GSMA 5G Cybersecurity Knowledgebase & NESAS Whitepaper

(November 22)

Contents

1. Progress of 5G Cybersecurity Standardization

GSMA, the global industry organization for mobile network operators, in May 2021,released the 5G Cybersecurity Knowledge Base. The purpose of this Cybersecurity Knowledge Base is to help stakeholders manage risks in the 5G ecosystem. This release comes in the wake of a number of publications in recent years related to 5G security in Europe, including but not limited to the NIS directive, the EU Cybersecurity Act, the EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks, the ENISA Threat Landscape for 5G networks, the Network Equipment Security Assurance Scheme (NESAS), the 5G Toolbox and others. And as members of the GSMA are working on implementing all the different security requirements and recommendations, the GSMA 5G Cybersecurity Knowledge Base has been built to serve as a guide to help view these documents as a whole.

As depicted below in Fig. 1; 5G faces security challenges and opportunities brought by new services, architectures, and technologies, as well as higher user privacy and protection requirements. The industry needs to understand the requirements of diversified scenarios and better define 5G security standards and technologies to address the associated risks. Hence, 5G cybersecurity is a shared responsibility that involves key stakeholders including MNOs, interconnection providers, vendors, application developers, service providers and governments, each with a clearly defined set of responsibilities which (when fully met) can enable the deployment and operation of 5G systems in a secure manner.

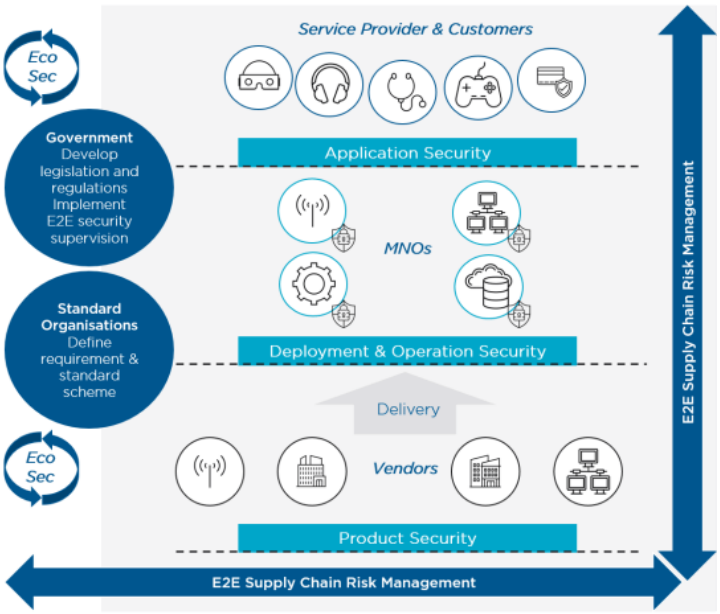


Fig. 1 - Cybersecurity – A Shared Responsibility

The GSMA believes 5G security risks can be addressed through the deployment of coordinated and verifiable security measures based on common standards. The standards provide a solid security foundation and they need to be continuously reviewed and updated to reflect the latest security research and newly identified attack vectors. In addition, MNOs need to constantly evaluate their individual risk and adjust their protections in accordance with the latest mitigation measures and their specific needs.

Standardization of 5G security is important for many reasons. To ensure that the various stakeholders are able to benefit from each other's expertise, to create a common language for communicating regarding risk management, and to help both small and large operators and market achieve their desired level of security maturity. But standardization also serves another valuable purpose – to limit the possibility of a security discussion getting obscured by political agendas, and to ensure that the appropriate focus and perspective is kept on the actual threats and the effective mitigation measures.

As shown in Fig.2 below; the industry as a whole has to work together to address new security risks faced by 5G architectures, technologies, and services, and address potential security challenges through unified 5G security standards, common 5G security concepts, and an agreed 5G security framework. During 2020, 111 companies (including their subsidiaries) from around the world sent technical experts to six SA3 meetings for the development of 5G security standards. The 3GPP SA3 Working Group has established 42 projects to analyze security threats and risks in various 5G scenarios. Project conclusions are being drawn gradually and implemented in security standards.

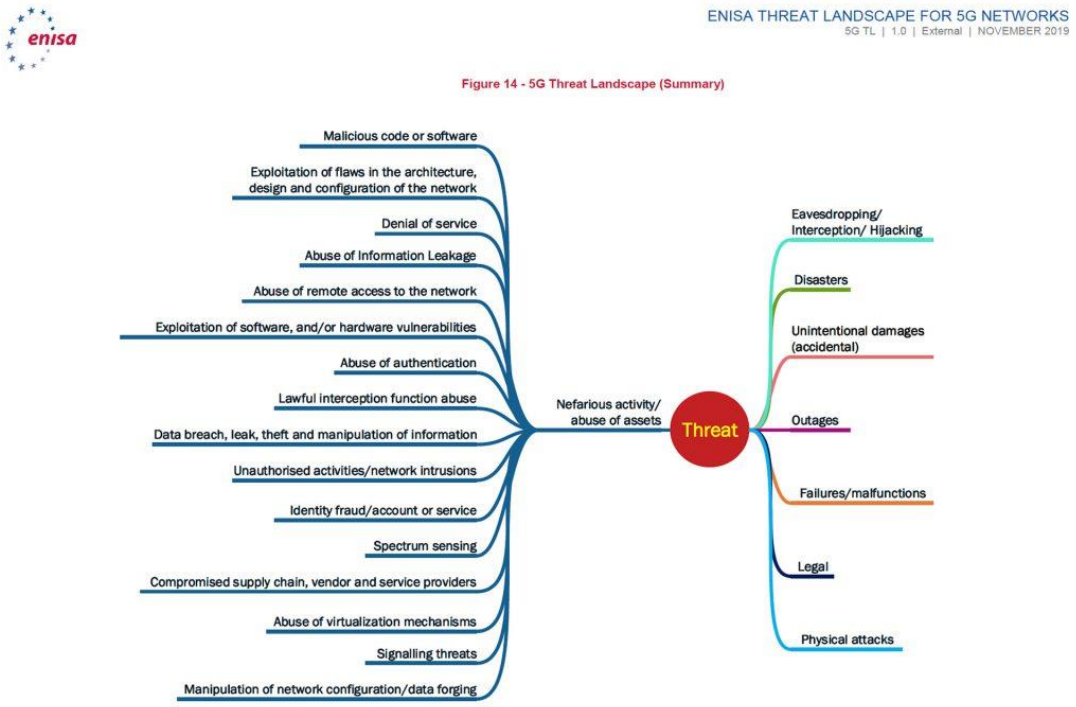


Fig. 2 – 5G Threat Landscape

(ENISA Threat Landscape For 5G Networks – November 2019)

5G is an evolution of 3G and 4G technology that will enable new kinds of services. For example, ultra-reliable-low-latency communications (uRLLC) will make self-driving cars possible, and massive machine-type communications (mMTC) will underpin smart manufacturing. There is no fundamental difference between 5G and 4G network architecture; the core networks and radio access networks (RAN) are still separated. Moreover, 5G offers stronger guarantees regarding privacy and security protection than either 3G or 4G.

