Cyber and Critical Technology International Engagement Strategy (CCTIES)

Huawei Australia submission to the
Department of Foreign Affairs and Trade

16 June 2020

Dr David Soldani
Huawei Technologies

Contents

HUAWEI

Abbreviations

ANSSI	National Cybersecurity Agency of France
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIMM	Building Security in Maturity Model
BSZ	Beschleunigte Sicherheitszertifizierung
CC AVA	Common Criteria vulnerability assessment Class AVA
CIA	Confidentiality, Integrity and Availability (CIA triad)
CIoT	Consumer IoT
CPA	Certified Public Accountant
CSPN	Certification de Sécurité de Premier Niveau
DDoS	Distributed Denial of Service
EC	European Commission
ENISA	European Union Agency for Network and Information Security
GSMA	GSM Association
ICT	Information and Communication Technology
IEEE	Institute of Electrical and Electronics Engineers
ILAC	International Laboratory Accreditation Cooperation
IoT	Internet of Things
IIoT	Industrial IoT
ISO	International Organization for Standardization
MSDL	Military Scenario Definition Language
NCSC	National Cyber Security Centre of UK
NESAS	Network Equipment Security Assurance Scheme
NIS CG	Network and Information Security Cooperation Group
NIST	National Institute of Standards and Technology
OWASP	Open Web Application Security Project
SAMM	Software Assurance Maturity Model
SCAS	Security Assurance Specifications
SDO	Standards Development Organization
SE	Secure Elements

Introduction

Huawei welcomes the opportunity to provide this submission in response to the Department of Foreign Affairs and Trade call for submissions on the development of Australia's Cyber and Critical Technology International Engagement Strategy (CCTIES) (Australian Government, 2020).

The Government requested 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 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 questions 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*. This document sheds light on the *technical development of a cyber space* and Huawei Technologies is willing to collaborate with the Department and contribute to it, in order to achieve the objectives and realise the vision for Australia, as presented in the following sections.

HUAWEI

Objectives, values and principles

Australia should further strengthen its approach by including cybersecurity – ensuring Confidentiality, Integrity and Availability (CIA) of information[1] that requires security – at the heart of its political, economic and safety priorities: *trust*, *security* and *fight against cybercrime* should be at the core of the new Australia's 2020 Cyber Security Strategy to meet the rapidly evolving cyber threat environment (Australian Government, 2019).

In order to realise this vision the Department of Foreign Affairs and Trade should take, but not limited to, the following actions (European Commission, 2017):

A. *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.

B. *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, transparency; and respects fundamental human rights including the right to privacy, taking advantage of the booming global cybersecurity market.

C. *Pursue a collaborative and information sharing, risk-management framework that provides an objective and transparent basis for knowing which products and services are worth of trust*, in particular with regard to new 5G technologies and emerging sectors such as Artificial Intelligence (AI), Cellular Vehicle to X (C2X), Internet of Things (IoT), Industrial IoT (IIoT) and Consumer IoT (CIoT) (5G Americas, 2020), (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.

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

Cyberspace and critical technology

Devices and system 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, 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 CIoT 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, healthcare, and government. 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. In short, 5G deployment will enable a *new generation of 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 (US Department of Defense, 2020), as 5G systems and related capability enable digitised government and industry.

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 than cyber security in the past:

- *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.

As we speak, 386 operators in 125 countries are investing in 5G, and 81 carriers in 42 countries have already launched one or more 5G services (GSA, 2020). In little more than six months, China will have more than doubled its number of 5G base-stations and will

have a staggering 600,000 5G operational nodes. There are already some 36 million 5G end-users in the Chinese market just one year after 5G spectrum licenses were allocated (CGTN, 2020).

The key thing to remember, when we think of 5G, *although its architecture is well set in stone* (Soldani, et al., 2018), it is a technology that is *constantly evolving and will continue to evolve over the next decade* or so until we hit 6G (Nokia, 2020), (Ericsson, 2020).

Indeed, the second phase of 5G is currently being finalised in 3GPP, with the Rel-16 version of technical specifications (3GPP, 2020a). Also, the features to be included in Rel-17 (3GPP, 2020b) have been already agreed and scheduled for completion by the end of 2021.

