NTRA
National Telecom Regulatory Authority
الجهاز القومي لتنظيم الإتصالات

5G Cyber Security Framework: Draft

EG|CERT
EGYPTIAN COMPUTER EMERGENCY READINESS TEAM

TLP: White

The Traffic light Protocol (TLP)

The Traffic Light Protocol (TLP) was created in order to facilitate greater sharing of information. TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs four colors to indicate expected sharing boundaries to be applied by the recipient(s). The protocol includes four colors (traffic lights), which are detailed as follows:

Red – Not for disclosure, restricted to participants only:
Sources may use TLP: RED when information cannot be effectively acted upon by additional parties. Recipients may not share TLP: RED information with any parties outside the specific exchange, meeting, or conversation in which it was originally disclosed

Amber – Limited disclosure, restricted to participants' organizations:

Sources may use TLP: AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside the organizations involved. Recipients may only share TLP: AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm.

Green – Limited disclosure, restricted to the community:

Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector. Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.

White – Disclosure is not limited:
Sources may use TLP: WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. TLP: WHITE information may be distributed without restriction.

About Version

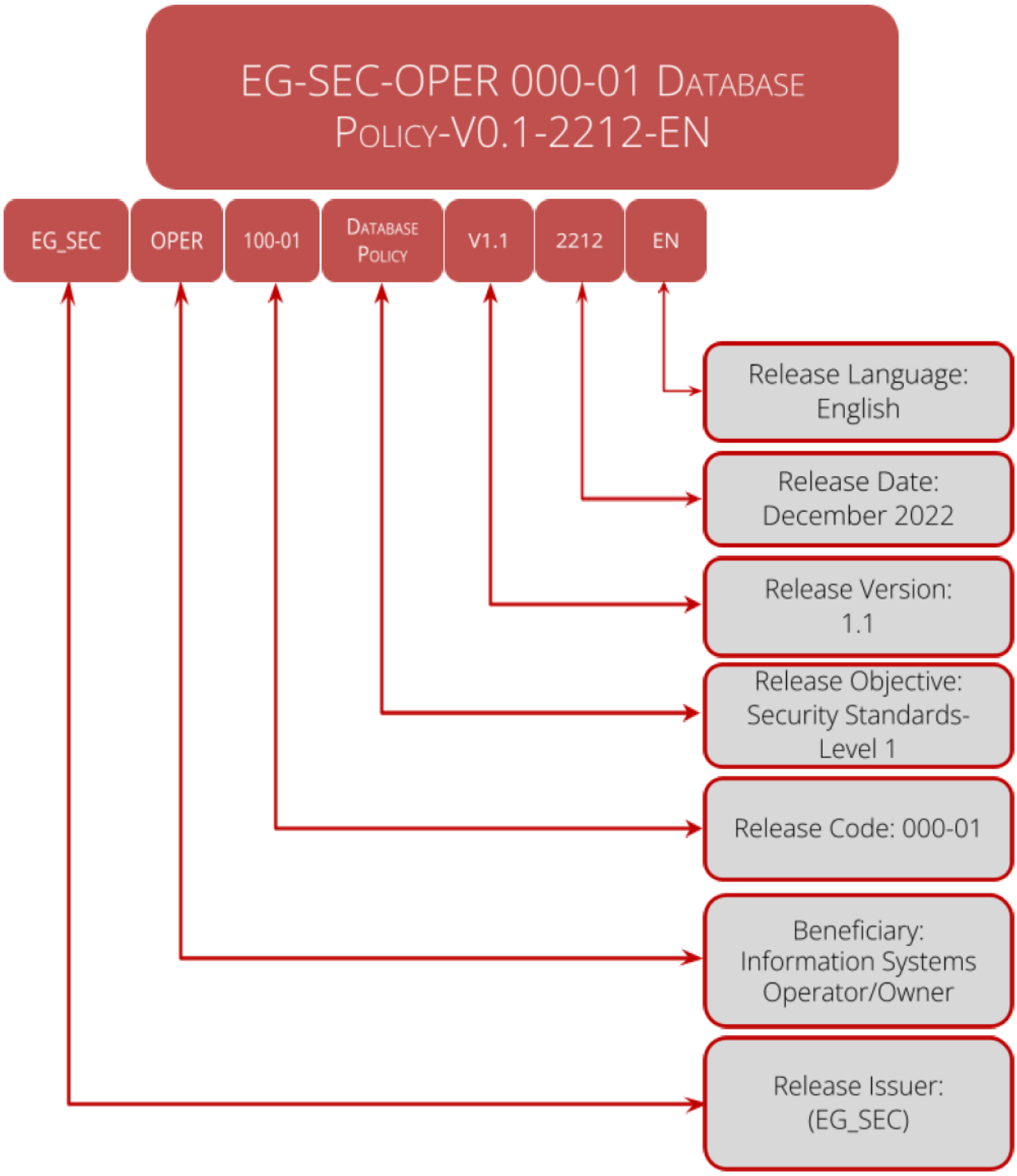

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

INTRODUCTION

OVERVIEW

5G is already transforming and enhancing mobile connectivity. With its high speeds and low latency, almost all businesses and industries are now in the position to digitize applications and services they couldn't dream of not long ago. With 5G networks, billions of devices and IoT (the internet of things) are inter-connectable leading to use cases like smart cities, AR/VR on mobile networks, remote medicine and much more. The potential is practically unlimited.

However, the massive potential and almost unlimited connectivity bring about many security challenges. Security capabilities are a critical element for 5G-ready success. And with the increase of the amount of devices using 5G, it is essential to provide security standards and guidelines to increase the level of security of devices and networks. That is mandatory in order to maintain end users' security and privacy.

OBJECTIVE

The objective of this document is to provide a preliminary version of the 5G cybersecurity framework in the ARE. Well known global 5G standards and guidelines are considered including the NIST SP 1800-33A, the ENISA 5G cybersecurity standards, the GSMA Securing the 5G Era, the Huawei 5G security and the NOKIA 5G security, for securing the 5G network components.

The document explains the 5G network architecture from a cybersecurity point of view, provides challenges and threats of 5G technology briefly, and gives a set of baseline controls to ensure security of these network elements, along with a 5G security assurance process that should be performed to ensure compliance to the baseline guidelines provided.

The framework provides a set of security baseline requirements and a security assurance process for ensuring security of the 5G network provided by the operators as well as ensuring security of applications, systems, and services that use 5G networks to operate. Thus, ensuring security of the whole system to maintain a high level of security for consumer organizations and individuals as well who use and benefit from these 5G enabled technologies, applications, systems, and services.

This framework is mainly intended for both 5G network operators and organizations using and managing 5G enabled technologies. The framework provides different sets of baseline security requirements. Defining the applicable set of security requirements is done according to the perspective of the framework's user, whether it is an 5G network operator entity or an entity providing 5G enabled technologies.

TARGET AUDIENCE

The target audience are technology, security, and privacy program managers who are concerned with how to identify, understand, assess, and mitigate risk for 5G NR networks. The framework is targeting organizations planning to deploy, operate, and use 5G NR networks in the Arab Republic of Egypt, including:

- Commercial mobile network operators.
- Potential private 5G network operators.
- Organizations using and managing 5G enabled technologies.