3GPP 5G standards have inherited existing 4G security standards and improved upon these standards. In terms of 5G, new security mechanisms and measures have been designed for cloud, mobile edge computing (MEC), and network slicing.5G faces security challenges and opportunities brought by new services, architectures, and technologies, as well as higher user privacy and protection requirements. The industry needs to understand the requirements of diversified scenarios and better define 5G security standards and technologies to address the associated risks.

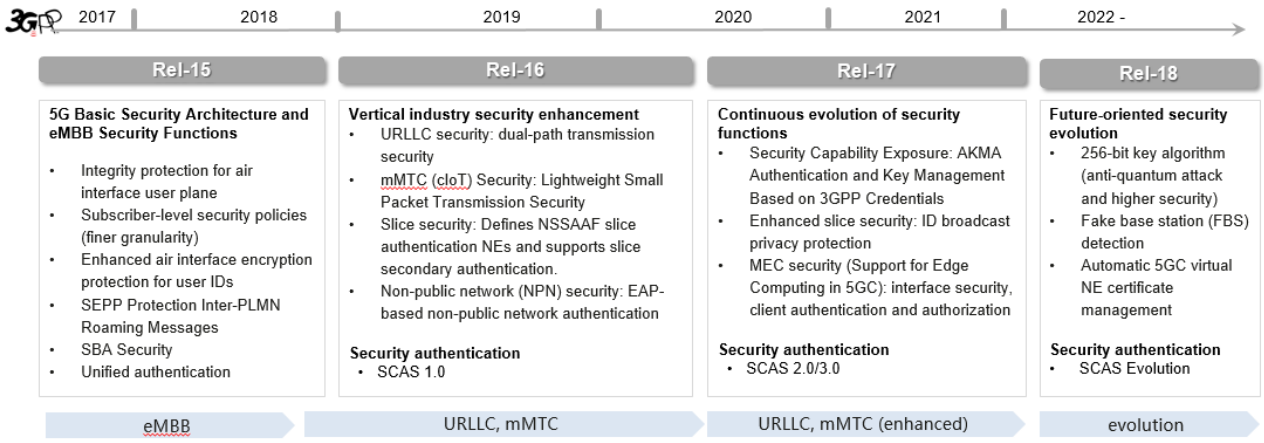


Fig. 3 – 5G Security Guidelines Progress 3GPP

(https://www.3gpp.org/specifications-technologies/releases;

Courtesy from Huawei Technologies)

2. Introduction of GSMA Network Equipment Assurance Scheme (NESAS)

GSMA Network Equipment Assurance Scheme (NESAS) defines security requirements and an assessment framework for secure product Development and Product Lifecycle Processes, as well as security test cases for the security evaluation of network equipment. NESAS is of value to both operators and vendors, it is intended to be used alongside other mechanisms to ensure a network is secure, in particular an appropriate set of security policies covering the whole lifecycle of a network.

Fig. 3 – NESAS Overview 2.2.0

https://www.gsma.com/security/network-equipment-security-assurance-scheme/

Cyber security assessment mechanisms shall follow globally accepted uniform standards to ensure that their operations are cost-effective and sustainable for the ecosystem. NESAS jointly defined by the GSMA and 3GPP is used to assess the security of mobile network equipment. It provides an industry-wide security assurance framework to improve the security level across the mobile industry. NESAS defines the security requirements and assessment framework for security product development and lifecycle processes, and uses security test cases in the

Security Assurance Specifications (SCAS) defined by 3GPP to assess the security of network equipment. Figure 4 depicts both Vendor and Operator lifecycles, together with assigned responsibilities and the scope of NESAS.

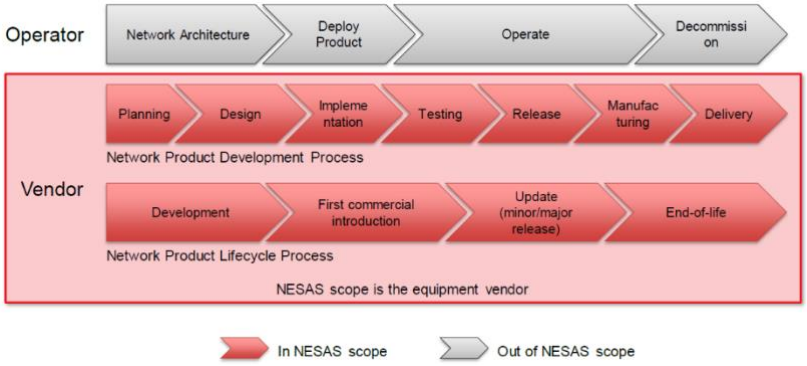


Fig. 4 – Responsibility, Accountability and NESAS scope

https://www.gsma.com/security/wp-content/uploads/2022/10/FS.13-v2.2.pdf

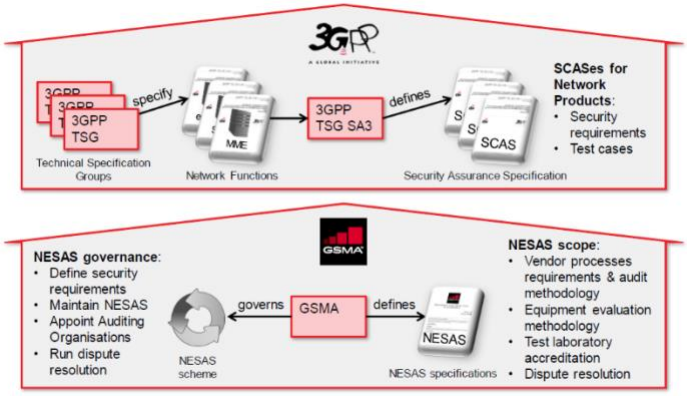


Fig. 5 – Roles of 3GPP and GSMA in NESAS

https://www.gsma.com/security/wp-content/uploads/2022/10/FS.13-v2.2.pdf

The GSMA released NESAS 1.0 in October 2019, continued to evolve NESAS based on industry requirements, released NESAS 2.0 in February 2021 Figure 4 depicts both Vendor and Operator lifecycles, together with assigned responsibilities and the scope of NESAS.

