EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA THREAT LANDSCAPE FOR 5G NETWORKS

Threat assessment for the fifth generation of mobile telecommunications networks (5G)

NOVEMBER 2019

ABOUT ENISA

The European Union Agency for Cybersecurity (ENISA) has been working to make Europe cyber secure since 2004. ENISA works with the EU, its member states, the private sector and Europe's citizens to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. Since 2019, it has been drawing up cybersecurity certification schemes. More information about ENISA and its work can be found at www.enisa.europa.eu.

EDITORS
Marco Lourenço, Louis Marinos, ENISA

CONTACT
For contacting the authors please use enisa.threat.information@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

ACKNOWLEDGEMENTS
We would like to thank the members of the 5G Threat Analysis Expert Group, Ioannis Askoxylakis, Pascal Bisson, Jean-Philippe Wary, Panagiotis Papadimitratos and Jorge Cuellar for supporting the ENISA team in information collection, knowledge transfer in the subject matter and revision of interim drafts of this report.

ISBN: 978-92-9204-306-3, DOI:10.2824/49299

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Due to its impact expected in the economy and society, the fifth generation of mobile telecommunications (5G) is one of the most important innovations of our time. Expectations grow with the broadband capabilities of 5G, accessible to everyone and everywhere at a better quality and reliability. From a conceptual perspective, 5G technology promises to deliver low latency, high speed and more reliable connections to new generations of autonomous systems and edge-type devices, covering both massive and critical machine-type communications.

Furthermore, 5G technology is driven by use cases with a wide range of requirements. One of the first commercial offers expected, is the Fixed Wireless Access (FWA) for dense urban areas. Other use cases, such as the ones demanding dedicated coverage, vertical solutions (i.e. connected vehicles), manufacturing, Industry 4.0, IIoT, energy, and healthcare, will come at a later stage. Experts agree that verticals will be the main driving force in future deployments of 5G Networks. These will play an essential role in investment strategies of Mobile Network Operators MNOs.[1]

The fifth generation of mobile telecommunications (5G) is one of the most important innovations of our time due to the impact expected in the economy and society.

As networks and applications evolve further, there will be even more opportunities to enhance existing use cases in addition to more verticals becoming part of the 5G infrastructure. As an example, 5G will be highly beneficial for industrial use cases demanding higher data rates and lower latency such as augmented reality (AR) and AI-based applications. Significant bandwidth capabilities will assure the consistency of high-resolution images and video streaming, similarly to sensor-rich environments with high connection density.

In the realm of this transition, the industry forecasted 1.5 billion users subscribed to a 5G network and coverage to reach over 40 percent of the world's population by 2024.[2] According to the European 5G Observatory, citizens should have 5G access by 2020.[3] In terms of geographical coverage, 5G is expected to be deployed first in dense urban areas and later, in less populated sub-urban and rural areas.

Mobile communication systems have been prone to security vulnerabilities from their very inception. In the first generation (1G) of mobile networks, mobile phones and wireless channels became a target for illegal cloning and masquerading. In the second generation (2G), message spamming became common, not only for pervasive attacks but also for injecting false information or broadcasting unwanted marketing information. In the third generation (3G), IP-based communication enabled the migration of Internet security vulnerabilities and threats into the wireless domain. With a growing demand for IP based communications, the fourth generation (4G) enabled the proliferation of smart devices, multimedia traffic, and new services into the mobile domain. This development led to a more complex and dynamic threat landscape[4,5].

With the advent of the fifth generation (5G) of mobile networks, security threat vectors will expand, in particular with the exposure of new connected industries (Industry4.0) and critical services (connected vehicular, smart cities etc.). The 3G revolution, introducing internet

[1] https://nis-summer-school.enisa.europa.eu/#program, accessed September 2019.
[2] https://www.ericsson.com/assets/local/mobility-report/documents/2019/ericsson-mobility-report-world-economic-forum.pdf, accessed September 2019.
[3] http://5gobservatory.eu/wp-content/uploads/2019/01/80082-5G-Observatory-Quarterly-report-2-V2.pdf, accessed September 2019.
[4] http://www.webtorials.com/main/resource/papers/lucent/paper94/MobileNetworkThreats.pdf, accessed September 2019.
[5] https://ieeexplore.ieee.org/document/7547270, accessed Spetember 2019.

connectivity into the mobile network infrastructure, is replicated in 5G connected services and vertical infrastructures. The integration with and exposure to the data network, is even more prevalent across the 5G network.

The growing concerns over availability and protection of user data and privacy will exacerbate with the security challenges introduced 5G. Hence, the most critical challenges relate to the resilience of the network and the protection of content and metadata of 5G communications.

This report draws an initial threat landscape and presents an overview of the challenges in the security of 5G networks. Its added value lays with the creation of a comprehensive 5G architecture, the identification of important assets (asset diagram), the assessment of threats affecting 5G (threat taxonomy), the identification of asset exposure (threats – assets mapping) and an initial assessment of threat agent motives.

The ENISA 5G Threat Landscape is fully aligned with the EU Coordinated Risk Assessment of the Cybersecurity of 5G networks.

The content of this Threat Landscape is fully aligned with the EU-Wide Coordinated Risk Assessment of 5G networks security.[6] The EU-wide Coordinated Risk Assessment, published on the 9th of October 2019 by the European Commission, which built on the methodological approach developed for the threat landscape, presents in Section 2(D) ten high-level risk scenarios based on the information provided by Member States within National Risk Assessments.

The ENISA 5G Threat Landscape leverages from and complements this information by providing a more detailed technical view on the 5G architecture, sensitive assets, cyberthreats affecting the assets and threat agents. The information produced for this Threat Landscape is based on publicly available information published by 5G standardisation groups and bodies (i.e. ETSI, 3GPP, 5GPPP) and 5G stakeholders such as operators, vendors, national and international organisations. An expert group with experts from mobile operators, vendors, research and European Commission has contributed to ENISA's work with information on existing 5G material, current developments in the market and research and quality assurance of the current document. Moreover, the members of the NIS CG, European Commission and ENISA have reviewed the current document.

In particular, the content of this Threat Landscape includes:

- A detailed architecture, outlining the most important/critical 5G infrastructure components, through nine detailed 'Zoom-ins' of 5G architectural elements mentioned in section 2 (B) of the Coordinated Risk Assessment. Examples of these elements include the core network functions (NFV), management and network orchestration (MANO), radio access network (RAN), and others;

- A detailed threat assessment on 5G infrastructure components considering the identified sensitive assets. The assessed threats refine/extend the ones presented in section 2 (A) of the Coordinated Risk Assessment. A mapping provided in the annexes show the relationships of the both reports (see Annex C, a mapping between ten risk scenarios and assessed threats);

- An initial assessment of the motives and capabilities of threat agents concerning 5G assets, extending the information provided in section 2 (A) of the Coordinated Risk Assessment;

[6] https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security, accessed October 2019.

- The provision of a more complete list of stakeholders involved in activities related to 5G, derived from the ownership of the identified sensitive assets, but also from input received from involved experts.

The ENISA 5G Threat Landscape provides a basis for future threat and risk assessments, focussing on particular use cases and/or specific components of the 5G infrastructure, which may be conducted on demand by all kinds of 5G stakeholders.

LIST OF ACRONYMS AND ABBREVIATIONS

3GPP	3rd Generation Partnership Project
5GC	5G Core
5G-PPP	5G Infrastructure Public Private Partnership
AADU	Active antenna distributed unit
AF	Application function
AKA	Authentication and key agreement
AMF	Access and mobility management function
AP	Access point
API	Application programming interface
ARLC	Air radio link control
ARP	Address resolution protocol
ARPF	Authentication credential repository and processing function
ARPU	Average revenue per user
AS	Access stratum
AUSF	Authentication server function
BH	Backhaul
CN	Core network
COTS	Commercial of the shelf
CSMF	Communication service management function
CU	Control unit (RAN)
DCSP	Data Centre Providers
DN	Data network
DU	Distributed unit (RAN)
E2E	End-to-end
EM	Element management
eMBB	Enhanced mobile broadband
ENISA	European Union Agency for Network and Information Security
EPC	Evolved Packet Core
ETSI	European Telecommunications Standards Institute
FH	Fronthaul
gNB	Base station
HSM	Hardware security modules
IaaS	Infrastructure as a Service
IoT	Internet of things
IP	Internet protocol
ISAC	Information sharing and analysis centres
ISO	International standards organisation
IXP	Internet Exchange Point
LEA	Law Enforcement Agency
MANO	Management and orchestration
MBB	Mobile broadband
Mbps	Megabits per second
MEC	Multi-access edge computing
MIMO	Multi-input multi-output
mMTC	Massive machine-type communication
MNO	Mobile network operator
MTC	Machine Type Communications
NAS	Non access stratum
NBI	Northbound interface
NCA	National Certification Authorities
NCSC	National cybersecurity coordinator/agency/centre
NEF	Network exposure function
NF	Network function
NFVI	Network function virtualisation infrastructure
NOP	Network operator
NR	New radio

NRA	National Regulator
NRF	Network repository function
NS	Network slice
NSD	Network service descriptor
NSM	Network security management
NSMF	Network slice management function
NSSF	Network slice selection function
NSSMF	Network slice subnet management function
NTC	National 5G test centres
OSS/BSS	operations support system/business support system
PDCP	Packet data conversion protocol
PDU	Protocol data unit
PCF	Policy control function
QoS	Quality of service
RAT	Radio access technology
RU	Radio unit (RAT)
SA	Security architecture
SaaS	Software as a Service
SC	Service costumers
SDAP	Service data adaptation protocol
SDN	Software defined network
SEAF	Security anchor functionality
SEE	secure execution engines
SEPP	Security edge protection proxy
SIDF	Subscription identifier de-concealing function
SLA	Service level agreement
SMF	Session management function
SMS	Short message service
SMSF	SMS function
SP	Service providers
SSA	NFV security services agent
SSP	NFV security services provider
SUCI	Subscription concealed identifier
TEE	Trusted execution engines
TPM	Trusted platform module
TRxP	Transmission and reception point
TTM	Time to market
UDM	Unified data management
UDR	Unified data repository
UDSF	Unstructured data storage function
UE	User equipment
UPF	User plane function
URLLC	Ultra-reliable low-latency communication
USIM	Universal subscriber identity module
V2V	Vehicle to vehicle protocol
V2X	Vehicle to everything protocol
VISP	Virtualisation infrastructure service providers
VIM	Virtualised infrastructure manager
VNFD	VNF descriptor
VNFM	VNF manager
VNFFGD	VNF forwarding graph descriptor
VLD	Virtual link descriptor

1. INTRODUCTION

The ENISA Threat Landscape for 5G Networks report delivers some of the most relevant aspects related to the type, origin and objectives of cybersecurity threats targeting this new generation of mobile networks. To better understand these threats, it is essential to know what is at stake and what can be compromised. This report represents a first attempt to identify the most critical components (assets) in a 5G Network, which may become a target to various cybersecurity threats. The task of assessing threats has posed multiple challenges: the overall 5G Infrastructure is a very complex ecosystem in which legacy and contemporary mainstream technologies converge. The production of a comprehensive 5G architecture covering all essential elements/functions constitutes another challenging task. The creation of a coherent and comprehensive architecture employing elements from existing generic 5G architectures requires an alignment with existing and ongoing work produced by standardisation bodies and other relevant entities (e.g. 3GPP, 5GPPP, ITU, ETSI and GSMA). The comprehensive 5G architecture presented in this report is further detailed in various 'Zoom-ins', providing more information on the most sensitive 5G components.

To better understand the cyberthreats affecting 5G Networks, it is essential to know the most critical assets that may be targeted by malicious actors and the threat exposure of these assets.

Another challenge is to identify the threat exposure to specific 5G assets, which are still in an early specification stage within the technology industry, Service Providers and Mobile Network Operators (MNO). Moreover, given that 5G Networks are currently in a pilot phase, the lack of known incidents and information about weaknesses makes the analysis of threat exposure even more challenging. This fact forced us to identify possible 5G cyberthreats by assessing the threat exposure on various subsystems based on previous experience. By analysing existing material - including EU-Wide Coordinated Risk Assessment of 5G networks security -we also collected theoretical cyberthreats identified by analogy to existing mobile networks. For similar reasons, it has been challenging to find relevant information on threat agents targeting 5G components. Hence, the discussion on threat agents is based on the assumption that various motives may justify an attack. Finally, some bibliographical references used as a baseline for this report are still considered as 'work in progress' by the authors (standardisation bodies, vendors, operators, regulators and policymakers). This makes the information collection process even more difficult as it brings 'white spots' for some content that is potentially relevant for the analysis of threats (e.g. vulnerabilities, mitigation controls, implementation guidelines, etc.).

For all the reasons mentioned above, it is worth noticing that this first attempt to analyse 5G threats and assets will need to be extended. It will require regular updates to increase the level of detail, completeness and inclusion of new developments. ENISA may further elaborate this assessment to include more details both at the levels of the 5G infrastructure and the relevant cyberthreats, when requested and on-demand from stakeholders (e.g. European Commission and Member States – NIS Cooperation Group).

For the time being, this report aims at supporting various stakeholders understanding the relevant cyberthreats and the asset exposure within the 5G ecosystem. When requested, ENISA is in a position to support stakeholders 'drilling down' the analysis further, by including granular details from the components in focus and examine the relevance of the assessed cyberthreats.

1.1 POLICY CONTEXT

The present report was prepared following the European Commission Recommendation (EU) 2019/534 of 26 March 2019 Cybersecurity on 5G networks,[7] requesting the Member States to carry out a risk assessment of the 5G network infrastructure. In this recommendation, the European Commission requested ENISA to provide support to the Member States in this exercise by preparing a threat landscape reviewing the most critical aspects of the technology.

Moreover, in the new ENISA regulation, the need to analyse current and emerging risks is expressed. In line with this role, ENISA regulation stipulates that: "the Agency should, in cooperation with Member States and, as appropriate, with statistical bodies and others, collect relevant information." [8] More specifically, it is stated that it should "enable effective responses to current and emerging network and information security risks and threats." [9]

Therefore, the ENISA 5G Threat Landscape aims at contributing to the EU Cybersecurity Strategy and more specifically, to ongoing policy initiatives related with the security of networks and information systems; it streamlines and consolidates available information on cyberthreats and their evolution.

1.2 SCOPE AND METHODOLOGY

The overarching nature of 5G, its complexity, the lack of information on existing deployments, the width and depth of existing specifications and the large number of potential stakeholders involved, makes the assessment of cyberthreats a difficult task. Being aware of this challenge, the European Commission issued a recommendation urging EU Member States to assess the risks and requesting ENISA to outline the corresponding cyberthreats.[10] This report is the main deliverable of this activity. This assessment was not the first attempt for ENISA to describe the landscape. In 2016, ENISA published a Threat Landscape and Good Practice Guide for Software Defined Networks/5G.[11]

The objectives, working modalities, method and scope set for this report are as follows:

- The main objective of this report is to provide a comprehensive overview of the 5G architecture while describing the decomposition of its sensitive assets, structured in accordance with the level of exposure to various cyberthreats. This 5G architecture provides a better overview of the supporting infrastructure and its main components and facilitates the identification of sensitive assets.

- To reduce the amount of material presented in this report, the focus was put on the RAN and CORE components, leaving out any interconnected services, APIs, application components and various sectors/verticals (e.g. Transportation, eHealth, Industrial Internet-of-things (IIoT), Smart Environments, etc.).

- To keep the related material to a manageable size, not every detail from 5G specifications were included in this report. Instead, we considered the various relevant network functions, virtualisation functions, radio access network, network management functions and data household of the relevant components. Detailed information and

[7] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019H0534, accessed September 2019.
[8] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:JOL_2013_165_R_0041_01&qid=1397226946093&from=EN, accessed September 2019.
[9] https://www.enisa.europa.eu/publications/ed-speeches/towards-a-new-role-and-mandate-for-enisa-and-ecsm, accessed September 2019.
[10] https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks, accessed September 2019.
[11] https://www.enisa.europa.eu/publications/sdn-threat-landscape, accessed September 2019.

security requirements for various protocols and interfaces were also not included in this report. These may be included at a later stage in an on-demand basis.

- Technical vulnerabilities were intentionally left out of scope to reduce complexity and to optimise available resources. We plan to assess and analyse technical vulnerabilities in detail in future versions of this report.

- This report does not prescribe any mitigation measures/security controls to reduce the 5G Network exposure. This is ongoing work of various committees. Another reason is the high complexity of 5G infrastructures and the low number of implementations: while some mitigation measures are mentioned in specifications, there are still no good practices in the protection of 5G Infrastructures. A significant amount of work will be required - including the extrapolation of good practices of existing mobile communication - to define security controls needed to protect 5G infrastructures. This work may be performed in future iterations of the 5G threat analysis by taking into account the results of ongoing initiatives (research projects, standardisation work, etc.).

- The scope of this report is in line with previous work developed by ENISA, in particular, the Threat Landscape for Software-Defined Networks/5G.[12]

- This threat landscape complements the information provided in the EU Consolidated Risk Assessment by providing an in-depth analysis of assets and threats, without exposing any confidential information. This principle has been followed during the decomposition of 5G assets and the preparation of the cyberthreat taxonomy. This approach will help future on-demand risk assessments using the present threat landscape (e.g. further focusing the scope in various asset categories, threat types, etc.).

- The report does not contain any content related to current 5G deployment strategies of vendors and MNOs. Instead, it reflects the state-of-play in 5G specification/development work (e.g. 5G-PPP), rather than current 5G deployments/migration paths. It is planned to review this scope in future versions of the threat landscape, pursuing the engagement of stakeholders involved in 5G implementations.

- The development of this report followed a 'best-effort' approach. The collected information is not exhaustive but representative of the matters covered.

- To collect relevant technical knowledge, ENISA has set up an expert group consisting of individuals that are involved in 5G activities from vendors, operators, research/academia and European Commission. The selection has been made based on professional merits of the selected individuals (i.e. ad personam), while at the same time trying to cover the skills from the most representative stakeholder types that are currently engaged in 5G activities.

- The content of this report was restricted to components/matters found in relevant open-source material covering the entire specification, security requirements and research results related to 5G network functions (NFs).

The method adopted for this study is in line with the methodology developed by ENISA for the preparation of its annual Cyberthreat Landscape. According to this methodology, the process

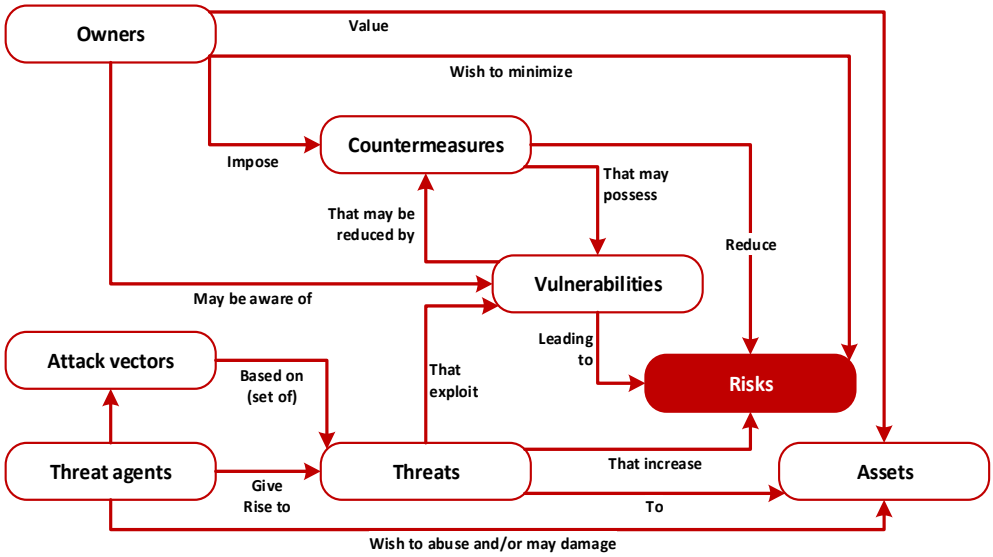
[12] https://www.enisa.europa.eu/publications/sdn-threat-landscape, accessed September 2019.

requires an initial identification of critical assets within the architecture before performing a threat assessment, which evaluates the different levels of asset exposure.

The elements of cyberthreats and the relationship to risks are graphically depicted in**Error! Reference source not found.**. The report describes the different relationships between assets, threats and threat agents. In future versions of this report, we will cover vulnerabilities and countermeasures (mitigation measures/security controls).

The 5G threat landscape may be useful to carry out detailed threat analyses and risk assessments for telecom operators and service providers according to their particular needs and mandate.

Figure 1: Methodology adopted based on ISO 27005



Threats play a central role in a risk assessment, especially when considering the different components of risks. The ISO 27005, a widely adopted risk management standard, defines that risks emerge when: “Threats abuse vulnerabilities of assets to generate harm for the organisation”.[13]

Following this methodology, we have identified assets, threats and threat agents. These constitute the core of the 5G Threat Landscape presented in this report. Furthermore, the identification and analysis of assets and cyberthreats are based on the study of specifications, white papers and literature, without attempting any interpretation/evaluation of the assumptions stated in these reports.