To conclude, this document is intended for:

- 5G NR Operators inside the ARE.
  Operators responsible for deploying and providing 5G networking and communication.
- 5G NR Technology Users inside the ARE.
  Organization providing 5G enabled applications, systems, or services (applications, systems, or services that use 5G technology for communications).

DISCLAIMER

It should include brief responsibilities and commitment.

DEFINITIONS AND ACRONYMS

TERMS AND DEFINITIONS

The framework	Wherever called in this document, it refers to the 5G cybersecurity framework in the ARE
5G NR	A new Radio Access Technology (RAT) developed by 3GPP for the 5G (fifth generation) mobile network.
3GPP	3GPP™ is a partnership project bringing together national Standards Development Organizations (SDOs) from around the globe initially to develop technical specifications for the 3rd generation of mobile, cellular telecommunications, UMTS.
5G Access Network	The 5G Access Network (3GPP) identifies an access network, either the 5G-RAN and/or non-3GPP access network, that connects to the 5G Core Network.
5G RAN	Consists of antennas, radios, baseband (RAN Compute), and RAN software to enable incredible speeds and mobility.
5G Core Network	The heart of a 5G mobile network. It establishes reliable, secure connectivity to the network for end users and provides access to its services.
User Equipment	Devices such as smartphones, computers, and Industrial Control Systems (ICS) generate data that is then transmitted to a base station, small cell, satellite, or Internet Exchange Points (IXP).

ACRONYMS

ARE	The Arab Republic of Egypt
5G NR	Fifth Generation New Radio
4G LTE	Fourth Generation Long-Term Evolution
3GPP	Third Generation Partnership Project
ITU-R	International Telecommunication Union - Radiocommunication Sector
GSMA	Global System for Mobile Communications Association
5G-AN	5G Access Network
5GC	5G Core Network
NSA 5G	Non-Standalone 5G
SA 5G	Standalone 5G
eMBB	Enhanced Mobile Broadband
mMTC	Massive Machine-Type Communications
URLLC	Ultra-Reliable and Low-Latency Communications
UE	User Equipment

5G New Radio (NR) Technology

Fifth Generation (5G) is the 5th generation mobile network. It is a new global wireless standard after 1G, 2G, 3G, and 4G networks. 5G enables a new kind of network that is designed to connect virtually everyone and everything together, including machines, objects, and devices. 5G networks aim at providing value-added services with advanced performance such as low-latency communications, high reliability, high data rates and capacity to support an increasing number of connected devices. 5G aims to provide a flexible platform to integrate vertical industries and a wide range of services and applications such as autonomous driving, robotics, augmented and virtual reality, remote healthcare, and more. 5G wireless technology is meant to deliver higher multi-Gbps peak data speeds, ultra low latency, more reliability, massive network capacity, increased availability, and a more uniform user experience to more users. Higher performance and improved efficiency empower new user experiences and connect new industries.

5G NR Use Cases:

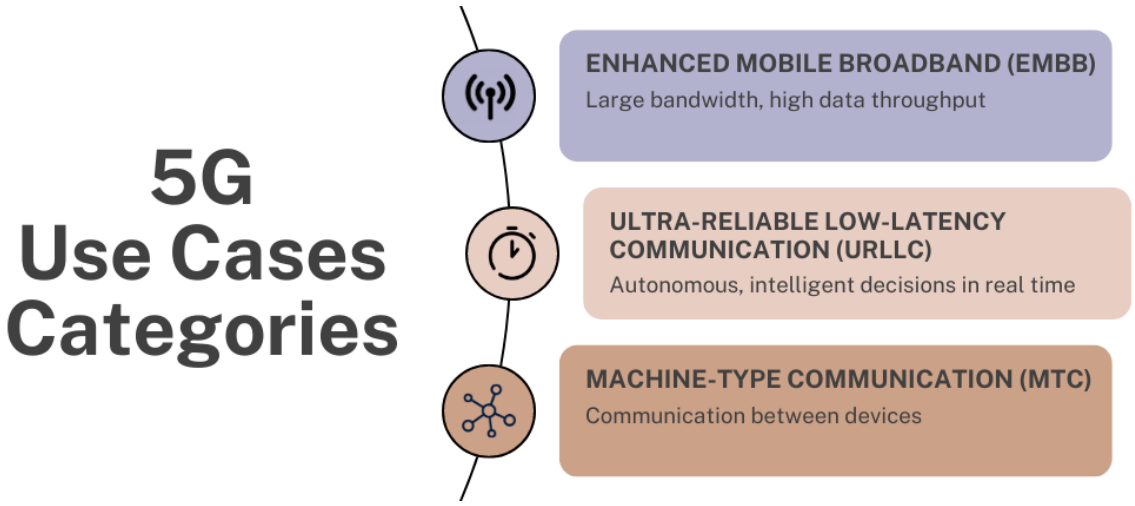

Figure-1: 5G Use cases categories

5G use cases vary by industry and enterprise, but most 5G use cases can be grouped around one of the following three categories, as described in figure-1. 5G networks need to meet the requirements of unprecedented connectivity in these three major scenarios, as stated by the International Telecommunication Union - Radiocommunication Sector (ITU-R) in their "Emerging Trends in 5G/IMT2020" document and described in figure-2. Operators must also be in position to offer these three (3) major 5G communications scenarios:

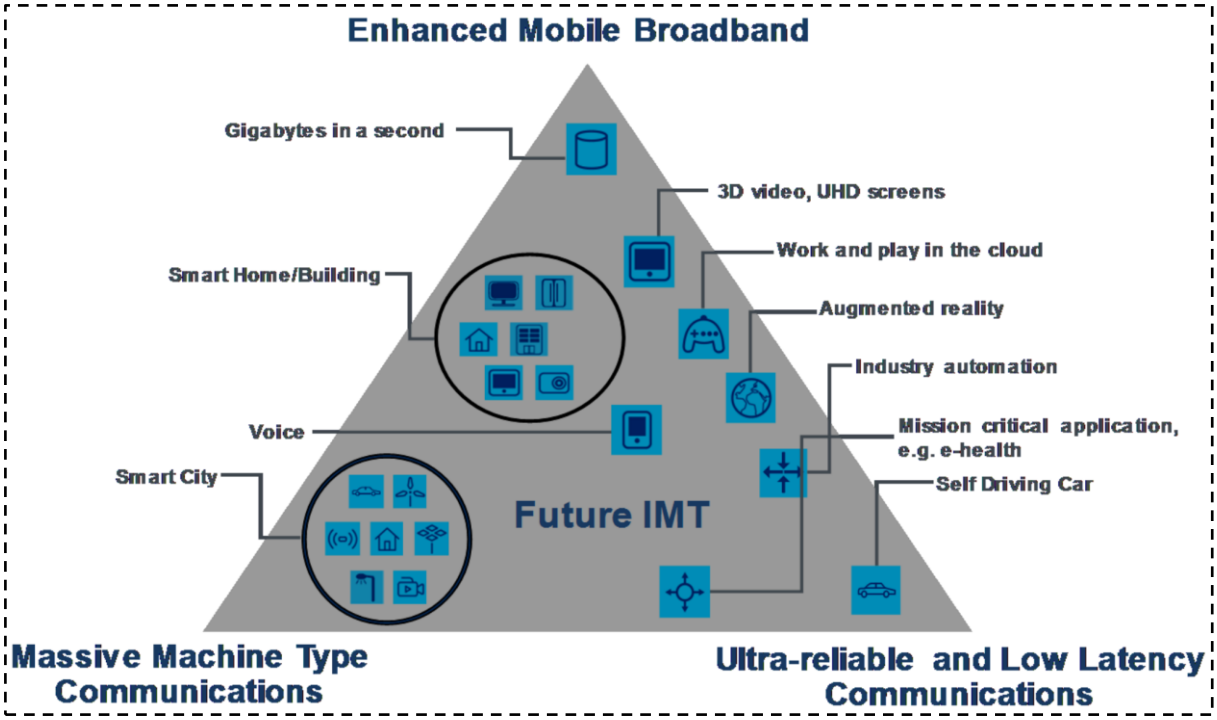

Figure-2: Various 5G scenarios – as defined by: ITU-R IMT-2020

- **Enhanced Mobile Broadband (eMBB):** focuses on services that require ultra-high bandwidth, such as high-definition video (4K/8K), virtual reality (VR), and augmented reality (AR), meeting user demands for a digital life.
- **Ultra-Reliable and Low-Latency Communications (URLLC):** focuses on latency-sensitive services, such as autonomous driving/assisted driving, Internet of Vehicles (IoV), and remote control, meeting user demands for a digital industry.
- **Massive Machine-Type Communications (mMTC):** focuses on scenarios requiring high-density connections, such as intelligent transportation, smart grid, intelligent manufacturing (Industry 4.0), and smart logistics, meeting user demands for a digital society.

5G Deployment Architecture:
Non-Standalone (NSA) vs. Standalone (SA) Deployment

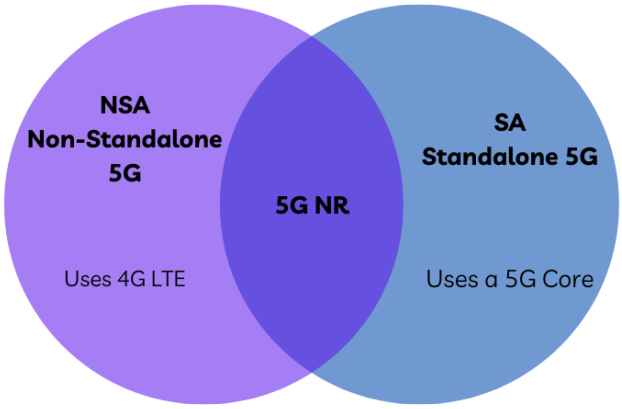

Figure-3: 5G deployment Architectures

Mobile network operators have two main approaches to choose from when deploying 5G, as shown in figure-3 and further explained in figure-4:

1. Non-standalone (NSA) deployment.
2. Standalone (SA) deployment.

NON-STANDALONE 5G

NSA dominated as the top choice for initial 5G deployments among MNOs, thanks to existing cellular infrastructure. But, as SA 5G deployments take off, it's important to understand the distinctions between the two. Both approaches are valid ways of constructing a 5G network, but the chosen deployment mode determines how efficiently the 5G network operates. Both NSA and SA use the 5G New Radio (5G NR) interface, enabling them to deliver features and capabilities based on the standards defined by the 3rd Generation Partnership Project (3GPP). 5G NR offers myriad use cases, but one of its most essential features is it provides a path from 4G LTE to 5G.

The drawback of NSA 5G, however, is it can't deliver certain capabilities that a pure, unfettered SA 5G network can. For example, NSA doesn't enable the low latency that is one of the biggest draws to 5G. Another disadvantage of NSA is it requires a higher level of energy to power 5G networks with 4G infrastructure. 5G NR is more energy-efficient than LTE, IEEE reported, but using two different forms of cellular technology massively increases power consumption in a network. Benefits of NSA 5G includes but not limited to, reduced costs, easy deployment, fast rollout, and pathway to SA 5G.

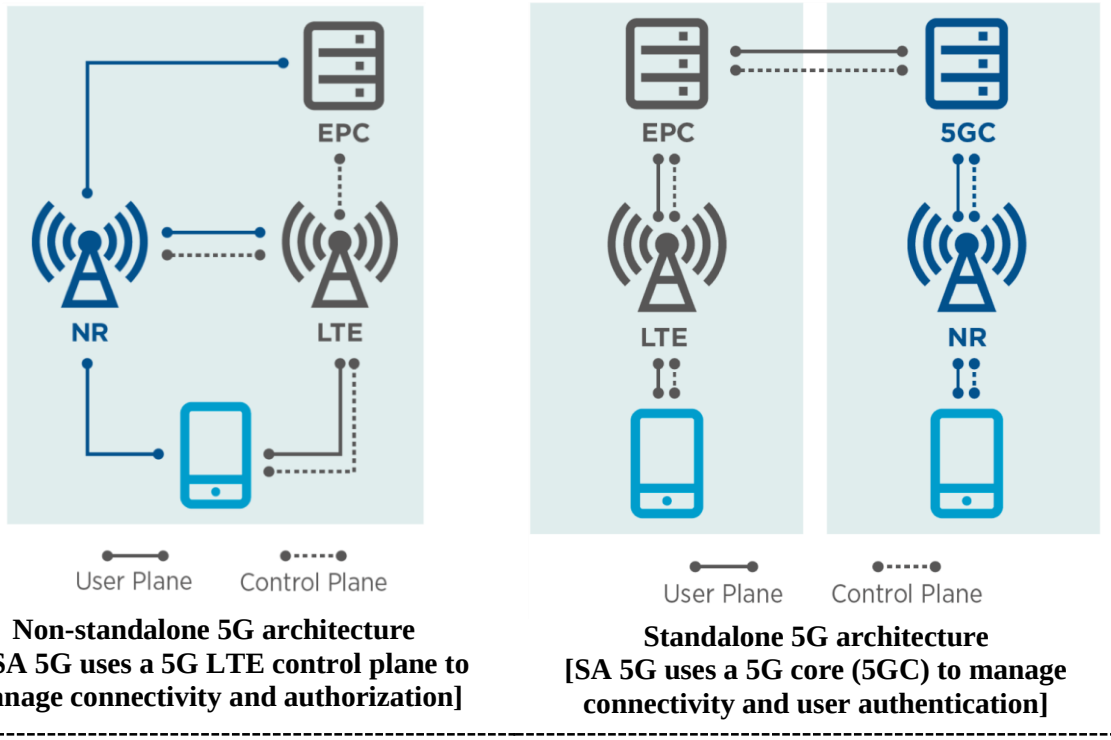

Figure-4: 5G Deployment Architecture: Non-standalone 5G vs. Standalone 5G – Source: GSMA: securing the 5G era

STANDALONE 5G

SA 5G networks include both a 5G RAN and a cloud-native 5G core, something NSA networks lack and substitute with a 4G core. SA networks can perform essential 5G functions, such as reducing latency, improving network performance and centrally controlling network management functions, because of their 5G cores.

The biggest disadvantage of SA is it's costly to implement and time-consuming for network professionals to learn the new 5G core infrastructure. Regardless, MNOs are making the shift to SA because NSA can serve as a step toward 5G networking, but it isn't considered true 5G due to its reliance on 4G LTE. Benefits of SA 5G include reducing power consumption, as it uses only one method of cellular connectivity and uses less power to support a network, and supporting more 5G use cases, i.e., it can deliver essential 5G services to power ultrafast, and scalable networks.