The first 5G release (Rel-15) has addressed predominantly the immediate needs of enhancing the mobile broadband experience, but the Rel-16 and Rel-17 take 5G toward the full 5G vision, balancing the needs of mobile broadband operators with expansion into new markets including vertical players.

3GPP Release 16 is the foundation for the Industrial IoT, supporting (3GPP, 2020a): Ultra-Reliable Low-Latency Communications (URLLC) with the ability to achieve unprecedented levels of reliability, down to packet error rates of 10^{-6} ("six nines"); integration with IEEE Time-Sensitive Networking (TSN); Private Networks (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 UE with USIM card; and 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); and vehicular communication ("V2X"), featuring a *sidelink* for direct communication between devices. Beyond this, it supports Full 5G System Resilience with security features for service-based interfaces (SBI), Transport Layer Security (TLS) and Token-based authorization; Wireless-Wireline Convergence (WWC); Future Railway Mobile Communication System (FRMCS – Phase 2); Network Slice-Specific Authentication and Authorization (NSSAA), which allows a third party to add, remove users to and from a network slice instance; Network Automation Phase

2; Integrated Access & Backhaul (IAB); Device Power Saving; Mobility Enhancement; and Enhanced MIMO with multiple Transmission and Reception Points (TRP).

3GPP Release 17 targets a wider ecosystem expansion, supporting (3GPP, 2020b): native Time Sensitive Communication (TSC); High-Accuracy Positioning (cm-level); Sidelink enhancement for public safety and pedestrians; Multicast; Non-Terrestrial Networks (Satellite and HAPS); FRMCS enhancements (FRMCS – Phase 3; 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.

So, once we get to Rel-16 and Rel-17 then we will see an expansion of the ecosystem that can take advantage of 5G, by adding many features to provide the full range of functionality required by new industry segments, as well as making 5G networks easier to deploy and operate, end to end. Indeed, further down the track the next 5G progression of Rel-18 and beyond will meet the needs of new market opportunities and deliver huge value for much of the present decade.

However, 5G technologies present several security challenges due to their innovative, software-driven nature and its use in a wide range of services and applications (Batas, 2020), as discussed in the above sections. Challenges exacerbated by the fact that we are becoming increasingly dependent on the confidentiality, integrity and availability (CIA triad) of data.

On 9th October 2019, the EU Network and 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 capabilities (resources) and intention/attempt (motivation):

- *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/subcontractor, and associated with an *organized crime group*.

- Most critical 5G assets: *Core Network Functions (5G Core), Network Function Virtualisation (NFV) and Management and Orchestration (MANO)*.

In Europe, the European Commission, the Member States and corresponding cyber security agencies are working together with Communication Service Providers (CSPs, operators) and technology suppliers (vendors) in order to provide continuity of mobile network services while managing potential risks and concerns relating to these mobile networks and their underlying technologies, and detailed in the following sections.

Greatest risk and/or opportunities

Shared responsibility for risk management (information and communication service providers, on the one hand, and equipment and third-party suppliers, on the other); leverage *market forces* to drive greater assurance and transparency; risk informed *procurement requirements* for buyers of ICT; encourage telecom equipment suppliers to develop *minimum industry standards* for assurance and transparency; the need to support *conformance programmes* and *independent testing*; and *effective risk mitigation plans* are necessary to address current and new emerging threats as much as possible, as there is no such thing as 100% assurance event for other essential services besides telecommunications (Batas, 2020).

5G will progressively support essential services and demand for a greater *cross-sector collaboration* than exclusively within the telecommunications field between operators and suppliers so building trust in cyberspace is another important requirement (Batas, 2020), (European Commission, 2020b).

However, trust goes beyond technical or operational measures and requires a dialogue between nations to set up *diplomatic norms* for acceptable state and state-sponsored behaviour in the 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*.

It is of vital importance that the Department and its agency partners, especially the Australia Cybersecurity Centre (ACSC), 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; have specific and prioritized outcomes, and deliverables, for this engagement, 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, as discussed in the following.