Currently, the NESAS ecosystem has been established and together with. 3GPP has initiated security evaluation of multiple 5G network equipment. Major equipment vendors and operators are actively participating in the NESAS standard formulation. Mainstream equipment vendors actively participated in NESAS evaluation, where Huawei's RAN and core network are the first to pass its audit and security function tests. The world's top audit bodies and well-known testing labs have been qualified for evaluation. Multiple tier-1 operators require that NESAS be included in 5G bidding documents.

Document History	Date Published
Version 2.2	20 October 2022
Version 2.1	28 January 2022
Version 2.0	05 February 2021
Version 1.1	20 July 2020
Version 1.0	07 October 2019

Fig. 65– NESAS- Releases and Revisions

https://www.gsma.com/security/resources/fs-13-network-equipment-security-assurance-scheme-overview/

NESAS promotes security cooperation and mutual trust in the global mobile communications industry, and enables operators, equipment vendors, and other stakeholders to jointly promote 5G security construction. It provides customized, authoritative, efficient, unified, open, and constantly evolving cyber security assessment standards for the communications industry and is a positive reference for stakeholders such as operators, equipment vendors, and government regulators.

NESAS brings the following benefits to equipment vendors:

- Provides accreditation from the world's leading mobile industry representative body
- Delivers a world-class security review of security related processes
- Offers a uniform approach to security audits
- Avoids fragmentation and potentially conflicting security assurance requirements in different markets

NESAS brings the following benefits to mobile operators:

- Sets a rigorous security standard requiring a high level of vendor commitment
- Offers peace of mind that vendors have implemented appropriate security measures and practices
- No need to spend money and time conducting individual vendor audits

NESAS brings the following benefits to regulators:

- Developed by the mobile communications industry as a whole to prevent standards fragmentation
- Open; maintained by the industry; continuously evolving and enhanced
- Cost-effective; innovative; low market entry barrier; driving security benefits

Fig. 7 – NESAS Industry Ecosystem

Compilation from https://www.gsma.com/security/network-equipment-security-assurance-scheme/

Courtesy from Huawei Technologies

For 5G network, NESAS provides the right kind of standards: customized, authoritative, global, efficient, unified, open, and constantly evolving. So far, a four-in-one (Vendors, audit institutions and Labs, regulator) ecosystem has been formed.The industry is supposed to work together to make positive contributions to the sustainable development of the global unified security assesment for 5G.

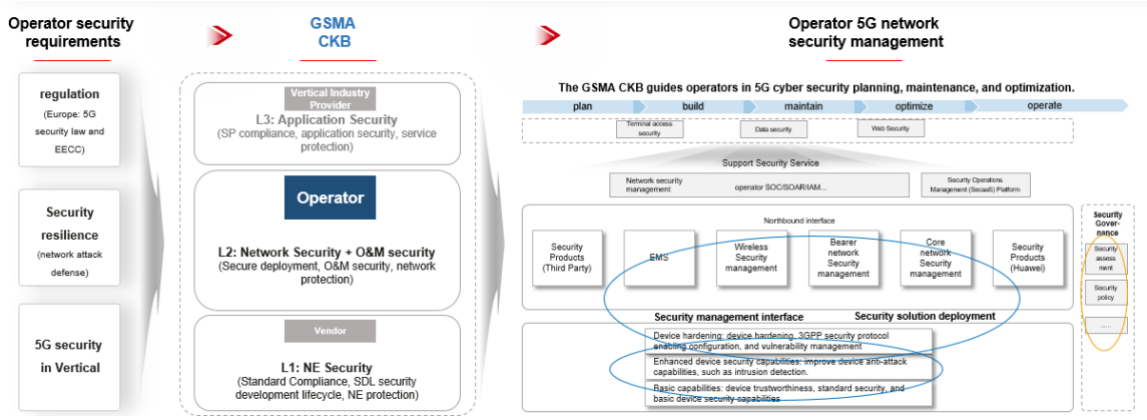
Introduction of GSMA 5G Cyber Security Knowledge Base

As Mobile Network Operators (MNOs) around the globe introduce and launch 5G systems, communications networks will face new security threats and challenges. Understanding, mapping and mitigating these existing and upcoming security threats in an objective, speedy and effective manner has become essential. To help operators and others in the 5G ecosystem, the GSMA has conducted a comprehensive threat analysis involving industry experts from across the eco-system including MNOs, vendors, service providers, and regulators, as well as collecting input from public sources such as 3GPP, ENISA and NIST, and mapped these threats to appropriate and effective security controls.

GSMA has collated this analysis into a 5G Cybersecurity Knowledge Base (5G CKB) to provide useful guidance on a range of 5G security risks and mitigation measures. The 5G Cybersecurity Knowledge Base is an industry effort that composes a comprehensive threat landscape designed to help key stakeholders (such as MNOs, equipment vendors, regulators, application developers and service providers) understand the security threats posed by 5G networks in a systematic and objective fashion. It provides essential insights for the stakeholders' risk management strategy as well as guidance covering best practices and risk mitigation measures.

A comprehensive 5G Cybersecurity Knowledge Base to help stakeholders identify, map and mitigate risks

5G Cybersecurity Knowledge Base facilitates and encourages collaboration to protect networks and services against disruption and unauthorized access as well as the prevention and mitigation of risks.5G CKB will help to enhance 5G security competencies and capabilities and will strengthen the work of carriers, enterprises, oversight agencies and regulators. At an operational level, 5G CKB offers clear instructions for taking step-by-step actions to build security assurance while considering the entire risk spectrum of 5G end-to-end networks.5G CKB serves as a bridge between the requirements of operators' supervision compliance, security resilience improvement, and enabling 5G application security and the construction of 5G network planning, maintenance, and operation security capabilities.



