On Australia's Cyber and Critical Technology International Engagement Strategy Towards 6G

How Australia may become a leader in Cyberspace

David Soldani
Huawei Technologies

Abstract: In response to the call by the Australian Department of Foreign Affairs and Trade for submissions on the development of Australia's Cyber and Critical Technology International Engagement Strategy, this paper reviews the most *critical technologies*; related risks and opportunities; best practices, policies and security frameworks in other countries; relevant government, industry, civil society and academia cooperation initiatives; and proposes how Australia may became a leader in the global Cyberspace. To realise this vision, Australia should play a major role among selected international organizations; support the continuous evolution of *critical technologies*; adopt a proper technology security assurance scheme; and enforce a certification and accreditation process – against a predetermined set of appropriate security standards and policies – for security authorisation in Australia. This could be achieved with the formulation and implementation of an *Australia's defence-in-depth strategy*, augmented by a *Zero-Trust model*, which enhances security for untrusted domains, and within trusted domains, and meets the baseline requirements of cyber security for the Internet of Things.

Keywords: 5G, 6G, Cyber Security, Cyber defence, Zero Trust.

Introduction

This paper responds to the call by the Department of Foreign Affairs and Trade (the Department) for submissions on the development of Australia's Cyber and Critical Technology International Engagement Strategy (CCTIES) (Australian Government, 2020a).

The Department requested respondents to consider at least one of the following questions:

1. What should Australia's key international cyber and critical technology *objectives* be? What are the *values and principles* Australia should promote regarding Cyberspace

http://doi.org/10.18080/jtde.v8n4.340

and critical technology?

2. How will *Cyberspace and critical technology* shape the international strategic/geopolitical environment out to 2030?
3. What *technological developments and applications* present the greatest risk and/or opportunities for Australia and the Indo-Pacific? How do we balance these risks and opportunities?
4. How should Australia pursue our *cyber and critical technology interests* internationally?
5. How can *government, industry, civil society and academia cooperate* to achieve Australia's international cyber and critical technology interests?
6. What *policies and frameworks* exist in other countries that demonstrate best practice approach to international cyber and technology policy issues?

The following sections touch upon all the above requests with a somewhat greater focus on Questions 2, 4, 5 and, especially, Question 6. The focus of the questions is on Australia's development and cooperation in the *global Cyberspace*.

The article sheds light on key areas the Department should focus on, and the international organisations to collaborate with: this, in respect of the security of *critical technologies*, and in doing so to take the necessary joint actions with likeminded countries. This will ensure these *critical technologies* are not manipulated and deployed for nefarious purposes in Australia (Australian Government, 2020b).

Objectives, Values and Principles

Cybersecurity ensures the Confidentiality, Integrity and Availability (CIA) of information[i]. Australia should strengthen its approach by including cybersecurity at the heart of its political, economic and safety priorities. *Trust*, *security* and *fight against cybercrime* should be at the core of Australia's 2020 Cyber Security Strategy in order to counter the rapidly evolving cyber threat environment (Australian Government, 2019).

In order to realise this vision, the Department should consider following in the footsteps of the European Union (EU) (European Commission, 2017), and take the following actions that will set Australia apart, overtaking the EU, and make it a leader:

- *Increase cybersecurity capabilities and international cooperation* by raising Australia's cybersecurity competences to the same level of development as other countries leading in this field and ensuring efficient exchanges of information and cooperation at cross-border level, especially in the Association of Southeast Asian

http://doi.org/10.18080/jtde.v8n4.340

Nations (ASEAN) markets, where there is a strong demand for cybersecurity solutions.

- *Make Australia a strong international player in cybersecurity* and ensure that consumers, enterprises (including SMEs), and public administrations have access to the latest *digital security technology*, which is interoperable, competitive and trustworthy; ensures resilience and transparency; and respects fundamental human rights, including privacy preservation, taking advantage of the booming global cybersecurity market.
- *Pursue a collaborative and information sharing, risk management framework and labelling scheme that provides an objective and transparent basis for knowing which products and services are worthy of trust*: in particular, with regard to new technologies and emerging sectors – such as 5G, 6G, Artificial Intelligence (AI), Cellular Vehicle to X (C2X), Internet of Things (IoT), Industrial IoT (IIoT) and Consumer IoT (CIoT) (5G Americas, 2020a; European Commission, 2020b). Australia should adhere to the principle of "*openness and transparency*" and explore strategic and fundamental solutions based on facts with international stakeholders.

Cyberspace and Critical Technology

Devices and systems increasingly become more intelligent and more connected in many business processes and cross-sector industrial applications, such as transport, finance, healthcare, energy, agriculture, mining and manufacturing (Batas, Men & Smitham, 2020).

As more devices connect to the Internet, cyber security of Consumer IoT becomes a growing concern. People entrust their personal data to an increasing number of online devices and services. Products and appliances that have traditionally been offline are now connected and need to be designed to withstand cyber threats. For example, the baseline requirements for the cybersecurity of Consumer IoT are reported in ETSI (2020).

Fifth-generation wireless communications technologies (5G) will enable vastly more smart devices to connect to the Internet and among themselves, thereby accelerating the digital transformation that is already underway in manufacturing, transportation, education, healthcare and government. Some use cases and applications supported by 5G are depicted in Figure 1. Consumer devices from vehicles to medical implants will become more capable via 5G connections to new multi-access edge computing (MEC) servers and cloud services, algorithms and applications.

http://doi.org/10.18080/jtde.v8n4.340

Figure 1. Example of use cases and applications supported by 5G.

In short, 5G deployment will enable a *new generation of the knowledge economy, increasing productivity, growing new businesses and spurring innovation*. As a result, those nations and countries that master the advanced 5G technologies will have a long-term economic advantage as 5G systems and related capability enable digitised government and industry (US Department of Defense, 2020).

5G will bring computing power to the end user. It will increase the use of sensors and machine-to-machine communications to enable, smarter faster decisions, sometimes implemented automatically. This will make us increasingly dependent on technologies in a manner and to a degree that we have never experienced before, making two things much more important in security deployment than ever before:

- *Availability,* as we need to know these services will be there when we need them.
- *Integrity*: data, on which the analysis and decision-making depends, are accurate.

Three-hundred-and-ninety-two operators in 126 countries are investing in 5G, and 92 carriers in 38 countries have already launched one or more 5G services (GSA, 2020a), as illustrated in Figure 2.

China is said to more than double the number of its 5G base stations and will have 600,000 5G operational nodes. One year after 5G spectrum licenses were allocated there are already 36 million 5G end-users in the Chinese market (CGTN, 2020).

Comparatively in Australia, Telstra has more than 1,500 5G sites on-air across selected areas of 53 Australian cities and towns. Optus has more than 860 5G sites live across six major cities and several major towns.

http://doi.org/10.18080/jtde.v8n4.340

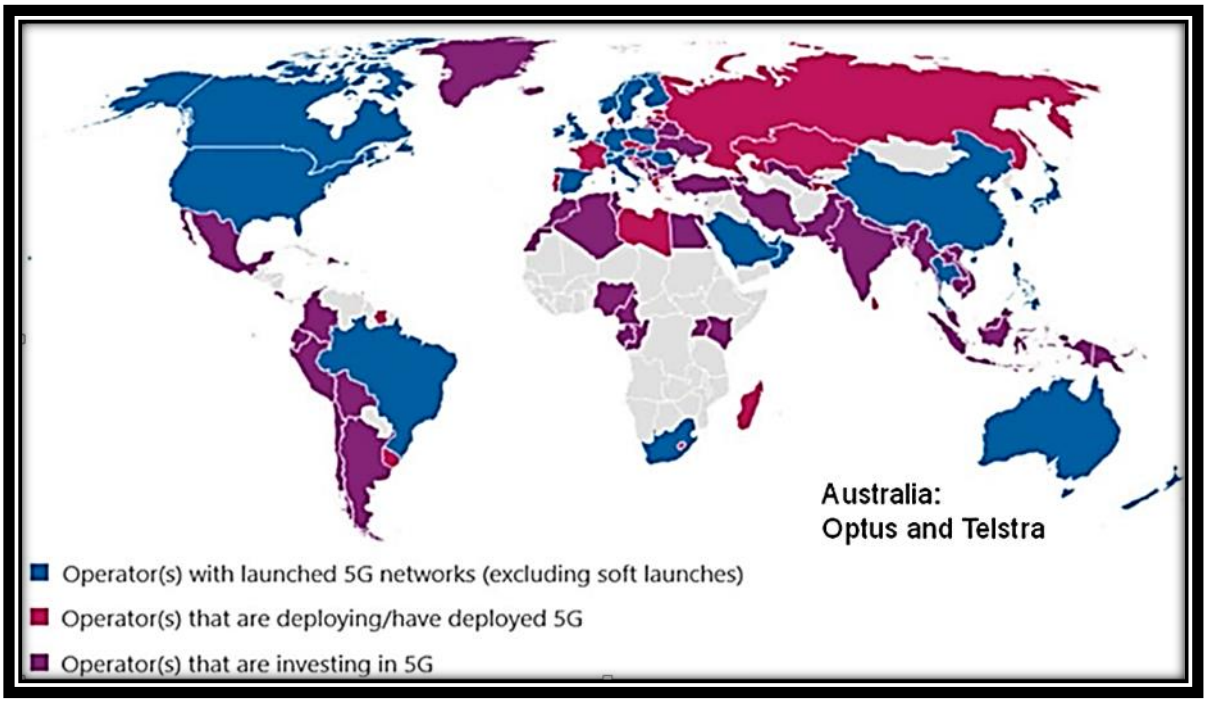


Figure 2. Map of global operator investments in 5G (GSA, 2020a).

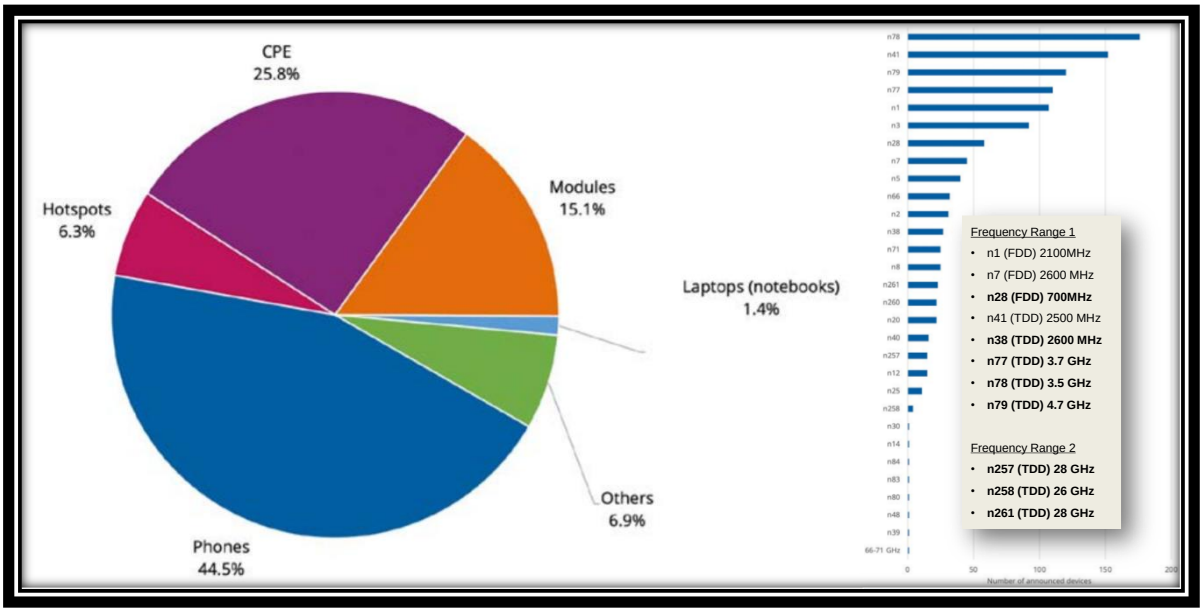


Figure 3. Announced 5G devices, by form factor and spectrum support, by specific band (GSA, 2020b).