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

To address the challenges to enhance cyber security, the European Union Agency for Network and Information Security (ENISA) published the analysis of the incident reports that the organization has been collecting from all Member States (including UK) and consolidating since 2012 (ENISA, 2019).

- *System failures* are the most common root cause, 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 categorized 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.

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, use market forces to incentivise greater assurance and transparency, to address 5G security that allow operators to take responsibility for the overall implementation (Huawei, 2019).

Government, industry, civil society and academia cooperation

The Department should ensure cooperation with the European Commission (EC) and other Member States, their partner cybersecurity agencies – such as ENISA, the Federal Cyber Security Authority in Germany (BSI) and the National Cybersecurity 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 Group*", in order to support and facilitate strategic collaboration and exchange of information between

partners and promote a swift and effective operational cooperation on specific cybersecurity incidents and sharing information about identified threats and vulnerabilities.

To this end, it is important to obtain support from all telecommunications suppliers and service providers in relevant industry sectors, in order to enable a much greater accountability of cyber incidents (Bartock, 2020).

It also requires a broad and *well-trained workforce*. 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, design, develop and operate advanced technologies for 5G, 6G and beyond.

Policies and frameworks in other countries

Ensuring cybersecurity throughout international collaboration and finding a balance between technology integration, human capital investments and 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. And even more is needed in the years to come, as service applications based on the IoT, 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 *cyber space* and for reaping the full benefits that 5G will have to offer for people and businesses and government services.

The "*Recommendation on Cybersecurity of 5G Networks*" (European Commission, 2019c), "*Cybersecurity Certification Framework*" (European Commission, 2019d), and "*Connectivityfor a Competitive Digital Single Market - Towards a European Gigabit Society*" (European Commission, 2019b) are examples of relevant policies directed at improving the security and ensure future prosperity of all member states (including UK) in Europe, and gain trust from people, homes and organizations 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 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 Cybersecurity 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 Cybersecurity Act*" establishes an *EU certification framework for ICT digital products, services and processes* that enables the creation of *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 schema for ICT products exist in the EU, and globally. But, without a common framework for a *global valid cybersecurity 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 cybersecurity 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).

To express the cybersecurity 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 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 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 setup an *EU 5G regulatory framework*, in cooperation with the industry, as detailed in the next section.

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 *security evaluation scheme* for network equipment, using the 3GPP defined security specifications and test cases, i.e., 3GPP SCAS (3GPP, 2020c).

Figure 1 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 2):

- 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.
- Level of security of network equipment is tested and documented. (Tests are conducted by accredited test laboratories.)