As mentioned above, in the part of 5G scenarios or use cases, all three features, i.e., eMBB, mMTC, and URLLC, support an array of industries and services, including emerging sectors, such as IoT. However, SA 5G is the only deployment mode that supports all three specifications. NSA 5G can only enable enhanced mobile broadband because it has a 4G core that can extend to support the specification. SA can enable all three features because it has a more powerful and more flexible 5G core.

5G SECURITY: CHALLENGES, THREATS AND RISKS

When addressing 5G NR security, it should be considered that the 5G network inherits the 4G LTE network security framework, but provides enhanced security features.
5G cybersecurity can be divided into three layers based on the security model in the communications industry: application security, network security, and product security, as explained in figure-5.

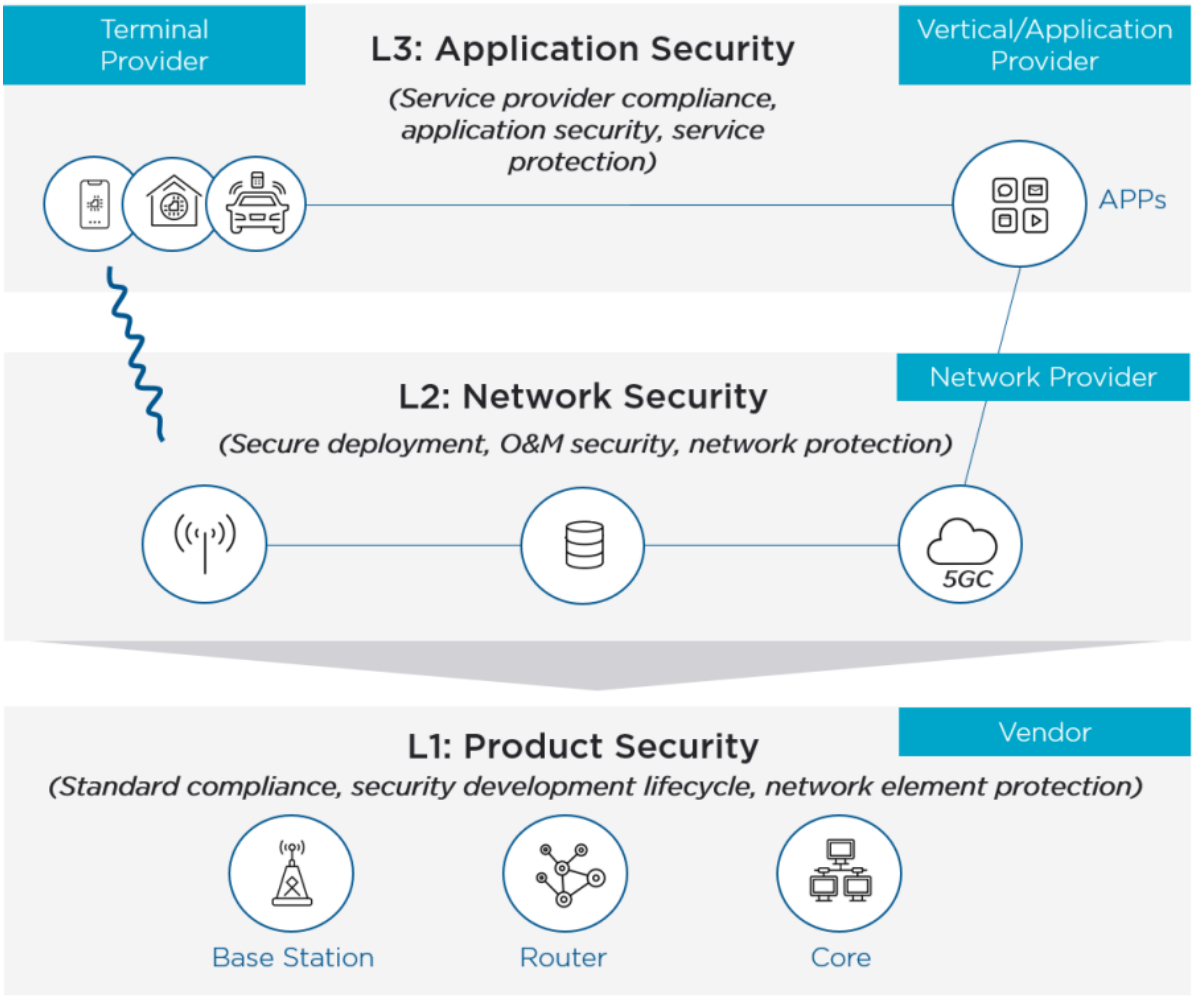

Figure-5: 5G Three-layer cybersecurity model – Source: GSMA: 5G cybersecurity knowledge-base

5G SECURITY CHALLENGES

Table-1 provides a brief list of most common security challenges facing the 5G network cybersecurity. Challenges are divided into three domains, which are the three layers provided in the three layer cybersecurity model as in figure-5.

Table-1: 5G Security challenges

Domain	Security Challenges
Product Security	1. Physical security 2. Base station security 3. Asset mapping 4. Vendor compliance to cybersecurity standards 5. Secure Development Life Cycle
Network Security	1. Secure Deployment 2. Decentralized security 3. Reduced isolation on the network level 4. Transitioning and 3G/4G security vulnerabilities carryover 5. Network monitoring 6. Holistic security orchestration and management (O&M) 7. Accountability 8. Network slicing
Application Security	1. Connectivity diversity 2. Lack of security in most IoT devices 3. Service Protection 4. Application criticality

A. Product Security:

This security domain includes the security of all the hardware products used in the 5G physical network. This includes the base stations, routers, switches, …etc. It is the responsibility of the vendor to ensure that the equipment is secure and to clarify the security capabilities of the equipment. There are many noteworthy cybersecurity standards in this domain, the most famous one is NESAS which is globally recognized by the equipment manufacturers as a cybersecurity assurance standard. The current challenges in this domain are the following:

1. Physical security

The ability to apply practices that are similar to the practices being applied in 3G/4G networks in terms of base station physical security will pose a challenge since the coverage of 5G cells is way minor than the coverage of the cells of its predecessors, which means that way more cells will be needed to cover the same area, with each

needing reliable connectivity and physical security. Physically securing the environment where base stations are physically exposed, ensuring that access is restricted to authorized personnel only.

2. **Base station security**

The real challenge for the base station equipment is that it must be secured by the vendors and must have the following minimum-security capabilities:

• Hardware Hardening: The hardware is hardened by disabling the unused ports, enabling tampering detection alarms, and triggering an alarm upon any port state change.

• Secure Boot: The hardware equipment must be able to verify the boot chain and verify the bootloader, kernel, and applications to prevent tampering with the equipment during the boot process.

• OS Hardening: Harden the OS security settings by disabling unused services and applications, disable logins from OS users, and use the latest security patches.

• Base Station Encryption: All the encryption keys and sensitive data in the base station must be stored in secure tamper resistant hardware.

• Rogue Base Station Detection: The base station hardware and firmware must be able to detect the rogue base stations in the area of coverage, and report to the operator.