Looking at the 5G ecosystem, by the end of July 2020, 18 form factors were announced. These included phones, head-mounted displays, hotspots, indoor CPE, outdoor CPE, laptops or notebooks, modules, snap-on dongles or adapters, industrial grade CPEs or routers (also referred to as gateways or modems), drones, robots, tablets, TVs, cameras, USB modems, a switch, a vehicle on-board unit (OBU) and a vending machine. A total of 91 vendors announced available or forthcoming 5G devices. The devices include a total of 364 regional variants, and phones that can be upgraded using a separate adapter. Excluded from this list are operator-

http://doi.org/10.18080/jtde.v8n4.340

branded devices, which are essentially rebadged versions of other phones. Over 162 of these devices are said to be commercially available (GSA, 2020b).

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). Whereas the first 5G release (Release 15) predominantly addressed the immediate needs of enhancing the mobile broadband experience, the release of the 16th and the 17th versions take 5G toward the full 5G vision, balancing the needs of mobile broadband operators with expanding 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, 2020b). The 3GPP 5G high level roadmap is depicted in Figure 4.

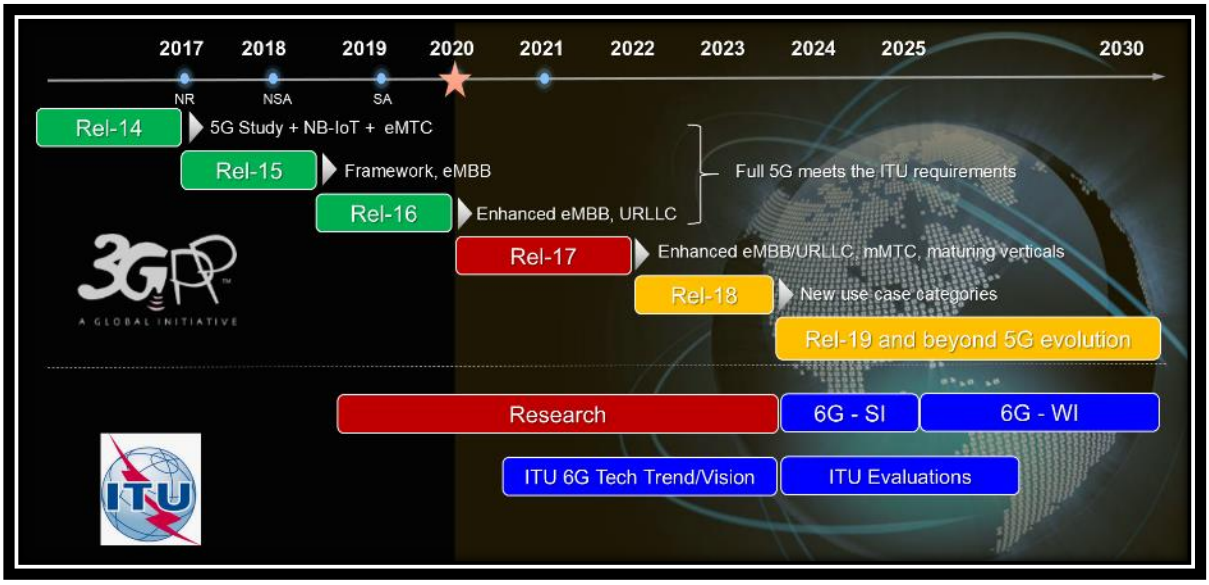


Figure 4. 3GPP 5G roadmap (Soldani, 2020b).

Release 16 forms the foundation for supporting Industrial IoT. It has an Ultra-Reliable Low-Latency Communications (URLLC) functionality that has the 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

http://doi.org/10.18080/jtde.v8n4.340

authorization; 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 1). The support extends to Network Automation Phase 2; Integrated Access & Backhaul (IAB); Device Power Saving; Mobility Enhancement and Enhanced Massive MIMO with multiple Transmission and Reception Points (TRP) (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 Consumer IoT. It will support native Time Sensitive Communication (TSC); High-Accuracy Positioning (cm-level); Sidelink enhancement for public safety and pedestrians; Multicast; Non-Terrestrial Networks (NTN), such as GEO and LEO satellites; and FRMCS enhancements (FRMCS – Phase 2). Further support will be provided to Network Slicing enhancements; Network Automation enhancements; New Radio in the 52–71 GHz frequency range; Device Power Saving enhancements; Further enhanced MIMO; Multiple USIMs; Cloud gaming QoS; and "NR-light" for IIoT and CIoT, particularly suitable for industrial cameras, high-end wearables, smart grid applications, high-end logistic trackers, and healthcare monitoring. This is illustrated in Figure 5 (3GPP, 2020b).

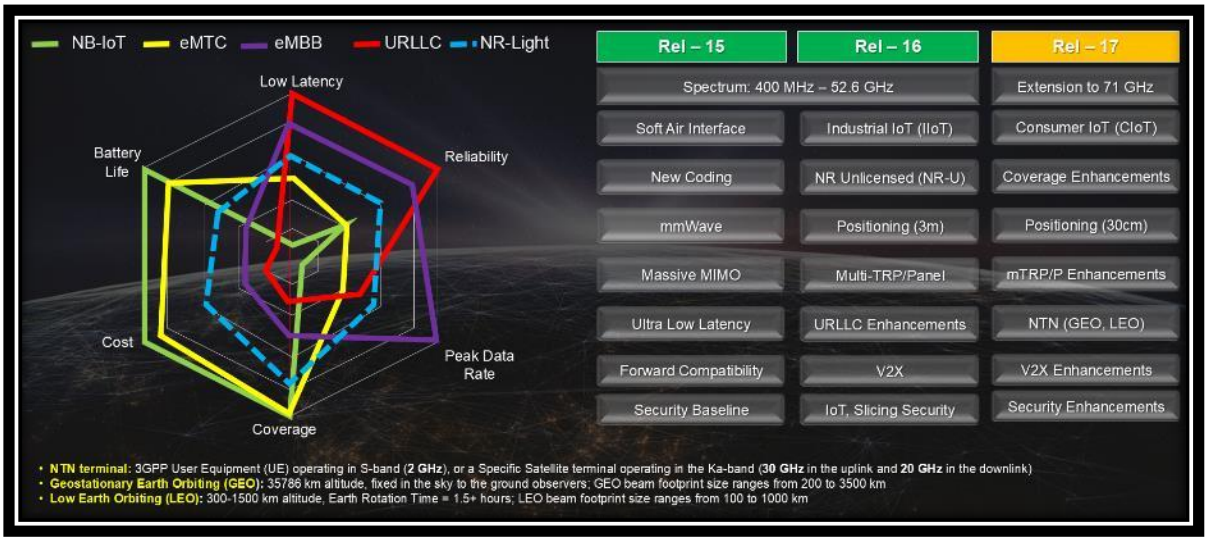


Figure 5. 3GPP R15, 16 and 17 supported spectrum and key features (3GPP, 2020b).

The release of versions 16 and 17 will witness an expansion of the ecosystem that can take advantage of 5G. As depicted in Figure 5, 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. The progression of 5G with Release 18 and beyond will meet the needs of new market opportunities and deliver great value, towards 6G, which is expected to be specified by 2030.

http://doi.org/10.18080/jtde.v8n4.340

The 6G wireless architecture will be shaped by five key constituents (Figure 6): *virtual-X*, *tactile*, *inferencing*, *sensing* and *learning*. AI will be the dominant service and application. 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 (Tong, 2020). This will allow us to apply wireless sensing capabilities; and 6G wireless will operate as a sensor network. The network and devices can perform real-time (RT) sensing, which will be the fabric to link the physical world and the cyber world.

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; 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) (Soldani, 2020a). New compression technologies will be required to train the neural networks.

On the network side, we have the 6G Base Station (BS) node and 6G Edge Node. The BS will have all sensing capabilities to sense the environment in RT and for the ML capabilities. The Edge Node will be mostly used for ML, so the classical data centre at the edge will become the Neural Edge, and the BS will become the neural node.

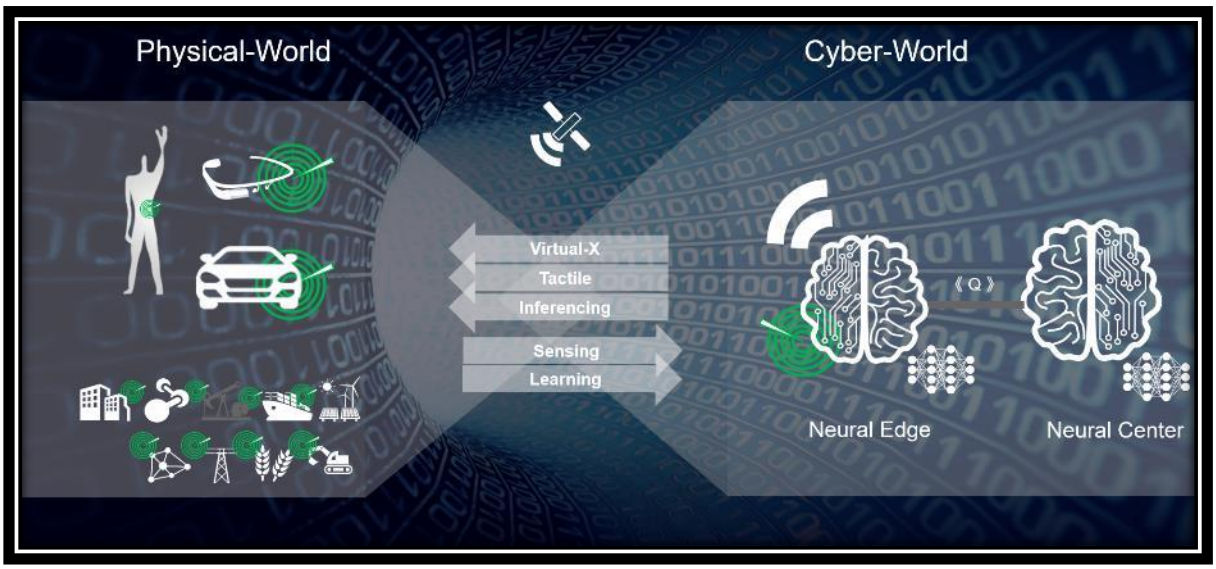


Figure 6. 6G Wireless network architecture (Tong, 2020).