5G Cybersecurity Knowledge Base provide practice guide for MNOs to manage 5G network security

- **End-to-end security:** The NESAS provides security for 5G NE devices, and the 5G security knowledge base provides security for carrier network planning, construction, maintenance, optimization, and operation.
- **Practice guide:** Operators can use the 5G security knowledge base as an important reference and basis to improve 5G security assurance.
- **Collaboration with all parties:** Operators can cooperate with equipment vendors, application providers, and regulatory agencies to comply with security requirements set by the knowledge base.
- **Security assessment:** Operators can implement security control measures in the knowledge base and make assessment based on the GSMA security maturity model.

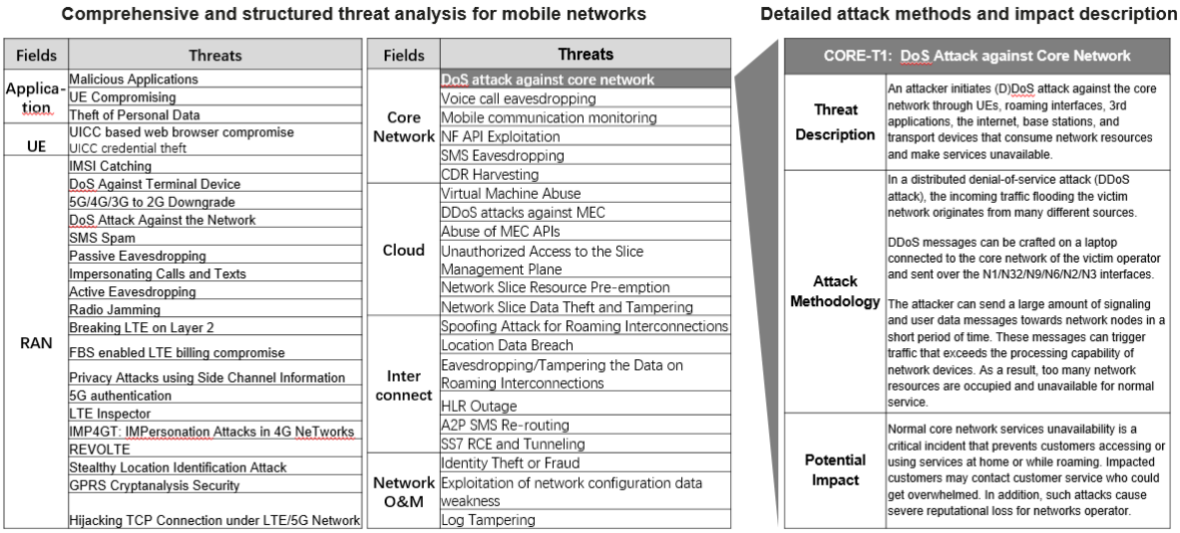


Fig. 8 – 5G Cybersecurity Knowledgebase guides to manage 5G security

https://www.gsma.com/security/5g-cybersecurity-knowledge-base/

Defines the Risk Mitigation Responsibilities of Stakeholders

vendors, service providers, customers, government, developers. or the Take an example of scenario Ceore-T1: DoS Attack against Core Network, in the 5G Cybersecurity knowledge base we can see the Mitigation Measures, it- recommended three stakeholders were involved and each stakeholder with a clearly defined set of responsibilities to enable the deployment and operation of 5G systems in a secure manner.F5G cybersecurity is a shared responsibility that involves key stakeholders including MNOs,

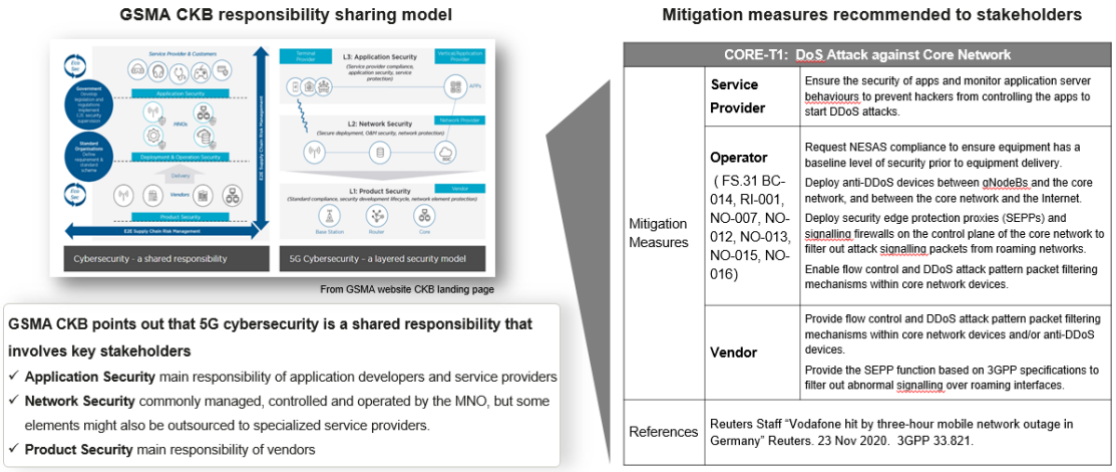


Fig. 9 – 5G cybersecurity shared responsibility and layered model and clear defined migration measures

https://www.gsma.com/security/5g-cybersecurity-knowledge-base/

- For the Service Provider, vertical industry application security requires multi-party collaboration, to ensure 5G application end-to-end security, not only depending on operators' network security.
- For operators, Network security and O&M security are the responsibilities of operators. Operators plan, design, and deploy devices and security capabilities provided by vendors on the entire network.
- For vendor, network element security is mainly the responsibility of the product provider. It focuses on the compliance of the vendor, the Secure Development Lifecycle (SDL), and the security anti-attack capability of the product.

Provides a Baseline Security Control that Mobile Operators can Consider Deploying

5G Cybersecurity Knowledge Base defines security control baselines for mobile network reference implementation, which are classified into Technological controls and Business controls. Operators using these controls can compare the listed controls with their deployed internal security controls, identify and assess potential gaps, and then respond to outstanding gaps within their organization.

