieved from <file:///C:/Users/d00441814/Downloads/GSA-5G-Market-Snapshot-April-2021.pdf>
- 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/>
- 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/>

- 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*. Retrieved from https://www.researchgate.net/publication/344352771_Non-Terrestrial_Networks_in_5G_Beyond_A_Survey
- Soldani, D. (2020). On Australia's Cyber and Critical Technology International Engagement Strategy Towards 6G – How Australia may become a leader in Cyberspace. Retrieved from <https://jtde.telsoc.org/index.php/jtde/article/view/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/2ifg!ScLDgw>
- Soldani, D. (2021c). Radio Access Network Evolution. IEEE Public Lecture. Retrieved from <https://youtu.be/2yKXSZAINml>
- Soldani, D. (2021d). 5G Security. *Cyber Defense eMagazine*, February 2021. Retrieved from: https://cyberdefensemagazine.tradepub.com/free/w_cyba111/prgm.cgi
- 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*. Retrieved from: <https://ieeexplore.ieee.org/document/7047266>
- 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>
- Tong, W. (Ed.), Zhu, P. (Ed.) (2021). 6G: The Next Horizon From Connected People and Things to Connected Intelligence. *Cambridge University Press*. Retrieved from: <https://www.booktopia.com.au/6g-the-next-horizon-wen-tong/book/9781108839327.html>
- Yaacoub, E., & Alouini, M. S. (2020). A Key 6G Challenge and Opportunity—Connecting the Base of the Pyramid: A Survey on Rural Connectivity. *Proceeding of IEEE. Vol. 108, No. 4*. Retrieved from <https://www.techrxiv.org/ndownloader/files/21648993>