Quantum (Q) key distribution technology can be deployed for the fibre-optic link between the Neural Centre and the Neural Edge. NTN is 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.

http://doi.org/10.18080/jtde.v8n4.340

In a nutshell, 6G wireless is transforming from *connected everything* (information world) to *connected intelligence* (intelligent world). 6G wireless is the technology to deliver artificial intelligence to everyone, anywhere and at any time (Tong, 2020).

A high-level roadmap on how connectivity will evolve is depicted in Soldani (2020b). Today, we dwell in an *information world* characterised by remote control of digital devices, connected with 5G, IPv6+, Fixed 5G, and WiFi-6 technology, supporting 1-10 Gbps speeds, 10 ms latency, five nines reliability, and 1 million connections per square kilometre.

This is followed by an *intelligent world* featured by intelligent exoskeletons, 360° high-definition AR/VR and mixed reality (MR), provided by enhanced versions of the technologies available today.

We will arrive in the *holographic world* by 2030, characterised by unmanned robotic platforms and true-to-life holography (i.e. fully immersive interactive experience), only possible with the deployment of 6G, New IP, Fixed 6G, and WiFi-7 technologies, supporting 100 Gbps speeds, 1 Tbps anywhere transmission, both on the ground and via satellites, latency below 1 ms, "seven nines" reliability, and 10 million connections per square kilometre (Soldani, 2020b).

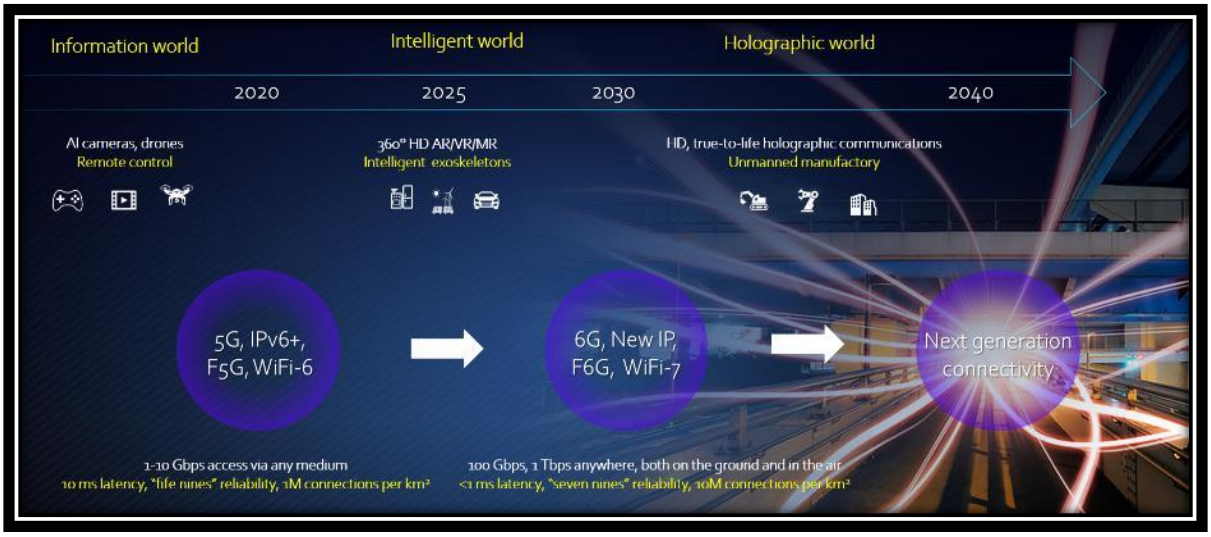


Figure 7. 6G Wireless network architecture (Soldani, 2020b).

Greatest Risk and/or Opportunities

There is a *shared responsibility* for risk management between information and communication service providers, equipment vendors and third-party suppliers. Market forces must be leveraged to drive greater assurance and transparency. *Procurement requirements* for buyers of ICT must be risk informed. Telecom equipment suppliers must be encouraged to develop *minimum industry standards* for assurance and transparency. There is a need to support *conformance programmes* and *independent testing;* and *effective risk*

http://doi.org/10.18080/jtde.v8n4.340

mitigation plans are necessary to address current and new emerging threats (Batas, Men & Smitham, 2020).

5G will progressively support essential services. This demands greater *cross-sector collaboration* between operators and suppliers – more than the partnership it seeks within the Telecoms field. As a result, building trust in Cyberspace is another important requirement (Batas, Men & Smitham, 2020; European Commission, 2020b).

Trust goes beyond technical or operational measures. Trust requires a dialogue between nations to set up *diplomatic norms* for acceptable state and state-sponsored behaviour in Cyberspace. Suppliers can build greater trust through *cooperation*, *openness* and *transparency*, ensuring a culture of security across sectors vital for our economy and society, which rely heavily on the use of information and communication technology (ICT).

Digital technologies and infrastructures, like 5G, present many new opportunities for economic growth and threats to the security of information and communications. The Department should work together with *industry* to build these technologies *in a way that ensures trust, security, safety* and *the protection of fundamental human rights*.

Since currently there are no relevant initiatives is place in Australia, it is vital that the Department and its agency partners, especially the Australia Cybersecurity Centre (ACSC), develop and fully implement a *Standards Engagement Plan* and actively participate in the 3rd Generation Partnership Project (3GPP) and Global System for Mobile Communications Association (GSMA) initiatives; for this engagement, it should have specific and prioritised outcomes, and deliverables, in Australia's interest, including strengthening the Australia's requirements and influence in those key organizations, and promoting high-quality contributions to 5G, 6G, and beyond, technologies and corresponding network equipment security assurance schema (discussed below).

Cooperating and collaborating at international level is essential for the Department in order to engage and drive towards a *trustworthy foundation* to enhance the security both of 5G networks and of technology built upon them, in a reliable, secure, resilient, and transparent manner (Soldani, 2019).

Cyber and Critical Technology Interests Internationally

Despite their advanced functionalities, 5G technologies pose several security challenges. This is essentially due to their innovative, software-driven nature and their use in a wide range of services and applications (Batas, Men & Smitham, 2020). The security challenge is exacerbated by the fact that the ecosystem is becoming increasingly dependent on the confidentiality, integrity and availability of data (the CIA triad). The EU Network and

http://doi.org/10.18080/jtde.v8n4.340

Information Security (NIS) Cooperation Group published its EU-wide Risk Assessment on 5G security that highlights shared technical and non-technical concerns (European Commission, 2019a). Conclusions were drawn based on the capabilities and the motivations of a potential attacker. *Integrity* and *availability* of 5G were of major concern, on top of the existing *confidentiality* and *privacy* requirements. Severe threats included compromised confidentiality and availability associated with an insider within a telecom operator or subcontractor, and associated with an *organized crime group*. Most critical 5G assets were Core Network Functions (5G Core), Network Function Virtualisation (NFV) and Management, and Orchestration (MANO).

The European Commission, the Member States and corresponding cybersecurity agencies are working together with Communication Service Providers (CSPs) and technology suppliers in order to provide continuity of mobile network services while managing cyber risks and concerns relating to these mobile networks and their underlying technologies.

To address the challenges to enhance cybersecurity, the European Union Agency for Network and Information Security (ENISA) published an analysis report of telecom security incidents, which the organisation has been collecting from all Member States (including the UK) and consolidating since 2012 (ENISA, 2019). *System failures* are the most common root cause, constituting roughly two thirds every year. In total, system failures account for 636 of incident reports (68% of the total). For this root cause category, over the last 7 years, the most common causes were *hardware failures* (36%) and *software bugs* (29%). The second most common root cause over the 7 years of reporting is *human errors* with nearly a fifth of total incidents (17%, 162 incidents in total). *Natural phenomena* come third at just under a tenth of total incidents (9%, 89 incidents in total). Only 4% of the incidents are categorised as *malicious actions*. In the period 2012-2018, two thirds of the malicious actions consist of *Denial of Service* (DoS) attacks, and the rest are mainly *damage to physical infrastructure*.

System failure and human error constitute the greatest risk and should be the focus of risk evaluation. The potential risks in any given product should be evaluated based on *factors* having a material effect on product security, such as the product security architecture, security mechanisms, and security features.

On the basis of the EU coordinated risk assessment of the cybersecurity of 5G networks that followed (European Commission, 2019a) – from the EU Network and Information Security (NIS) Cooperation Group – mitigation measures aim to *reinforce cross-sector collaboration between suppliers, operators, and service providers*, and also to raise the *transparency and openness of the suppliers* towards EU Member States.

http://doi.org/10.18080/jtde.v8n4.340

Governments in EU Member States can drive toward a *trustworthy foundation* to enhance the security of EU 5G networks addressing technical and non-technical risks through greater *public-private sector collaboration*, such as in the definition of security requirements; development of unified, international, globally recognised standards for network equipment security assurance scheme and compliance, as discussed in detail in the following sections; and promoting the widespread acceptance and implementation of international norms of responsible behaviour as well as confidence-building measures in Cyberspace.

The Department should work closely, at international level, with all relevant industries and partners to deliver a consistent set of regulations, and use market forces to incentivise greater assurance and transparency, to address 5G security that allows operators to take responsibility for the overall implementation (Huawei, 2019).

Cooperation between Government, Industry, Civil Society and Academia

Singapore, Indonesia and Thailand signed a Memorandum of Understanding (MoU) with Australia, which outlines cybersecurity cooperation in key areas. Those initiatives form a very good base for international companies to springboard into ASEAN markets, where there is strong demand for cybersecurity solutions (Barton, 2020).

Also, in Australia, there are many ongoing collaboration programs, such as, but not limited to, the list below (Barton, 2020):

- Cyber Security Cooperative Research Centre[ii], which encourages collaborations between industry, researchers and governments. Research programs include critical infrastructure security and cybersecurity as a service.
- Cooperative Research Centre Grants[iii] (CRC) and Project Grants (CRC-P), which provide funding for industry-led research collaborations.
- Next Generation Technologies Fund[iv] (NGTF), a government initiative with an investment of $730 million over the decade to June 2026. A forward-looking program focusing on research and development in emerging and future technologies.
- Australian Cyber Collaboration Centre[v] (A3C), which raises the awareness for business and acts as the translator between business, Government, industry and cyber specialists within the ecosystem.

However, we would need more investments in developing more *rigorous engineering practices* and move towards high-quality security software and hardware components by design, in compliance with standardised security requirements and fit-for-purpose testing for technology (Soldani, 2019).

http://doi.org/10.18080/jtde.v8n4.340

In Australia, the Common Criteria (CC) regime and Australasian Information Security Evaluation Program (AISEP) have not met the expected results and little of the government technology in use today has common criteria certification. For example, the AISEP scheme should be revamped together with the Protective Security Policy Framework (PSPF) into a program that can achieve a real step up for government and critical-infrastructure systems (Moore, 2020).

In Europe, to this end, many successful initiatives are ongoing, looking at trustworthy technology to increase the level of customers' confidence in products and services, and, especially, for development and deployment of resilient ICT infrastructures.