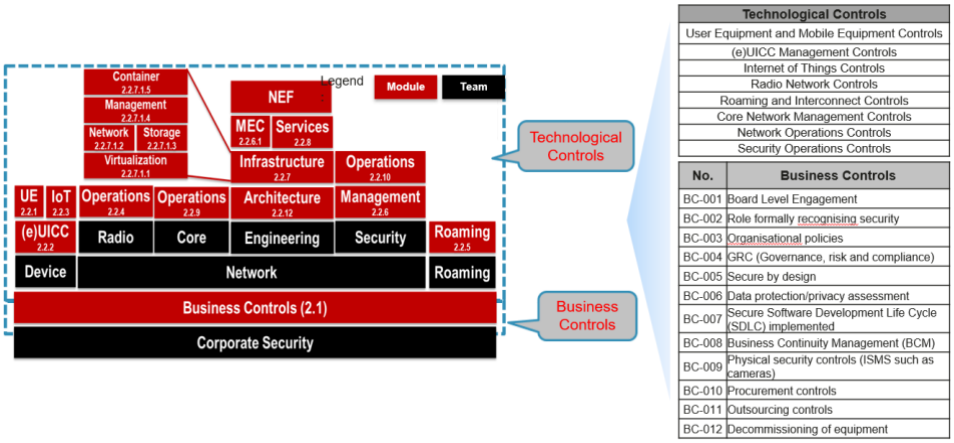


Fig 10 – 5G CKB provide Baseline Security Control considerations

https://www.gsma.com/security/5g-cybersecurity-knowledge-base/

3. Global Development and Implement

3.1 NESAS Development and Implement

The industry collaborated to make positive contributions to the sustainable development of the global unified security assessment for 5G.In global, 3GPP 5G has officially become the ITU IMT-2020 5G technical standard in July 10, 2020.

[July 10, 2020] With more than 200 delegates and experts from government authorities, telecommunications manufacturing and operation enterprises, and research institutions around the world, The ITU-R WP 5D#35e teleconference announces that the 3GPP 5G technology (including NB-IoT) meets the requirements of the IMT-2020 5G technical standard and is officially accepted as the ITU IMT-2020 5G technical standard. With the close collaboration of various countries and industries around the world, ITU has completed the milestone of the IMT-2020 5G technology standard as planned and ushered in an intelligent world of Internet of Everything.

The IMT-2020 technical standard is the name given by the ITU to the 5G standard, that is, the next-generation mobile communication technology to be used after 2020. To ensure the advancement of 5G technologies, the ITU has formulated detailed evaluation methods and indicator requirements. From 2016 to the present, the selected candidate technologies have been evaluated in detail in three 5G target application scenarios:

- eMBB (Enhanced Mobile Broadband),
- URLLC (Low-latency and High-Reliability Communication),
- mMTC (Large Machine-to-Machine Communication).

The 3GPP 5G technology meets the requirements of the IMT-2020 technical standard in terms of services, spectrum, and technical performance indicators, and has advanced technical capabilities such as a peak rate exceeding 20 Gbit/s, a communication delay of less than 1 ms, and support for 1 million devices per square kilometer. Meets various 5G application requirements.

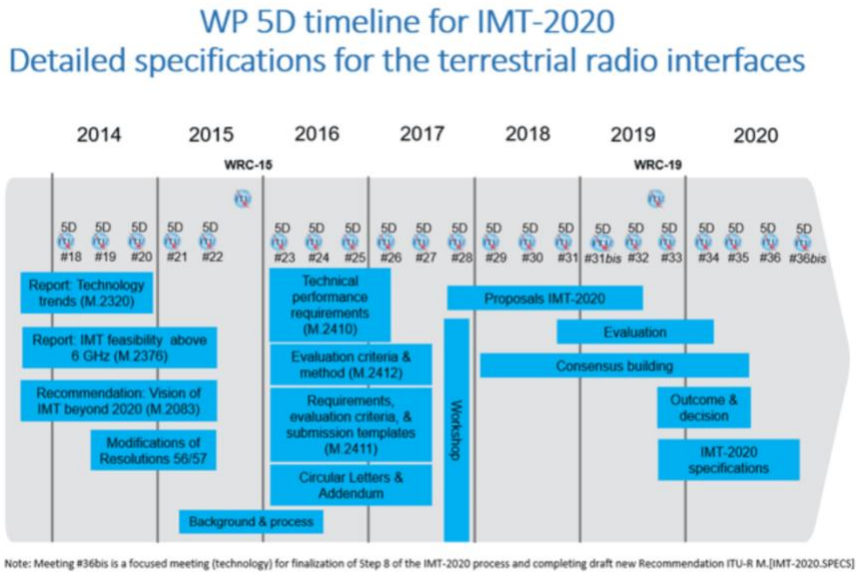


Fig.11 - ITU-R WP 5D IMT-2020 Timeline

https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2020/Pages/default.aspx

The ITU-R WP 5D is one of the most important working groups of the ITU. It is responsible for the standardization of the International Mobile Telecommunications (IMT) terrestrial wireless communication technology. Over the past 20 years, the 3G (IMT-2000) and 4G (IMT-Advanced) mobile communication technologies developed by ITU-R WP 5D have achieved great success worldwide. Under the leadership of ITU-R WP 5D, countries and regional organizations around the world will continue to cooperate. ITU-T Study Group 17 (Security) followed 3GPP SA3 security standards and research on cutting-edge technology security.

ITU-T work programme SG17 X.5Gsec-guide based on the 3GPP 5G security architecture.

According to ITU procedures, as described in **ITU-T Recommendation A.5**, any normative reference to documentation produced outside the ITU (other than ISO and IEC texts) needs to be evaluated by the study group or working party before a decision is made to incorporate the reference in an ITU-T Recommendation.

This TD contains the A.5 justification information for new X.5Gsec-guide "Security guideline for 5G communication system".

This draft recommendation is based on the 3GPP 5G security architecture.