1.3 TARGET AUDIENCE

The objective of this report is to support stakeholders carrying out more detailed threat analyses and risk assessments focussed on particular elements of the 5G infrastructure. Given the current maturity of both 5G specifications and deployments, it is very likely that this need exists across all types of involved stakeholders. Publicly available threat and risk analyses demonstrate the current level of existing 5G assessments that are at rather high and/or abstract level. To this extent, the information provided in this report may help stakeholders to understand the details of 5G infrastructures and the corresponding threat exposure. Moreover, it outlines the gaps supporting the identification of ‘known unknowns’. We believe that this could be a valuable contribution towards the identification areas of future work.

[13] https://www.iso.org/standard/75281.html, accessed September 2019.

Experts working in the telecommunication sector, operators, vendors, and service providers may find this report useful to carry out detailed threat analyses and risk assessments in accordance with their particular needs and mandate (e.g., protect a specific number of components based on asset impact analysis, respond to specific vulnerabilities with customized mitigation measures among others). Both the asset inventory and threat taxonomy can be used as-is or further developed by telco operators or other stakeholders through their own threat analysis and risk assessments. The assessment of threats and vulnerabilities may also enrich a more in-depth analysis of certain components, as far as they are relevant to the assets deployed by the MNOs.

Moreover, many other non-technical stakeholders (e.g. policy-makers, regulators, law enforcement, among others) may find this report useful to understand the current state of threats and respective mitigation practices and measures. For example, the threat landscape identified in this report may support policy actions in the areas of 5G networks, SDN, NFV, cybersecurity, critical infrastructure protection, and other sectors/verticals that plan to use the 5G Network.

Finally, research projects may find the information this report useful in a twofold manner: to be used for threat/risk assessments of newly developed 5G components or to be used as a guide to conduct gap analysis, driving thus new research projects.

1.4 STRUCTURE OF THE REPORT

This report presents the results of the assessment conducted during the research work using the following structure:

- **Chapter 2** presents the stakeholders having a role in deployment, operation and supervision of the 5G infrastructure. They constitute an essential part of the 5G ecosystem. Furthermore, stakeholders are the ones responsible for mitigating the threats identified in this report by introducing specific countermeasures that reduce the risks.

- **Chapter 3** presents the architectural framework of 5G technology by offering a generic architecture and providing various ‘Zoom-ins’ describing the details of various components. These details will contribute to the process of identifying the critical assets of the technology.

- **Chapter 4** presents the 5G asset types identified in our study by providing an overview and identifying groups in the form of a mind map available in annex A. The assets were identified based on the multiple vulnerabilities pointed by the various contributors.

- **Chapter 5** presents a taxonomy of threats. Interrelated threats have been grouped to form a taxonomy that is presented as a detailed mind map in Annex B.

- **Chapter 6** provides information on threat agents. It is a first approach towards the assessment of potential motives emerging from the abuse/misuse of 5G assets.

- **Chapter 7** provides recommendations and conclusions drawn from the threat analysis.

The material used in the analysis produced for this report, which is referenced in footnotes through URLs, was last accessed on the day of publication of this study. The referenced material will help interested readers to dive into further detail in the complexity of the 5G infrastructure when needed.

2. 5G STAKEHOLDERS

Stakeholders will play different roles in the 5G ecosystem. Among other things, these entities will be responsible for assuring the security of the network at different levels and in separate layers. According to the 5G-PPP White Paper on the architecture,[14] the list of stakeholder roles in the 5G ecosystem is the following:

- Service customers (SC);
- Service providers (SP);
- Mobile Network Operators (MNO) also known as Network Operators (NOP);
- Virtualisation Infrastructure Service Providers (VISP);
- Data Centre Providers (DCSP).

Through the elaborations of this report, some additional stakeholders have been identified. Their role is being characterized by the ownership/responsibility relationships to the 5G assets described in this document. In addition, they have been assessed from input received from involved experts. Although their role is not fully defined yet, it is believed that they are/will be concerned with various issues related to the security of the 5G ecosystem. In the following list, we present a short indicative note for each entity and its role:

- **Internet Exchange Points (IXPs)**: Being an important part of current Internet infrastructure, IXPs (data network) providers play an important role in 5G, as they support the end-to-end throughput of the data traffic.[15]

- **National Regulators (NRAs):** Regulators will be asked to regulate various areas of the 5G infrastructure (frequencies, identifiers, traffic laws, etc.).[16]

- **Information sharing and analysis centres (ISACs):** ISACs will have to collect and share 5G related intelligence. This can be achieved either by means of existing ISACs and/or specific 5G ISACs.

- **National cybersecurity coordinators/agencies/centres (NCSCs):** Existing cybersecurity centres need to engage in 5G infrastructure matters in order to evaluate and scrutinize major risks at national level, emanating from 5G infrastructure deployments.[17]

- **National 5G Test Centres (NTCs):** The creation of national 5G test centres has been taken forward in some Member States in order to assess the quality and security of 5G solutions.[18] It is expected that this trend will lead to the creation of such facilities in multiple EU Member States.

- **National Certification Authorities (NCAs):** Given the fact that certification is a major security control to be implemented for 5G components, it is expected that various

[14] https://5g-ppp.eu/wp-content/uploads/2019/07/5G-PPP-5G-Architecture-White-Paper_v3.0_PublicConsultation.pdf, accessed September 2019.
[15] http://www.leedsgrowthstrategy.co.uk/wp-content/uploads/2017/09/WHY-5G-IN-LEEDS.pdf, accessed September 2019.
[16] http://www.emergonline.org/wp-content/uploads/2018/12/Introduction_to_5G_Amman.pdf, accessed September 2019.
[17] https://www.ft.com/content/29eb5d28-e10d-11e8-8e70-5e22a430c1ad, accessed September 2019.
[18] https://dcnnmagazine.com/networking/telecoms-networking/manyooth-university-opens-radiospace-5g-test-centre/, assessed September 2019.

players will be active in definition and implementation of national 5G certification and accreditation schemes.

- **Competent EU institutions and European Commission Services:** These entities will play a significant role in the coordination of national activities, standardisation work, research projects and policy initiatives.

In different roles, the entities mentioned above should have different levels of concern regarding 5G assets, among other things carrying responsibility for the risk mitigation affecting those assets. Stakeholders must develop strategies that, independently or co-responsibly, allow reduction of exposure to cyberthreats.

Annex D shows the **relationships between Stakeholders and 5G asset groups,** helping the reader to understand their potential involvement in the (risk/threat) management of the assets.

3. 5G NETWORK DESIGN AND ARCHITECTURE

To support the identification of the most sensitive assets, a 5G architecture was developed for this report. This architecture resulted from the analysis of various publicly available reports published by standardisation, research and scientific bodies (e.g. [14, 19,24,25,26,27,28]). This task aimed at establishing a common and coherent understanding over the components of the 5G architecture. Despite a large number of documents referring to various aspects of the 5G architecture (e.g. individual network functions, interfaces, security functions, various 5G domains, etc.), only a few provide a compressive overview. For the present work, the visualisation of the different components in a modular and general manner was required. Once the comprehensive technical 5G architecture has been defined, and after reviewing known weaknesses of components, it was possible to list the sensitive assets and describe the most relevant threats.

For this reason, the approach taken for this report was to develop a generic 5G architecture and provide the details of individual key components by means of 'Zoom-ins', allowing further detailing of their functionality and purpose. By doing so, besides the generic 5G architecture depicted, we deliver a number of detailed views of particular components, namely: Core Network, Management and Network Orchestrator (MANO), Radio Access Network (RAN), Network Function Virtualisation (NFV), Software Defined Network (SDN), Multi-access Edge Computing (MEC), User Equipment (UE), Security Architecture (SA) and 5G Physical Infrastructure components.

To deal with complexity, both at the level of the generic 5G architecture and individual 'Zoom-ins', the details of the various interfaces and protocols have not been considered. A short description of the purpose and functionality is provided in a separate table for each individual component. A generic 5G architecture and the corresponding 'Zoom-ins' will help the identification of sensitive assets presented in chapter 4.2.

3.1 5G USE CASES

The description of the network design and architecture is started by explaining the different Use Cases defined for 5G Networks. 3GPP defined these Use Cases as part of its New Services and Markets Technology Enabler (SMARTER) project.[19] The objective behind SMARTER was to develop high-level use cases and identify which features and functionalities are required to enable them. The process started in 2015 and resulted in over 70 use cases, initially grouped into five categories, which have been reduced to three. The three sets of Use Cases are as follows.

- **Enhanced mobile broadband (eMBB).**[20] Defined as an extension to existing 4G broadband services, eMBB will be the first commercial 5G service enabling faster and more reliable downloads. The thresholds defined in the ITU requirements for eMBB sets at a minimum of 20Gbps for downlink and 10Gbps for uplink. Furthermore, the minimum requirement for eMBB mobility interruption time is 0ms.

[19] https://5g-ppp.eu/wp-content/uploads/2016/11/01_10-Nov_Session-3_Dino-Flore.pdf, accessed September 2019.
[20] https://5g.co.uk/guides/what-is-enhanced-mobile-broadband-embb/, accessed September 2019.

- **Ultra-reliable low latency communication (URLLC).** The promise to delivery ultra-reliable and low-latency communication for 5G wireless networks is considered of capital importance. URLLC is designed to support businesses on mission critical communication scenarios, such as emergency situations, autonomous systems operations, among others.[21] Examples include public safety services, operations of mining, autonomous vehicles, oil and gas pipelines, robots, medical and entertainment. Achieving URLLC represents one of the major challenges facing 5G networks.

- **Machine Type Communications (MTC)**.[22] This Use Case is expected to play an essential role in the future of 5G systems. In the seventh framework programme (FP7) project METIS, [23] MTC has been further classified as 'massive machine-type communication' (mMTC) and 'ultra-reliable machine-type communication' (uMTC). While mMTC is about wireless connectivity to tens of billions of machine-type terminals, uMTC is about availability, low latency, and high reliability. The main challenges in mMTC is to deliver scalable and efficient connectivity for a massive number of devices sending very short packets, which is not done adequately in cellular systems designed for human-type communications. Furthermore, mMTC solutions need to enable wide area coverage and deep indoor penetration while having low cost and being energy efficient. For MTC, ITU defined a minimum requirement for connection density of 1,000,000 devices per km^2.

Multiple deployment scenarios for eMBB, mMTC and URLLC can be envisioned in future implementations of this technology. A study developed by ETSI identified some of these future scenarios presented in Table 1.[24]

Table 1 - 5G deployment scenarios

Deployment Scenarios
Indoor hotspot
The indoor hotspot deployment scenario focuses on small coverage per site/TRxP (transmission and reception point) and high user throughput or user density in buildings. The key characteristics of this deployment scenario are high capacity, high user density and consistent user experience indoor.
Dense urban
The dense urban microcellular deployment scenario focuses on macro TRxPs with or without micro TRxPs and high user densities and traffic loads in city centres and dense urban areas. The key characteristics of this deployment scenario are high traffic loads, outdoor and outdoor-to-indoor coverage. This scenario will be interference-limited, using macro TRxPs with or without micro TRxPs. A continuous cellular layout and the associated interference shall be assumed.
Rural
The rural deployment scenario focuses on larger and continuous coverage. The key characteristics of this scenario are continuous wide area coverage supporting high-speed vehicles. This scenario will be noise-limited and/or interference limited, using macro TRxPs.
Urban macro

[21] https://arxiv.org/pdf/1801.01270.pdf, accessed September 2019.
[22] https://www.researchgate.net/profile/Carsten_Bockelmann/publication/305881263_Massive_Machine-type_Communications_in_5G_Physical_and_MAC-layer_solutions/links/5ad996fba6fdcc293586dbcd/Massive-Machine-type-Communications-in-5G-Physical-and-MAC-layer-solutions.pdf, accessed September 2019.
[23] https://metis2020.com/, accessed September 2019.
[24] https://www.etsi.org/deliver/etsi_tr/138900_138999/138913/14.02.00_60/tr_138913v140200p.pdf, accessed September 2019.

The urban macro deployment scenario focuses on large cells and continuous coverage. The key characteristics of this scenario are continuous and ubiquitous coverage in urban areas. This scenario will be interference-limited, using macro TRxPs (i.e. radio access points above rooftop level).
High speed
The high-speed deployment scenario focuses on continuous coverage along track in high speed trains. The key characteristics of this scenario are consistent passenger user experience and critical train communication reliability with very high mobility. In this deployment scenario, dedicated linear deployment along railway line and the deployments including SFN scenarios captured in Section 6.2 of 3GPP TR 36.878 are considered, and passenger UEs are located in train carriages.[25] For the passenger UEs, if the antenna of relay node for eNB-to-Relay is located at top of one carriage of the train, the antenna of relay node for Relay-to-UE could be distributed to all carriages.
Extreme long distance coverage in low density areas
The extreme Long Range deployment scenario is defined to allow for the Provision of services for very large areas with low density of users whether they are humans and machines (e.g. Low ARPU regions, wilderness, areas where only highways are located, etc). The key characteristics of this scenario are Macro cells with very large area coverage supporting basic data speeds and voice services, with low to moderate user throughput and low user density.
Urban coverage for massive connection
The urban coverage for massive connection scenario focuses on large cells and continuous coverage to provide mMTC. The key characteristics of this scenario are continuous and ubiquitous coverage in urban areas, with very high connection density of mMTC devices.

The main drivers identified for these Use Cases - reflected in the requirements and specifications of 5G Networks - are bandwidth, latency, availability, reliability, efficiency and coverage. In the next sections, we will present the critical elements of the network architecture that will enable these Use Cases.

3.2 GENERIC 5G ARCHITECTURE

The generic 5G architecture is presented through its main components depicted as labelled boxes. These boxes have been arranged based on layers, depicting their functional role in the 5G architecture (i.e. virtualisation layer and physical infrastructure layer). This architecture aims at providing an overview of the main groups of foreseen 5G functionality and is a consolidation of components/functions found in the analysed material (e.g.[14,19,24,25,26,27,28]).

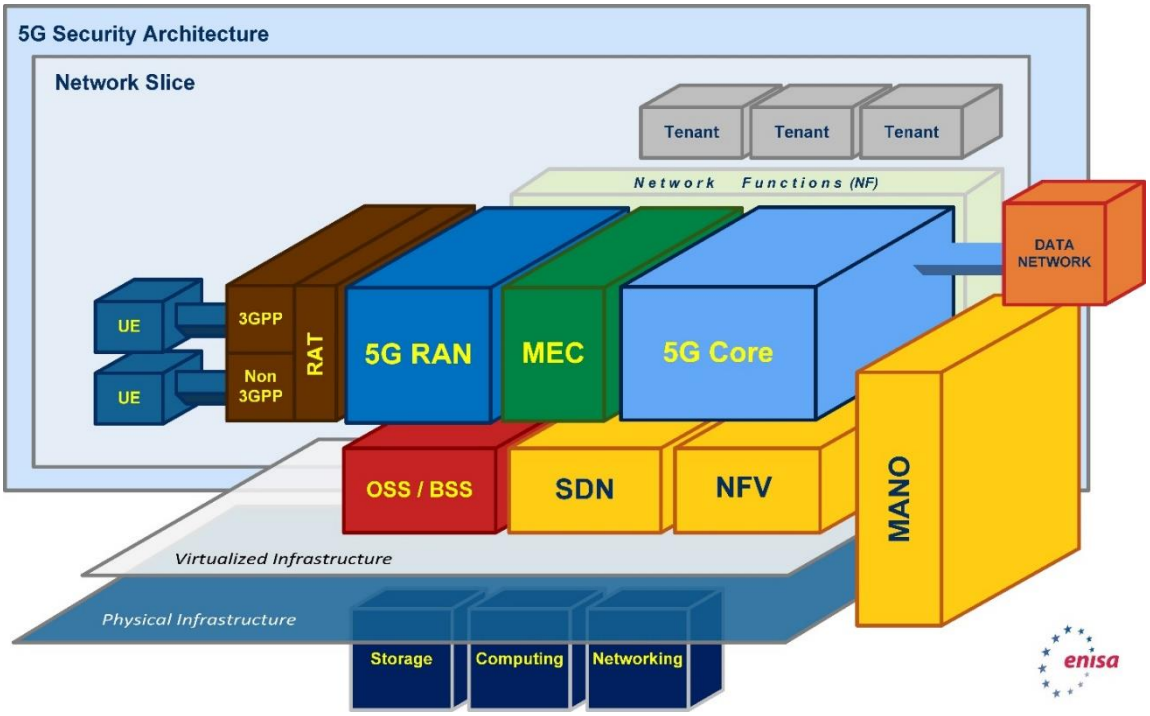
Specifically in 5G, the architecture was designed in a way that connectivity and services of data can be supported, enabling techniques such as Network Function Virtualisation (NFV), Network Slicing (NS) and Software Defined Networking (SDN). This service-based architecture meets multiple functional and performance requirements built upon new use cases in a cost efficient way.

The generic 5G architecture presents an overview of the various components that are further detailed and depicted through specific 'Zoom-ins' in forthcoming sections. It is worth mentioning that for the OSS/BSS component, no 'Zoom-in' was developed. However, it has been included in the generic 5G architecture for consistency reasons.

The 5G generic or high-level technical architecture is depicted in the following figure:

[25] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2885, accessed September 2019.

Figure 2: 5G High-level technical architecture



3.3 CORE NETWORK ARCHITECTURE (ZOOM-IN)

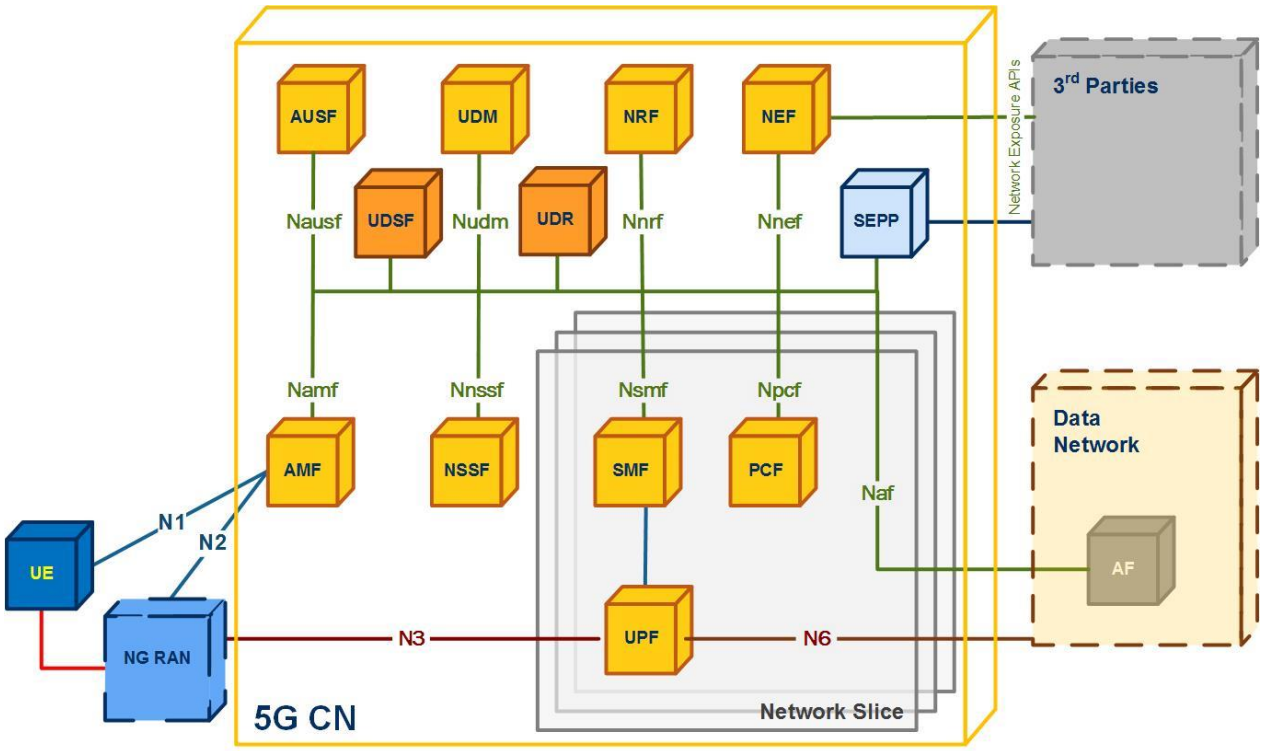
One of the most important innovations in the 5G architecture is the complete virtualisation of the Core network. As an example, the 'softwarisation' of network functions will enable easier portability and higher flexibility of networking systems and services (Control-User Plain Separation, CUPS). The Software Defined Network (SDN) brings simplified management together with innovation through abstraction. Network Function Virtualisation (NFV) provides the enabling technology for placing various network functions in different network components on the basis of performance needs/requirements; and eliminates the need for function- or service-specific hardware. SDN and NFV, complementing each other, improve the network elasticity, simplify network control and management, break the barrier of vendor-specific or proprietary solutions, and are thus considered as highly important for future networks. These novel network technologies and concepts - heavily relying on 'softwarisation' and virtualisation of network functions will introduce new and complex threats.