The Department should ensure cooperation with the European Commission (EC) and other Member States, their partner cyber security agencies – such as ENISA, the Federal Cyber Security Authority in Germany (BSI) and the National Cyber Security Agency of France (ANSSI) – and a closer collaboration with international industry partners (Huawei, 2019), such as 3GPP and GSMA – on 5G *security specifications* (3GPP, 2020c) and *network equipment security assurance scheme* (GSMA, 2020).

This could be achieved by setting up an international "*Collaboration Working Group*", comprising public and private parties, and under the Department supervision, in order to support and facilitate strategic collaboration and exchange of information between partners and promote swift and effective operational cooperation on specific cyber-security labelling schemes, incidents and sharing information about identified threats and vulnerabilities. To this end, it is important to involve all suppliers and service providers in relevant industry sectors, in order to enable a much greater accountability of cyber incidents (Bartock, Cichonski & Souppaya, 2020).

For instance, in Singapore, the government, in collaboration with industry, will work with likeminded international partners to establish mutual recognition arrangements for a Cybersecurity Labelling Scheme (CLS), as Singapore, similar to Australia, is a small market with limited ability on its own to shift the global IoT device market toward an enhanced security standard. This will involve aligning the CLS with widely accepted global security standards for consumer IoT devices (Singapore Cyber Security Agency, 2020).

It also requires a broad and *well-trained workforce* (Industry Advisory Panel, 2020). The Department, in collaboration with academia, industry and interagency partners, should identify the necessary skills and develop a human capital plan that assembles distinguished experts, and extends to the next generation of talent, who will be needed to formulate a *strategic research and innovation agenda* (SRIA) for Australia, and design, develop and operate advanced technologies for 5G, 6G and beyond.

http://doi.org/10.18080/jtde.v8n4.340

Policies and Frameworks in Other Countries

Ensuring cyber security throughout international collaboration and finding a balance between technology integration, human capital investments and the innovation ecosystem will be critical to enhancing productivity in the next decade (Soldani, 2019).

Since the telecom sector today is an enabler for the entire digital economy and society, Australia needs to act quickly with new policies and regularity frameworks to secure its global competitiveness and prosperity in the near future (Huawei, 2019).

In numerous countries, such as Europe, China, South Korea, Singapore and Japan, significant changes have taken place within the ICT field, and patterns of consumption and needs have been radically shifting, demanding access to an ever-increasing array of *digital services*, which place an ever-increasing demand on the *ICT infrastructure* across which they are provided. Even more performance and security requirements will be placed on the ICT infrastructure in the years to come, as service applications based on the IoT, artificial intelligence, distributed computing and extended reality (ER) will further develop and grow (European Commission, 2019b).

The full economic and social benefits of this digital transformation may be achieved only if the Australian Government can ensure widespread deployment and take-up of very high capacity networks, in rural as well as urban areas and across all of society.

Australia needs an effective technology-focussed industrial strategy, and it is essential that policymakers and industry leaders get the CCTIES right and invest in developing skills and local industrial capacity if they want to provide opportunity for all in the era of the 4th Industrial Revolution.

A close EU-wide and Australia cooperation is indispensable, both for developing strong international *Cyberspace* and for reaping the full benefits that 5G will have to offer for people, businesses and government services.

The "*Recommendation on Cyber Security of 5G Networks*" (European Commission, 2019c), "*Cyber Security Certification Framework*" (European Commission, 2019d), and "*Connectivity for a Competitive Digital Single Market – Towards a European Gigabit Society*" (European Commission, 2019b) are examples of relevant policies directed at improving security and ensuring future prosperity of all member states (including the UK) in Europe, and gaining trust from people, homes and organisations within the Union.

Following the Commission Recommendation for a common European approach to the security of 5G networks, 24 EU Member States completed the first step and the EU-wide risk assessment in October 2019 (European Commission, 2019a). The completion of the risk

http://doi.org/10.18080/jtde.v8n4.340

assessments underline the commitment of Member States not only to set high standards for security, but also to make full use of this ground-breaking technology. Europe wants all key players, big and small, to accelerate their efforts in building a common framework aimed at *ensuring consistently high levels of security to develop a European approach to protecting the integrity of 5G*.

Within the above framework, in January 2020, the Network and Information Systems (NIS) Cooperation Group, which leads the cooperation efforts together with the Commission, output a "*Toolbox of Mitigating Measures*" to manage the risks identified in the risk assessments at Member-State and EU level (European Commission, 2020a).

Following the entry into force of the "*EU Cyber Security Act*" (European Commission, 2019e), the Commission and ENISA have set up an *EU-wide certification framework* (European Commission, 2019d), in collaboration with industry; and Member States are collaborating with the EC and ENISA to prioritise the certification scheme covering 5G networks and equipment.

The "*EU Cyber Security Act*" establishes an *EU certification framework for ICT digital products, services and processes* that enables the creation of *a tailored and risk-based EU certification scheme*.

Certification plays a critical role in increasing trust and security in products and services that are crucial for digital markets. Today, a number of different security certification schemes for ICT products exist in the EU, and globally. But, without a common framework for a *global valid cyber security certification protocol or programme or ecosystem*, there is an increasing risk of fragmentation and barriers towards a Global Digital Single Market.

The EU certification charter will provide the "*EU-wide certification scheme*" as a comprehensive set of *rules, technical requirements, standards and procedures*. This will be based on agreement at EU level for the evaluation of the security properties of a specific ICT-based product or service, e.g., smart cards. It will attest that ICT products and services which have been certified in accordance with such a scheme comply with specified requirements.

In particular, each European scheme will specify:

- The categories of products and services covered.
- The cyber security requirements, for example by reference to standards or technical specifications.
- The type of evaluation (e.g., self-assessment or third-party evaluation).
- The intended level of assurance (e.g., basic, substantial and/or high).

http://doi.org/10.18080/jtde.v8n4.340

To express the cyber security risk, a certificate may refer to *three assurance levels* (basic, substantial, high) that are commensurate with the level of the risk associated with the intended use of the product, service or process, in terms of the probability and impact of an incident. For example, a high assurance level means that the product that was certified has passed the highest security tests. The resulting certificate will be recognised in all EU Member States, making it easier for businesses to trade across borders and for purchasers to understand the security features of the product or service.

At the same time, the industry is actively contributing to integrate the 3GPP Security Assurance Specifications (SCAS) (3GPP, 2020c) and Network Equipment Security Assurance Scheme (NESAS), jointly defined by 3GPP and GSMA (GSMA, 2020), certification and accreditation frameworks with the upcoming EU Toolbox, and the new Certification Scheme.

In particular, the German national cyber security authority (BSI) is working together with ENISA to adapt the 3GPP SCAS-GSMA NESAS model to the new European Cyber Security Act and set up an *EU 5G regulatory framework*, in cooperation with the industry, as detailed in the next section.

Also, in Germany, the Federal Network Agency has recently published the draft of the catalogue of security requirements for the operation of telecommunications and data processing systems, as well as for the processing of personal data (Bundesnetzagentur, 2020). The catalogue forms the basis for the security concept and for the technical precautions and other measures to be taken to increase the security of the networks and services. The catalogue requires in particular that (Bundesnetzagentur, 2020):

- Critical components are certified.
- Trustworthiness declarations are obtained from manufacturers and system suppliers.
- Product integrity is ensured.
- Safety monitoring is introduced.
- Only trained specialists are used in safety-relevant areas.
- Sufficient redundancies are available.
- Monocultures are avoided.

The catalogue has been submitted for notification to the EC and is also be available in English. Changes may occur until this process is completed, as, at the time of writing, a public consultation on the draft catalogue is ongoing in Germany.

http://doi.org/10.18080/jtde.v8n4.340

GSMA NESAS Model

The GSMA NESAS is an industry-defined voluntary scheme through which vendors subject their product development and lifecycle processes, and network equipment, to a comprehensive security audit and testing against the currently active NESAS 1.0 release and its security requirements (GSMA, 2020).

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

Figure 8 presents the roles and work split between the two organisations:

- GSMA defines and maintains the *NESAS specifications*, which cover assessment of Vendor Development and Product Lifecycle processes, NESAS Security *Test Laboratory accreditation*, and *Security Evaluation* of network equipment. (GSMA also defines a *dispute resolution* process and governs the overall scheme.)
- 3GPP defines *Security Requirements and Test Cases* for network equipment implementing one or more 3GPP network functions – defined in the Security Assurance Specifications (SCAS): 3GPP TS 33.X (3GPP, 2020c).

The NESAS approach consists of the following steps (see Figure 9):

- Equipment Vendors define and apply secure design, development, implementation, and product maintenance processes.
- Equipment Vendors assess and claim conformance of these processes with the NESAS defined security requirements.
- Equipment Vendors demonstrate these processes to independent auditors that GSMA has selected.
- The level of security of network equipment is tested and documented. (Tests are conducted by accredited test laboratories.)

http://doi.org/10.18080/jtde.v8n4.340

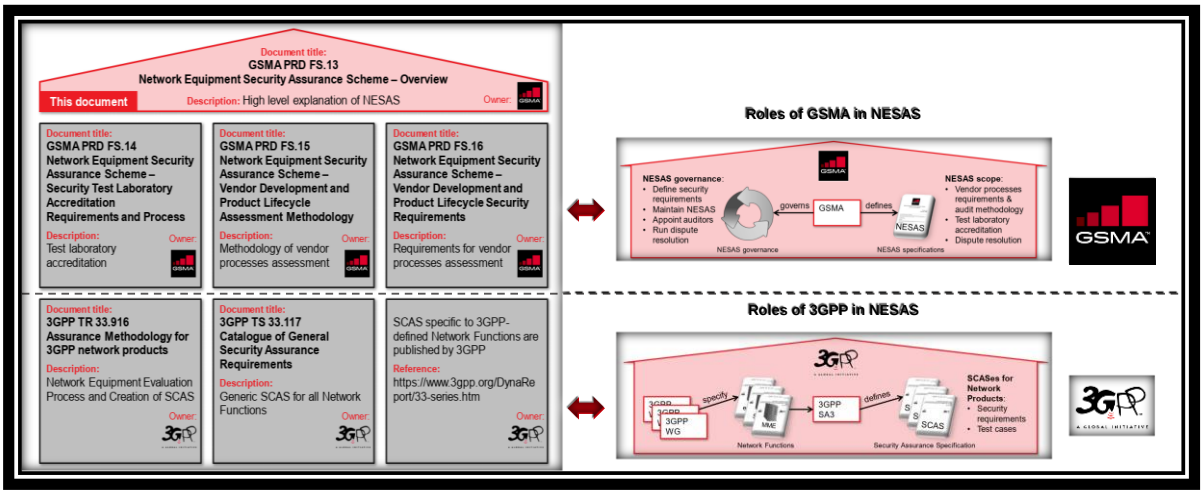


Figure 8. 3GPP and GSMA deliverables, roles and work split (GSMA, 2020).