[2017-2020] : [SG17] : [Q2/17]

[Declared patent(s)]

Work item:	X.5Gsec-guide
Status:	[Carried to next study period]
Approval process:	TAP
Type of work item:	Recommendation
Version:	New
Provisional name:	-
Equivalent number:	-
Timing:	-
Liaison:	3GPP, GSMA
Supporting members:	-
Subject/title:	Security guideline for 5G communication system
Summary:	Connected IoT devices and mobile applications require wireless network access that is resilient, secure and able to protect individuals' privacy. The 5G communication system should be designed to meet these high level requirements. There is a need for defining security framework for 5G communication system, which could be a concrete ground for developing further detailed technical Recommendations in 5G security subjects. This Recommendation provides security guidelines for 5G communication system. It identifies all components related to security of 5G communication system. It describes generic 5G architecture and its domain identifies threats to and provides security capabilities of each component, taking into account unique network features. This draft recommendation is based on the 3GPP 5G security architecture.
Comment:	-
Base text(s):	[SG17-TD4160/PLEN (2022-01)]
Contact(s):	Mee Yeon Kim, Editor Keundug Park, Editor Heung Youl Youm, Editor

More details as: https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=15006

Range	Achievement
Global	3GPP 5G has officially become the ITU IMT-2020 5G technical standard in July 10, 2020. Note：**International Mobile Telecommunications-2020** (**IMT-2020 Standard**) are the requirements issued by the ITU Radiocommunication Sector (ITU-R) of the International Telecommunication Union (ITU) in 2015 for 5G networks, devices and services.
EU	EU recognizes the NESAS-CCS as a unified certification standard under the EU Cyber Security Act from. https://www.enisa.europa.eu/news/enisa-news/calling-on-you-5g-experts-join-us-on-5g-cybersecurity-certification
Germany	Germany Security Catalogue 2.0 recognized NESAS as a 5G security certification standard and worked with all parties to promote the development of a unified 5G certification standard in the EU from 2020. https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/220705_Zertifizierung_5G-Komponenten.html
Austria	The Austrian telecom regulator RTR has adopted the SCAS standard for telecom security regulation in the Telecom Cyber Security Regulation 2020 (TK-NSiV 2020). Official support for inclusion of NESAS into the EU cyber security certification framework 2020.07. 04

	https://www.rtr.at/TKP/aktuelles/veroeffentlichungen/veroeffentlichungen/Verordnungen/Telekom-Netzsicherheitsverordnung_2020_(TK-NSiV_2020.de.html
Netherlands	Regulation of the Minister of Economic Affairs and Climate of 1 October 2021, no. WJZ/20056324, containing further rules regarding the security and integrity of public electronic communications networks and services (Telecommunications Security and Integrity Regulations). https://zoek.officielebekendmakingen.nl/stcrt-2021-42618.html
China	NESAS has been approved as the basic standard for 5G security assessment and has been implemented by China's IMT 2020 promotion team. All 5G equipment suppliers in the Chinese market comply with the NESAS standard system. Approximately 1.5 million 5G sites in China's 5G networks (as of December 2021) were expected to be NESAS compliant and certified. http://www.caict.ac.cn/kxyj/qwfb/bps/202002/t20200204_274118.html
Singapore	Singapore government has acknowledged NESAS (IMDA 21 GHz Public Consultation Document) on 26 July 2021. https://www.imda.gov.sg/-/media/Imda/Files/Regulations-and-Licensing/Regulations/Consultations/2021/Next-Wave-of-5G-Growth-and-Deployment-in-Singapore/21-GHz-Public-Consultation-Document.pdf?la=en&hash=871CDE093D95FA731129030985E8DECD
Thailand	The Office of the National Broadcasting and Telecommunications Commission (NBTC) officially released the national 5G security guideline to call for stakeholders of Thailand telecom industry to comply NESAS standards on 3rd Nov. 2021. https://www.nbtc.go.th/News/govnewspartner/51190.aspx
Philippines	Philippines Department of Information and Communications Technology（DICT） officially released the national 5G security guideline, recognized and adopted NESAS to call for stakeholders of Philippines telecom industry to comply NESAS standards on 1st July 2022. https://dict.gov.ph/ https://dict.gov.ph/wp-content/uploads/2022/07/The-Need-for-Philippines-Security-Standards-and-Framework-in-5G-Equipment-2022-07-01.pdf
Laos	Laos Ministry of Technology and Communications（MTC） officially released the national 5G security guideline,recognized and adopted NESAS on 1st July 2022. https://mtc.gov.la/index.php?r=site%2Fdetail&id=897
The Arab League	The Arab League officially recognized and adopted the NESAS standard by cyber security white paper on October 22, 2021. https://www.mtcen.gov.tn/index.php?id=119&L=-1%5C%27&tx_ttnews%5Btt_news%5D=4335&cHash=8004500dd3cd4237a6fa9226d916c7df

OIC-CERT 5G Security Framework Promotion Plan	**Mutual Certification Mechanism Implementation:** implement the certification mechanism with security standards (NESAS/SCAS, cloud security, etc) in some key/pilot OIC member states in 2022, which would be selected from different regions and states, later. The finally confirmed key/pilot countries should satisfy with following one or more conditions: ① Have friendly relationships with each other selected ones; ② Be good at propagation and impact expansion; ③ Have good wiliness to strength cyber security capacity. https://www.oic-cert.org/en/events/5g/index.html#.YodGRKhByUk https://www.zawya.com/en/press-release/companies-news/oic-cert-5g-security-framework-working-group-kicks-off-global-series-of-cybersecurity-workshops-in-malaysia-bn7ttyiy
Indonesia	Indonesia multi-stakeholder achieved the consensus on NESAS scheme to strengthen national 5G security resilience on 12th Aug 2021 https://republika.co.id/berita/qxuwrz368/teknologi-5g-hadir-jaminan-keamanan-siber-harus-diperkuat
Sri Lanka	Sri Lanka cert and multi-stakeholder achieved the consensus on NESAS scheme to be national 5G security standard on 30th Nov 2021. https://www.ft.lk/it-telecom-tech/5G-roll-out-challenges--Governance--legislation--awareness--capacity-and-NESAS-standards/50-726824

3.2 OIC–CERT 5G Cybersecurity Framework Development

Overview of OIC–CERT 5G Cyber Security Framework

Referring to OSI and TCP/IP protocols, telecommunication industry has been divided into equipment, network and application layers. It is thus more practical that the OIC-CERT 5G cyber security framework focus on the security of equipment, network and application, respectively.

A layered security structure benefits to clarify roles and responsibilities of implement and deploy cyber security requirements. To ensure targeted cyber security requirements can be deployed effectively and uniformly by OIC member states, unified standard and certification are decided as the foundation of this framework.

Fragmentation and potentially conflicting cyber security requirements and compliance for OIC member states could be avoided. Besides, trust needs to be based on the truth, while truth must be verifiable, and the verification should depend on the unified standards.

This framework does not define any standards and certification schemes, because applying or developing them depends on actual requirements for stakeholders. And there have been good standards and certifications able to be directly used.