The Core network is the central part of the 5G infrastructure and enables new functions related to multi-access technologies. Its main purpose is to deliver services over all kinds of networks (wireless, fixed, converged).[26]

The Core network has been defined by 3GPP[27] and its structure is as follows:

[26] https://www.nokia.com/networks/portfolio/5g-core/#defining-a-new-5g-core, accessed September 2019.
[27] https://www.etsi.org/deliver/etsi_ts/123500_123599/123501/15.02.00_60/ts_123501v150200p.pdf, accessed September 2019.

Figure 3: Core network architecture zoom-in



A description of the elements of the 5G Core network is as follows:

Element	Short description
Access and Mobility Management function (AMF)	(As defined in 3GPP TS23.501 Section 6.2.1)[28] AMF may include the following functionalities: ▪ Termination of RAN CP interface; ▪ Termination of NAS, NAS ciphering and integrity protection; ▪ Registration management; ▪ Connection management; ▪ Reachability management; ▪ Mobility Management; ▪ Lawful interception; ▪ Provide transport for SM messages between UE and SMF; ▪ Transparent proxy for routing SM messages;

[28] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144, accessed September 2019.

	▪ Access Authentication; ▪ Access Authorization; ▪ Provide transport for SMS messages between UE and SMSF; ▪ Security Anchor Functionality; ▪ Location Services management for regulatory services; ▪ Provide transport for Location Services messages between UE and LMF as well as between RAN and LMF and ▪ EPS Bearer ID allocation for interworking with EPS; UE mobility event notification.
Session Management function (SMF)	(As defined in 3GPP TS23.501 section 6.2.2[28]) SMF may include the following functionalities: ▪ Session Management; UE IP address allocation & management (DHCPv4 and v6 (server and client) functions); ▪ Respond to Address Resolution Protocol (ARP) requests and / or IPv6 Neighbour Solicitation requests; ▪ Selection and control of UP function; ▪ Configures traffic steering at UPF to route traffic to proper destination; ▪ Termination of interfaces towards Policy control functions; ▪ Lawful interception; ▪ Charging data collection and support of charging interfaces; ▪ Control and coordination of charging data collection at UPF; ▪ Termination of Session Management parts of NAS messages; ▪ Downlink Data Notification; ▪ Determine Session and Service Continuity mode of a session. ▪ Roaming functionality; ▪ Handle local enforcement to apply QoS SLAs (VPLMN); ▪ Charging data collection and charging interface (VPLMN); ▪ Lawful intercept (in VPLMN for SM events and interface to LI System) and ▪ Support for interaction with external DN for transport of signalling for PDU Session authentication/authorization by external DN.

	(NOTE: Not all of functionalities are required in an instance of a Network Slice. In addition to the functionalities of the SMF described above, the SMF may include policy related functionalities as described in clause 6.2.2 in TS 23.503)[29]
User plane function (UPF)	UPF supports: ▪ Packet routing & forwarding; ▪ Packet inspection; ▪ QoS handling; ▪ It acts as external PDU session point of interconnect to Data Network (DN), and ▪ Is an anchor point for intra- & inter-RAT mobility.
Policy Control Function (PCF)	PCF supports: ▪ Unified policy framework; ▪ Policy rules to CP functions and ▪ Access subscription information for policy decisions in UDR.
Network Exposure Function (NEF)	NEF supports: ▪ Exposure of capabilities and events; ▪ Secure provision of information from external application to 3GPP network and ▪ Translation of internal/external information.
Network Repository Function (NRF)	NRF supports service discovery function and maintains NF profile and available NF instances.
Unified Data Management (UDM)	UDM supports: ▪ Generation of Authentication and Key Agreement (AKA) credentials; ▪ User identification handling; ▪ Access authorization and ▪ Subscription management.
Authentication Server Function (AUSF)	AUF supports authentication for 3GPP access and untrusted non-3GPP access.
Application Function (AF)	AF interacts with the Core network in order to provide services, for example to support the following: ▪ Application influence on traffic routing; ▪ Accessing Network Exposure Function and

[29] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3334, accessed September 2019.

	▪ Interacting with the Policy framework for policy control.
Unified Data Repository (UDR)	UDR supports the following functionality: ▪ Storage and retrieval of subscription data by the UDM; ▪ Storage and retrieval of policy data by the PCF; ▪ Storage and retrieval of structured data for exposure; ▪ Application data (including Packet Flow Descriptions (PFDs) for application detection and ▪ AF request information for multiple UEs), by the NEF. (see also 3GPP TS23.501 section 6.2.11)[28]
Unstructured Data Storage Function (UDSF)	The UDSF is an optional function that supports storage and retrieval of information as unstructured data by any NF.
Network Slice Selection Function (NSSF)	The NSSF offers services to the AMF and NSSF in a different PLMN via the Nnssf service based interface. (see 3GPP TS 23.501 and 3GPP TS 23.502) [28]
Security Edge Protection Proxy (SEPP)	SEPP is a non-transparent proxy and supports the following functionality: ▪ Message filtering and policing on inter-PLMN control plane interfaces and ▪ Topology hiding.
Nausf, Nnrf, Nudm, Nnef, Namf, Nmssf, Nsmf, Npcf, Naf	These are service-based interfaces exhibited by 5G Core Control-plane functions.
N1	Reference point between the UE and the AMF.
N2	Reference point between the RAN and the AMF.
N3	Reference point between the RAN and the UPF.
N6	Reference point between the UPF and a Data Network.

3.4 NETWORK SLICING (NS) (ZOOM-IN)

One of 5G's key features will be the opportunity for network slicing[30]: the segmentation of a single physical network into multiple virtual ones in accordance with particular use cases. A clear benefit of 5G network slicing for operators will be the ability to deploy only the functions necessary to support specific customers and particular market segments.[31]

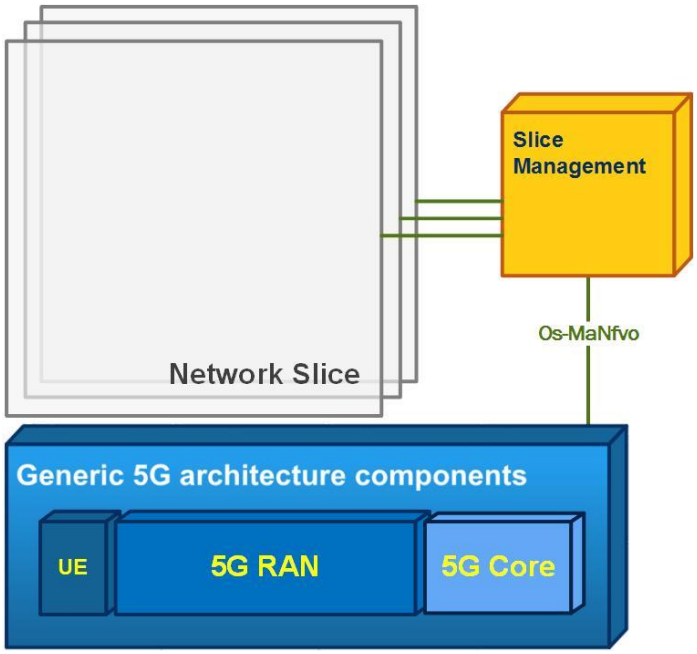
Communication between autonomous cars, for instance, requires minimal latency (the lag time it takes for a signal to travel), but not necessarily high throughput (the amount of data a network can process per second) while a use-case such as augmented reality will take more bandwidth.

[30] https://www.sdxcentral.com/5g/definitions/5g-network-slicing/, accessed September 2019.
[31] www.5gamericas.org/files/3214/7975/0104/5G_Americas_Network_Slicing_11.21_Final.pdf, accessed September 2019.

With slicing, these needs can be accommodated by delegating each to its own network-within-a-network.

Network Slicing components are presented in relation to the impacted elements of the network architecture, as depicted in the various 'Zoom-ins'. This cross-reference/mapping is an alternative means for describing slice functions of 5G. The dependency of slices with the various components of the 5G generic architecture is shown in the figure below:

Figure 4: Dependencies of slices with the generic 5G architecture components



The various slice functions of 5G are as follows:

Relevant element	Referenced generic 5G architecture components	Slice function
Network Slice Management Function (NSMF)	Access Network, Core Network	This function is responsible for the management (including lifecycle) of NSIs. It derives network slice subnet related requirements from the network slice related requirements. NSMF communicates with the NSSMF and the CSMF
Network Functions (NF)	Access Network, Core Network	A network slice instance (NSI) contains Network Functions (Access Network or Core Network).

Infrastructure (Physical, Virtual)	Access Network, Core Network, Transport	The NSI is realized via the required physical and logical resources.
SDN Controller	Access Network, Core Network	The NSI is realized via the required physical and logical resources. the tenant SDN controller dynamically configures the (other) inner network slice's VNFs, and properly chains them to build up the Network Service(s) that the slice needs to accommodate for a given use case.
NFV Orchestrator	Management and Orchestration	Since SDN and NFV are considered enabling techniques for network slicing, MANO activities are concerned with the orchestration perspective that involves transforming a service using NFV infrastructure. Each of the network slices serving a tenant comprises an NFVO. The NFVO dynamically manages the lifecycle of the network slice constituent network service(s).
VNF Manager	Management and Orchestration	VNF Manager is responsible for VNF lifecycle management (e.g. instantiation, update, query, scaling and termination). Each of the network slices serving a tenant comprises one or several VNFM(s). The VNFM(s) perform(s) lifecycle management operations over the slice VNFs.
Operations Support System/Business Support System (OSS/BSS)	Management and Orchestration	Since Network Services and VNF operations are highly correlated, once it is made aware by the NFVO that a Network Service has been instantiated, there is a need for the OSS, VNF configuration and chaining tasks.

Communication Service Management Function (CSMF)	Management and Orchestration	This function is responsible for translating the communication service related requirement to network slice related requirements. The CSMF communicates with the Network Slice Management Function (NSMF).
Os-Ma-nfvo	Management and orchestration, Resources	the Os-Ma-nfvo reference point can be used for the interaction between 3GPP slicing related management functions and NFV-MANO. To properly interface with NFV-MANO, the NSMF and/or NSSMF need to determine the type of NS or set of NSs, VNF and PNF that can support the resource requirements for a NSI or NSSI, and whether new instances of these NSs, VNFs and the connectivity to the PNFs need to be created or existing instances can be re-used.

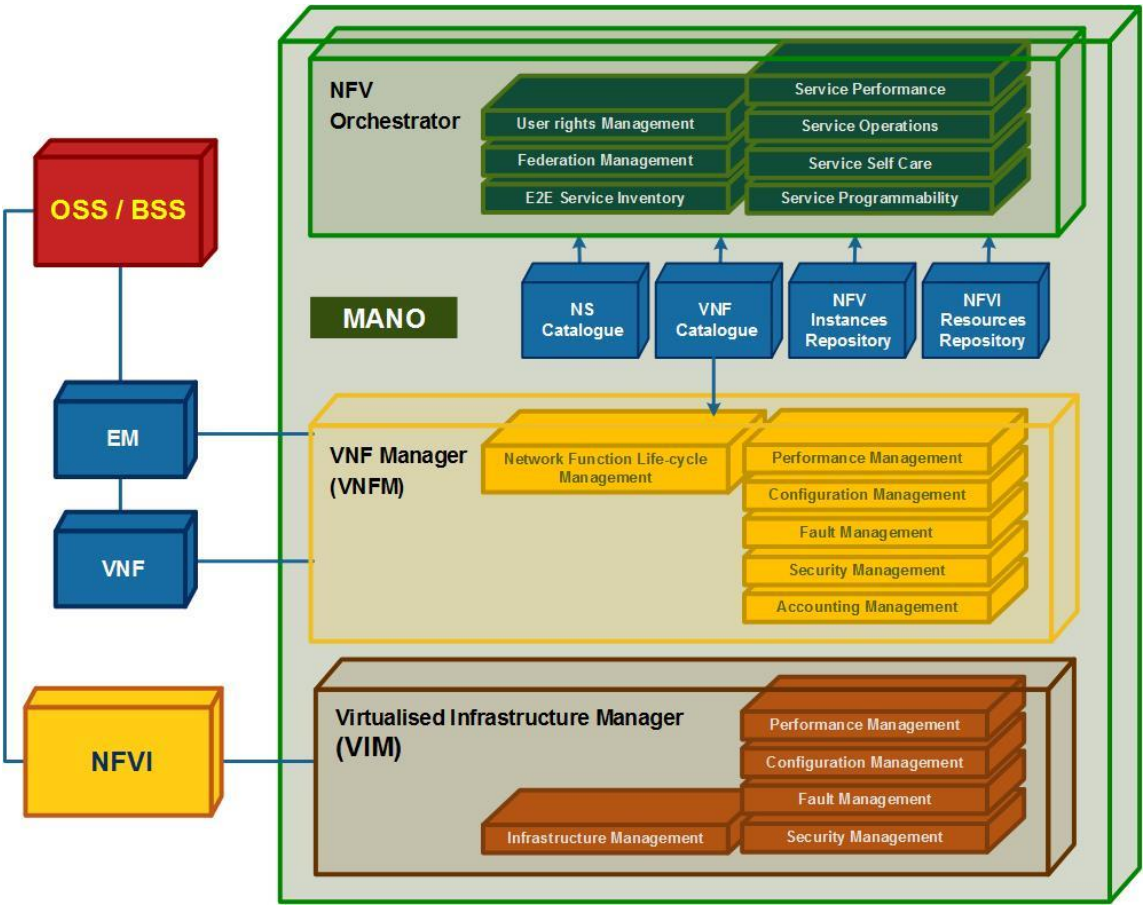
3.5 MANAGEMENT AND NETWORK ORCHESTRATOR (MANO) (ZOOM-IN)

Management and Network Orchestrator is one of the most important components of the 5G infrastructure. It is responsible for the configuration and management of all significant components/functions of 5G, including Network Function Virtualisation (NFV), Virtualised Network Functions (VNF) management, and Virtualised Infrastructure Management (VIM). The MANO structure presented here corresponds to the ETSI MANO concept.[32]

The structure of the MANO architecture is depicted in the following figure:

[32] https://www.ietf.org/proceedings/88/slides/slides-88-opsawg-6.pdf, accessed September 2019.

Figure 5: MANO architecture zoom-in



A short description of the various elements of MANO shown in this figure is as follows:

Element	Short description
NFV Orchestrator (NFVO)	The NFV Orchestrator has two main responsibilities: ▪ the orchestration of NFVI resources across multiple VIMs and ▪ the lifecycle management of Network Services.
VNF manager (VNFM)	The VNF Manager is responsible for the lifecycle management of VNF instances.
Virtualised infrastructure manager (VIM)	The Virtualised Infrastructure Manager (VIM) is responsible for controlling and managing the NFVI computing, storage and networking resources, usually within one operator's Infrastructure Domain. A VIM may be specialized in handling a certain type of NFVI resource (e.g. compute-only, storage-only, networking-only), or may be capable of managing multiple types of NFVI resources (e.g. in NFVI-Nodes).
Element Management (EM)	The Element Management is responsible for:

	• Configuration for the network functions provided by the VNF. • Fault management for the network functions provided by the VNF. • Accounting for the usage of VNF functions. • Collecting performance measurement results for the functions provided by the VNF. • Security management for the VNF functions.
NFV Infrastructure (NFVI).	The NFVI encompasses all the hardware (e.g. compute, storage, and networking) and software (e.g. hypervisors) components that together provide the infrastructure resources where VNFs are deployed.
Operations Support System/Business Support System (OSS/BSS)	OSS/BSS functions provide management and orchestration of systems including legacy ones and may have full end-to-end visibility of services provided by legacy network functions in an operator's network. Processes covered by OSS/BSS include: Network Management, Service delivery / fulfilment / assurance, Customer Relationship management and Billing.
NS Catalogue	The NS Catalogue represents the repository of all of the on-boarded Network Services, supporting the creation and management of the NS deployment templates (Network Service Descriptor (NSD), Virtual Link Descriptor (VLD), and VNF Forwarding Graph Descriptor (VNFFGD) via interface operations exposed by the NFVO.
VNF Catalogue	The VNF Catalogue represents the repository of all of the on-boarded VNF Packages, supporting the creation and management of the VNF Package (VNF Descriptor (VNFD), software images, manifest files, etc.) via interface operations exposed by the NFVO.
NFV Instances repository	The NFV Instances repository holds information of all VNF instances and Network Service instances. Those records are updated during the lifecycle of the respective instances, reflecting changes resulting from execution of NS lifecycle management operations and/or VNF lifecycle management operations.
NFVI Resources repository	As such, the NFVI Resources repository plays an important role in supporting NFVO's Resource Orchestration and governance role, by allowing NFVI reserved/allocated resources to be tracked against the NS and VNF instances associated with those resources (e.g. number of VMs used by a certain VNF instance at any time during its lifecycle).

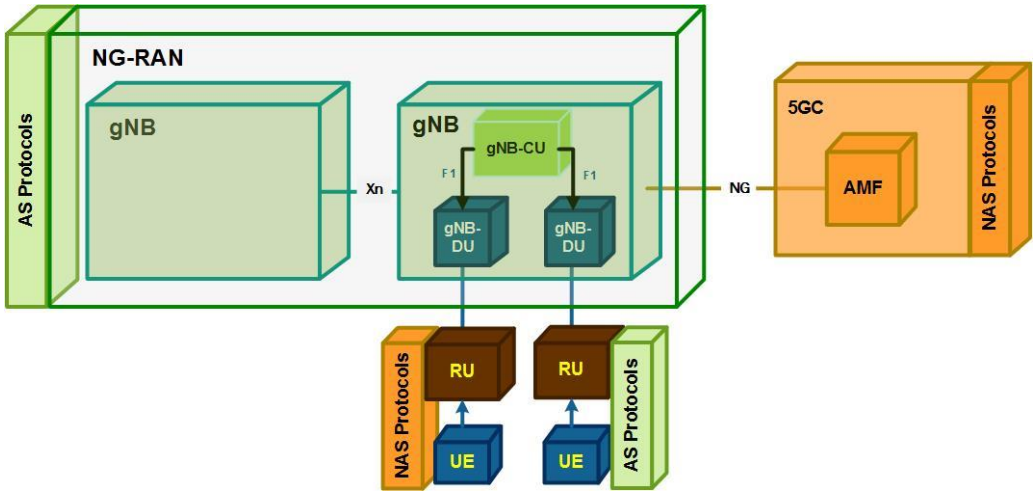
Network Function Lifecycle Management	Management aspects of a VNF include traditional Fault Management, Configuration Management, Accounting Management, Performance Management, and Security Management (FCAPS) ▪ Configuration for the network functions provided by the VNF. ▪ Fault management for the network functions provided by the VNF. ▪ Accounting for the usage of VNF functions. ▪ Collecting performance measurement results for the functions provided by the VNF. ▪ Security management for the VNF functions.

3.6 RADIO ACCESS NETWORK (RAN) (ZOOM-IN)

The baseline architecture described by 5G-PPP and the latest 3GPP specifications on NG-RAN, identifies as the main innovation the split of the F1 interface into Centralized Unit (CU) and Distributed Unit (DU), with a Service Data Adaptation Protocol (SDAP). The SDAP architecture includes a Packet Data Conversion Protocol (PDCP) located in the CU and an Air Radio Link Control (ARLC) located in the DU. All this is based on IP transport on a TNL/Ethernet network, very similar to the mobile backhaul of today. Another key aspect of the NG-RAN is the ability to provide small-cell coverage to multiple operators 'as-a-service' in two-tier architecture. These tiers are in support of the previously mentioned 5G use cases providing low latency services and high processing power.