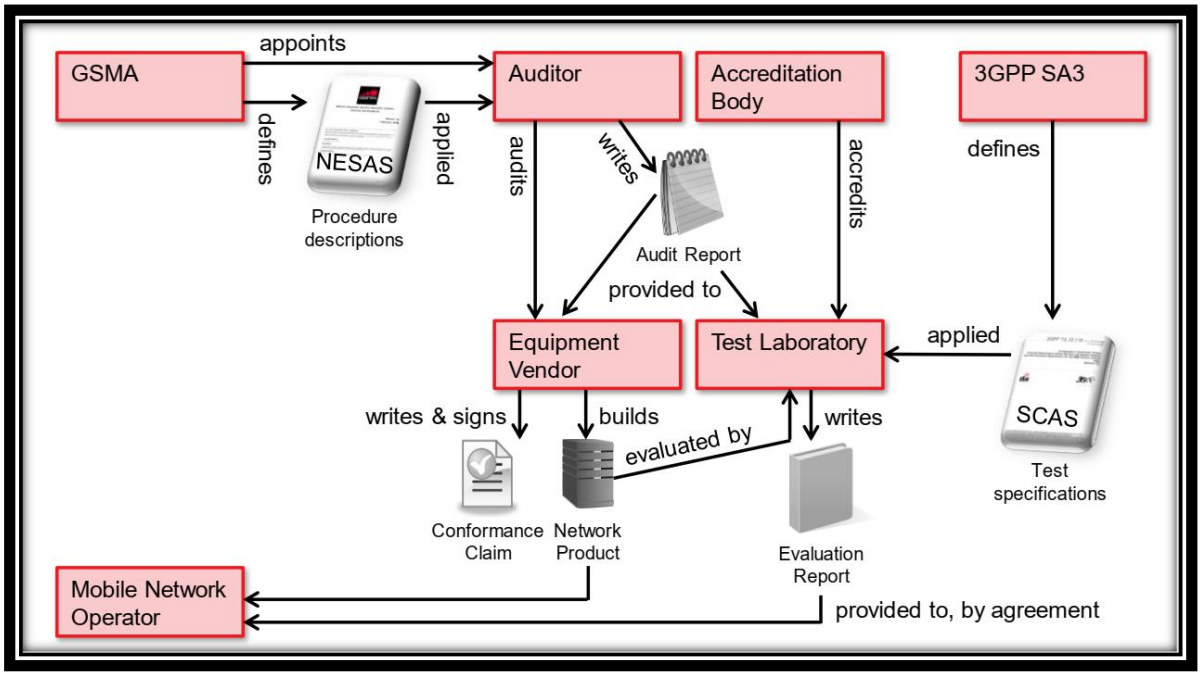


Figure 9. NESAS high level process (GSMA, 2020).

Figure 10 illustrates the involvement of many public and private organisations in the NESAS process. The NESAS is widely supported by security authorities (such as ENISA in EU, ANSSI in France and BSI in Germany) and industry organisations, globally. The NESAS 1.0 release was finalised in October 2019. Since then, two European firms (ATSEC and nccgroup) were selected by GSMA; Ericsson, Nokia and Huawei openly support NESAS as a unified cyber security certification framework for mobile network equipment, and more than ten operators have requested NESAS compliancy, before deploying 5G equipment in their countries.

http://doi.org/10.18080/jtde.v8n4.340

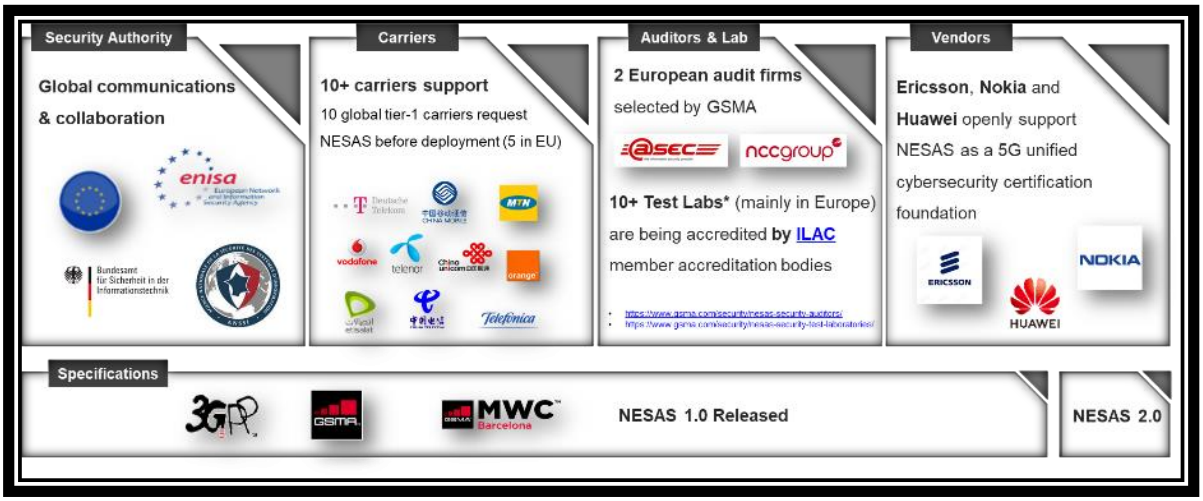
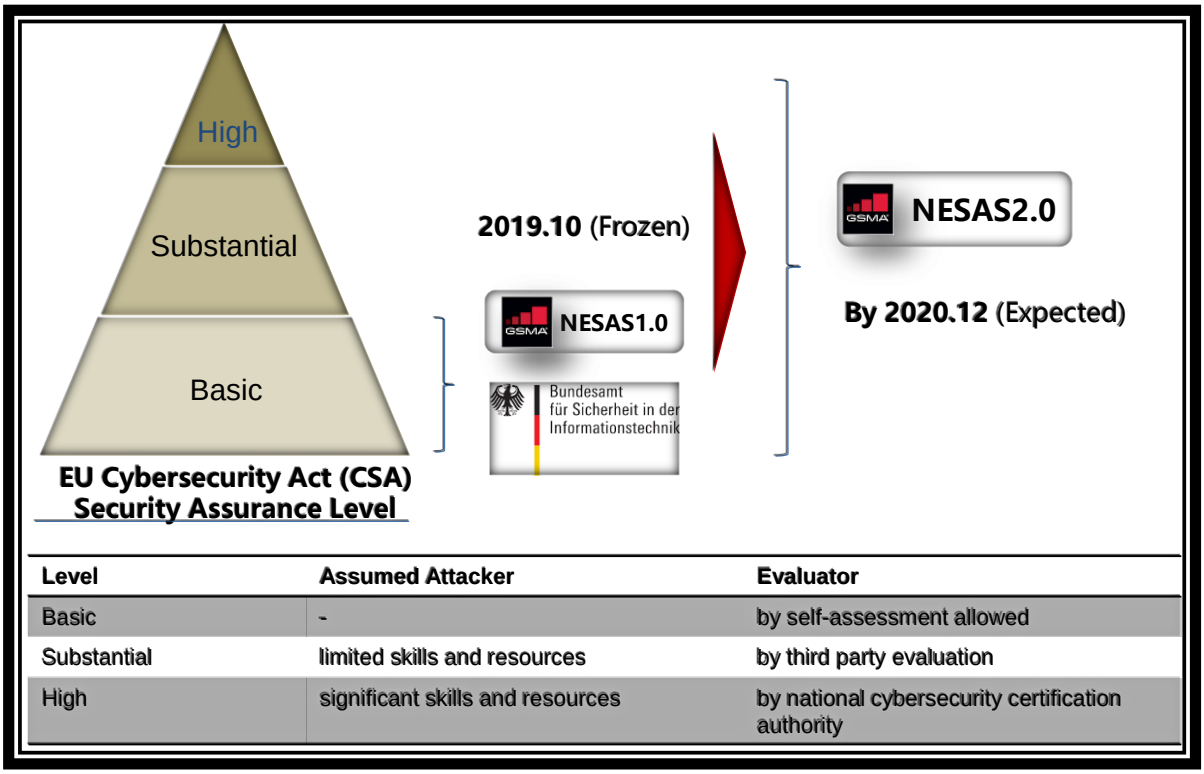


Figure 10. NESAS process widely supported by security authorities and industry organisations, globally.

GSMA appoints the Audit Firms and recognises the competency of the International Laboratory Accreditation Cooperation (ILAC) member accreditation bodies to assess and accredit security test laboratories.

Security test laboratories that are deemed by an ILAC member to have satisfied the ISO 17025 and NESAS requirements, and that have been ISO 17025 accredited, will be considered to have achieved NESAS accreditation.

The NESAS 1.0 framework was approved in October 2019 and comprises the technical specifications depicted in Figure 8.



Level	Assumed Attacker	Evaluator
Basic	-	by self-assessment allowed
Substantial	limited skills and resources	by third party evaluation
High	significant skills and resources	by national cybersecurity certification authority

Figure 11. NESAS Evolves as a solid security assurance basis.

http://doi.org/10.18080/jtde.v8n4.340

The NESAS specifications will be further improved by the end of this year to meet the security assurance level in compliance with the EU Cyber Security Act (European Commission, 2019e). This will possibly encompass: *Penetration Tests*, *Cryptographic Analysis* and *Software Engineering*, as exemplified in Figure 11, in alignment with the best industry standards and practises, as depicted in Figure 12.

Furthermore, the NESAS – defined for mobile systems security – fully validates the characteristics of mobile communication services, in terms of threat analysis and modelling, and significantly simplifies the Common Criteria (CC), featuring short accreditation and evaluation time, and low cost, and meeting the development needs of new technologies, such as cloud, digitisation, and software-defined everything.

The CC and companion Common Methodology for Information Technology Security Evaluation (CEM) are intended for the IT industry and define no equipment test specifications for mobile communication in product process (PP).

Moreover, the CC cover the general R&D process and lifecycle management audit, but lack of specialty on telecommunication such as 5G, and also suffer from complicated accreditation, long period, and high cost.

A comparison between the NESAS and CC frameworks is shown in general terms and in terms of technical requirements in Figure 13 and Figure 14, respectively.

NESAS 2.0	Penetration test	Cryptographic analysis	Software engineering capability
Industry Benchmarking	1. BSZ 2. CSPN 3. CPA 4. CC AVA (bypassing, tampering, direct attack, monitor, misuse) 5. MSDL/BSIMM/OWASP SAMM	1. BSI TR 02102 2. ANSSI RGS_B series 3. NCSC CPA 4. NIST FIPS140-2, NIST SP800-90A 5. NDcPP (ISO19790:2012, NIST SP800-90A)	1. NCSC Secure development and deployment 2. MSDL 3. BSIMM 4. OWASP SAMM 5. NIST standards 6. ISO standards

Figure 12. How the NESAS is expected to evolve according to stakeholders' requirements.

Accreditation/ Evaluation System	NESAS	CC
Organization owner	GSMA/3GPP	CCRA (Common Criteria Recognition Arrangement)
Standards scope & completeness	Audit/Evaluation report (Not certificate)	1~7 EALs (Evaluation Assurance Levels)
Standards progress	NESAS/SCAS standard/specifications (2019.10)	CC released years ago, **operated maturely**
Number of accredited labs & auditing companies	Several labs and 2 auditing companies now	About **77** labs globally
Operators' recognition	**High**	**Low**
Telecommunication Assurance	Only one professional standard	N/A
Process & TTM	Simple processes & 3-6 months	Complex processes & 12-18 months (EAL4+)

PP: Protection Profile; CC: Common Criteria

Figure 13. Comparison in general terms between NESAS and Common Criteria (CC).