A layered security approach —Roles & Responsibilities

Requirements for each layer are designed as a baseline to guide or assist OIC member states to direct and control 5G cyber security development.

It is thus easy and flexible for member states to not only understand security targets, but also combine with their realities to customise and build related 5G cyber security efficiently.

In practice, requirements are dynamic along with many aspects, such as security technologies, security mind-set and awareness, laws and regulations, current threat landscape and so on. It means that an iterative update of security requirements in different periods is essential.

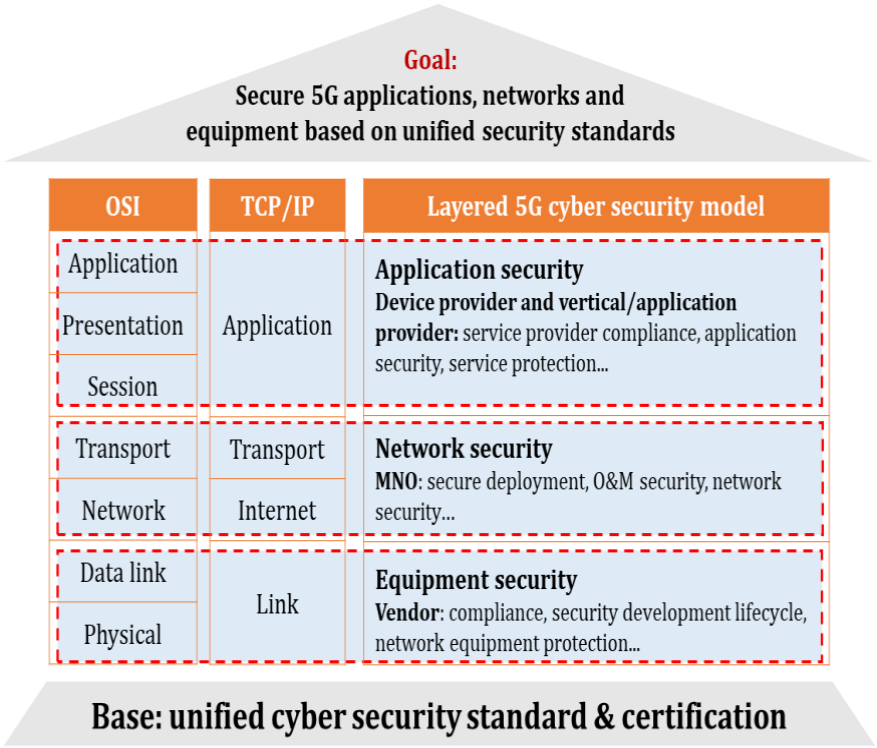


Fig. 12 – Layered architecture and corresponding roles and responsibilities

https://www.oic-cert.org/en/journal/vol-4-issue-1/2.html#.Y3x44HZBw2w

A shared responsibility and collaboration

5G cybersecurity is under a shared responsibility for key stakeholders, including mobile network operators, interconnection providers, vendors, application developers, service providers and governments.

In the OIC-CERT 5G Cyber security risk repository, it is clear that counter measures against a same threat may involve more than one actors, which include government and national regulators, mobile network operators, equipment vendors and service providers.

Generally speaking, government and industry share similar goals of mitigating cybersecurity threats to network infrastructures, preventing against cyberattacks, and reducing the impact of illegal cyber behaviors.

Also, public-private partnerships should be leveraged to ensure that both industry and government achieve the desired policy outcome of more secure 5G networks.

More details as: https://www.oic-cert.org/en/events/5g/index.html#.YodGRKhByUk

4. Recommendation and Way Forward

Various security certification methods have been created over the last 30 years to assess the security postures of suppliers and operators. NESAS, the Network Equipment Security Assurance Scheme, is a security advancement aimed at 5G communication. The NESAS framework covers security standard requirements and the assessment of the quality and characteristics of telecommunication equipment from the planning, design and development phase.

This framework can be used by manufacturers to develop and manufacture equipment of high quality and safety features. Telecom operators can also apply this framework to develop policies and measures to provide the most secure telecommunication services. The NESAS framework can be used to create a nationally neutral and transparent security standard. Regional and international level for telecommunication regulators.

Unified cybersecurity standards, as well as compliance methods that include standardized verification and testing, can aid in the development of a greater level of confidence and a more competitive, transparent playing field. In contrast to a world with various standards and diverse supply chains, a cyberspace enabled by unified standards is more likely to stimulate vigorous competition, resulting in higher quality, cheaper costs, more innovation, improved security, and increased resilience.

The 5G Cybersecurity Knowledge Base includes the industry-consensus threat map, mitigation strategies and measures for different roles, and standards and best practices. With the full use of these suggestions and references coming from the 5G Cybersecurity Knowledge Base, 5G cybersecurity is verifiable and manageable. It is a powerful tool to help stakeholders systematically understand and respond to 5G cybersecurity threats at the technical level.The use of the NESAS standards and GSMA 5G Cybersecurity Knowledge Base can benefit all sectors in many dimensions of security in the telecom industry. The equipment manufacturers use the NESAS standards to guide the design of a complete product development process with security measures and manufactures equipment with standard safety features and features for use in telecommunication networks. Telecommunication service provider, regulatory organization and relevant agencies benefit from standard and end to end audit and assessment results. GSMA 5G Cybersecurity Knowledge Base facilitates and encourages collaboration to protect networks and services against disruption and unauthorised access as well as the prevention and mitigation of risks.

The 5G Cybersecurity Knowledge Base will help to enhance 5G security competencies and capabilities and will strengthen the work of carriers, enterprises, oversight agencies and regulators. At an operational level, the 5G Cybersecurity Knowledge Base offers clear instructions for taking step-by-step actions to build security assurance while considering the entire risk spectrum of 5G end-to-end networks.

The Security Solutions of the 5G Knowledge Base provide common methods for mitigating the various threats. These controls can be chosen, or even mandated by a regulator, based on a comprehensive risk assessment and consideration regarding which threats are most relevant for any given market or operator. There are technical mitigation solutions for all identified threats. At the political level, the discussion has at times been limited to either a ban or market limitations for certain vendors.