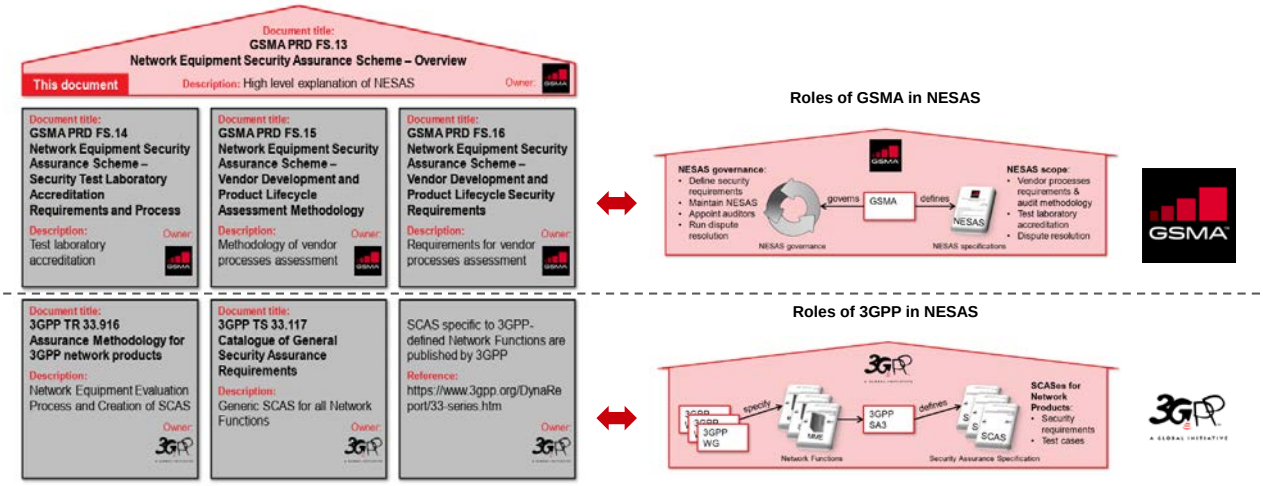


Figure 1. 3GPP and GSMA deliverables, roles and work split (GSMA, 2020).

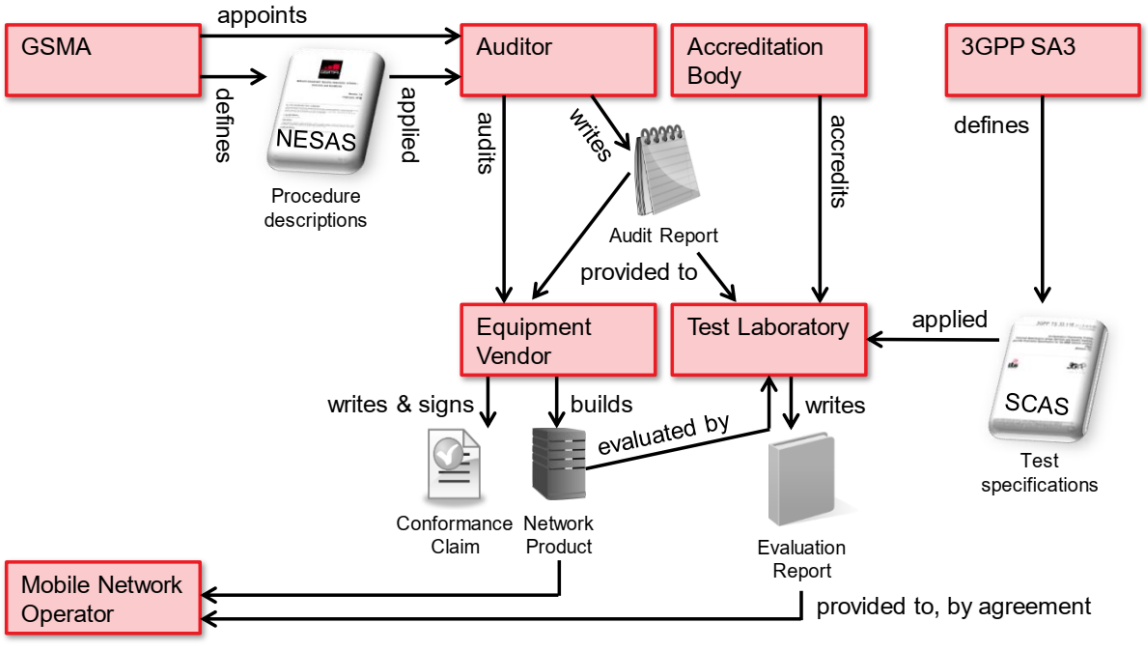


Figure 2. NESAS high level process (GSMA, 2020).

HUAWEI

Figure 3 illustrates the many public and private organisations involvement 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 organizations, 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 cybersecurity certification framework for mobile network equipment, and more than ten operators have requested NESAS compliancy, before deploying 5G equipment in their countries.