On 24 August 2020, the GSMA announced that the world's leading mobile network equipment vendors, Ericsson, Huawei, Nokia and ZTE, had successfully completed an assessment of their

http://doi.org/10.18080/jtde.v8n4.340

product development and lifecycle management processes using the GSMA's NESAS (GSMA, 2020). The process audited, the products developed under the audited process, and a summary report for each vendor are reported in Figure 15.

NESAS Product Development & Lifecycle Audit		CC Product Development & Lifecycle Audit	
1	Security by design	ADV_ARC/FSP/HLD/LLD/ST	√
2	Version control system	ALC_CMC (on-site audit)	√
3	Change tracking	ALC_CMC (on-site audit)	√
4	Source code review	-	×
5	Security testing	ATE_COV/DPT/FUN	√
6	Staff education	-	×
7	Vulnerability remedy process	ALC_FLR (Flaw Remediation)	√
8	Vulnerability remedy independence	-	×
9	Information security management	ALC_DVS (Developer Security)	√
10	Automated build process	ALC_CMC (on-site audit)	√
11	Build environment control	ALC_CMC (on-site audit)	√
12	Vulnerability information management	-	×
13	Software integrity protection	ALC_DEL (Delivery with DS)	√
14	Unique software release identifier	ALC_CMC (CI Identification)	√
15	Security fix communication	-	×
16	Documentation accuracy	ALC_CMC (on-site audit)	√
17	Security point of contact	-	×
18	Source code governance	ALC_CMC (on-site audit)	√
19	Continuous improvement	ALC_CMC (on-site audit)	√
20	Security documentation	AGD_OPE/PRE	√

Test	Contents of equipment evaluation test	SCAS	CC
SCT (security compliance test)	Sensitive info. storage, transfer, protection during access to system, privacy protection (FDP/FCS/FPR)	√	√
	System overflow, secure start-up, robustness of data input, software integrity (FRU/FPT)	√	√
	Authentication (credential/password), token policy, account lock, principle of least authority (FIA)	√	√
	Log out, overtime auto protection (FTA)	√	√
	Security log, log rotate, log access authorization (FAU)	√	√
	Admin account, user account, IP/ICMP Process (FIA)	√	√
	https, web server log, session ID, input examination	√	√
	Message filtering, robustness of protocol, GTP-C/U filtering	√	√
	Security enhancement of baseline requirement	√	×
	OS Security enhancement	√	×
	Webserver Security enhancement	√	×
	Management/User plane separation (FDP/FPT)	√	√
	FCS (cryptographic algorithm implementation check, random number generator, etc.)	×	√
BVT (basic vulnerability test)	Port scan	√	√
	Known vulnerability scan	√	√
	Robust test for interface protocol	√	√
EVA (enhanced vulnerability analysis)	**Penetration test**	×	√
	Source code scan	×	√

Figure 14. Comparison in terms of technical requirements between NESAS and Common Criteria (CC).

Company	Month of Audit	Process Audited	Products Developed Under Audited Process	Summary Report
Huawei Technologies Co. Ltd.	March 2020	Huawei Integrated Product Development (IPD) – 10.0	LTE eNodeB and 5G gNodeB Product Lines	https://www.gsma.com/security/wp-content/uploads/2020/08/Huawei-RAN-NESAS-Audit-Report-Summary-Report-Mar-2020.pdf
Huawei Technologies Co. Ltd.	May 2020	Huawei Integrated Product Development (IPD) – 10.0	5G Core product line for UDG, UDM, UNC, UPCF	https://www.gsma.com/security/wp-content/uploads/2020/08/Huawei-RAN-NESAS-Audit-Report-Summary-Report-Mar-2020.pdf
Nokia Solutions and Networks Oy	May 2020	Nokia MN CREATE Process v18.3	LTE eNB (SRAN) and 5G gNB Products	https://www.gsma.com/security/wp-content/uploads/2020/08/Nokia-NESAS-Audit-Summary-Report-May-2020.pdf
Ericsson	June 2020	Ericsson DNEW Development Framework	eNodeB and gNodeB Product Lines	https://www.gsma.com/security/wp-content/uploads/2020/08/2-Ericsson-NESAS-Audit-Summary-Report-Jul-2020.pdf
ZTE Corporation	July 2020	High Performance Product Development (HPPD) Process 2017	5G NR and ZXUN USPP Product Lines	https://www.gsma.com/security/wp-content/uploads/2020/08/ZTE-NESAS-Audit-Summary-Report-Jul-2020.pdf

Figure 15. Audited process, audited products developed and summary report for all vendors (GSMA, 2020).

As described above, 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 the mobile industry*, because it has been developed following established practices and schemes that provide *trustworthy security assurance* (GSMA, 2020).

http://doi.org/10.18080/jtde.v8n4.340

Zero Trust Model

Zero Trust is a cyber security paradigm focused on security controls to prevent unauthorised access to data (resources) and services coupled with making the access control enforcement as grainy as possible, as defined in Rose *et al.* (2020). This could be achieved by policy enforcement of geo-location, and mandatory authentication and authorisation of peer entities to establish the needed verification. For instance, in 5G, each element should utilise a robust code signing stack at both the silicon and software layers, so that all the layers involved can be trusted (5G Americas, 2020b).

To achieve Zero Trust, operators need to adapt a default "deny all" mentality and start opening up network lanes and endpoints according to the least privileges principle.

This new paradigm will allow the replacement of hardware and software in the network — with low quality implementations — with physical and logical elements with substantially more trust built into the product(s) from the supply chain perspective.

Since Zero Trust is an iterative process, operators must put in place proper network operations – including in both centralised and distributed locations – to log and inspect all traffic across user, control and management planes; and, especially, monitor both virtual network (slice) and physical and infrastructure on an ongoing basis.

Zero Trust augments a *defence-in-depth security strategy* – also known as layered defence, where controls of various types and kinds overlap each other in coverage – and cannot be achieved without the full participation of all the elements in the trust chain for a network.

An example of the defence-in-depth approach augmented by a Zero Trust model for 5G security deployment, is shown in Figure 16 (Soldani, 2019). The 5G system supports:

- All 3GPP SCAS requirements and fundamental security control enhancements, such as, but not limited to, the following: user plane (UP) integrity protection, UP security policy, roaming security, user privacy preservation (encryption of international mobile subscriber identity), unified authentication and 256-bit encryption algorithm.
- Equipment security (3-plane isolation, data security, host intrusion detection and Trusted Execution Environment, TEE).
- Sub-solutions to Radio Access Network (RAN) security (e.g. rogue base station detection, secure transmission), Multi-Access Edge Computing (MEC) security (MEC platform hardening, MEC security operations, e2e encrypted local network), Core Network security (multi-layer isolation and hardening, disaster and elastic recovery), Network Slicing security (slice isolation, encryption and protection, differentiated slice security), and Massive Connectivity security (signaling domain anti-DDoS and date

http://doi.org/10.18080/jtde.v8n4.340

domain anti-DDoS).

- Security management, which includes an Element Management System (EMS) layer, for situational awareness, anomaly detection, trusted integrity measurements, certificate management, log auditing, and Network Element (NE) vulnerability management; and an end-to-end (e2e) Security Operation Centre (SOC), for security situational awareness, AI-based threat analysis and detection, security orchestration and Network Element (NE) vulnerability management.

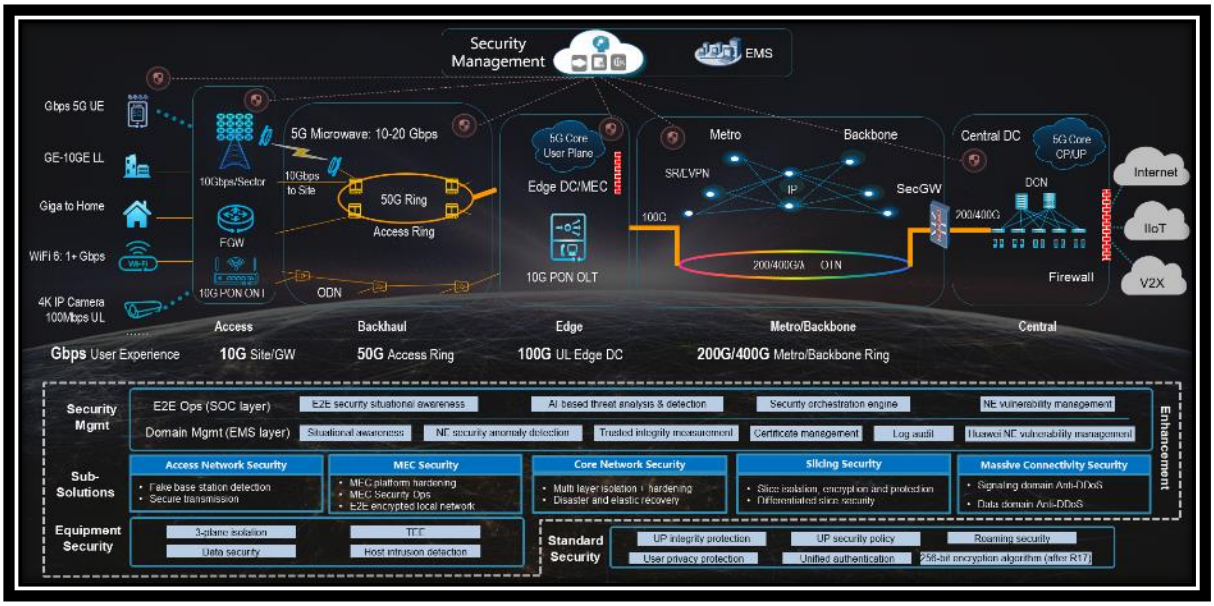


Figure 16. Example of defence-in-depth, Zero Trust, solution for 5G security deployment (Soldani, 2019).