The structure of the RAN architecture is depicted in the figure below:

Figure 6: RAN architecture zoom-in



The elements of the RAN architecture are as follows:

Element	Short description
User Equipment (UE)	User equipment is any device used by users to communicate within the 5G infrastructure. Besides a SIM, user equipment may be home appliances of any kind (e.g. computer, IoT devices,etc.).
Radio Unit (RU)	Is an element connecting user equipment with the operator network.
gNB	Next generation Node/Base Station is a node providing NR user plane and control plane protocol terminations towards the UE, and connected via the NG interface to the 5GC.
gNB Distributed Unit (gNB-DU)	gNB-DU a logical node hosting RLC, MAC and PHY layers of the gNB or en-gNB, and its operation is partly controlled by gNB-CU. One gNB-DU supports one or multiple cells. One cell is supported by only one gNB-DU. The gNB-DU terminates the F1 interface connected with the gNB-CU.
gNB Central Unit (gNB-CU)	gNB-Central Unit (CU) is a logical node hosting RRC, SDAP and PDCP protocols of the gNB or RRC and PDCP protocols of the en-gNB that controls the operation of one or more gNB-DUs. The gNB-CU terminates the F1 interface connected with the gNB-DU.
Access and Mobility Management function (AMF)	AMF is a Network Function (NF). It includes some or all following functionalities: ▪ Termination of RAN CP interface; ▪ Termination of NAS ; ▪ NAS ciphering and integrity protection; ▪ Registration management; ▪ Connection management; ▪ Reachability management; ▪ Mobility Management; ▪ Lawful intercept; ▪ Transport for SM messages between UE and SMF; ▪ Transparent proxy for routing SM messages; ▪ Access authentication; access authorization; ▪ Transport for SMS messages between UE and SMSF; security anchor functionality (SEAF) ;

	▪ Location services management; transport for Location Services messages between UE and LMF and between RAN and LMF; ▪ EPS Bearer ID allocation for interworking with EPS: ▪ UE mobility event notification.
F1	Logical interface with the F1 Application Protocol. (defined in ETSI TS 138 473). [33]
Xn	Xn is a network interface between NG-RAN nodes; 3GPP TS 38.420 specifies Xn interface general aspects and principles.[34]
NG interface	NG interface is an element defined by ETSI[35] that has as purpose to logically separate signalling and data transport network.
Non Access Stratum (NAS)	NAS is a functional layer in the protocol stack between UE and Core Network. (NAS) protocol for 5G System. (defined in 3GPP TS 24.501). [28]
Access Stratum (AS)	AS is a functional layer in the protocol stack between UE and RAN responsible for transporting data over the wireless connection and managing radio resources.

3.7 NETWORK FUNCTION VIRTUALISATION (NFV) (ZOOM-IN)

NFV introduces a new concept for service providers to accelerate the deployment of new network services in support of their revenue and growth plans. It translates to the use of standard IT virtualisation technologies applied to the deployment of Network Functions, aiming at a faster provision of new network services. With this, several providers formed the NFV ISG under the European Telecommunications Standards Institute (ETSI). The foundation of NFV's basic requirements and architecture resulted from the work produced by ETSI NFV ISG. [36,37]

Although 5G networks will be very different compared to its predecessors in some regards (e.g. through the use of virtualisation and support for diverse and critical non-telecom-oriented services), they still share similarities and will reuse and extend existing concepts that have proved successful and are widely adopted.

The NFV has a tight interaction with Virtual Network Functions (VNF), MANO and OSS/BSS and security management components. The NFV 'Zoom-in' presented in Figure 7 includes the following network functions (NF):

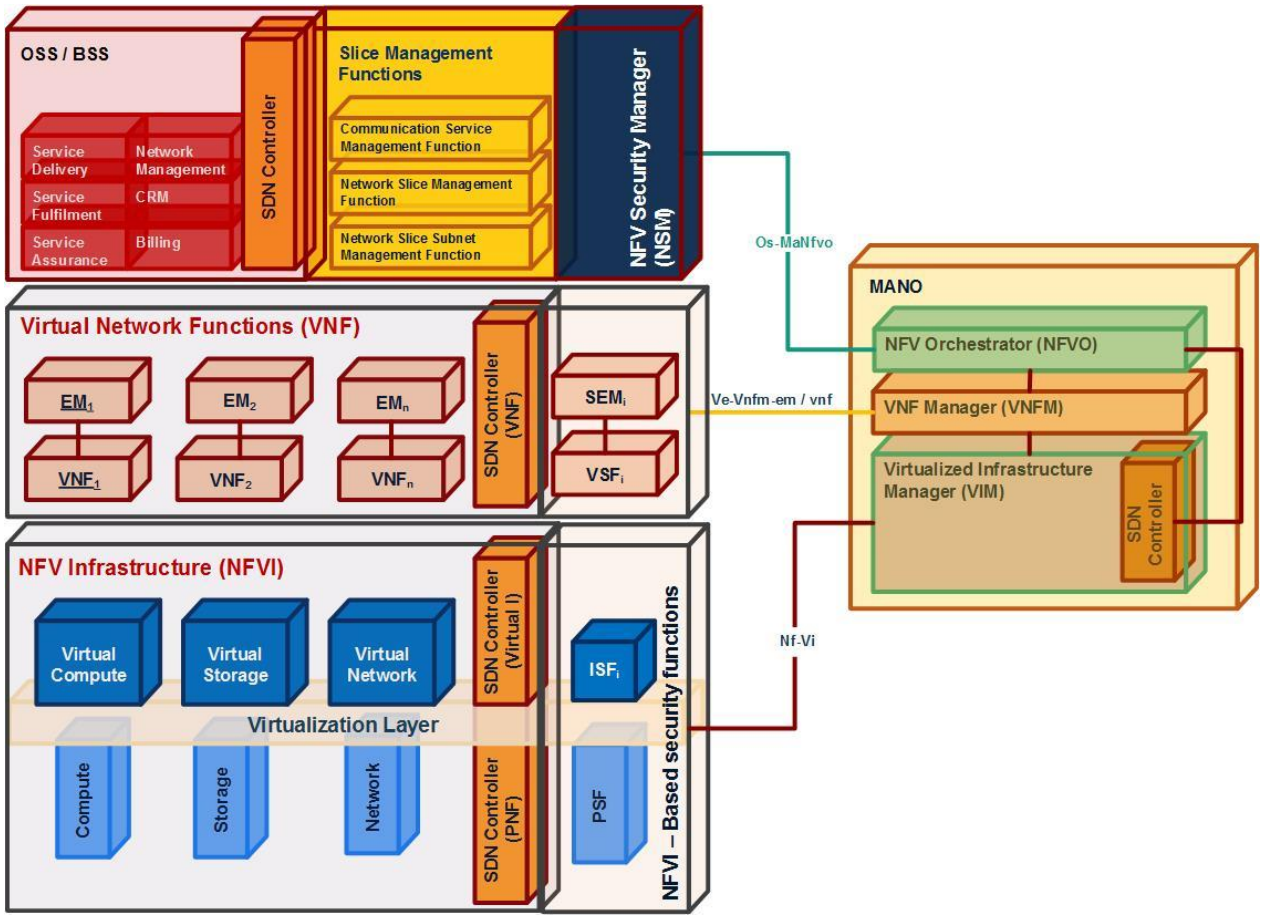
- Authentication Server Function (AUSF)
- Access and Mobility Management Function (AMF)
- Unstructured Data Storage Function (UDSF)

[33] https://www.etsi.org/deliver/etsi_TS/138400_138499/138473/15.03.00_60/ts_138473v150300p.pdf, accessed September 2019.
[34] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3225, accessed September 2019.
[35] https://www.etsi.org/deliver/etsi_ts/138400_138499/138401/15.02.00_60/ts_138401v150200p.pdf, accessed September 2019.
[36] https://www.etsi.org/technologies/nfv, accessed September 2019.
[37] https://www.sdxcentral.com/networking/nfv/?c_action=num_ball, accessed September 2019.

- Network Exposure Function (NEF)
- Network Repository Function (NRF)
- Network Slice Selection Function (NSSF)
- Policy Control Function (PCF)
- Session Management Function (SMF)
- Unified Data Management (UDM)
- Unified Data Repository (UDR)
- User Plane Function (UPF)
- Application Function (AF)
- 5G-Equipment Identity Register (5G-EIR)
- Security Edge Protection Proxy (SEPP)
- Network Data Analytics Function (NWDAF)

The structure of NFV architecture and its interfaces to related components is shown in the figure below:

Figure 7: NFV architecture zoom-in



The elements of the NFV architecture are as follows:

Element	Short description
Operations Support System/Business Support System (OSS/BSS)	OSS/BSS functions provide management and orchestration of systems including legacy ones and may have full end-to-end visibility of services, provided by legacy network functions in an operator's network. Processes covered by OSS/BSS include: Network Management, Service delivery / fulfilment / assurance, Customer Relationship management and Billing.
Virtualised Network Function (VNF)	A VNF is a virtualisation of a network function in a legacy non-virtualised network. ETSI GS NFV 001 provides a list of use cases and examples of target network functions (NFs) for virtualisation. Functional behaviour and state of a NF are largely independent of whether the NF is virtualised or not. The functional behaviour and the external operational interfaces of a Physical Network Function (PNF) and a VNF are expected to be the same.
Element Management (EM)	The Element Management is responsible for: • Configuration for the network functions provided by the VNF. • Fault management for the network functions provided by the VNF. • Accounting for the usage of VNF functions. • Collecting performance measurement results for the functions provided by the VNF. • Security management for the VNF functions.
NFV Infrastructure (NFVI)	The NFV Infrastructure corresponds to the total of all hardware and software components which build up the environment in which VNFs are deployed, managed and executed. The NFV Infrastructure can span across several locations, i.e. places where NFVI-PoPs are operated. The network providing connectivity between these locations is regarded to be part of the NFV Infrastructure. From the VNF's perspective, the virtualisation layer and the hardware resources look like a single entity providing the VNF with desired virtualised resources.
Hardware Resources	In NFV, the physical hardware resources include computing, storage and network that provide processing, storage and connectivity to VNFs through the virtualisation layer (e.g. hypervisor). Computing hardware is assumed to be COTS as opposed to purpose-built hardware. Storage resources can be differentiated between shared network attached storage (NAS) and storage that resides on the server itself. Computing and storage resources are commonly pooled.

	Network resources are comprised of switching functions, e.g. routers, and wired or wireless links.
Virtualisation Layer and Virtualised Resources	The virtualisation layer abstracts the hardware resources and decouples the VNF software from the underlying hardware, thus ensuring a hardware independent lifecycle for the VNFs. In short, the virtualisation layer is responsible for: •Abstracting and logically partitioning physical resources, commonly as a hardware abstraction layer. i) Enabling the software that implements the VNF to use the underlying virtualised infrastructure; ii) Providing virtualised resources to the VNF, so that the latter can be executed.
Virtualised Infrastructure Manager	From NFV's point of view, virtualised infrastructure management comprises the functionalities that are used to control and manage the interaction of a VNF with computing, storage and network resources under its authority, as well as their virtualisation. According to the list of hardware resources specified in the architecture, the Virtualised Infrastructure Manager performs resource and operations management. Multiple Virtualised Infrastructure Manager instances may be deployed.
NFV Orchestrator	The NFV Orchestrator is in charge of the orchestration and management of NFV infrastructure and software resources, and realizing network services on NFVI
VNF Manager	VNF Manager is responsible for VNF lifecycle management (e.g. instantiation, update, query, scaling, termination). Multiple VNF Managers may be deployed; a VNF Manager may be deployed for each VNF, or a VNF Manager may serve multiple VNFs.
Os-Ma-nfvo	This reference point is used for exchanges between OSS/BSS and NFV Orchestrator, and supports the following: • Network Service Descriptor and VNF package management. • Network Service instance lifecycle management • VNF lifecycle management • Policy management and/or enforcement for Network Service instances, VNF instances and NFVI resources • Querying relevant Network Service instance and VNF instance information from the OSS/BSS. • Forwarding of events, accounting and usage records and performance measurement results regarding Network Service instances, VNF instances, and NFVI resources to OSS/BSS, as well as and information about the associations between those instances and NFVI resources

Ve-Vnfm-em	This reference point is used for exchanges between EM and VNF Manager, and supports the following functions: VNF instantiation / VNF instance query / VNF instance update / VNF instance scaling out-in, and up-down / VNF instance termination / Forwarding of configuration and events from the EM to the VNFM / Forwarding of configuration and events regarding the VNF from the VNFM to the EM. NOTE: This reference point is only used if the EM is aware of virtualisation.
Ve-Vnfm-vnf	This reference point is used for exchanges between VNF and VNF Manager, and supports the following: VNF instantiation / VNF instance query / VNF instance update / VNF instance scaling out-in, and up-down / VNF instance termination / Forwarding of configuration and events from the VNF to the VNFM / Forwarding of configuration, events, etc. regarding VNF, from the VNFM to the VNF / Verification that the VNF is still alive/functional.
NFVI - Virtualised Infrastructure Manager (Nf-Vi)	This reference point is used for: Specific assignment of virtualised resources in response to resource allocation requests / Forwarding of virtualised resources state information / Hardware resource configuration and state information (e.g. events) exchange.
NFV Security Manager (NSM)	NSM is the logical functional block for overall security management, e.g. on the behalf of network services. In cooperation with MANO blocks dedicated to managing the virtualised network, the policy driven NSM is specialized to manage the security on a network service over its entire lifecycle. It covers the following functionalities: • Security Policy Planning, designs and optimizes security policies for specific targets of protection (e.g. network services). • Security Policy Enforcement & Validation automates the deployment and supports lifecycle management of security functions as defined in the design phase, then configure security policies on the security functions. In addition, during lifetime of a network service, the validation and re-configuration/remediation of associated security policies is supported, also in automated manner. • NFVI Security Manager (ISM) – see below.
NFVI Security Manager (ISM)	NFVI Security Manager is the logical function dedicated to security management in NFVI layer. It builds and manages the security in NFVI to support NSM requests for managing security of network services in higher layer.

Security Element Manager (SEM)	SEM refers to Element Manager managing Security Functions.
Virtual Security Function (VSF)	This element is a special type of VNF running on top of NFVI with tailored security functionality (e.g. firewall, IDS/IPS, virtualised security monitoring functions like vFEP, vTap). VSFs are mainly required to protect the other VNFs, which constitute a network service. VSF is managed by either dedicated VNFM or generic VNFM with respect to its lifecycle.
NFVI-based Security Function (ISF)	This element is a security function provided by the NFV Infrastructure. It includes virtualised security appliances or software security features (e.g. hypervisor-based firewalls) and hardware-based security appliances/modules/features (e.g. Hardware Security Modules, Crypto Accelerators, or Trusted Platform Modules).
Physical Security Function (PSF)	This element is a conventionally realized security function in the physical part of the hybrid network. Even if a telco network is virtualised, additional PSFs are still needed, for instance to protect the NFV infrastructure (and inherently, the Network Services running on top) as a whole. PSF is part of the non-virtualised traditional network and not maintained by the NFVI provider, hence it is managed by the SEM instead of the VIM.
NFVI - Virtualised Infrastructure Manager (NF-Vi)	This reference point is used for: Specific assignment of virtualised resources in response to resource allocation requests / Forwarding of virtualised resources state information / Hardware resource configuration and state information (e.g. events) exchange.

3.8 SOFTWARE DEFINED NETWORK (SDN) (ZOOM-IN)

5G will be driven by the influence of software managing network functions, known as Software Defined Network (SDN) and Network Function Virtualisation (NFV). The key concept that underpins SDNs is the logical centralisation of network control functions by decoupling the control and packet-forwarding functionality of the network. While SDN separates the control and forwarding planes, NFV primarily focuses on optimising the network services themselves. NFV complements this vision through the virtualisation of these functionalities based on recent advances in general server and enterprise IT virtualisation. The SDN threats presented in this document are also the ones described in the ENISA Thematic Landscape SDN/5G[38] **Error! Bookmark not defined.**.

As previously mentioned, the fundamental concept of SDN relies on decoupling the control and the packet forwarding functionality in the network. In classic networks, these two functionalities are under the responsibility of the forwarding devices (physical) of the network. In SDN, these two functionalities have been separated into two functionality planes: the control plane and the

[38] https://www.enisa.europa.eu/publications/sdn-threat-landscape, accessed October 2019.

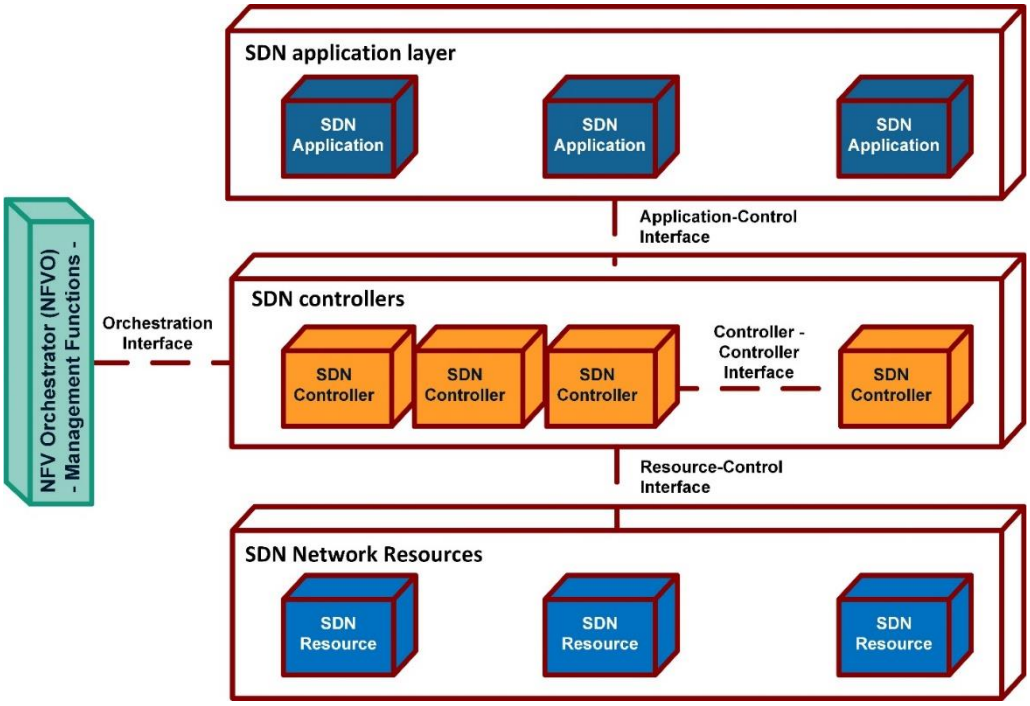
data plane. The separation of these two functionality planes in SDNs has two significant consequences:

a) it reduces the difficulty in the configuration and alteration of the control functions of the network, as this functionality has no longer the responsibility of the forwarding devices of the network that tend to have proprietary implementations (e.g., operating systems), and

b) it enables the implementation of more consistent control policies through fewer and uniformly accessible controllers.

The typical SDN architecture, as described by the Open Networking Foundation,[39] is shown in the figure below:

Figure 8: SDN architecture zoom-in



[39] https://www.opennetworking.org/, accessed September 2019.

The elements of the SDN architecture are as follows:

Element	Short description
SDN controller	SDN Controller: The SDN Controller is a logically centralized entity in charge of: • Translating the requirements from the SDN Application layer down to the SDN Resources and • Providing the SDN Applications with an abstract view of the network (which may include statistics and events).
SDN Application	SDN Applications are programs that explicitly, directly, and programmatically communicate their network requirements and desired network behaviour to the SDN Controller. Multiple case scenarios might be envisioned, for the position of the SDN applications in the NFV architectural framework, such as: • the network hardware might be a physical appliance talking to an SDN controller, or a complete solution including multiple SDN components, such as SDN controller + SDN application for instance; • the VIM might be an application interfacing with an SDN controller in the NFVI - for instance OpenStack Neutron as a VIM interfacing with an SDN controller in the NFVI; • the SDN application might be a VNF talking to an SDN controller, being Virtualised or not. For instance a PCRF VNF might talk to an SDN controller for some policy management for traffic steering; • the SDN application might be an element manager interfacing with an SDN controller to collect some metrics or configure some parameters, and • the SDN application might be an application interfacing with an SDN controller for instance in the OSS-BSS for tenant SDN service definitions.
SDN resources	Multiple scenarios might be envisaged for the actual location of SDN resources: • physical switch or router; • virtual switch or router; • e-switch, software based SDN enabled switch in a server NIC and • switch or router as a Virtual network function (VNF).