• Anti-DDoS mechanism: The base stations must be able to detect DDoS attacks and mitigate these attacks through using specific control mechanisms.

3. **Asset mapping**

One of the most important steps that we need to take when handling 5G security challenges is critical asset mapping and understanding all networks and services utilizing 5G should be analyzed in order to map all associated critical assets so that they can be prioritized in security planning and management, this is always the first step towards securing any given environment.

4. **Vendor compliance to cybersecurity standards**

The equipment vendors must comply with the cybersecurity standards when designing the equipment. For example: a secure end-to-end encrypted OTA update mechanism must be designed, using secure encryption algorithms according to the latest FIPS and NIST recommendations, …etc. This shall ensure that the equipment is using secure firmware, hardware, and secure communication.

5. **Secure Development Life Cycle**

The vendors must comply with the secure development life cycle during the design and development phases of the equipment. The real challenge in this case is performing

security testing on every part of the hardware and software during the development, then performing penetration testing on the final product after the implementation phase. To do so, the vendor must implement the SDLC process in the development departments and must have a strategy for patching the resulting vulnerabilities from the security testing.

B. NETWORK SECURITY:

5G networks have a very special nature, they replace the legacy hardware based mobile networks with a virtualized environment, this virtual environment is extremely flexible, it is designed and built around the functionality. NF (network function) and NFV (network function virtualization) are key concepts in 5G networks. Each 5G network can differ from other networks with its own design and functions depending on the connected devices and the covered applications and services. This inherently creates security problems that are specific to 5G technology. In the current section, we discuss 5G network specific security challenges.

1. **Secure Deployment**

Currently, all the 5G vendors are planning to support cloud architecture because this strategy facilitates low-cost network deployment and service provisioning. The challenge here is that the vendor must be able to conform with the related cybersecurity standards while deploying the network. For example, the European Telecommunications Standards Institute (ETSI) is responsible for standard formulation for network functions virtualization (NFV) technologies used in cloud architecture. The vendors are planning to globally follow this standard for the cloud deployment of the 5G networks.

2. **Decentralized security:**

5G networks have way more hardware points of contact than their predecessors, which makes it a lot harder to perform security checks. The nature of SDN (Software Defined Network) makes some traditional network security concepts such as deploying firewalls and other security devices at certain points of the network an old practice that needs to be adapted to this new technology. The traditional intrusion detection, log management, security event management and correlation, will not apply in the same way that it does for traditional physical networks.

3. **Reduced isolation on the network level:**

In legacy networks NFs (network functions) where usually performed through physical devices, in 5G networks however these network functions are performed virtually which results in this isolation between the different functions that the network performs, since network segmentation is a vital part of securing any network, this characteristically makes the network less secure, performing network segmentation from a security point of view will be done virtually (within the same network slice)

4. **Transitioning and 3G/4G security vulnerabilities carryover:**

Migrating from 3G/4G to 5G is not a simple or easy thing to execute, it requires replacement of hardware along with massive software changes this produces security challenges, security professionals need to make sure that they don't carry over the existing security problems associated with 3G/4G networks into the 5G ecosystem they also need to address the security problems that are bound to come up when they use a hybrid of 4G and 5G during transitioning stages. Most 5G networks still rely on a 4G network cores and they only use 5G connections when they need more bandwidth and lower latency this creates a problem because 3G/4G networks have some security issues that were resolved in 5G, there is a downgrade attack (aka cross protocol attack) were

hackers manipulate phone connections into downgrading to Legacy networks enabling themselves to access 3G/4G security loopholes For example the International mobile subscriber identity (IMSI) is protected in 5G, in the downgrade attacks hackers are able to force the phone into sending their IMSI number unencrypted so that they can monitor the users' activity (although they cannot read the content of their messages, but their identity is not protected to the same level as in 5G)

5. **Network monitoring**

Network monitoring has always been a challenge due to the fact that the traffic is usually larger than the human capacity to monitor properly in order to detect any malicious traffic and deal with it in a timely efficient manner. Security professionals have always struggled with innovating new ways to augment traffic monitoring using AI, Threat intelligence and automation amongst many other techniques to spot the anomalies in the increasing magnitude of the traffic going through their networks. With the introduction of the phenomenal speeds associated with 5G traffic, the mission will be much harder. Dealing with real-time gigantic network traffic will pose a genuine challenge for security professionals.

6. **Holistic security orchestration and management (O&M)**

Security orchestration and management of a network as complicated as 5G network is a nightmare, the level of correlation and organization of security management, avoiding cumbersome process and procedures' duplication or mis-deployment, all this needs to be carefully designed and managed. Established mutual agreements and security related policies need to exist between the different PLMNs (Public Land Mobile Networks) and the IPX (entity) providers, for example, covering X.509 PKI solution for using TLS when securing the 5G inter-domain SBA control plane traffic between the IPX entities and the Security Edge Protection Proxy SEPPs in different PLMNs.

7. **Accountability**

It is only natural that there will be differences in security policies, procedures and equipment between the different PLMN (public land mobile networks) and different service providers, if no rules regarding the accountability and segregation of security duties and responsibilities are established, there are bound to be a lot of mistakes that can produce different security threats and risks.

8. **Network slicing**

One of the main factors that make 5G great is network slicing, it allows mobile operators to create multiple logical blocks that distinctively differentiate types of traffic allocating and prioritizing resources to suit these different types providing segments of their network to specific customer use cases. This is a main differentiator that makes 5G much faster and reliable, however, it has its security drawbacks. The nature of traffic going through every slice of the network is totally different from the traffic going through other network slices, this reflects greatly on security. There is a very common saying that circles around amongst security professionals, "In order to secure a network, you need to understand its nature and the nature of the traffic passing through this network".

Since the traffic going through every slice of the 5G network is different that the traffic going through other network slices, it is imperative that the security professionals take this into consideration, this can make the security measures for every network slice very different that its counterpart in other slices Because what we will be looking for as a source of threat in a given network slice will be very different than what we will be trying to catch in another slice.
Each network slice is meant to have its own function, resources and security policies, the whole network should not be affected by the compromise of a single network slice, in theory, but in practice different slices share resources, so, this is bound to create security risks not to mention the fact that historically hackers have used different techniques to disguise their data to be able to penetrate networks and reach their target. So, it is not wise to assume that you are risk-free just because the network slice that you are using has a reasonable level of separation from other network slices.
A seasoned security professional wouldn't apply the same rules and features, settings in the above security devices/solutions to every network slice in a 5G network, every slice of that work needs its own rules and features according to the traffic passing through the slice in question. We can't treat IoT traffic the same way that we treat mobile data or smart automotive data. Each of them has its own nature, each of them has different cyber-attacks that apply to its nature, topology and data transmission protocols, each of them includes different types of assets (for a given slice data availability can be extremely critical for another slice data integrity can be most critical and for a third slice data confidentiality can be the most critical element to protect). The critical assets handled by a certain network slice can be our guide to protecting this slice.

C. APPLICATION SECURITY:

The nature of the devices connecting to the 5G networks need to be considered while architecting security, one of the main attributes that are exclusive to the 5th generation of mobile communication is the variety of the devices and applications connecting to the network, is enabled by the new traffic speed and low latency provided by the 5G technology.