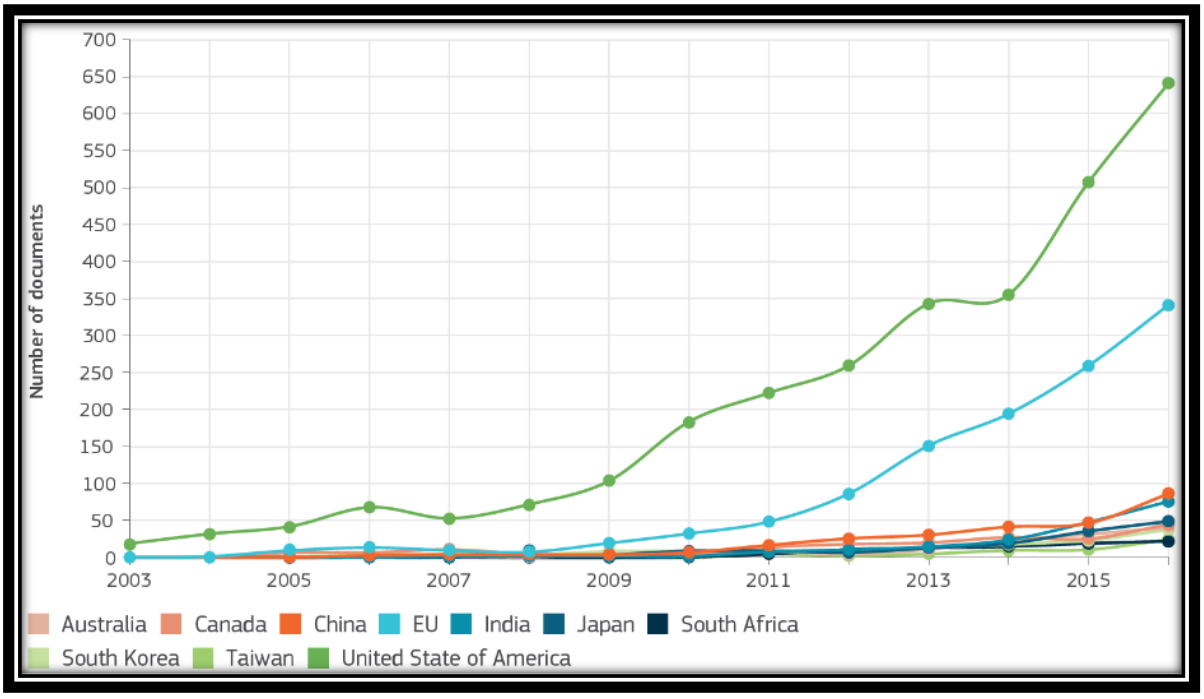


Figure 17. Scientific publications in cyber security per country (Joint Research Centre, 2020).

http://doi.org/10.18080/jtde.v8n4.340

Australia Competitiveness and International Collaboration

As presented in Joint Research Centre (2020), research and development are primary indicators of the liveliness and competitiveness of a sector and its capacity to stay abreast of a given field.

Analysis of the cyber-security scientific literature indicates that the USA leads scientific research in cyber security, with half the publications. The EU is in second place with a quarter of the total number of publications, while the remaining quarter aggregates the scientific production of all the remaining non-EU countries (dominated by China, Canada and Japan), as shown in Figure 17. The majority of publications are concentrated in the security management, network security, data security and privacy, and cryptography domains (Joint Research Centre, 2020).

An analysis of the collaboration networks (see Figure 18) shows how the USA is the EU's strongest partner as regards its overall scientific production in cyber security, followed by China and Canada.

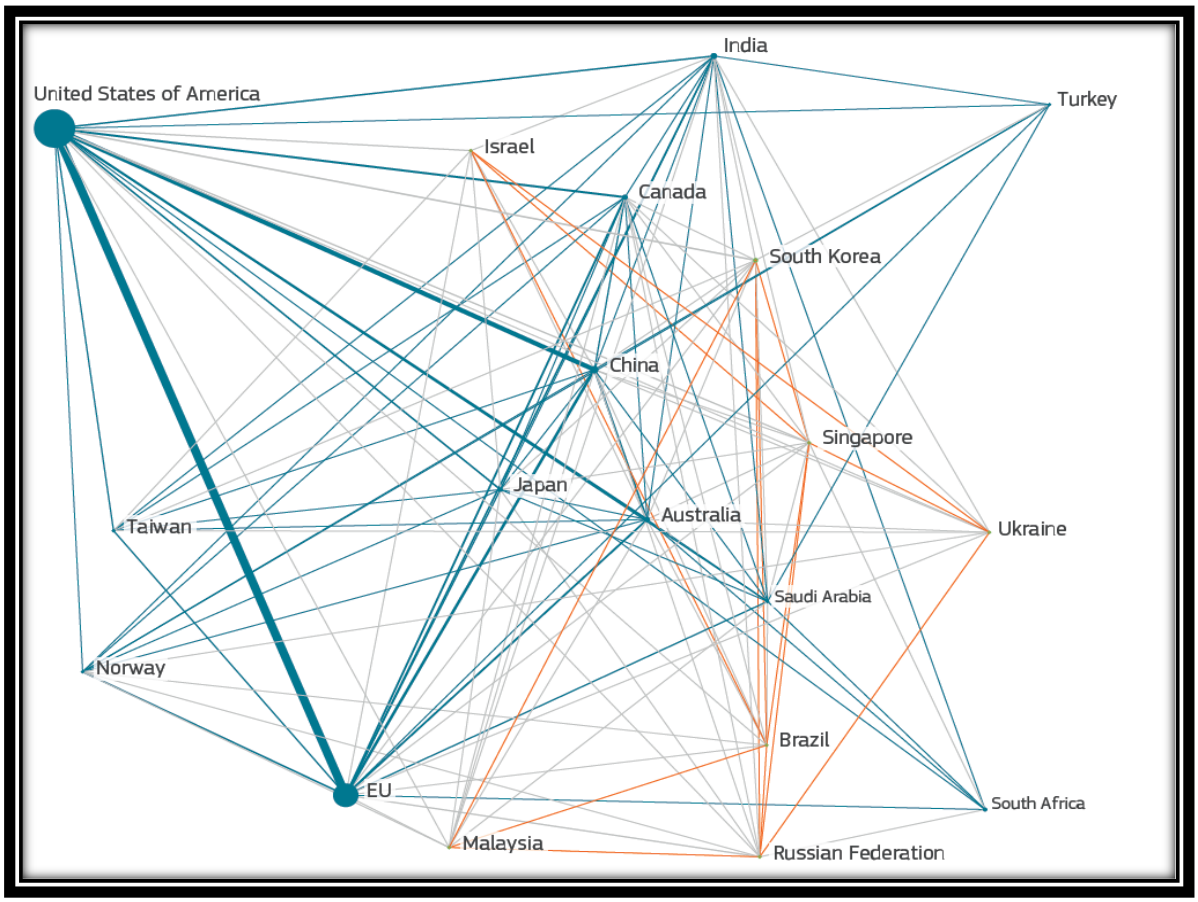


Figure 18. Country share of scientific publications in cyber security (size of nodes = number of projects, edge between nodes = project(s) in common, colours identify communities of countries collaborating more often) (Joint Research Centre, 2020).

http://doi.org/10.18080/jtde.v8n4.340

Figure 19 gives a picture of patents in the cyber security sector where patent filing is dominated by China, followed by the USA, while Australia does not have a prominent position (Joint Research Centre, 2020).

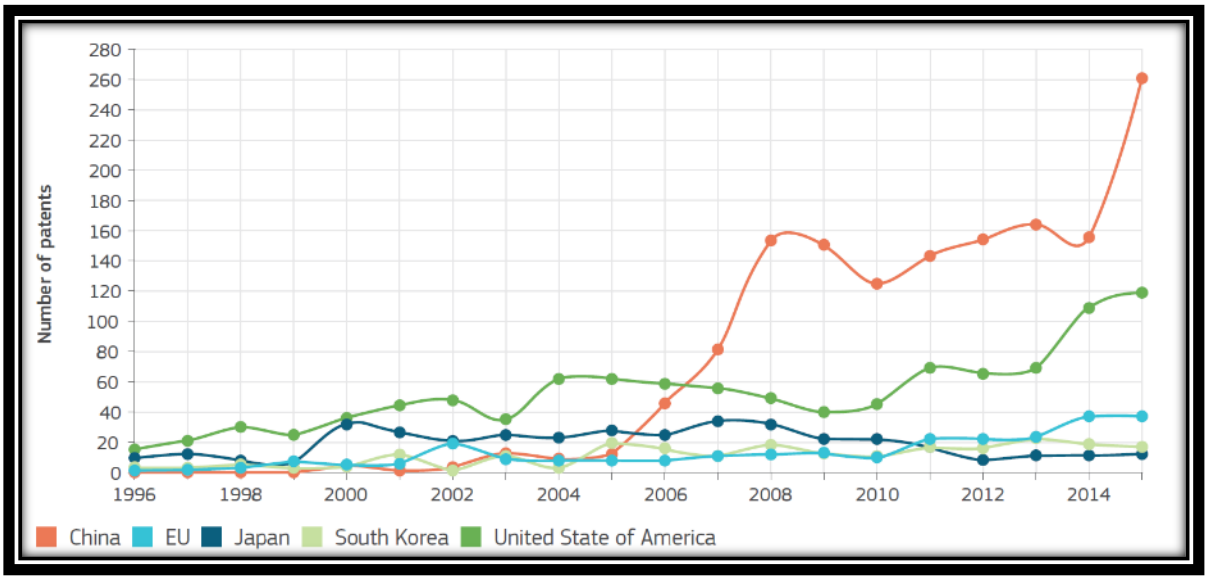


Figure 19. Patents in cyber security per country (Joint Research Centre, 2020).

The overall picture provided by this analysis shows that the Australian research landscape could be much more vibrant, productive and recognised at the global level. This could be improved by:

- Strengthening and enlarging the collaboration of cyber security research organisations across States/Territories and with the European Commission.
- Streamlining and stabilising the R&D cooperation between industry and academia.
- Better coordinating research funding across Australia and involvement in Horizon Europe[vi] – an ambitious €100 billion research and innovation program to succeed Horizon 2020.
- Co-designing research plans between funding bodies and recipients.
- Supporting the sharing of highly expensive infrastructures (in an Open Laboratory Initiative approach).
- Setting up an Australian Cybersecurity Industrial, Technology and Research Competence Centre and a Network of National Coordination Centres, aiming to create a more collaborative and synergetic Australian cyber security competence ecosystem.

Discussion and Recommendations

The Australia's 2020 Cyber Security Strategy (Australian Government, 2020b) has been recently unveiled and, while it delivers a reasonable foundation on which to build, there is still clearly much work to be done to deliver a truly comprehensive strategy for Australia (Moore, 2020).

http://doi.org/10.18080/jtde.v8n4.340

A huge amount of work went into crafting this strategy with recommendations being delivered from many public and private organisations and individuals. Some of the key recommendations from the Industry Advisory Panel (Industry Advisory Panel, 2020), led by Andy Penn, Telstra CEO, were incorporated into the new 2020 Cyber Security Strategy. This includes, but is not limited to, the following:

- Strengthening the pipeline of skilled cyber security professionals.
- Clearly defining all critical infrastructure and systems of national significance.
- Appointing an Industry Advisory Committee to guide the Government on cyber security, including on implementation of current recommendations.

Yet, experts bemoan a lack of detail in the "what" and "how" of the cyber strategy (Smith, 2020). For example, some of the most important recommendations of the Industry Advisory Panel that would need further consideration are:

- Proactive mitigation strategies and strengthening of systems essential for end-to-end resilience of critical infrastructures.
- Measures to build trust in technology markets through transparency, such as product labelling.
- Promoting international law and increase operational-level cooperation with international partners.
- Getting major vendors to sign up to a voluntary 'secure by design' charter to leverage international best practice.
- Working with industry to increase Australia's role in shaping international cyber security standards.
- Encouraging diversity, transparency and competition in digital supply chains.
- Accelerating the adoption of appropriate standards to ensure digital products and services are 'secure by design'.
- Implementing a dynamic accreditation or mandatory cyber security labelling scheme.