3.9 MULTI-ACCESS EDGE COMPUTING (MEC) (ZOOM-IN)

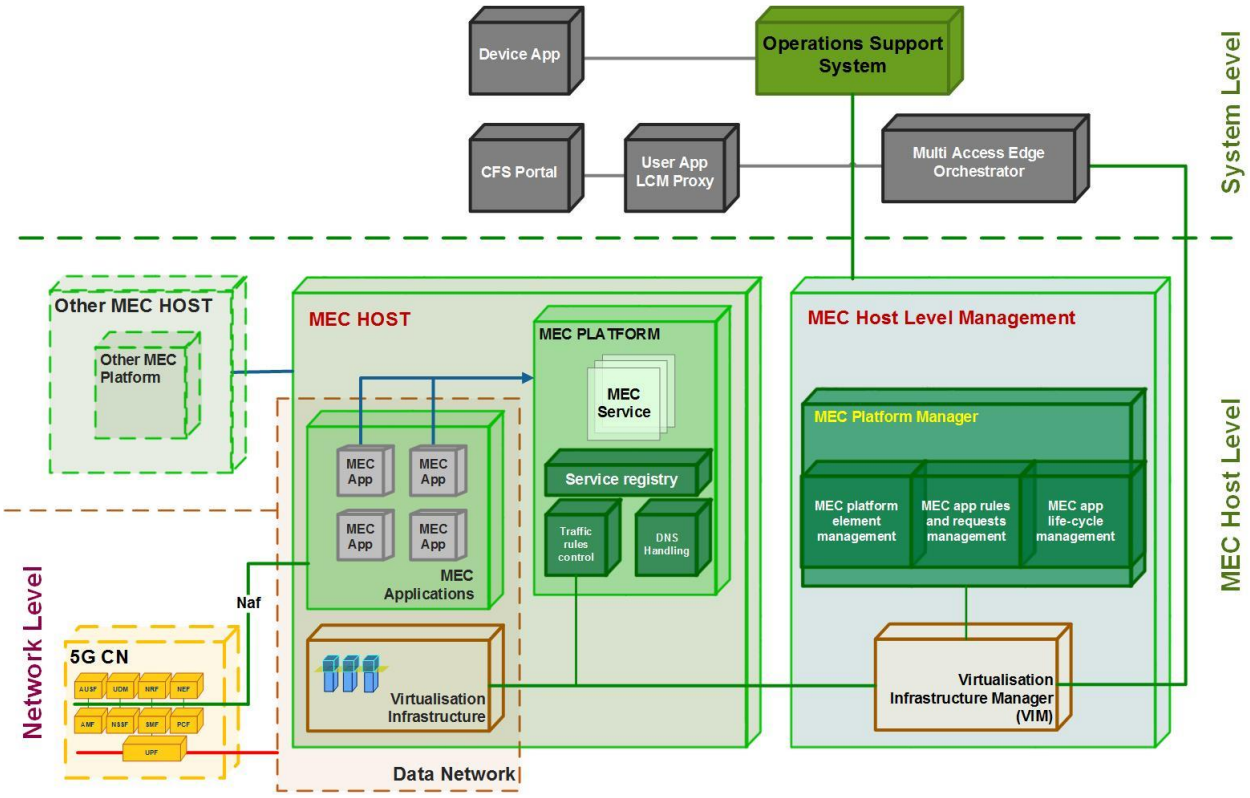
Multi-access Edge Computing (MEC) stands for the provision of cloud computing capabilities at the edge of the network, that is, for high bandwidth, low latency end- user applications.[40] MEC is located in the logical vicinity of base stations through authorised third parties willing to offer processing and storage capabilities to subscribers of the 5G network. MEC is a novel approach in the 5G ecosystem that enhances mobile user experience by covering services that, in previous generations, were using the run-time of end-user devices.

Through the capabilities of MEC, a variety of services can be bundled/converged into a single component, such as video, location services, virtual reality, etc. It is expected that MEC is going to emerge following the evolution of application services and verticals and will be one of the main drivers for a wider coverage and penetration of 5G Networks.

Besides offering these services, MEC takes an important role in the 5G infrastructure. It possesses orchestration functions, interacts with the 5G policy component and supports life-cycle matters of the offered applications.

The structure of MEC and its elements is shown in the figure below:

Figure 9: MEC architecture zoom-in



[40] https://www.etsi.org/technologies/multi-access-edge-computing?jjj=1568718105743, accessed September 2019.

The elements of MEC are as follows:

Element	Short description
Customer facing service (CFS) portal	The customer facing service portal allows operators' third-party customers (e.g. commercial enterprises) to select and order a set of MEC applications that meet their particular needs, and to receive back service level information from the provisioned applications.
Device application	Device applications as defined in the present document are applications in the device (e.g. UE, laptop with internet connectivity) that have the capability to interact with the MEC system via a user application lifecycle management proxy.
User application life-cycle management (LCM) proxy	The user application lifecycle management proxy allows device applications to request on-boarding, instantiation, termination of user applications and when supported, relocation of user applications in and out of the MEC system. It also allows informing the device applications about the state of the user applications. The user application lifecycle management proxy authorizes requests from device applications in the device and interacts with the OSS and the multi-access edge orchestrator for further processing of these requests.
Multi-access edge orchestrator	The multi-access edge orchestrator is the core functionality in MEC system level management, responsible for the following functions: maintaining an overall view of the MEC system; on-boarding of application packages; selecting appropriate MEC host(s) for application instantiation; triggering application instantiation and termination; triggering application relocation as needed when supported.
MEC host	MEC host is an entity that contains a MEC platform and a virtualisation infrastructure which provides compute, storage, and network resources, for the purpose of running MEC applications.
Virtualisation infrastructure	It provides compute, storage, and network resources for the MEC applications. The virtualisation infrastructure includes a data plane that executes the traffic rules received by the MEC platform, and routes the traffic among applications, services, DNS server/proxy, 3GPP network, other access networks, local networks and external networks.
MEC platform	It is the collection of essential functionality required to run MEC applications on a particular virtualisation infrastructure and enable them to provide and consume MEC services. The MEC platform can also provide services.

MEC applications	MEC applications are instantiated on the virtualisation infrastructure of the MEC host, based on configuration or requests validated by the MEC management.
MEC service	It is a service provided via the MEC platform either by the MEC platform itself or by a MEC application.
Service registry	In MEC, the services produced by the MEC applications are registered in the service registry of the MEC platform – as opposed to the network functions and the services they produce which are registered in the Network Resource Function (NRF).
Data Plane	Data plane described in this diagram is only a representation of the execution environment for the traffic rules and routing. Mapping of all or part of MEC data plane functionality to any functional element(s) of a real network architecture implies a specific deployment option of MEC in such a network architecture.
MEC host level management	It handles the management of the MEC specific functionality of a particular MEC host and the applications running on it. Is comprised of the MEC platform manager and the virtualisation infrastructure manager.
MEC platform manager	The MEC platform manager is responsible for the following functions: • Managing the life cycle of applications including informing the multi-access edge orchestrator of relevant application related events; • Providing element management functions to the MEC platform and • Managing the application rules and requirements. The MEC platform manager also receives virtualised resources fault reports and performance measurements from the virtualisation infrastructure manager for further processing.
Virtualisation infrastructure manager	The functionality provided by the virtualisation infrastructure manager in this ‘Zoom-in’ overlaps generally with the functionality provided by the VIM described in the NFV ‘Zoom-in’.
Inter-MEC system communication	Inter MEC systems communication is implementing three interfaces that are necessary for the communication between various MECs. In particular: • A MEC platform should be able to discover other MEC platforms that may belong to different MEC systems;

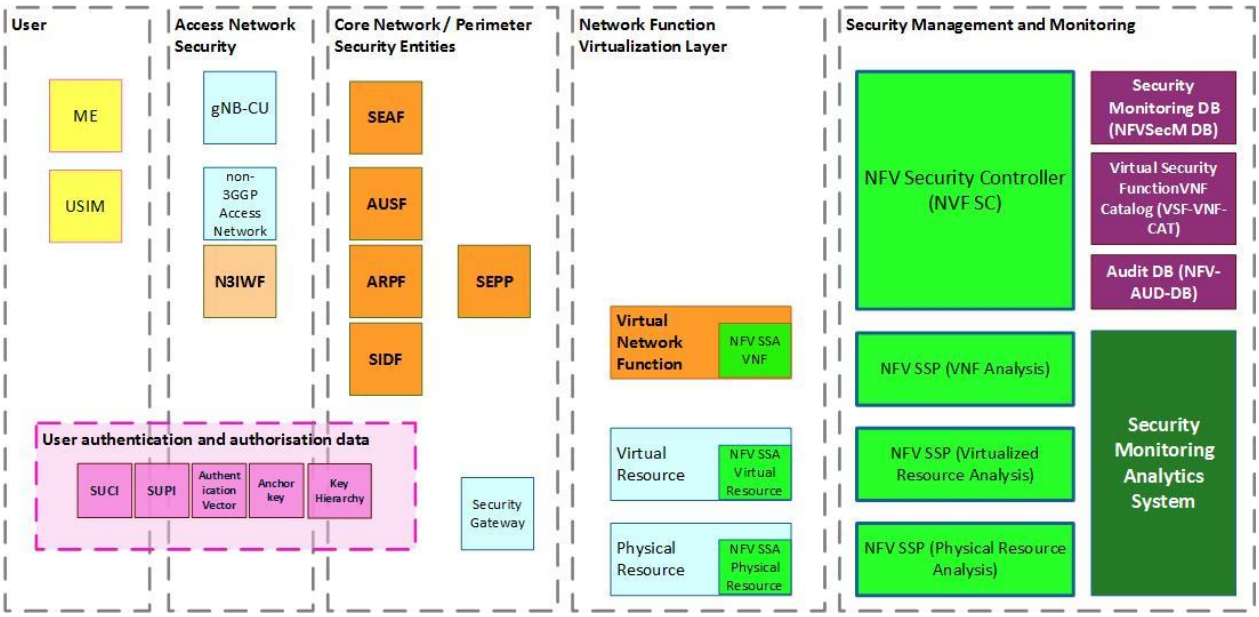
	• A MEC platform should be able to exchange information in a secure manner with other MEC platforms that may belong to different MEC systems. • A MEC application should be able to exchange information in a secure manner with other MEC applications that may belong to different MEC systems.

3.10 SECURITY ARCHITECTURE (SA) (ZOOM-IN)

The 5G security architecture consists of various network functions (NF) and components that are responsible for securing end-to-end communications, providing authentication functions and various other security functions. The 5G security architecture consists of components that are part of various other architectures ('Zoom-ins' in terms of this report), acting thus in a horizontal manner across all other architectures. In particular, security functions are securing the access of users within the radio access network (RAN), they cover security functions in the core network and perimeter entities (edge computing) and they provide security functions in the Network Function Virtualisation (NFV). Finally, a set of elements is covering security management functions, audit and analytics.

The detailed structure of the 5G security architecture is shown in the following figure:

Figure 10: 5G Security Architecture zoom-in



The elements of the 5G security architecture are as follows:

Element	Short description
Mobile Equipment (ME)	ME stands for all kinds of mobile equipment that can be connected to the 5G network. ME can be sensors, IoT components, connected autonomous systems, eHealth devices, etc.
Universal Subscriber Identity Module (USIM)	USIM is the SIM card of 5G.It is a platform for securing access and communication in 5G. It is the only security module mentioned in 3GPP specification.
5G Node Base Station Central Unit (gNB-CU)	Some security requirements for gNB-CU have been formulated by 3GPPP. Though not a security element per se, these requirements increase the security properties of gNB and – when implemented - are considered to be relevant to the security architecture.
Non-3GPP Access Network	Security for non-3GPP access to the 5G Core network is achieved by a procedure using IKEv2 as defined in RFC 7296 to set up one or more IPsec ESP security associations. The role of IKE initiator (or client) is taken by the UE, and the role of IKE responder (or server) is taken by the N3IW.
Security Anchor Function (SEAF)	The *SEAF* will create for the primary authentication a unified *anchor* key KSEAF (common for all accesses) that can be used by the UE and the serving network to protect the subsequent communication[41].
Authentication server function (AUSF)	The Authentication server function (AUSF) shall handle authentication requests for both, 3GPP access and non-3GPP access. The AUSF shall provide SUPI to the VPLMN only after authentication confirmation if authentication request with SUCI was sent by VPLMN. The AUSF shall inform the UDM that a successful or unsuccessful authentication of a subscriber has occurred.
Authentication credential Repository and Processing Function (ARPF)	ARPF selects an authentication method based on subscriber identity and configured policy and computes the authentication data and keying materials
Subscription Identifier De-concealing Function (SIDF)	The SIDF is responsible for de-concealment of the Subscription Concealed Identifier (SUCI) and shall fulfil the following requirements: • The SIDF shall be a service offered by UDM.

41 https://www.researchgate.net/profile/Andreas_Kunz2/publication/319527681_Overview_of_5G_security_in_3GPP/links/59b116d80f7e9b37434a8248/Overview-of-5G-security-in-3GPP.pdf, accessed September 2019.

	• The SIDF shall resolve the SUPI from the SUCI based on the protection scheme used to generate the SUCI.
Security Edge Protection Proxy (SEPP)	The 5G System architecture introduces a Security Edge Protection Proxy (SEPP) as the entity sitting at the perimeter of the mobile network. The SEPP shall act as a non-transparent proxy node.
NFV Security Services Agent (SSA)	The NFV SSA exists in both the NFVI domain and in VNF domain. NFV SSA in VNF domain may exist as a separate VSF, or within a VNF. The NFV SSA is responsible for securely receiving the Security Monitoring policy and implementing the same.
NFV Security Controller (SC)	The NFV SC may interface with other security systems (e.g. Security Analytics), security databases and other policy engines. The NFV SC orchestrates system wide security policies. The NFV SC acts as a trusted 3rd party that resides independently. An NFV SC manages NFV SSAs (like VSFs) to keep them in a consistent state according to the policy specified. SC also facilitates secure bootstrapping of SSAs (like VSFs), managing instances of SSAs, secure pairing up with SSA's VNFMs and EMs, personalize the SSAs, policy management, integrity assertion, credential management, facilitate clustering of multiple SSAs into a distributed appliance, monitoring of SSAs for failure and remediation.
NFV Security Services Provider (SSP)	The NFV SSP is located within the VIM and VNFM, and is responsible for security monitoring policy orchestration received from the Security Controller (NFV SC) and interacting with the various VIM/VNFM components to implement the policy across various systems comprising the NFVI/VNF. Furthermore, NFV SSP is also responsible for receiving the telemetry data from various NFV SSAs, and optionally making some analysis based on this data.
NFV Security Monitoring Database	The NFV SecM-DB is a secure database consisting of security data used for deploying NFV system wide Security Monitoring. This includes Security Monitoring policy and configurations, security credentials for facilitating secure communications between the various Security Monitoring components, and credentials for secure storage of telemetry, including tenant-specific security policies.
SA/VSF Catalog Database (VSF-NVNF-CAT)	The NFV VSF-VNF-CAT is a repository for Security Services Agents like the Virtual Security Functions (VSF) VNFs. The catalogue has capability to add and remove SSAs (VSF) packages and/or images, and also includes a VSF VNFD containing meta data and information about that VSF VNF. Once the SSA (VSF) package or instance is

	added to the catalogue, it becomes available for orchestration.
Audit DB	The NFV AUD-DB is a secure database consisting of security audit information.
Security Monitoring Analytics System	The Security Monitoring Analytics system securely receives Security Monitoring telemetry from across the NFV systems, including the MANO and all the NFVIs that may be geographically distributed. The analytics system applies advanced machine learning techniques on the telemetry to perform advanced detection of security anomalies and emerging threats in the system. This system also can trigger remediation actions through the NFV SC.
Subscription Concealed Identifier (SUCI)	A one-time use subscription identifier, which contains the Scheme-Output, and additional non-concealed information needed for home network routing and protection scheme usage.
Authentication Vector	A vector consisting of RAND, authentication Token (AUTN) and Hash eXpected RESponse (HXRES).
Anchor Key	The security key KSEAF provided during authentication and used for derivation of subsequent security keys.
Key Hierarchy	Hierarchy of cryptographic key derived from Anchor Key. (as defined in ETSI TS 133 501 section 6.2.) [42] It includes the following keys: KAUSF, KSEAF, KAMF, KNASint, KNASenc, KN3IWF, KgNB, KRRCint, KRRCenc, KUPint and KUPenc.

3.11 5G PHYSICAL INFRASTRUCTURE (ZOOM-IN)

One of the most important aspects in the transition from previous generations of mobile telecommunications into 5G is the 'softwarisation' of network functions, previously performed by physical appliances. Furthermore, some of these physical components were mostly proprietary and incompatible with other solutions. With 5G, the network software can run in any commercial-of-the-shelf (COTS) hardware, making MNOs less dependent on manufacturers.

This significant change will allow great scalability, quicker deployments, cost efficiency and integration between different components of the network. However, the high level of virtualisation will increase the impact of failures: a shared physical component will serve multiple functions (e.g. virtual functions, slicing, user equipment functions, etc.), playing thus a significant role in the service provisioning chain. At the same time this also greatly increases the complexity of the software implementation, which itself is associated with new threats.

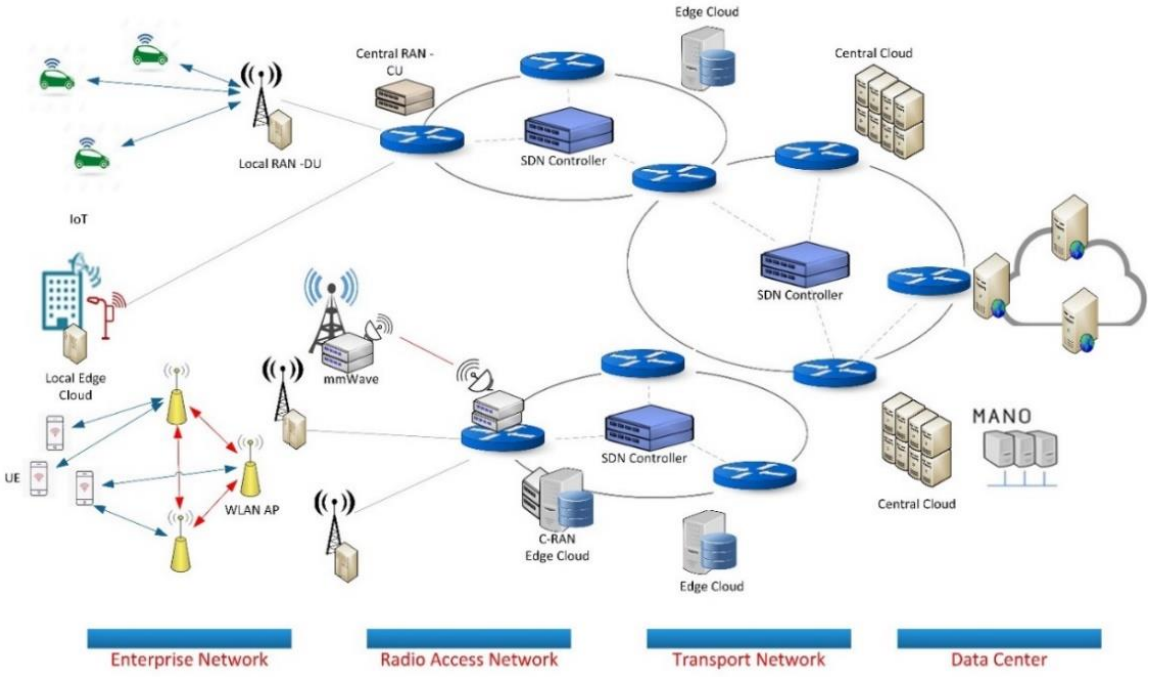
Nonetheless, the physical 5G architecture is going to remain exposed to more generic threats that are pertinent to physical components, such as: damage/theft, sabotage, natural disasters, outages, failures and malfunctions, just to name the most important ones. While in previous

[42] https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/15.01.00_60/ts_133501v150100p.pdf, accessed September 2019.

mobile networks such failures had a more 'restricted' influence in service provisioning, with the 5G virtualisation failures of physical components may have an amplified impact, typical to shared resources. This fact increases the criticality of 5G physical infrastructure components, as multiple services are going to depend on them.

The 5G physical infrastructure is depicted in the following figure:

Figure 11: 5G physical architecture zoom-in



The physical architecture shows all hardware components required for:

- Enterprise Network (out of scope of this report apart from UE);
- Radio Access Network consisting of RAN-CU, C-RAN MEC and mmWave routers;
- Transport network (backhaul) consisting of Edge Could, and SDN controller/switches and
- Data centre consisting of Central Cloud, MANO and SND controllers.

Note that this architecture does not contain details of some (important) security related hardware components such as Hardware Security Modules (HSM), Secure Execution Engines (SEE), Trusted Execution Engines (TEE), Trusted Platform Module (TPM), etc. These components are not entirely covered in 5G specifications considered in this report and may be added in future versions of this report.

4. 5G ASSETS

4.1 METHODOLOGICAL CONVENTIONS

As commonly defined, an asset is anything that has value to an individual or organisation and therefore requires protection. Besides being valuable to an organisation, assets may contribute to the fulfilment of legal obligations,

In a typical ICT system, assets can be:

a) hardware, software and communication components;
b) communication links between them;
c) data that control the function of the system, are produced and/or consumed by it, or flow within it;
d) the physical and organisational infrastructure within which the 5G system is deployed, and;
e) the human agents who interact with the system and may affect its operation (e.g., users, system administrators etc.).

Due to its value, a digital asset becomes a target for threat agents. Threat agents are human or software agents, which may wish to abuse, compromise and/or damage assets. Threat agents may perform attacks, which create threats that pose risks to assets.

In the overview of 5G assets provided in the remainder of this report, we have classified assets into different categories, described in section 4.2. Furthermore, we have grouped assets according to their position within the 5G architecture and their exposure.