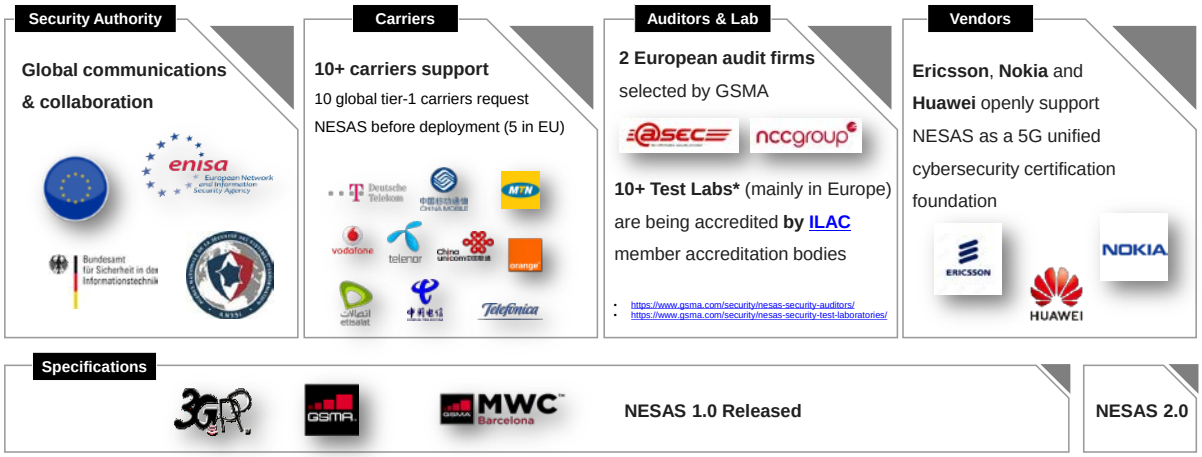
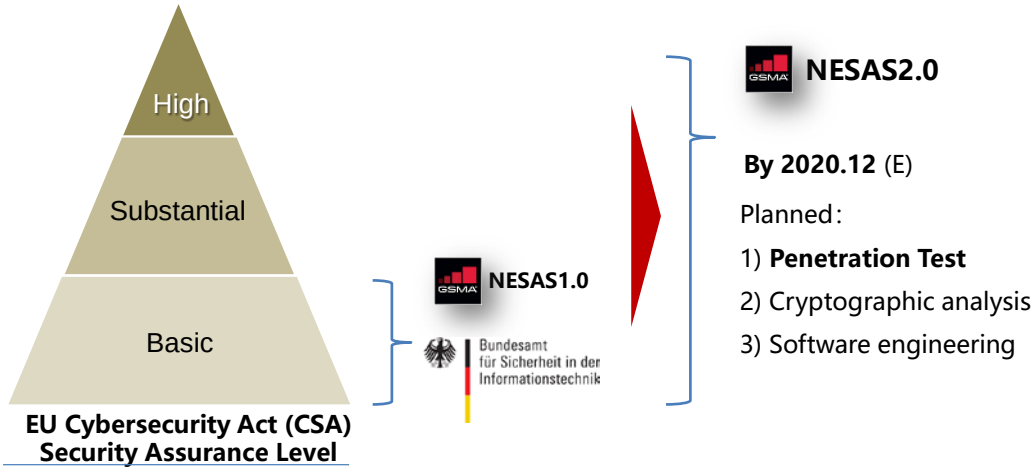


Figure 3. NESAS process widely supported by security authorities and industry organizations, globally.

GSMA appoints the Audit Firms and recognizes 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.



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 4. NESAS Evolves as a solid security assurance basis.

The NESAS 1.0 framework was approved in October 2019. It consists of the specifications depicted in Figure 1.

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 encompass: *Penetration Tests*, *Cryptographic Analysis* and *Software Engineering*, as exemplified in Figure 4, in alignment with the best industry standards and practises, as depicted in Figure 5.

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, digitization, 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, also suffering 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 6 and Figure 7, 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 5. NESAS Evolves according to the EU CSA, NIS-CG, etc. 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 6. NESAS vs. CC: Comparison in general terms.

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 7. NESAS 1.0 vs. CC (EAL4): Comparison in terms of technical requirements.

Conclusions

We recommend that the Department of Foreign Affairs and Trade works closely with the European Commission (EC) and other Member States, their partner cybersecurity 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).

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.

HUAWEI

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 cybersecurity standards and recommended practices for relevant 5G use cases and scenarios, as well as showcase how 5G security features can be properly utilized.

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

Furthermore, the Australian Government and private sector should collaborate with the following organizations 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 (European Commission, 2019c) and the recommendations of the Paris Call in 2020 (Paris Call, 2020).