1. Connectivity diversity

One of the main issues that make 5G networks insecure is the fact that it connects a multitude of devices and applications, each of these devices is a potential entry points for hackers and poses a potential threat especially when we consider the fact that IoT devices are inherently insecure.

2. Lack of security in most IoT devices

From a security point of view, the first and most severe problem associated with IoT devices is the fact that most IoT devices do not consider security right from early stages of design not to mention deployment and production modes, along with the fact that in a lot of cases software patches are not that easy to apply. This can clearly be seen in many of the cyber-attacks associated with IoT devices like the Mirai botnet attack.5G has the potential of creating the golden era for IoT devices connectivity. The existence of billions of IoT devices connected to 5G networks Will create millions of possible

beach points especially with the variety that will accompany these devices from smart TVs, Smart refrigerators, smart illumination systems to smart locks and the list goes on unendingly. A good level of understanding of the nature of the device that is connecting to a certain 5G network can be our main tool to defend different slices and segments of the network against attacks that might originate from certain connected devices.

3. **Service Protection**

In cyber security you are only as strong as your weakest link, in 5G security our weakest link is IoT devices, the advantages of applying security measures to IoT devices should be communicated to IoT device manufacturers in order to encourage them to produce more secure devices, aside from applying strong regulations to mitigate the threats associated with these devices.

From the Network points of view there should be a classification where IoT devices with different levels of security would be addressed differently from a traffic monitoring, network segmentation and security measures point of view.
There are plenty of cybersecurity standards which target securing the IoT services in different industries. The challenge here is forcing the application developers and IoT device manufacturers and service providers to comply with these IoT cybersecurity standards. These standards include: IoT Security Foundation cybersecurity guidelines, UK Best Practice for IoT cyber security, ..etc.
One of the main advantages of 5G is the power efficiency enabled by the technology, where 5G connected devices can maintain steady connection with low power consumption. For a lot of data types, encryption is a necessity to maintain data integrity and confidentiality. With the fact that a decent level of data encryption Applied to different IoT devices will create a need for more processing power and more power consumption hence larger cost, it is rare to find an IoT devices that applies sufficient encryption to protect the data collected, stored or transmitted by this device. This enables attackers to easily identify and use IoT devices connected to a certain network planning and executing more precise and effective cyber-attacks.
Some examples of cyber-attack we're IoT devices can be utilized:

- Distributed denial of service DDOS
- Man-in -the-middle attack (MITM)
- Data sniffing

4. **Application criticality**

Some applications that use 5G networks for connectivity are definitely more critical than others, devices used in critical applications that can directly affect human life should always be treated differently than applications with lower risk profile, enabling more cohesive security prioritizing and incident management.

5G Security Risks:

5G network has its exceptional data transfer rates and it also has its very special connectivity diversity, these two qualities along with the virtual nature of the network pose security risks that need to be comprehended by security professionals to secure this environment, in the next section we will try to map these risks with the challenges that were discussed in the previous section.

1. Lack of User Awareness:

The lack of user awareness is a problem that faces security professionals everywhere, common user mistakes and social engineering that exploits the lack of awareness are usually the main entry point for hackers into any organization, in this regard, people tend to fancy the use of any new technology that makes their life easier disregarding the security and privacy concerns associated with this technology, technology users need to be educated on the importance of understanding different technologies and how they can be used against them and their organizations, how they should apply the software updates, how they shall not keep the default username and password on any of the IoT devices that they use and how they need to integrate security into the process of selecting and buying a product.

2. 5G Equipment Provisioning:

Importing 5G equipment and technology have been restricted in several countries including the US, Britain, Australia, Germany and other countries in Eastern Europe because there are concerns that equipment producers have deliberately built loopholes into the equipment. Small businesses tend to ignore 5G security recommendations to avoid enduring the cost of replacing their equipment with other equipment that is compliant with the national security standards and their respective countries, some countries are doing their efforts to resolve this issue in July 2021 the federal communications commission (FCC) agreed to subsidize small telecom companies to replace equipment from untrusted suppliers to avoid the risk associated with the usage of non-security compliant equipment.

3. Physical Threats:

5G networks antennas cover much smaller areas than 3G and 4G antennas, this entails installation of numerous antennas and base stations, this provides hackers with new physical targets.

4. The Use of Common Internet Protocols:

While previous generations 2G/3G/4G have primarily used SS7 and diameter protocols the fact that 5G uses common Internet protocols like HTTP & TLS made the entry barrier lower for both operators and hackers.

5. Critical Applications:

A massive risk associated with 5G network compromise would be the nature of the applications that use the 5G network to connect. For example, medical applications, transportation, and autonomous driving. These applications deal directly with people and can directly endanger human life. So, while 5G networks are used for the smallest things like low-end IoT devices, it is also used to cover connectivity for some very critical applications, this poses huge risks that need to be handled carefully.

6. Distributed Denial of Service DDoS:

An attacker can overload a network and take it all off-line, the magnitude of traffic in 5G networks Will not make it any easier to defend against such attacks.

7. Botnet Attacks:

A hacker can gain control of any number of devices connected to a certain network and use them collectively to launch massive cyber-attacks. The heavy presence of IoT devices in 5G networks makes botnets an especially dangerous risk, specially in launching DDoS attacks.

8. Man-In-The-Middle Attack (MITM):

The attacker is able to intercept communications between two parties and alter the data for their benefit.

9. Data Sniffing:

The fact that a lot of IoT devices data are not encrypted, data sniffing and interception compromise data confidentiality enabling the hacker to abuse this data inflicting harm to their victim.

10. Data Extraction:

The unprecedented connection speed of 5G enables data extraction rates that would enable any attacker to extract huge amounts of data in a very short period of time.

11. Privacy:

When using IoT devices, privacy is always the main concern. Privacy becomes more in scope when we have very high speed connectivity network like 5G. The ability to transfer all kinds of data (video, audio, …etc) collected by smart IoT devices in this high-speed network enables potential attackers and privacy violators to gain access to data that they are not supposed to access, violating the privacy of average users.

12. Use of Open-source Software:

The increased use of open-source software that comes with the large variety of applications used in 5G poses a lot of security challenges, especially to the Secure by design principle and preventing deliberate security flows.

13. SUPPLY CHAIN:

Due to the very large numbers of connected devices, new risks are introduced such as counterfeit components, poor design, malicious software and hardware, which may cause IP (intellectual property) theft, network integrity compromise and network failure.

14. MALICIOUS INSIDERS DETECTION:

Due to the size of the Network, the diversity of connected devices and the complexity of the associated supply chains, the risk of having malicious insiders in any of the aforementioned elements should always be considered.

15. ASSOCIATED TECHNOLOGIES THAT MAKE 5G LESS SECURE:

The following technologies are strongly related to 5G and they should be considered when addressing any 5G security related issues.
LTE-advanced, radio access networks (RANs), massive MIMO (maMIMO), millimeter wave (mmWave), artificial intelligence (AI), software-defined networking (SDN), edge computing, network function virtualization (NFV), the internet of things (IoT), cloud computing, and network slicing.
While these technologies vary in their level of security problems and associated vulnerabilities, they represent possible threats and potential entry points for hackers.

THE 5G CYBER SECURITY FRAMEWORK

ABOUT THE FRAMEWORK

The 5G security framework provides a set of security requirements and controls along with a security assurance mechanism for ensuring the security of the 5G NR deployed architecture and components.