4.2 ASSET CATEGORIES

5G assets have been derived from the provided architecture, including the details depicted in the various 'Zoom-ins'. The asset diagram is structured using asset groups according to their exposure to threats. By taking into account the role of assets in maintaining the security-related properties of confidentiality, availability and integrity (known as CIA triad),[43,44] an initial assessment of their importance has been developed. In doing so, the emphasis has been given to asset groups responsible for maintaining the overall security and availability of the 5G infrastructure and that are known targets of cyber-attacks.

In the present chapter, we present the various assets categories used for structuring 5G assets, together with a mapping showing the role of these asset categories for maintaining the CIA security properties. A detailed asset decomposition diagram with all 5G assets considered in this threat landscape can be found in Annex A.

The asset categories are shown in Figure 12 and their content is as follows:

Policy: Policy Control Functions (PCF) are performing provisioning, management of sessions related to consumer functions. These functions can be used for charging control (e.g. usage and charging), policy control and application detection control.[45] The functions are applied to

[43] https://en.wikipedia.org/wiki/Information_security, accessed September 2019.
[44] https://geek-university.com/ccna-security/confidentiality-integrity-and-availability-cia-triad/, accessed September 2019.
[45] https://www.etsi.org/deliver/etsi_TS/129500_129599/129512/15.01.00_60/ts_129512v150100p.pdf, accessed September 2019.

data flow detection, gating, Quality of Service traffic screening, etc. Given their role in the management of policy issues related to consumers, these functions may be targeted in order to influence monetary matters (charging) of 5G network usage.

Management processes: This asset group summarizes important processes assigned to development, deployment and operation of the entire set of components of the 5G infrastructure. They include configuration, network management, software development process, continuity, key and access rights management, etc. it seems that these processes will play a significant role in guaranteeing security and trust in 5G operations, and in component development in particular.[46,47] Some certifications based on process-level assurance schemes for 5G have been already announced.[48]

Business applications: Similar to previous generation mobile networks, these assets are representing commissioning and customer relationship management that are necessary in order to implement business-related matters within the 5G Network (referred to as Operational Support Systems – OSS and Business Support Systems – BSS). Such functions will be implemented through policy control functions. Being a vital part of customer maintenance and billing purposes, the assets in this category are exposed to manipulation (integrity) attacks. Confidentiality of subscriber information might also be targeted by attacks.

Business services: In a 5G context, this asset group refers to the components required to deliver a specific service that is monetized by a provider and/or MNO. An example is the delivery of horizontal, business, government, critical and emergency services.

Protocols: This asset group represents (main) communication protocols used within the 5G infrastructure. It covers protocols that are used in network communications, radio communications and security. Knowingly, protocols are common attack points with a series of threats, such as reconnaissance, eavesdropping, SYN flood, replay and man-in-the-middle attacks.

Data network: This asset group represents the connectivity to external data, content, services and other resources available outside the 5G network. The data network is also used to interconnect different 5G networks, operators and providers.

Slicing: This asset group represents all 5G functions that are responsible for the creation and management of slicing. Slices are virtualised independent logical networks that carry out the network communication between the user equipment and 5G services. Slices are end-to-end network communication links that are virtually multiplexed and mapped to resources of the virtualised physical network platform. While 4G allowed for APN (Access Point Name), in 5G slicing is taking place initially on a static base and later on a dynamic basis. Slicing is considered as one of the main advantages of 5G networks enabling low network latency.

Data: With this asset group, the entire data household for the operation of 5G are covered, notably confidential and/or security-related 5G data. Though not necessarily exhaustive at this stage of the analysis, this asset group covers information related to: user data, system and configuration data, security-related data, network data (configuration, edge, logs, API-data, SDN-data, etc.). It is expected that 5G data such as user, security and configuration information

[46] https://www.3gpp.org/news-events/1569-secam_for_3gpp_nodes, accessed September 2019.
[47] https://www.gsma.com/security/network-equipment-security-assurance-scheme/, accessed September 2019.
[48] https://www.gsma.com/aboutus/workinggroups/wp-content/uploads/2017/03/FS.14-NESAS-Security-Test-Laboratory-Accreditation-Pilot-Release_0.7.pdf, accessed September 2019.

will be subject to cyber-attacks with the aim to breach them. Main motives are monetization and unnoticed access to the network.

Human assets: Considered as one of the most important asset groups, human assets represent all individuals involved in the operation and use of the 5G network. Under this asset category, we include operator's staff (including tenants and security operators), 3rd party personnel and end-users. Of particular importance are operator and 3rd party data that are related to administration credentials. Members of this asset group may be involved in insider threat, information leakage and unintentional damages through errors.

Time: Time is an important asset group within 5G networks. It plays a significant role in many time-dependent functions (e.g. quality of service, network management, virtualisation management, etc.). The most critical interplay between time and network functions concerns security functions (such as key management, encryption and timestamps). Time inaccuracies may lead to failures and manipulations that can have far-reaching consequences to the availability of network functions. It is worth mentioning that the reduction of time inaccuracies in 5G has not yet been fully addressed in the current specifications and 5G virtualisation practices.

Legal: Assets of this category are related to various contractual agreements and Intellectual Property Rights (IPRs), that are either subject to bilateral of service provisioning among various 5G stakeholders or are related to IPR rights of the used services and components. Several cyber-threats, especially the ones that may lead to service unavailability and/or degradation may significantly affect these assets. Such an impact will have legal and monetary consequences for the party failing to provide their agreed services.

Legacy: This asset group encompasses all legacy systems connected to the 5G network or used within migration paths (e.g. from 2G to 5G). This asset group includes physical network functions (PNFs), service gateways, management entities, packet gateways, legacy protocols, legacy encryption infrastructure, etc. This asset group is exposed to unintentional damage threats and such that are concerned with the management of phased-out components (e.g. software and configuration maintenance).

Data storage/repository: This asset encompasses all assets (mainly network functions) that implement the persistence of and access to the stored 5G data. Though not fully exhaustive at this stage of the analysis, it covers the unified data repository function (UDF) and the storage functions for security-related information (catalogue database, security monitoring database and audit database). Due to its importance for the entire system security, this asset group may be subject to attacks aiming at compromising sensitive system information.

Physical infrastructure: This asset group includes all physical assets of 5G, mainly IT components, cabling and data centres and user equipment. More precisely, assets grouped in this category are network hardware, cloud and operator data centres, user equipment of all kinds, and radio access hardware. Despite the virtualised structure of the 5G network and all involved network functions, there will be a strong dependency on the physical infrastructure, especially in the initial migration/hybrid 5G deployments. Moreover, to deliver the required security services, some cryptographic hardware components at the data centre will play a critical role, while at the same time being potential points of failure. The entire physical infrastructure can be found in the corresponding 'Zoom-in' in the 5G architecture chapter (see chapter 3.11).

Management and orchestration (MANO): This asset group stands for the entire set of assets related to management and orchestration. MANO is considered to be the most critical part of the 5G infrastructure as it is responsible for managing the entire set of network functions, their

virtualisation and entire software life-cycle related hereto. The main parts of MANO are the Network Function Virtualisation (NFV) orchestrator, the Virtual Network Function (VNF) manager, and the virtualised infrastructure manager. Given its important role, MANO is going to be exposed to numerous attacks with potentially major impact on the entire managed 5G infrastructure environment. The assets of MANO are also depicted in detail in the corresponding 'Zoom-in' in the 5G architecture chapter (see chapter 3.5).

Radio Access Network (RAN): This asset group represents the logical components making up the functions of the Radio Access Network (RAN hardware is not part of this asset group). It includes mainly distribution unit and control unit of radio access. The RAN components and their interconnections can be found in the corresponding 'Zoom-in' in the 5G architecture chapter (see chapter 3.6).

Network Functions Virtualisation (NFV): This asset group contains all network functions that are virtualised to depart from proprietary dedicated hardware. NFV is a 5G specific architecture that virtualises classes of network node functions and physical network functions (PNF) into blocks that take over the entire connectivity actions necessary for communication services. This asset group also includes all security functions, that is, functions that cope will all the required authentication, monitoring and subscription. Security functions are considered particularly sensitive, as they use key material to perform operations. As such, they will be exposed to attacks aiming at breaching this information and compromise the entire security part of the 5G network. The entire NFV structure can be found in the corresponding 'Zoom-in' in the 5G architecture chapter (see chapter 3.7).

Software Defined Networks (SDN): This group contains the assets related to the SDN network controller, virtual network switches, data plane, application plane and control plane. Detailed information about SDN assets can be found in a previous ENISA thematic threat landscape covering SDN[38]. The contents of this report are still valid and can be used to obtain information about threat exposure and threat mitigation w.r.t. these assets. Due to its importance for 5G, SDN is considered within this document for completeness purposes. Due to its important role for the setup and management of the entire virtualised 5G network, SDN is regarded as a key component for the availability and integrity of network functions. The entire SDN architecture can be found in the corresponding 'Zoom-in' in the 5G architecture chapter (see chapter 3.8). References to SDN functions used from within other parts of the 5G architecture are shown in the various other 'Zoom ins' (e.g. NFV 'Zoom-in').

Lawful Interception (LI): Lawful Interception assets are concerned with the 5G functions implementing all provisions for performing lawful surveillance, providing thus legally sanctioned access to 5G private communications of all kinds. Interested readers can find detailed information on 5G LI provisions in this document.[49,50] Though not analysed much further in this document, these functions deserve special attention as they do provide any information processed in 5G networks. As such, LI (related functions and data) is a target for manipulations and other malicious actions (e.g. unlawful surveillance, weaponisation of interception, manipulation of information, etc.).

Transport: Transport assets represent all communication channels used for network transfer. This asset group includes satellite communication, fibre optics communication, micro-waves communication, Ethernet, as well as wireless and Near Field Communication (NFC). These assets are crucial for the availability of communication. However, with the virtualisation of the

[49] http://statewatch.org/news/2019/jun/eu-council-ctc-5g-law-enforcement-8983-19.pdf, accessed September 2019.
[50] https://www.etsi.org/deliver/etsi_ts/133100_133199/133127/15.00.00_60/ts_133127v150000p.pdf, accessed September 2019.

network architecture, transport becomes less important compared with previous generations of mobile communications.

Virtualisation: The role of virtualisation functions in 5G is crucial. With this asset group, we summarise assets that are related to virtual machine technologies and the hypervisor. Due to the massive virtualisation in 5G, these two components are decisive for the functionality of the entire network. Given the trend of using common open-source software for these two components, new vulnerabilities, when exploited, will multiply attack impact in the underlying technology platform. It is expected that hypervisors will be subject to attacks. With the ability to access and manage computer memory, attackers may access cryptographic material in case of operations performed in this memory (i.e. absence of dedicated crypto-hardware).

Cloud: Cloud technology will be extensively used within the 5G architecture, either through the provisioning of SaaS or IaaS. In the asset diagram, this group contains the logical cloud services. The hardware part related to cloud is covered in the physical infrastructure asset group. Cloud will be used as a platform by tenants to control storage and processing resources. Existing threats targeting cloud, when materialized, may unveil multiple confidential information, while at the same time affecting the availability of the entire 5G infrastructure.

Multi-access Edge Computing (MEC): This group consists of assets related to the decentralisation of cloud functions (storage of data and computing) located closer to the user or edge device. This group is further decomposed within this document using a specialised 'Zoom-in' of the 5G architecture (see chapter 3.9). This material can be used to decompose this asset group further.

Application Programming Interfaces (APIs): Application Programming Interfaces (APIs) are of great importance to the 5G ecosystem as they enable the exposure of functionalities across different networks. It allows applications and services to program network functions, to interconnect various networks and operators. 5G is also responsible for the introduction of REST API concept into telecommunications systems. REST,[51] which stands for Representational State Transfer is a set of constraints that, when applied to the design of a system, creates a software architectural style. The exposure of functionalities is a common concept used by modern software design, especially for web-services which are offered over the internet. REST APIs are defined along with a number of common principles which are referred to as REST architectural style.

Security Controls: This asset group contains some of the security controls that are relevant for communication networks in general and 5G in particular. They include, but are not limited to: incident management, DoS protection, intrusion prevention, intrusion detection, firewalling, network traffic analysis and security edge protection proxy. As these controls are key for the security of the network, they are considered as exposed to a variety of cyberthreats and are expected to be targets of attacks. Knowing that the mentioned controls are far from being exhaustive, they are a first attempt to enlist basic 5G security measures, also referenced within various specifications/5G architectures. Although they could be considered as security controls too, this asset group does not contain parts of the 5G security architecture, which are subsumed under network functions. The 5G security architecture was also depicted in a 'Zoom-in' (see chapter 3.10). In future versions of the 5G threat landscape, this asset group will be amended with additional assets (i.e. mitigation measures). This amendment will follow ongoing work in standardisation committees upon publication and will be subject to future versions of the 5G threat landscape.

[51] https://www.riverpublishers.com/journal/journal_articles/RP_Journal_2245-800X_617.pdf, accessed August 2019.

Figure 13: Used 5G asset categories

In the following table, we provide the relevance of the identified asset groups with regard to the CIA triad.

Table 2: Relevance of asset groups to the maintenance of CIA properties

Asset Group	CIA Triad		
	Confidentiality	Integrity	Availability
Policy	●	●	●
Management processes	●	●	●
Business applications	●	●	●
Business services	●	●	●
Protocols	●	●	●
Data network	●	●	●
Slicing	●	●	●

Data	🔴	🔴	🔴
Human assets	🔴	🟡	🟡
Time	🟢	🟡	🔴
Legal	🔴	🔵	🟡
Legacy	🔴	🔴	🟡
Data storage/repository	🔴	🔴	🟡
Physical infrastructure	🟡	🔴	🔵
Management and orchestration (MANO)	🔴	🔴	🔴
Radio access network (RAN)	🟡	🔵	🟡
Network functions virtualisation (NFV)	🔴	🔴	🔴
Software defined networks (SDN)	🔴	🔴	🔴
Lawful Interception (LI)	🔴	🟡	🟢
Transport	🔵	🟡	🔴
Virtualisation	🔴	🔴	🔴
Cloud	🟡	🟡	🔵
Application programing interfaces (APIs)	🟡	🔴	🔴
Security controls	🔴	🔴	🟡

Legend:

Very high relevance of asset group to maintain the property: 🔴
High relevance of asset group to maintain the property: 🟡
Medium relevance of asset group to maintain the property: 🔵
Low relevance of asset group to maintain the property: 🟢
Very low relevance of asset group to maintain the property: 🟢

The assignment of these security properties has been performed at the level of asset groups. We recommend performance of this exercise in higher detail, depending on the focus of prospective threat assessments. In this case, to achieve a more precise mapping, users of this document should obtain a more accurate internal evaluation of these properties.

Concluding this chapter, it is worth mentioning that due to its complexity and the early stage of 5G networks (development, deployment, specification) the asset mapping is an ongoing task that will need some time to reach a mature stage. This is due to a variety of reasons/issues regarding the parameters of current 5G activities (narrow time windows for the creation of reports, resource issues, knowledge transfer, vendor's enrolment, etc.). These challenges will be sufficiently managed in future assessment of 5G threats.

5. 5G THREATS

5G introduces significant innovation to mobile networks by integrating multiple and different types of technologies. While these are unquestionable benefits, the risks and threats are yet to be fully unserstood. The complexity and extension of the attack surface – as described in section 4.2 and presented in Annex A - makes the activity of accurately defining the 5G threat landscape a laborious task. The 5G threat landscape combines traditional IP-based threats with the all-5G network (core, access and edge), insecure legacy 2/3/4G generations and threats introduced by virtualisation technology.

5.1 TAXONOMY OF THREATS

The list below presents a list of high-level categorization of threats based on ENISA threat taxonomy.

- **Nefarious activity/abuse (NAA):** This threat category is defined as “intended actions that target ICT systems, infrastructure, and networks by means of malicious acts with the aim to either steal, alter, or destroy a specified target”.
- **Eavesdropping/Interception/ Hijacking (EIH)**: This threat category is defined as “actions aiming to listen, interrupt, or seize control of a third party communication without consent”.
- **Physical attacks (PA):** This threat category is defined as “actions which aim to destroy, expose, alter, disable, steal or gain unauthorised access to physical assets such as infrastructure, hardware, or interconnection”.
- **Damage (DAM):** This threat category is defined as intentional actions aimed at causing “ destruction, harm, or injury of property or persons and results in a failure or reduction in usefulness”.
- **Unintentional Damage (UD):** This threat category is defined as unintentional actions aimed at causing “destruction, harm, or injury of property or persons and results in a failure or reduction in usefulness”.
- **Failures or malfunctions (FM):** This threat category is defined as “Partial or full insufficient functioning of an asset (hardware or software)”.
- **Outages (OUT):** This threat category is defined as “unexpected disruptions of service or decrease in quality falling below a required level“.
- **Disaster (DIS):** This threat category is defined as “a sudden accident or a natural catastrophe that causes great damage or loss of life”.
- **Legal (LEG):** This threat category is defined as “legal actions of third parties (contracting or otherwise), in order to prohibit actions or compensate for loss based on applicable law”.

In addition to the above general taxonomy, we also categorise threats depending on whether the exploitation target is part of core network, radio access, network virtualisation or generic infrastructure component. Based on this criterion, threats can be further categorised into:

- **Core Network threats:** These threats relate to elements of the Core Network that includes SDN, NVF, NS and MANO. The majority fall under the categories of 'Nefarious activity/abuse' and 'Eavesdropping/ Interception/ Hijacking'. 5G Core Network threats are described in detail in section 5.2.

- **Access network threats:** These threats relate to the 5G radio access technology (RAT), radio access network (RAN) and non-3GPP access technologies. These include threats related to the wireless medium and radio transmission technology. The majority of the threats fall under the categories of 'Eavesdropping/Interception/ Hijacking'. Access network threats are described in more detail in section 5.3.

- **Multi-edge computing threats:** These threats relate to components located at the edge of the network. The majority fall under the categories of 'Nefarious activity/abuse' and 'Eavesdropping/ Interception/ Hijacking'. 5G Multi Edge Computing threats are described in detail in section 5.4.

- **Virtualisation threats:** These are threats related to the virtualisation of the underlying IT infrastructure, network and functions. Virtualisation threats are described in more detail in section 5.5.

- **Physical Infrastructure threats:** These are threats related to the underlying IT infrastructure that supports the network. The majority fall under the categories of 'Physical attacks', 'Damage or loss of equipment', 'Equipment failures or malfunctions', 'Outages', 'Disaster'. Physical infrastructure threats are described in more detail in section 5.6.

- **Generic threats:** These are threats that typically affect any ICT system or network. The generic threats are important to mention since these help defining and framing the ones specific to 5G. As an example: many 5G specific threats may result in a network service shutdown that in general terms is defined as a Denial of Service (DoS) threat. The Generic threats are described in more detail in section 5.7.

- **SDN threats:** These are threats related to the SDN functions that are omnipresent in the entire 5G infrastructure. For this document, we build on the threats identified in the ENISA Thematic Landscape SDN/5G.

5.2 CORE NETWORK THREATS

Abuse of remote access: This threat consists of a malicious actor having remote access to critical network components and take control of a virtual machine to perform other types of attacks. Remote access is a standard practice within the tech industry, to facilitate maintenance and operational procedures performed in clients. By gaining illegal access to the remote access function, a malicious actor can connect to operating systems and applications, in a critical domain of the network. With access to a machine in the network, a malicious actor can engage in other activities such as tampering configuration data and distribution of malware.

Authentication traffic spikes: This threat relates to a massive number of authentication requests sent by a malicious actor in a short time. A malicious actor initiates traffic spikes or emphasizes the effects of natural traffic spikes with IoT devices aiming to connect. Consequently, the network will experience more signalling and authentication requests that is

capable of handling. This kind of attack may be considered as a special case of denial of (authentication) service. Potentially, the authentication of authorized devices may fail resulting in the loss of connectivity.[53]

Abuse of user authentication/authorization data. This threat relates to the disclosure of long-term keys for authentication and security controls conducted by an insider or hostile or untrustworthy personnel operating in the Core Network.

Abuse of third party hosted network functions: This threat relates to availability issues and disclosure of sensitive data due to core network functions hosted on third-party cloud service providers' systems. An untrustworthy cloud service provider could access, interrupt and modify user/control plane traffic traversing its premises on behalf of the MNO.

Abuse of lawful interception function: This threat relates to the abusive use of the lawful interception function (based on the law) performed by a network operator/access provider/service provider (NWO/AP/SvP), making available certain information to a law enforcement monitoring facility. This threat also considers the unauthorised access to this function when hosted outside the operator's network. If a vendor/supplier has access to the mobile network then it will be possible for him to manipulate this function and bypass the audit mechanisms in a way that the abuse is not detected by the MNO.