On the other hand, the security solutions offered in the 5G Cybersecurity Knowledge Base are effective regardless of vendor origin. In fact, introducing as many vendors as possible to ensure vendor diversity in an industry with a limited amount of options, is considered a key measure for risk reduction. The basis for this is that downtime in mobile networks is largely due to natural events, software and hardware faults, configuration errors and power loss.The Baseline Security Controls provide suggested measures of maturity. Through these baselines it is possible for an operator to compare itself to the industry average, and it could potentially be possible for a regulator to compare operators in a market. The baselines also provide a good checklist to assess internal security maturity compared to a desired maturity level, and the gaps would provide a very useful roadmap towards that level. Based on this, a 5G network security strategy can be built.

Cybersecurity Malaysia support and recognize the importance of adopting security standards such as GSMA 5G Cybersecurity Knowledge Base, NESAS and OIC–CERT 5G Cyber Security Framework as it can use this standards and measures as a regulatory basis to standardize telecommunication services that are effective and provide the highest level of security for subscribers. The most important benefit is the process by which all sectors play a role in driving modern and secure telecommunication services particularly collaboration to develop more secure telecommunication services using the NESAS framework and GSMA 5G Cybersecurity Knowledge Base as a key guideline.Building a security strategy based on a common understanding of threats and effective measures gives both operators, regulators and customers a degree of confidence that the work being done to protect 5G networks is effective and relevant. Baselines for security maturity have not been a particularly voiced concern in the political discourse.

As security authorities have become aware of a lack of maturity among some of their operators, their focus has been on removing potentially risky vendors rather than actually helping the operators reach a level of security maturity where they would be able to manage risk. And as the threat actors are unlikely to be discouraged regardless of how many companies are removed from the supply chain, this approach creates a false sense of security and leaves potentially immature operators in charge of critical infrastructure.

Works Cited

1 "5G Cybersecurity Knowledge Base." *Security*, GSMA, www.gsma.com/security/5g-cybersecurity-knowledge-base/. Accessed 24 Nov. 2022.

2 "5G Roll-out Challenges: Governance, Legislation, Awareness, Capacity and NESAS Standards | Daily FT." *Www.ft.lk*, 2 Dec. 2021, www.ft.lk/it-telecom-tech/5G-roll-out-challenges--Governance--legislation--awareness--capacity-and-NESAS-standards/50-726824. Accessed 24 Nov. 2022.

3 "BSI Führt Zertifizierung Für 5G-Komponenten Ein (Archiviert)." *Bundesamt Für Sicherheit in Der Informationstechnik*, European Union Agency for Cybersecurity, www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/220705_Zertifizierung_5G-Komponenten.html. Accessed 24 Nov. 2022.

4 "Calling on You, 5G Experts! Join Us on 5G Cybersecurity Certification." *ENISA*, 7 June 2021, www.enisa.europa.eu/news/enisa-news/calling-on-you-5g-experts-join-us-on-5g-cybersecurity-certification. Accessed 24 Nov. 2022.

5 GSMA NESASG. *GSM Association Non-Confidential Official Document FS.13 -Network Equipment Security Assurance Scheme -Overview Network Equipment Security Assurance Scheme - Overview Version 2.2 Security Classification: Non-Confidential Copyright Notice Antitrust Notice*. 2022.

6 "GSMA Network Equipment Security Assurance Scheme (NESAS)." *Security*, www.gsma.com/security/network-equipment-security-assurance-scheme/. Accessed 24 Nov. 2022.

7 Hulk Zhang, et al. "OIC-CERT 5G SECURITY FRAMEWORK." *Www.oic-Cert.org*, www.oic-cert.org/en/journal/vol-4-issue-1/2.html#.Y3x44HZBw2w. Accessed 24 Nov. 2022.

8 Infocomm Media Developement Authority. *PUBLIC CONSULTATION ISSUED by the INFO-COMMUNICATIONS MEDIA DEVELOPMENT AUTHORITY on next WAVE of 5G GROWTH & DEPLOYMENT in SINGAPORE: POLICY ISSUES & PROPOSED REGULATORY DESIGN for 2.1 GHZ BAND*. 2021.

9 "ITU towards "IMT for 2020 and Beyond."" *ITU*, www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2020/Pages/default.aspx.

10 Klimaat, Ministerie van Economische Zaken en. "Regeling van de Minister van Economische Zaken En Klimaat van 1 Oktober 2021, Nr. WJZ/ 20056324, Houdende Nadere Regels Betreffende de Veiligheid En Integriteit van Openbare Elektronische Communicatienetwerken En -Diensten (Regeling Veiligheid En Integriteit Telecommunicatie)." *Zoek.officielebekendmakingen.nl*, zoek.officielebekendmakingen.nl/stcrt-2021-42618.html. Accessed 24 Nov. 2022.

11 Mee Yeon Kim, et al. "ITU-T Work Programme." *ITU*, www.itu.int/ITU-T/workprog/wp_item.aspx?isn=15006. Accessed 24 Nov. 2022.

12 "OIC-CERT | Organisation of the Islamic Cooperation - Computer Emergency Response Team." *Www.oic-Cert.org*, 22 Feb. 2022, www.oic-cert.org/en/events/5g/index.html#.YodGRKhByUk. Accessed 24 Nov. 2022.

13 "OIC-CERT 5G Security Framework Working Group Kicks off Global Series of Cybersecurity Workshops in Malaysia." *Www.zawya.com*, 10 Mar. 2022, www.zawya.com/en/press-release/companies-news/oic-cert-5g-security-framework-working-group-kicks-off-global-series-of-cybersecurity-workshops-in-malaysia-bn7ttyiy. Accessed 24 Nov. 2022.

14 Rahma Sulistya, and Dwi Murdaningsih. "Teknologi 5G Hadir, Jaminan Keamanan Siber Harus Diperkuat." *Republika Online*, 15 Aug. 2021, republika.co.id/berita/qxuwrz368/teknologi-5g-hadir-jaminan-keamanan-siber-harus-diperkuat. Accessed 24 Nov. 2022.

15 "Telekom-Netzsicherheitsverordnung 2020 (TK-NSiV 2020)." *RTR*, www.rtr.at/TKP/aktuelles/veroeffentlichungen/veroeffentlichungen/Verordnungen/Telekom-Netzsicherheitsverordnung_2020_(TK-NSiV_2020.de.html. Accessed 24 Nov. 2022.

16 "The 3GPP's System of Parallel Releases." *3GPP*, www.3gpp.org/specifications-technologies/releases. Accessed 24 Nov. 2022.