We recommend that the Department of Foreign Affairs and Trade works closely with the European Commission (EC) and other Member States, and their partner cyber security agencies – such as the EU Agency for Network and Information Security (ENISA), the Federal Cyber Security Authority in Germany (BSI) and the National Cybersecurity Agency of France (ANSSI) – and establishes a close collaboration with international industry partners – such as the 3rd Generation Partnership Project (3GPP) and GSMA Mobile for Development Foundation (GSMA) – on 5G *security specifications* (3GPP, 2020c) and *network equipment security assurance scheme* (GSMA, 2020).

http://doi.org/10.18080/jtde.v8n4.340

This will make it possible for Australia to:

1. Promote *market forces*, risk-informed procurement *requirements* for assurance and transparency and development of supplier-focused minimal industry *practices* to meet those requirements.
2. Deliver a consistent set of *regulations* and additional recommended *practices* to address 5G security that allow the corresponding stakeholders to take responsibility and action for its overall implementation, and adhere to the principle of openness and transparency.
3. Show willingness to explore strategic and fundamental solutions with all relevant stakeholders and establish *flagship projects* aimed at attesting how 5G commercial products can leverage cyber security standards and recommended practices for relevant 5G use cases and scenarios, as well as showcase how 5G security features can be properly utilised.

This *iterative approach* will provide the indispensable *flexibility* to take advantage of newly introduced 5G security capabilities to deliver proper *cyber security practice guides* with the necessary standard of quality for their intended use.

Furthermore, the Australian Government and private sector should collaborate with the following organisations and promote:

1. *Recommendations* from the Global Commission on the Stability of Cyberspace (Global Commission, 2019), which builds on, e.g., UN work on norms.
2. *Contributions* of the Global Forum on Cyber Expertise (GFCE, 2020) for cyber capacity building and support for Confidence Building Measures (CMB).
3. The Commission *recommendations* from November 2019 (Global Commission, 2019) and the recommendations of the Paris Call in 2020 (Paris Call, 2020).

In order to realise this vision in Australia, the Federal Government should establish a close collaboration with international industry partners, such as the 3rd Generation Partnership Project (3GPP) on 5G security assurance specifications (SCAS) and GSMA Mobile for Development Foundation (GSMA) on network equipment security assurance scheme (NESAS) (GSMA, 2020).

The Australian Federal Government should be a major player among those organisations, support the continuous evolution of the 3GPP 5G technical specifications with evolving usage scenarios, adopt the GSMA NESAS/3GPP SCAS for testing and evaluating telecoms equipment, and enforce a certification and accreditation process (Industry Advisory Panel, 2020), against a predetermined set of security standards and policies, for security authorisation in Australia.

http://doi.org/10.18080/jtde.v8n4.340

Furthermore, we advocate for a *Zero-Trust approach* to developing a Cyber Security framework – everything and every element should be checked and vetted thoroughly, no matter where it comes from (Soldani, 2020).

Our position is that adopting a Zero-Trust model can not only enhance security for existing 5G networks but also provide the framework for security architectures, as detailed by 5G Americas, in their recent white paper on "Security Considerations for the 5G Era" (5G Americas, 2020b).

5G brings about virtualisation, slices on private cloud, public cloud, and hybrid models, including data centres located even in different jurisdictions. This concept of "*5G without borders*" could bring security concerns and the Zero-Trust model may mitigate them to an acceptable level.

Zero Trust ensures that security is in place from untrusted domains (e.g., supply chain, Internet, user devices, other operators and partners) to and from within trusted domains (carrier networks).

Also, the Zero-Trust model meets the ETSI baseline requirements of cyber security for the IoT (ETSI, 2020).

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. (2020c). 3GPP Security Technical Specification 33 series. Retrieved from https://www.3gpp.org/DynaReport/38-series.htm

5G Americas. (2020a). The 5G Evolution: 3GPP Releases 16 and 17. Retrieved from https://www.5gamericas.org/wp-content/uploads/2020/01/5G-Evolution-3GPP-R16-R17-FINAL.pdf

5G Americas. (2020b). 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

Australian Government. (2019). Australia's 2020 Cyber Security Strategy. Retrieved from https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/cyber-security-strategy-2020

Australian Government. (2020a). Call for Submissions: Cyber and Critical Technology International Engagement Strategy (CCTIES). Retrieved from https://www.dfat.gov.au/news/news/call-submissions-cyber-and-critical-technology-international-engagement-strategy-ccties

http://doi.org/10.18080/jtde.v8n4.340

Australian Government. (2020b). Australia's Cyber Security Strategy 2020. Retrieved from https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf

Bartock, M., Cichonski, J., & Souppaya, M. (2020). 5G Cybersecurity – Preparing a Secure Evolution to 5G. National Institute of Standards and Technology (NIST). Retrieved from https://csrc.nist.gov/publications/detail/white-paper/2020/02/20/5g-cybersecurity-preparing-a-secure-evolution-to-5g/draft

Barton, A. (2020). Australian Cyber Security. Retrieved from https://eu.eventscloud.com/file_uploads/bbdd9c6962871568b3397cef0e43022a_TheStateofCyberSecurityUKandAustraliaWebinarSlides20200916.pdf

Batas, S., Men, M., & Smitham, M. (2020). Towards a Trustworthy Foundation to Enhance the Security of EU 5G Networks. *Huawei White Paper*. Retrieved from https://huawei.eu/story/trustworthiness-and-security-foundations-eu-5g

Bundesnetzagentur. (2020). Catalogue of security requirements for the operation of telecommunications and data processing systems and for the processing of personal data. Retrieved from https://ec.europa.eu/growth/tools-databases/tris/de/search/?trisaction=search.detail&year=2020&num=496

CGTN. (2020). China to build 600,000 5G bases in 2020 despite COVID-19 impact. Retrieved from https://news.cgtn.com/news/2020-06-06/China-to-build-600-000-5G-base-stations-in-2020-R65gk7tJcs/index.html

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

ETSI. (2020). Cyber Security for Consumer Internet of Things: Baseline Requirements. ETSI EN 303 645 V2.1.0. Retrieved from https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.00_30/en_303645v020100v.pdf

ENISA. (2019). Annual Report Telecom Security Incidents 2018. EU Cybersecurity Agency report. Retrieved from https://www.enisa.europa.eu/publications/annual-report-telecom-security-incidents-2018

European Commission. (2017). EU cybersecurity initiatives working towards a more secure online environment. Retrieved from https://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf

European Commission. (2019a). EU-wide coordinated risk assessment of 5G networks security. Retrieved from https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security

European Commission. (2019b). Connectivity for a Competitive Digital Single Market – Towards a European Gigabit Society. Retrieved from https://ec.europa.eu/digital-single-market/en/news/communication-connectivity-competitive-digital-single-market-towards-european-gigabit-society

http://doi.org/10.18080/jtde.v8n4.340

European Commission. (2019c). Commission Recommendation – Cybersecurity of 5G Networks. Retrieved from https://www.europeansources.info/record/recommendation-on-cybersecurity-of-5g-networks/

European Commission. (2019d). Cybersecurity Act – ENISA and Cybersecurity Certification Framework. Retrieved from https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act

European Commission. (2019e). The EU Cybersecurity Act. Retrieved from https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act

European Commission. (2020a). Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures. Retrieved from https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

European Commission. (2020b). On Artificial Intelligence – A European approach to excellence and trust. Retrieved from https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

Global Commission. (2019). Advancing Cyberstability. Final report. Retrieved from https://cyberstability.org/report/

Global Forum on Cyber Expertise (GFCE). (2020). Strengthening cyber capacity and expertise globally through international collaboration. Retrieved from https://thegfce.org/

GSA. (2020a). 5G Market Snapshot Member Report – August 2020. Retrieved from https://gsacom.com/technology/5g/

GSA. (2020b). 5G Devices: Executive Summary – August 2020. Retrieved from https://gsacom.com/technology/5g/

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/

Huawei. (2019). Huawei Technologies (Australia) submission to the Department of Home Affairs – Australia's 2020 Cyber Security Strategy Discussion Paper. Retrieved from https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-strategy-2020/submission-39.pdf

Industry Advisory Panel. (2020). Industry Advisory Panel Report. Retrieved from: https://www.homeaffairs.gov.au/cyber-security-subsite/files/2020-cyber-security-strategy-iap-report.pdf

Joint Research Centre. (2020). Cybersecurity – Our digital anchor. Science for Policy report by the Joint Research Centre (JRC), the European Commission's science and knowledge service. Retrieved from https://ec.europa.eu/jrc/en/facts4eufuture/cybersecurity-our-digital-anchor

http://doi.org/10.18080/jtde.v8n4.340

Moore, N. (2020). Interview with Malcolm Shore: cyber security veteran, online educator and former AISA board member. Retrieved from: https://www.aisa.org.au/Public/News_and_Media/Thought-Leadership-Library/Malcom-Shore-on-cyber-security-strategy-and-IoT.aspx

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/

Paris Call. (2020). Ensuring international cyberspace security. Retrieved from https://pariscall.international/en/

Rose, S., Borchert, O., Mitchell, S., & Connelly S. (2020). Zero Trust Architecture. National Institute of Standards and Technology (NIST), Special Publication 800-207. Retrieved from: https://www.nist.gov/publications/zero-trust-architecture

Singapore Cyber Security Agency (CSA). (2020). Singapore's safer cyberspace masterplan 2020 Retrieved from https://www.csa.gov.sg/news/publications/safer-cyberspace-masterplan

Smith, P. (2020). Experts bemoan lack of detail in cyber strategy. *Australian Financial Review*. Retrieved from https://www.afr.com/technology/experts-bemoan-lack-of-detail-in-cyber-strategy-20200806-p55j7m

Soldani, D. (2019). 5G and the Future of Security in ICT, *IEEE ITNAC, Auckland, NZ*. Retrieved from https://ieeexplore.ieee.org/Xplore/home.jsp

Soldani, D. (2020a). Australia's Cyber Security: Still more work to do. Retrieved from https://huaweihub.com.au/australias-cyber-security-still-more-work-to-do/

Soldani, D. (2020b). Introduction to 5G and the path to 6G. Webinar at AWISE 2020. Retrieved from https://www.youtube.com/watch?v=D4pi1Z821fw

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., 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. (2020). New Network Architecture for 6G. What next for wireless infrastructure Summit 2020. Retrieved from: https://www.youtube.com/watch?v=L4VXGQy-mQQ

US Department of Defense (DoD). (2020). 5G Strategy. Retrieved from https://www.defense.gov/Explore/News/Article/Article/1844423/dod-develops-secure-5g-mobile-telecommunication-network-strategy/

Endnotes

[i] This is true for data in use, at rest and in motion (transit). It also applies to any system and technology – such as AI, Cloud, IoT, 5G, 6G and beyond – used for processing, transmitting, manipulating and/or storing that data.

[ii] https://marketplace.service.gov.au/

[iii] https://www.business.gov.au/Grants-and-Programs/Cooperative-Research-Centres-CRC-Grants

[iv] https://www.dst.defence.gov.au/NextGenTechFund

[v] https://a3c.co/

[vi] https://ec.europa.eu/info/horizon-europe-next-research-and-innovation-framework-programme_en

http://doi.org/10.18080/jtde.v8n4.340