The set of applicable baseline security requirements are defined according to the perspective of the framework's user. Framework's main users might be a 5G network operator or an organization that provides 5G enabled technologies, applications, systems or services.

5G cybersecurity is a shared responsibility of key stakeholders, including network operators, interconnection providers, equipment vendors, application providers, standards organizations, governments, and regulators, each with their own clearly defined responsibilities. These responsibilities, when fulfilled, can enable the secure deployment and operations of 5G systems. Figure-6 states the major stakeholders of the 5G NR technology, it is mainly inspired by the ENISA 5G cybersecurity standards and the GSMA 5G cybersecurity knowledge-base.

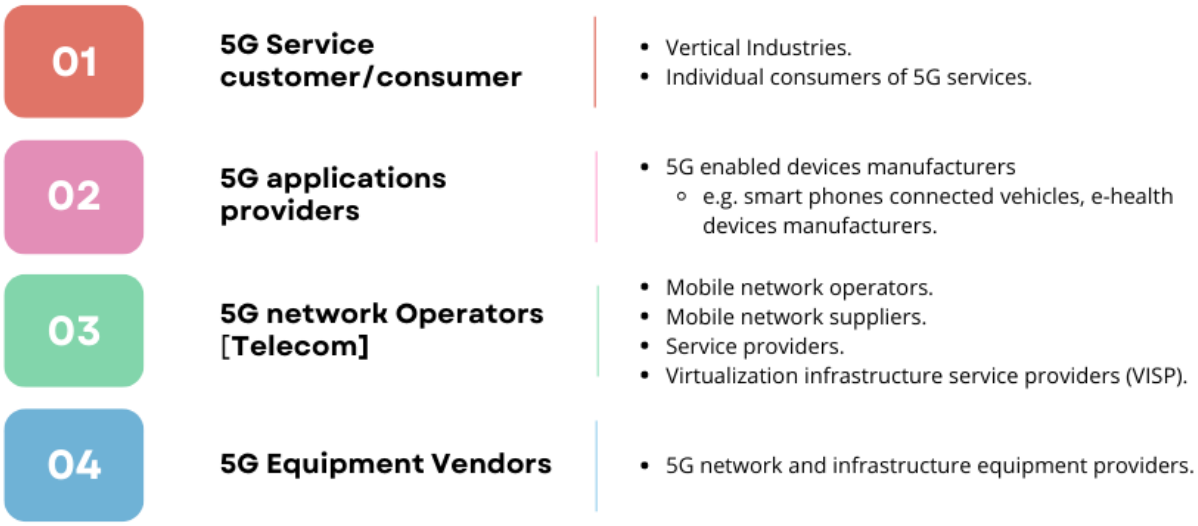

Figure-6: 5G technology major stakeholders

The 5G cybersecurity can be divided into three layers based on the security model in the communications industry, as described in figure-5. Figure-7 explains the three cybersecurity layers along with its focus and responsible entities.

Each security layer focuses on a certain category of security requirements to ensure security of the parts involved. This will be the base in categorizing the 5G cybersecurity requirements and controls.

Figure-7: Three layers of the 5G cybersecurity model & responsible entities

The security assurance mechanism, as presented in figure-8, starts with conducting a risk assessment procedure, followed by defining the applicable set of requirements and controls and finally a conformity assessment is carried out to ensure compliance of the 5G components of concern to the applicable set of controls.

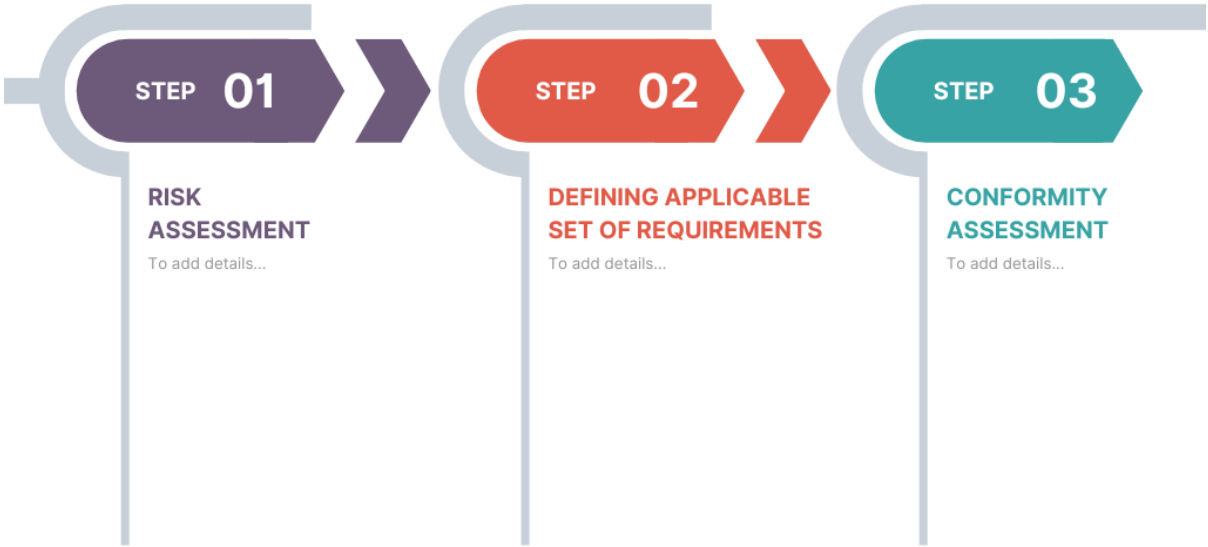

Figure-8: Security assurance mechanism procedures

RISK ASSESSMENT

5G networks will be cloud-based, its infrastructure (the physical telecom infrastructure) consists of interconnected data centers, or "clouds". These provide a virtualization environment, where network functions are running as virtual network functions on a shared infrastructure that provides virtualized compute, networking and storage resources.

Criticality classification:

Table-2: Criticality classification of 5G infrastructure assets

5G function/network element	Classification	Comment
Data Centres	Critical	- Data centres host: Critical 5G network functions, sensitive network and user data and interfaces to other networks. - towards the edge (DC) the risk may decrease as the impact of successful attacks is regional.
Transport networks **(nodes and links, e.g. optical switches and fibres; SDN switches)**	High	- physically exposed, disruption of network operation possible, - threat of wiretapping can be mitigated by encryption, - redundancy can overcome attacks against single transport nodes and links
IPX entities	High	- similar to transport networks, traffic can be protected using the 3GPP specified mechanisms or those specified by other entities such as the GSMA.
Non-virtualized base stations	Medium	- Attacks have usually local impact, redundant coverage from other base stations possible, sensitive data protected in the base station's secure environment; however injection of a DoS attack into the core is also a risk
Antenna	Low	- Low impact; only localized DoS attacks
UICC/USIM	Low	- high hardware security, very local impact when hacking or cloning a USIM

HIGH-LEVEL SECURITY CONTROLS [TECHNICAL REQUIREMENTS]

5G CYBERSECURITY BASELINE REQUIREMENTS

This section provides the high-level cybersecurity requirements controlling the security of the 5G technology. The controls are organized into a set of security capability domains, which are mainly categorized into either organizational or technical security requirements. Moreover, technical security requirements are divided into infrastructure (physical and virtual) security and network and service management security categories.