The Australian Government should be a major player among those organisations, and support the continuous evolution of the 3GPP 5G technical specifications with evolving usage scenarios and the importance of conformance/testing programmes, including the NESAS for telecom equipment (GSMA, 2020).

Huawei is willing to collaborate with governments, security agencies, regulators and other relevant public and private organizations to embed trust in all business processes, Telecoms supply chain, and enhance cybersecurity through research and innovation at global scale.

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. (2020.) 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

Australian Government. (2020.) 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

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

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

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

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

HUAWEI

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

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. (2020.) 5G Market Snapshot Member Report – June 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

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/

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; Shore, M; Mitchell, J; & Gregory, M. (2018.) The 4G to 5G Network Architecture Evolution in Australia. The Australian Journal of Telecommunications and the Digital Economy (AJTDE), Vol. 6, No. 4. Retrieved from https://jtde.telsoc.org/index.php/jtde/article/view/161

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/

HUAWEI

Biography

Dr David Soldani received a *M.Sc. degree*, Laura Vecchio Ordinamento, in Electronic Engineering with *magna cum laude* from Università degli Studi di Firenze, Italy, in 1994; and a *D.Sc. degree* in Technology with *distinction* from Helsinki University of Technology (Aalto University), 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, and University of New South Wales, Australia, respectively. In EU, he is qualified and authorized to exercise his profession in *Civil* and *Environmental*, *Industrial* and *Information* sectors. Dr. Soldani has been active in the information and communication technology (ICT) industry for more than 20 years, successfully working on 500+ research, innovation and customer services projects for 2G, 3G, 4G and 5G ICT systems and services, and contributing to 1000+ quality deliverables – from strategic research and innovation strategies, business and work plans formulation to modelling, simulations, emulations and proof of concepts of innovative solutions, products and services with partners and customers. From 1997 to 2006 he was at Nokia in various technical and research management positions. From 2007 to 2009 he served at Nokia Siemens Networks (NSN) as Head of Customer Networks & Solutions and Solutions & Services Innovation functions, Research Technology & Platforms (RTP), Munich, Germany. In this role, he was responsible for "driving the alignment between the RTP research portfolio, the NSN Network Architecture Vision and Technology Strategy, and future customer needs", and leading innovative research projects for improving fixed-mobile broadband solutions and services. Prior to joining Nokia, he was a research engineer at Rohde & Schwarz (R&S) and Sirti S.p.A., in Milan, Italy, and officer (lieutenant) at the Italian Military Navy, Livorno, Italy. From Feb 2009 to Aug 2016, he worked at Huawei European Research Centre (ERC), Munich, Germany, as Head of IP Transformation Research Centre (IPTRC), Head of Network Solution R&D (NSD) and, subsequently, Head of Central Research Institute (CRI) and VP Strategic Research and Innovation, in Europe; and represented Huawei in the Board of Directors of The 5G PPP Infrastructure Association (5G-IA) and NetWorld2020 European Technology Platform (ETP), in Europe. He then rejoined Nokia, and served as Head of 5G Technology, End to End, Global, until Mar 2018. He is currently back at Huawei Technologies, serving as Chief Technology Officer (CTO) and Cyber Security Officer (CSO), in Australia, and as ICT Expert at Huawei ASIA Pacific region, in Malaysia. Areas of his responsibilities and expertise include, but not limited to: *future wireless, network, big data value, IoT, artificial intelligence, cyber security, and multimedia technologies*. He has been selected many times to receive special awards in recognition of his role, commitment, professionalism, and outstanding contribution in the ICT industry; and, in 2016, he was granted a Distinguished Talent (DT) visa for his profession by the Australian Government. He has published or presented many international papers, contributed to standards and publication of many books, and holds several international patents. Since 2009, Dr. Soldani has been serving as Associate Editor in Chief (AEiC) of IEEE Network Magazine, and Guest Editor of IEEE Communications Magazine and IEEE MMTC E-Letters. He has taken part in a number of IEEE Technical Program Committees (TPC) for international conferences, journals, magazines and workshops, especially in areas of future wireless, network, computing and media technologies.