Application programming interface (API) exploitation: This threat involves exploiting application programming interfaces (APIs) to launch different types of attacks. Much of the openness and programmability offered by the new 5G network architecture relies on the expanded use of APIs. The exploitation can target different types of API naming internal network functions, internetworking interfaces, roaming interfaces, etc. exposed in different layers of the network. A poorly designed or configured API with inaccurate access control rules may expose core network functions and sensitive parameters. It is important to highlight that 5G infrastructure will rely on COTS solutions that extensively use open source APIs. The level of quality and scrutiny imposed in the development and implementation of proprietary solutions should also apply for COTS and open source components. The threat of having one small compromised API in the 5G core may place the entire network at risk.

Exploitation of poorly designed architecture and planning (network, services and security): Classified as unintentional damage - Inadequate design, planning or improper adaptation – this threat relates to issues arising from the multiple options and features that this technology has to offer from its original inception to implementation. The level of complexity and the difficulty to reach an optimal architecture, adequate security and operating procedures may lead to poor design and implementation. Design flaws are opportunities for malicious actors to exploit. By knowing that a particular feature that is not adequately implemented or protected, a malicious actor can exploit the breach and inject malware in the core network.

Exploitation of misconfigured or poorly configured systems/networks: Often identified as a vulnerability, it's the exploitation of misconfigured or poorly configured systems that qualifies as a threat. The exploitation of a misconfigured system that in essence is from an unintentional nature, creates the opportunity for a threat actor to reach critical assets in the network or stage an attack. Configuration flaws may happen at different stages of the solution implementation life-cycle such as product installation and maintenance. Examples include poorly configured APIs, network functions, access control rules, network slices, administration rights, virtualised environments, traffic isolation, edge nodes, orchestration software, firewalls, etc. It is worth

stating that this threat has consistently been a major cause of incidents reported to ENISA in the Article 13a security breach notification process[52].

Erroneous use or administration of the network, systems and devices: Classified as unintentional damage (erroneous administration of devices and systems) the errors resulting from a poorly maintained and administrated network may compromise the confidentially, integrity and availability of the network. An example of actions associated with a poorly administered system includes the lack of operational processes and procedures that could expose the network to an attack.

Fraud scenarios related to roaming interconnections: In a roaming scenario, the visited network needs to obtain authentication vectors from user's home network, that could abusively authenticate the user thus giving him access to serving MNO resources.[53]

Lateral movement: Classified as nefarious activity/abuse of assets, lateral movement is often adopted by threat agents to gain position in different components of the core network. Once a threat actor gains position, obtains enough time to perform reconnaissance activities to find weaknesses in the network. The threat of lateral movement is of a great concern due to the complex nature of and diversity of technologies used in a 5G Network. This fact allows threat actor to operate undetected for longer periods and fine-tune an attack.

Memory scraping: This threat arises when an attacker scans the physical memory of a software component in order to extract sensitive information that it is not authorised to have. While memory scraping can affect components of any layer of the network, this type of threat has been primarily identified for SDN application servers. While memory scraping threat may target different components of the core network, a core dump of an SDN controller (e.g. as the result of malicious software) can be used to exploit private data. Furthermore, SDN reconfiguration may require reboots that an attacker could use in order to attack the boot procedure. Once successfully performed, memory scraping can be used to extract sensitive SDN data (e.g. flow rules at the northbound API).

Manipulation of network traffic, network reconnaissance and information gathering: The threat includes the modification or falsification of data in transit (messages), injection of illegitimate data into the network, whether by replaying previous messages or by forging new messages, the use of traffic spikes and rerouting, modification of flow priorities.

Manipulation of network configuration data: Inadequate policies in the management and protection of critical configuration data may lead to unpredictable system behaviour and unauthorised access to critical platforms, with impact on the confidentiality and integrity of the network. This threat involves compromising a core network element (e.g. SDN controller, network function, management and orchestration function) by forging configuration data to launch other attacks (e.g. DoS). While configuration data forging may, in principle, relate to data held by any component of the network, this threat refers specifically to configuration and/or control plane data. Examples of configuration data manipulation are listed below.

- Routing tables manipulation
- Falsification of configuration data
- DNS manipulation

Malicious flooding of core network components: This threat involves flooding a network component with requests or traffic, compromising its availability. Flooding may occur during the

[52] https://www.enisa.europa.eu/topics/incident-reporting/for-telcos, accessed September 2019.

transmission of data, exhausting component resources and leading to a reduction or complete shutdown of the service provided by the component. This threat also considers other techniques such as amplification and saturation described below.

Amplification and flooding attacks take place in specific SDN components whereby a small stream of requests from a faked sender elicits a massive flood of responses. While protection from such attacks has been devised for many known network protocols, the exposure of several network functions (NFV) by SDN controllers presents a completely new landscape of threats.

Flooding attacks may come in the flavour of distributed DoS attacks, where a vast number of sources may be orchestrated to generate the message floods. These sources could, for example, be the members of a botnet, e.g. a collection of devices infected with malware to the point that they can all be controlled by an attacker to execute the attack. Flooding attacks may affect all kinds of external interfaces the network provides, including the radio interface, interfaces to external networks like the internet or other mobile networks.

Malicious diversion of traffic: This threat involves compromising a network element to divert traffic flows and allow a malicious actor to eavesdrop on network traffic. Traffic diversion is a threat relating to network elements of the data plane. A specific kind of traffic diversion that is available in virtualised networks is the network slice trespassing. This threat may occur when the mandatory isolation between slices is compromised in any active node or when the enforcing access to a slice in the edge equipment is either bypassed or misconfigured.

Manipulation of the network resources orchestrator: The threat considers the manipulation of the network resources orchestrator configuration to perform an attack. This threat includes modifying a network function behaviour by altering the settings in the orchestrator (E2E service inventory, service programmability) and consequently compromising the separation between network functions.

Misuse of audit tools: This threat is classified under nefarious activities/abuse of assets. Audit tools are used by MNOs to monitor the activity of the network and obtain information that can be used for multiple purposes such as optimisation, security, commercial, etc. This type of software tools retain information about the network and its users and provide an advantage to malicious actors to perform recognisance activities for an attack. A malicious actor typically uses insiders to the MNO with privileged access to these tools to extract sensitive information.

Opportunistic and fraudulent usages of shared resources. This threat relates to unauthorised access and/or modification of 5G connected devices critical data. End-to-end keys may be stolen or leaked from the centralized key servers. As a consequence, the end-to-end secured communication is vulnerable for different attacks and adversaries gain an access to the end-points. The root cause is the leaking of authentication, authorization and accounting (AAA) credentials from the MNO's employee network.[53]

Registration of malicious network functions. This threat is classified as nefarious activities or abuse of assets (NAA). An unauthorised network function (NF) or function embedding a Trojan, - introduced in the network by an insider (to the MNO) or a vendor/service provider - could be abusively installed in the service base architecture (SBA) and registered in the core network via NRF, in order to expose other malicious APIs. By having an unauthorized network function installed or activated, a malicious actor may have access to sensitive assets in the network to

[53] https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP_White-Paper_Phase-1-Security-Landscape_June-2017.pdf, accessed September 2019

perform other type of attacks such as DoS, distribution of malicious software, stealing sensitive information, etc.

Traffic sniffing: Sniffing is a popular method used by malicious actors to capture and analyse network communication information. With sniffing, a malicious actor is also able to eavesdrop data from network elements or links and steal valuable information. Sniffing can happen anywhere where there is constant traffic. In SDN for example, a malicious actor can take advantage of unencrypted communications to intercept traffic from and to a central controller. The data captured could include critical information on flows or traffic allowed on the network.

Side-channel attacks: This threat involves extracting information on existing flow rules used by network elements. The threat can be realised by exploiting patterns of network operations (e.g. exploiting the time required for establishing a network connection). Side-channel attacks are a threat relating to network elements of the data plane.

5.3 ACCESS NETWORK THREATS

Abuse of spectrum resources: The illegal use of these resources, due to the dynamic allocation/ reallocation of the same, may allow the occupation of specific idle spectrum band by imitating the characteristics of a legitimately licensed unit and causing interference in radio frequencies. This illicit occupation of the spectrum may also induce a network node to reject spectrum resources requested by unlicensed units - due to the apparent lack of idle resources – thus blocking someone out of the core network.

Address Resolution Protocol (ARP) poisoning: This kind of attack is also called ARP cache spoofing: a technique by which an attacker sends spoofed ARP messages onto the network. Generally, the aim is to associate the attacker's MAC address with the IP address of another host, such as the default gateway, causing any traffic meant for that IP address to be sent to the attacker instead.

Fake access network node: Classified as a nefarious activity, this threat considers the compromise of a base station (gnB) by masquerading as legitimate, facilitating different types of attacks such as man-in-the-middle or network traffic manipulation. The threat considers tampering the communication between the mobile user equipment (UE) and the network to initiate other malicious actions.

Flooding attack: This threat involves flooding radio interfaces with requests. Flooding occurs through the transmission of data that can exhaust component resources and lead to a reduction or complete shutdown of the radio frequency provided by the component.

IMSI catching attacks: This threat relates to cellular paging protocols that can be exploited by a malicious actor in the vicinity of a victim to associate the victim's soft-identity (e.g., phone number, Twitter handle) with its paging occasion. Through an attack dubbed ‘$mathsf{ToRPEDO}$’ a malicious actor can verify a victim's coarse-grained location information, inject fabricated paging messages, and mount denial-of-service attacks.

Jamming the radio frequency: Classified as a nefarious activity/abuse of asset, this threat refers to an intentional disruption/interference of the network radio frequency (NRF) causing the core network (and related services) to become unreachable for affected users. The threat also refers to the unavailability of the transport layer when using radio-based networks and interference with the geo-positioning system (GPS).

MAC spoofing: MAC spoofing is a technique for changing a factory-assigned Media Access Control (MAC) address of a network interface on a networked device. The MAC address that is hard-coded on a network interface controller (NIC) cannot be changed. However, many drivers allow the MAC address to be changed. Additionally, there are tools which can make an operating system believe that the NIC has the MAC address of a user's choosing. The process of masking a MAC address is known as MAC spoofing. Essentially, MAC spoofing entails changing a computer's identity to conduct an attack.

Manipulation of access network configuration data: This threat involves compromising an access network element (e.g. base stations) to forge configuration data and launch other attacks (e.g. DoS).

Radio interference: A threat in which the perpetrator seeks to make a network resource unavailable to its intended users by temporarily or indefinitely interfering or disrupting the Radio Access Network service. The introduction of compromised 5G devices in a radio access network will present a more substantial DoS threat.

Radio traffic manipulation: This threat considers the manipulation of network traffic at the base station level. A man-in-the-middle attack can be launched based on a rogue base station when malicious actor masquerades its Base Transceiver Station (BTS) as a real network's BTS. This threat is still considered valid due to backwards compatibility to previous generations of mobile technology. Other associated threats follow:

- Traffic redirecting

Session hijacking: This threat is classified as nefarious activity or abuse of asset and relates to attacks to open-air interfaces. The threat considers the theft of legitimate authenticated conversation session ID by a malicious actor, to control the whole session of specific traffic to conduct other types of attacks.

Signalling fraud: One of the areas of concern is the international signalling interconnection between networks which may be misused for fraud (e.g., false charging). Another example is the threat of greedy mobile nodes that transmit fake incumbent signals and force all other users to vacate a specific band (spectrum hole) to acquire its exclusive use.

Signalling storms: Mobile networks are subject to 'signalling storms' launched by malware or apps, which overload the bandwidth at the cell, the backbone signalling servers, and Cloud servers, and may also deplete the battery power of mobile devices. Signalling storms will be more challenging due to the excessive connectivity of UEs, small base stations, and high user mobility.

5.4 MULTI EDGE COMPUTING THREATS

False or rogue MEC gateway: The open nature of edge gateways, where even user-owned devices can become full-fledged participants (e.g. personal cloudlets, TV smart-box, etc.), creates a scenario where malicious actors can deploy their own gateway devices. This particular threat produces the same outcome as the Man-in-the-Middle attack.

Edge node overload. This threat relates to attacks against edge networks disrupting the vicinity of the affected networks, at a local or service-specific level. The overload may take place by flooding the edge node with request or traffic directed to this component, initiated by a specific mobile app or IoT device.

Abuse of edge open application programming interfaces (APIs): The abuse of open APIs in Multi Edge Computing nodes is done through the exploitation of vulnerabilities in MEC type of

applications. The need for open APIs in MEC is mainly to provide support for federated services and interactions with different providers and content creators. This threat can be associated with DoS, man-in-the-middle, malicious mode problems, privacy leakages, and VM manipulation.

5.5 VIRTUALISATION THREATS

Abuse on Data Centers Interconnect (DCI) protocol: Virtualised systems are deployed within data centers, hence, security threats of Data Centers should be considered. This threat relates to the exploitation of specific vulnerabilities of Data Centers Interconnect (DCI) protocols (e.g. lack of authentication and encryption). An attacker could create spoofed traffic in such a way that it traverses DCI links or to create a DoS attack of DCI connections.

Abuse of cloud computational resources: The abuse of powerful computing infrastructure, including both software and hardware components, could be easily achieved using a simple registration process in a cloud computing service provider. By taking advantage of the prevailing computing power of cloud networks, hackers can fire attacks in a very short time. For example, brute force attacks and DoS attacks can be launched by abusing the power of cloud computing.

Network virtualisation bypassing: Issues related to bad network slicing implementation and configuration or improper isolation can cause loss of data confidentiality/privacy (Data/traffic intercepted by entities of other slices). A network used by different tenants needs to assure that only legitimate traffic enters or leaves a network slice, but also that any switching element checks and enforces the traffic isolation by installing legitimate flow rules preventing slice trespassing. At core network level, the hostile actor would exploit hypervisor vulnerabilities and flow rules configuration to trespass slice isolation and disclose data belonging to other tenants.

Virtualised host abuse: This threat relates to applications running on virtualised hosts, abusing from shared resources from a virtualised environment. In virtual environments, where physical resources are shared between tenants, there may be a set of behaviours that result in the disclosure of sensitive information. For instance, exposure via scavenging in virtualised environments is even more serious than in physical systems. While interception is a common threat in physical systems (e.g., networking environments), its effect is further exacerbated in virtual environments because it permits cross-inspection of various tenant's data flow, as well as topology inference that could serve to set up a DoS attack.

5.6 PHYSICAL INFRASTRUCTURE THREATS

Manipulation of hardware equipment: This threat considers the inclusion of concealed hardware or software in the product by a vendor or supplier. This threat may occur at an initial stage of the product implementation or during maintenance with the application of uncontrolled updates and new features.

Natural disasters affecting the network infrastructure: Classified as natural or environmental disaster, this threat refers to natural events such as fires, floods and earthquakes that can affect 5G network equipment and therefore, the availability of the service at a local and regional level. Specific types of assets are more exposed to natural disasters such as radio access equipment (e.g. base stations) and network transport due to its installation on an outdoor environment.

Physical sabotage/vandalism of the network infrastructure: Classified as a deliberate physical attack, this threat relates to actions taken by actors aimed at destroying, disabling or stealing physical assets supporting the 5G Network. A physical attack to 5G critical assets may disrupt, interfere and ultimately cause unavailability of the network service. Despite the existence of physical protection mechanisms (e.g., physical surveillance and surveillance

cameras, security locks, security guards), physical breaches and insider threat attacks may still occur.

Threat from third parties' personnel accessing MNO's facilities. This threat consider the physical access to facilities and network physical infrastructure by third-party personnel, to perform maintenance activities and provide technical support. Hostile and untrustworthy operators could affect the security requirements of the network.

UICC format exploitation. New UICC formats could lead to new kind of vulnerabilities that may be exploited for data exfiltration, fraud or DoS purposes. Different types of new UICC components (like eUICC, iUICC, soft SIM, etc.) require new management protocols for the provisioning of user-profiles and their life cycle. These protocols can be exploited to create DoS toward the user or for fraud scenarios, including user impersonification.

User equipment compromising: New formats of user equipment, including low-cost insecure IoT devices, could introduce new kind of vulnerabilities, which may be exploited to target user data confidentiality and integrity. Abuses on hardware and software implementation on UE side to install malicious components may compromise confidentiality and integrity of subscriber profile data.

5.7 GENERIC THREATS

Denial of Service (DoS): DoS is a threat categorised under Nefarious Activity and Abuse of Asset (NAA), in which the perpetrator seeks to make a network resource unavailable to its intended users by temporarily or indefinitely interfering or disrupting the network service. The attack comprises the generation of a massive number of requests or with traffic in a way that the network becomes partly or completely unavailable for regular users. Multiple types of threats may lead to a denial of service such as flooding, amplification, signalling storm and saturation attacks. An attack combining multiple vectors may lead to a distributed DoS (DDoS) attack.

Data breach, leak, theft destruction and manipulation of information: This includes, but not limited to, the theft of personal information through unauthorised access to the systems and/or network, unauthorised access to and possible publication of personal identifiable information/biometric/medical (privacy breach), company confidential information (intellectual property, commercial and financial data) or government/state-related information (classified information). The theft, breach or leak of other types of data such as user credentials, encryption keys, network security logs, software configuration, etc. may also help malicious actor conducting different types of attacks.

Eavesdropping: Classified as Nefarious Activity and Abuse of Asset (NAA), eavesdropping is a threat in which the perpetrator seeks to tamper the application and communication layers from the various 5G network elements (SDN controller, network function, edge node, virtualisation orchestrator). It includes the eavesdropping on subscriber' data, confidential information, system time, subscriber location, electronic messages, signal of data relayed over the network. The threat actor monitors, spies and/or eavesdrop Nation-State citizens and/or organisations to track the location or access sensitive information.

Exploitation of software and hardware vulnerabilities: This type of threat enables a malicious actor to take advantage of unknown (to the vendor and user) or unpatched software or hardware flaws to perform an attack. Example include the exploitation of known hardware and software flaws such as meltdown, spectre and buffer overflow. It also includes the exploitation of other known vulnerabilities related to previous generations of mobile telecommunications and older signalling protocols such as SS7 (Signalling System 7) and Diameter.

Malicious code or software: The threat includes the installation and distribution of malicious software or the implant of specific code or software inside a product or updates. Examples of malicious software include malware, ransomware, virus, worms, trojans, SQL injections, rogue security software, rogueware and careware. An example of a malicious software in the 5G context considers the use of an unauthorised VNF that could abusively install and register itself into the core network in order to expose malicious APIs.

Compromised supply chain, vendor and service providers: This threat considers the intentional insertion by a vendor into the product of concealed hardware, malicious software and software flaws. It also considers the implementation of uncontrolled software updates, manipulation of functionalities, inclusion of functions to bypass audit mechanisms, backdoors, undocumented testing features left in the production version, among others.

This threat also relates to activities performed by untrustworthy third parties' personnel during product testing, maintenance, configuration and operation. Third parties' personnel have access to the network management facilities (both locally and via remote interface) in order to perform maintenance activities and provide technical support. This privileged access to the operation, administration and management (OAM) of the network provides an advantage to untrustworthy third parties' personnel to access various type of data such as (subscriber's, system and network configuration, telemetry data).

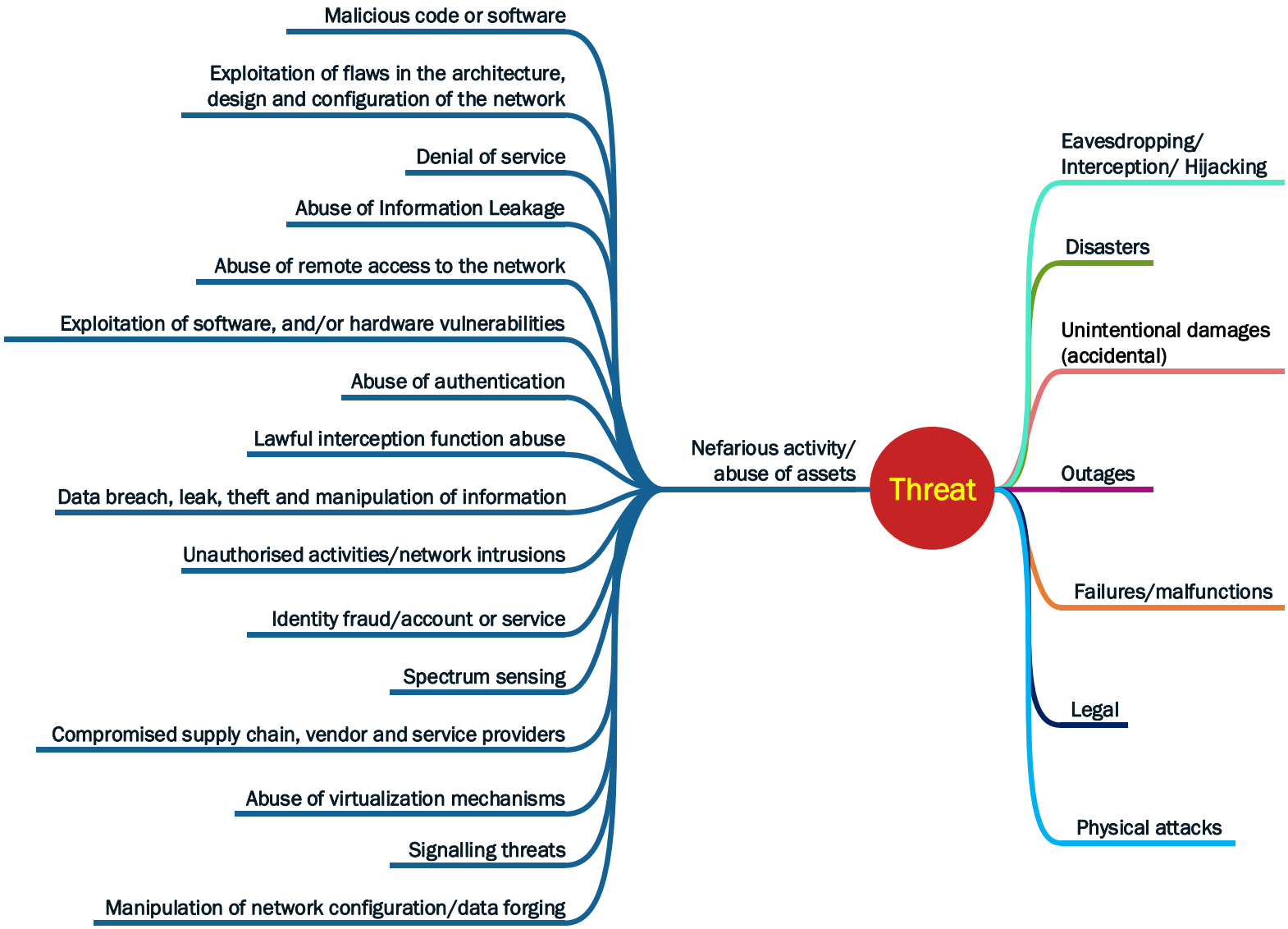
Targeted threats: Highly sophisticated attacks or advanced persistence threats may target sensitive information, e.g. state secrets, industrial secrets or intellectual property, or the availability of sensitive and critical services.