5G CYBER SECURITY CATEGORIES

Security domains are high-level categorizations used for cataloging the organizational and technical security controls considered. These categories are important and relevant to commercial and private 5G networks. Security domains are categorized according to the three-layer 5G cybersecurity model in figure-7 based on what assets need security into four main categories:

- **Product Security Category (PSC)**
  This category focuses on cybersecurity protection of trusted and secure cloud resources required for operating 5G, including both physical and virtualized infrastructures. Like 5G Core Network functions, radio access network (RAN) components, and associated workloads.

- **Network and Service Management Security Category (NSSC)**
  This category focuses on cybersecurity protection of 5G core network and service management assets.

- **Application Security Category (ASC)**
  This category focuses on cybersecurity of 5G enabled applications, services, and terminal (end-point) devices.

- **General Security Category (GSC)**
  This category focuses on cybersecurity protection of 5G core network and service management assets.

In these security categories and domains, the document follows the main requirements provided in the “5G cybersecurity standards” by the European Network and Information Security Agency (ENISA) and the “NIST Special Publication 1800-33B: 5G Cybersecurity” (NIST SP 1800-33B) by the National Institute of Standards & Technology (NIST).
The security technical requirements are organized into 12 Domains according to table 3. These technical requirements describe the required security controls for the service security level from a technical point of view.

Table-3: List of 5G security requirements categories and domains

Category		Domain	References
Technical Requirements	Product Security Category (PSC)	[PSC1]: Physical Infrastructure Security SO 9	ENISA 5G Cybersecurity Standards & NIST SP 1800-33B
	Network and Service Management Security Category (NSSC)	[NSSC1]: Network and Information Systems Access Control and Integrity SO 11, 12	ENISA 5G Cybersecurity Standards
		[NSSC2]: Critical Data Protection SO 13, 14	
		[NSSC3]: Subscriber privacy	NIST SP 1800-33B
		[NSSC4]: Radio network security	
		[NSSC5]: Authentication enhancements	
		[NSSC6]: Interworking & roaming security	
		[NSSC7]: Network slicing security	
		[NSSC8]: Internet security protocol recommended practice	
	Application Security Category (ASC)	[ASC1]: Application security	ENISA 5G Cybersecurity Standards & NIST SP 1800-33B
		[ASC2]: API security	
	General Security Category (GSC)	[GSC1]: Continuous Monitoring, Assessment SO 23, 24, 25, 26, 27 ISC-3.1	ENISA 5G Cybersecurity Standards

5G Cybersecurity Technical Requirements

This section provides technical and functional security capability domains. They are divided into product (physical and virtualized) security category, network and service management security category, application security category and general security category.

1. [PSC1]: Physical Infrastructure Security

This section includes security policies and controls for physical and environmental security, security of supplies. It follows the ENISA 5G Cybersecurity Standards selected security objectives SO9 and SO10 and the NIST SP1800-33B selected requirements from ISC-1.1 through ISC-1.5 and ISC-3.2.

Table-4: Physical infrastructure security requirements [Sample]

Req. No.	Security Requirement	Responsible Entity
PI-01	Prevent unauthorized physical access to facilities and set up adequate environmental controls, to protect provider assets against unauthorized access, burglary, fire, flooding, etc	
PI-02	Implement a policy for physical security measures and environmental controls. Industry standard implementation of physical and environmental controls. Apply reinforced controls for physical access to critical assets.	
PI-03	Evaluate the effectiveness of physical and environmental controls periodically. Review and update the policy for physical security measures and environmental controls, taking into account changes and past incidents.	
PI-04	Are there documented, additional, risk-based controls for physical security for MEC and base stations included in the policy for physical security measures?	
PI-05	Are there documented additional, adequate physical infrastructure controls (for example perimeter security for infrastructure and administrative premises, alarms, and CCTV for detecting and recording incidents), especially for equipment locations which are unmanned, in place?	

2. [NSSC1]: Network and Information Systems Access Control and Integrity

This section includes security policies and controls for physical and environmental security, security of supplies. It follows the ENISA 5G Cybersecurity Standards selected security objectives SO11 and SO12.

Table-5: Network & information systems access control & integrity requirements [Sample]

Req. No.	Security Requirement	Responsible Entity
NI-01		
NI-02		
NI-03		
NI-04		
NI-05		

To be completed…

3. [NSSC2]: Critical Data Protection

This section focuses on cybersecurity and protection of critical data.

Table-6: Critical data protection requirements [Sample]

Req. No.	Security Requirement	Responsible Entity
DP-01		
DP-02		
DP-03		
DP-04		
DP-05		

To be completed…

4. [NSSC3]: SUBSCRIBER PRIVACY

This section focuses on cybersecurity protection of 5G core network and service management assets.

Table-7: Subscriber privacy requirements [Sample]

Req. No.	Security Requirement	Responsible Entity
SP-01		
SP-02		
SP-03		
SP-04		
SP-05		

To be completed…

CONFORMITY ASSESSMENT

Conformity assessment is the final step of the 5G security assurance process, where conformity with the relevant security requirements is assessed. [To be completed…]

REFERENCES

- ETSI TS 133 501 V17.7.0 (2022-09): 5G; Security architecture and procedures for 5G System (3GPP TS 33.501 version 17.7.0 Release 17) - https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/17.07.00_60/ts_133501v170700p.pdf
- ETSI TS 133 501 V15.2.0 (2018-10): 5G; Security architecture and procedures for 5G System (3GPP TS 33.501 version 15.2.0 Release 15) - https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/15.02.00_60/ts_133501v150200p.pdf
- ENISA Threat Landscape for 5G Networks Report https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks
- ENISA: 5G Cybersecurity Standards https://www.enisa.europa.eu/publications/5g-cybersecurity-standards
- ENISA: NFV Security in 5G - Challenges and Best Practices - https://www.enisa.europa.eu/publications/nfv-security-in-5g-challenges-and-best-practices
- NIST SPECIAL PUBLICATION 1800-33A: 5G Cybersecurity https://csrc.nist.gov/publications/detail/sp/1800-33/draft
- NIST Special Publication 800-53A Revision 5: Assessing Security and Privacy Controls in Information Systems and Organizations - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar5.pdf
- NIST Special Publication 800-30 Rev. 1: Guide for Conducting Risk Assessments - https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final
- 5G Related Aspects in ITU-R Working Party 5D (Responsible group for terrestrial IMT in ITU-R) https://www.itu.int/en/membership/documents/missions/gva-mission-briefing-5g-28sept2016.pdf
- GSMA - Securing the 5G era - https://www.gsma.com/security/securing-the-5g-era/
- GSMA - 5G cybersecurity knowledge base - https://www.gsma.com/security/5g-cybersecurity-knowledge-base/
- Huawei 5G Security - White Paper - https://www-file.huawei.com/-/media/corp2020/pdf/trust-center/huawei-5g-security-white-paper-2021-en.pdf?la=en

- NOKIA 5G Security Risks and Mitigation Measures - https://www.nokia.com/sites/default/files/2021-05/Whitepaper-5G-security-Nokia-STC-March-31-2021.pdf
- NCTA: 5G Security & Protection Framework - https://www.nctatechnicalpapers.com/Paper/2021/2021-5g-security-protection-framework/download