Exploiting flaws in security, management and operational procedures: Not directly related with 5G, this threat will become relevant when dealing with the complexity of the technology and the need to introduce operational procedures to the management of the Network. This threat includes, but not limited to, the exploitation of flaws in the operational and security management of the network; configuration, update and patch management of the software. The errors from the lack or poorly design operational and security procedures may have consequences to the integrity and availability of the network.

Abuse of authentication: This threat may affect multiple network entry points such as user equipment (mobile devices and IoT), operation and management interfaces, roaming and vertical services. This threat includes the theft of user credentials, brute force of user accounts, password cracking, masking the user identity and impairment of an IoT grouping authentication as techniques used by threat actors to abuse the 5G authentication systems.

Identity theft or spoofing: This threat may materialise when a malicious actor successfully determines the identity of a legitimate entity and then masquerades to launch further attacks. Identity spoofing is a threat that can affect any software component or human agent. In this attack, the attacker spoofs the identity of a legitimate controller and interacts with the network functions controlled by the legitimate controller (i.e. elements of the data plane) to trigger several other types of attacks (instigate network flows, divert traffic, etc.). The use of social engineering, brute force user account/password cracking may also be used as a technique to spoof or steal user credentials.

Figure 14 - 5G Threat Landscape (Summary)



5.8 LIST OF 5G AND GENERIC THREATS

Threat Type	Threats	Potential Impact	Affected Assets	
Nefarious Activity/ Abuse of assets (NAA)	**Manipulation of network configuration/data forging** - Routing tables manipulation - Falsification of configuration data - DNS manipulation - Manipulation of access network and radio technology configuration data - Exploitation of misconfigured or poorly configured systems/networks - Registration of malicious network functions	- Information integrity - Information destruction - Service unavailability	- SDN, NFV, MANO - RAN, RAT	- System configuration data - Network configuration data - Security configuration data - Business services
	Exploitation of software, hardware vulnerabilities - Zero-day exploits - Abuse of edge open application programming interfaces (APIs) - Application programming interface (API) exploitation	- Information integrity - Information destruction - Service unavailability	- SDN, NFV, MANO - RAN, RAT - MEC - API - Physical infrastructure - Business applications - Security controls - Cloud, virtualisation	- Subscribers' data - Application data - Security data - Network data - Business services
	Denial of service (DoS) - Distributed denial of service (DDoS) - Flooding of core network components - Flooding of base stations - Amplification attacks - MAC layer attacks - Jamming of the network radio - Edge node overload - Authentication traffic spikes	- Service unavailability - Outage	- SDN, NFV - RAN, RAT - MEC - CLOUD	- Network services - Business services
	Remote access exploitation	- System integrity	- SDN, NFV, MANO - CLOUD	- Network services
	Malicious code/software - Injection attacks (SQL, XSS) - Virus - Malware - Rootkits - Rogueware - Worms/trojan	- Service unavailability - Information integrity - Information destruction - Other software asset integrity - Other software asset destruction	- Data network - Business applications - Security controls - Cloud, virtualisation	- Subscribers' data - Application data - Security data - Network data - Business services - Network services

- Botnet - Ransomware			
Abuse of remote access to the network	- Information integrity - System integrity	- SDN, NFV - RAN, RAT	- Subscribers' data - Application data - Security data - Network data
Abuse of information leakage - Theft and/or leakage from network traffic - Theft and/or leakage of data from cloud computing - Abuse on security data from audit tools - Theft/breach of security keys	- Information integrity - Information destruction - Information confidentiality	- Data storage/repository - - Subscribers' data - Cryptographic keys - Monitoring data - User subscription profile data	
Abuse of authentication - Authentication traffic spikes - Abuse of user authentication/authorization data by third parties' personnel	- Information integrity - Information destruction - Service unavailability	- Security data - Network service	- Subscribers' data - Application data - Security data - Network data
Lawful interception function abuse	- Information integrity - Information destruction	- Subscribers' data - User subscription profile data	
Manipulation of hardware and software - Manipulation of hardware equipment - Manipulation of the network resources orchestrator - Memory scraping - MAC spoofing - Side channels attacks - Fake access network node - False or rogue MEC gateway - UICC format exploitation - User equipment compromising	- Service unavailability - Information integrity - Information destruction	- Cloud data center equipment - User equipment - Radio access/units - Light data centers - SDN, MANO, NF - RAN, RAT - Virtualisation	- Subscribers' data - Network services
Data breach, leak, theft and manipulation of information	- Information integrity - Information destruction - Information confidentiality	- Subscribers' data - Subscriber geo locations - Financial data - Commercial data, IP - Configuration data - Service data - Network data	

	Unauthorised activities/network intrusions - IMSI catching attacks - Lateral movement	- Information integrity - System integrity	- User equipment	- Network services - Business services
	Identity fraud/account or service - Identity theft - Identity spoofing	- Service unavailability - Information destruction - Information integrity	- User subscription profile data - Subscribers' data	
	Spectrum sensing	- Service unavailability	- RAT - Radio access units	
	Compromised supply chain, vendor and service providers - Threat from third parties' personnel accessing MNO's facilities	- Service unavailability - Information integrity - Information destruction	- SDN, NFV, MANO - RAN, RAT - MEC - API - Physical infrastructure - Business applications - Security controls - Cloud, virtualisation	- Network services - Business services
	Abuse of virtualisation mechanisms - Network virtualisation bypassing - Virtualised host abuse - Virtual machine manipulation - Data center threats - Abuse of cloud computational resources	- Service unavailability - Information integrity - Information destruction	- Virtualisation - SDN, NFV, MANO - Cloud	- Network services - Business services
	Signalling threats - Signalling storms - Signalling fraud	- Service unavailability - Information integrity - Information destruction	- RAT - Radio access units - Protocols	- Network services - Business services
Eavesdropping/ Interception/ Hijacking (EIH)	**Nation state espionage**	- Information integrity - Information confidentiality	- Subscribers' data - Subscriber geo locations	
	Corporate espionage	- Information integrity - Information confidentiality	- Financial data - Commercial data - IP	
	Traffic sniffing	- Information integrity - Information confidentiality	- Data traffic - Subscribers' data - Subscriber geo location	

	Manipulation of network traffic, network reconnaissance and information gathering - Radio network traffic manipulation - Malicious diversion of traffic - Traffic redirecting - Abuse of roaming interconnections	- Information integrity - Information confidentiality	- Data traffic - Subscribers' data - Subscriber geo locations	
	Man in the middle/ Session hijacking	- Information integrity - Information confidentiality	- Data traffic - Subscribers' data - Subscriber geo locations	
	Interception of information	- Information integrity - Information confidentiality	- Data traffic - Subscribers' data - Subscriber geo locations	
Physical Attacks (PA)	**Sabotage of network infrastructure (radio access, edge servers, etc.)**	- Service unavailability - Information destruction - Information integrity	- Radio access units - ICT equipment - Light data center - Cloud data center	- Network services - Business services
	Vandalism of network infrastructure (radio access, edge servers, etc.)	- Service unavailability - Information destruction - Information integrity	- Radio access units - ICT equipment - Light data center - Cloud data center	- Network services - Business services
	Theft of physical assets	- Service unavailability - Information destruction - Information integrity	- Radio access units - ICT equipment - Light data center - Cloud data center	- Network services - Business services
	Terrorist attack against network infrastructure	- Service unavailability - Information destruction - Information integrity	- Radio access units - ICT equipment - Light data center - Cloud data center	- Network services - Business services
	Fraud by MNO employees	- Service unavailability - Information destruction - Information integrity	- Radio access units - ICT equipment - Light data center - Cloud data center	- Network services - Business services
	Unauthorised physical access to based stations in shared locations	- Service unavailability - Information destruction - Information integrity	- RAT - Radio access units	- Network services - Business services
	Misconfigured or poorly configured systems/networks	- Service unavailability - Information integrity	- Management processes - Policies	- SDN, NFV, MANO, API - RAN, RAT, MEC - Physical infrastructure

Unintentional damages (accidental) (UD)			- Legal - Human assets	- Business applications - Security controls - Cloud, virtualisation
	Inadequate designs and planning or lack of adaption - Outdated system or network from the lack of update or patch management - Errors from the lack of configuration change management - Poorly design network and system architecture	- Service unavailability - Information integrity	- Management processes - Policies - Human assets	- SDN, NFV, MANO - RAN, RAT - MEC - API - Physical infrastructure - Business applications - Security controls - Cloud, virtualisation
	Erroneous use or administration of the network, systems and devices	- Service unavailability - Information integrity	- Management processes - Policies - Human assets	- SDN, NFV, MANO - RAN, RAT - MEC, UE, API - Physical infrastructure - Business applications - Security controls - Cloud, virtualisation
	Information leakage/sharing due to human error	- Information integrity - Information confidentiality	- Data storage/repository - Management processes - Policies - Legal - Human assets	- Subscribers' data - Application data - Security data - Network data
	Data loss from unintentional deletion	- Information integrity - Information confidentiality	- Management processes - Policies - Human assets	- Subscribers' data - Application data - Security data - Network data
Failures or Malfunctions (FM)	**Failure of the network, devices or systems**	- Service unavailability - Information destruction - Information integrity	- Cloud data center - User equipment - RAT, Radio unit - Light data center	- Network services - Business services
	Failure or disruption of communication link	- Service unavailability - Information destruction - Information integrity	- Cloud data center	- Network services - Business services
	Failure or disruption of main power supply	- Service unavailability - Information destruction - Information integrity	- Cloud data center	- Network services - Business services
	Failure or disruption from service providers (supply chain)	- Service unavailability - Information destruction - Information integrity	- Network services - Business services	

	Malfunction of equipment (devices or systems)	- Service unavailability - Information destruction - Information integrity	- Radio access units - ICT equipment - Light data center - Cloud data center	- Network services - Business services
Outages (OUT)	**Loss of resources** - Human resources - Physical resources	- Service unavailability - Information destruction - Information integrity	- Human assets - Legal	- Network services - Business services
	Support services	- Service unavailability - Information destruction - Information integrity	- Human assets - Management processes - Policies - Legal	- Network services - Business services
	Data network (access)	- Service unavailability - Information destruction - Information integrity	- Cloud data center	- Network services - Business services
	Power supply	- Service unavailability - Information destruction - Information integrity	- Cloud data center	- Network services - Business services
Disasters (DIS)	**Natural disasters** - Earthquakes - Landslides	- Service unavailability - Information destruction - Information integrity	- Radio access units - ICT equipment - Light data center - Cloud data center	- Network services - Business services
	Environmental disaster - Floods, storms - Pollution, dust, corrosion - Fires, heavy winds - Unfavourable climatic conditions	- Service unavailability - Information destruction - Information integrity	- Radio access units - ICT equipment - Light data center - Cloud data center	- Network services - Business services
Legal (LEG)	**Breach of service level agreement (SLA)**	- Service unavailability - Information destruction - Information integrity	- Network services - Business services	
	Breach of legislation	- Service unavailability - Information destruction - Information integrity	- Network services - Business services	
	Failure to meet contractual requirements and/or legislation	- Service unavailability - Information destruction - Information integrity	- Network services - Business services	

6. THREAT AGENTS

In the next generation of Mobile Networks (5G), it is expected that the existing threat agent profiles will develop towards a new set of capabilities and motives. This is due to the overarching nature of the 5G Mobile Networks: they are going to play the role of 'networks of networks', thus completely changing the use of the Internet and similarly, interconnecting numerous verticals that until now have been operating in isolation. Due to their nature, 5G networks will deliver multiple added-value and critical services and functions to the economy and society. This will attract the attention of existing and new threat agent groups with a large variety of motives.

Given this complexity, it is expected that the following facts are going to change the attacker profile:

- A whole set of new vulnerabilities will expand the attack surface, exposure and number of critical assets.
- New tools/methods to exploit those vulnerabilities will be developed.
- New motives/ impacted targets are going to be observed due to the interconnected verticals/applications.
- Existing threat agent groups may be expanded with ones that have an interest in novel malicious objectives.

These facts may cause an unprecedented shift of capabilities and objectives of existing threat agent groups in ways that have not been seen in the past. The description of threat agent groups takes all these considerations into account at a theoretical level. This is because the 5th generation of mobile networks is not yet fully rolled-out and is currently in the pilot phase.

In the following descriptions, the threat agent groups introduced from ENISA Threat Landscape 2018[54] (ETL2018) are going to be used, extrapolated to the new facts potentially affecting attacker's profiles. Because of the latter, the new threat-agent group cyber-warriors will be added to the existing groups. This is due to the fact that 5G Mobile Networks are going to comprise a significant target for military operations, but also as a platform used for military purposes, as already mentioned in some sources[55,56].

ELT2018 categorizes thread agents as follows:

- Cyber criminals
- Insider (own, third parties)
- Nation states
- Hacktivists
- Cyber-fighters
- Cyber-terrorists
- Corporations
- Script kiddies

[54] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018, accessed September 2019.
[55] https://finabel.org/5g-implications-on-the-battlefield/, accessed September 2019.
[56] https://www.linkedin.com/pulse/5g-weapon-should-we-scared-dr-michelle-dickinson-mnzm-/, accessed September 2019.

Another nuance that will be important in the development of threat agent profiles is the ability to have legitimate access to the network: while legitimate internal and external employees are covered through the agent group 'Employees', one needs to take into account that almost all of the above mentioned external threat agents may have legitimate access to the network. This will take the hurdle of access to the attacked system(s), facilitating thus their malicious purposes.

Having said all the above, a short description of the 5G threat agent groups is as follows:

Cyber-criminals: Given the vast presence of this threat agent group in cyber-space and the advanced capabilities that they continue maintaining, it is likely that this threat agent group will keep its presence w.r.t. 5G Mobile networks. Given the statistics of activities of this threat agent group,[57] it looks like their attacks targeting multiple industries and governments may be channelled to the emerging 5G Mobile Networks.[58] Though not yet representing a significant monetizing vector, such attacks (or preparations hereto), will be part of their activities.[59] The anticipated number of vulnerabilities, the complexity and low level of maturity of the 5G network are indicative for this shift.[60] Legitimate access of cyber-criminals to the 5G network may exacerbate the threats posed by this group.

Insiders: Insiders are assumed to be a vital threat agent group in the 5G landscape mainly because these are MNOs employees, in constant proximity with the core of the technology representing a vast number of individuals. Other reasons substantiate the importance of this group naming the complexity of the network and a large number of stakeholders engaged in its use and operation. While the skill issue and increased complexity will surge the amount of unintentional damages significantly, dishonest insiders and 3rd party employees may misuse their access to vital network function to cause high impact/large scale availability issues in the network itself. Such incidents may have cascaded impact on interconnected industries/verticals. Given the fact that disgruntled/dissatisfied insiders are a primary target for high capability agents, they might be recruited to abuse their insider knowledge, e.g. through monetary rewards. Finally, given the current race for 5G patents/IPS matters, it is expected that this threat agent group will have an additional motive to increase their activities.

Nation States: This threat agent group is important due both to its ability to compromise future 5G Network and its potential motivation to do so. It is indisputable that vendors of 5G components – just like any other technology vendor– are in a better position to cause devastating attacks to the operation of self-developed components, especially when governments influence them. Given the importance of 5G to the sovereignty of nation-states, they will most probably be a target of state-sponsored attacks. Despite the numerous activities to setup vendor requirements namely, to understand the misuse vectors of various components and design the corresponding security controls, it will not prevent a nation state from attacking another country 5G Network. According to recent statistics,[57] attacks motivated by espionage represent a significant number in the 2019 threat landscape.

Cyber warriors: Cyberwar is, according to incident statistics,[57] the third most frequent motive and a trend that will inevitably keep up w.r.t. the 5G ecosystem. For many reasons, it is worth to say that 5G infrastructure will be one of the most vital components to protect in the technology landscape. This is mainly due to the need to maintain dominance, independence and

[57] https://www.hackmageddon.com/2019/08/12/june-2019-cyber-attacks-statistics/, accessed September 2019.
[58] https://blog.trendmicro.com/trendlabs-security-intelligence/telecom-crimes-against-the-iot-and-5g/, accessed September 2019.
[59] https://eandt.theiet.org/content/articles/2019/02/cybercrime-will-be-exacerbated-by-5g-mcafee-experts-say/, accessed September 2019.
[60] https://www.bbc.com/news/technology-49043822, accessed September 2019.

sovereignty of a country, especially the ones in which a vicinity between vendors and governments is being maintained (e.g. US, Europe, China). Moreover, there is evidence, that the military sector will be interested in using 5G[61,62], just as many security-related verticals (e.g. critical infrastructures). Such a development will amplify the protection requirements and the attractiveness of 5G as a target of cyberwar. Cyber warriors will maintain their presence in the cyberthreat landscape with a focus on 5G in both roles of defender and offender, depending on global geopolitical developments. It is expected that this is part of the agendas in the defence sector, especially in those countries that strive for technological dominance and influence.

Hacktivists: Though this threat agent group has a presence in the cyberthreat landscape (fourth position by means of number of incidents), it is not clear how it is going to be engaged in 5G malicious activities. While the most probable is to see this group engaging in regional campaigns, it cannot be excluded that it could achieve high impact activities in national and even global 5G infrastructures. Just as the efficiency of attacks of all other threat agent groups, this will depend heavily on: a) the maturity of 5G rollouts w.r.t. cybersecurity protection measures, b) the number of vulnerabilities of 5G components, c) the availability of 5G exploits/malicious tools and modus operadi and d) the skill set available to master 5G infrastructure complexity at the side of 5G stakeholders. Just as other threat agent groups, hacktivist will be able to gain legitimate access to 5G network, hence attacking from inside the network.

Corporations: Although this threat agent group has not enjoyed special attention in recent ENISA Threat Landscapes, it is believed that its role will increase in future editions of the report. The main reason lays in the intention to increase competitiveness and becoming part of the 5G ecosystem. On the other hand, corporations will be interested in tracking the development of patents and IPRs that are related to 5G infrastructure: given the emergence of 5G technology, this area is going to attract the attention of this threat agent group mainly. Other reasons for increased engagement are to trace the involvement of competitors to 5G procurements, understand business opportunities related to 5G and strengthen their role in the market. Due to the overarching nature of 5G, corporations from a large number of sectors/vertical will be potentially attracted by 5G developments, increasing thus the number of entries into this threat agent group.

Cyber-terrorists: There are multiple references to alleged interest from this threat group to produce harm to 5G infrastructures.[63,64] The main concern about future actions from this group is the concentration of 'values' that will take place as a result of a 5G deployment. 5G is going to (inter-) connect vast amounts of services that are vital to the society, governments and business and this will thus attract the attention of cyber-terrorist groups. Through the integration of multiple verticals, 5G will provide a single attack surface that once targeted, may result in damages in the physical space (e.g. hybrid threats). Although incident statistics do not provide evidence for significant activity of cyber-terrorists in the cyber-space, 5G stakeholder will need to take the protection of this infrastructure very seriously to avoid high impact events that would cause severe harm to society.[65] This effort requires multifaceted/multilevel protection controls involving coordinated activities of numerous stakeholders at a scale that had never existed before 5G. This is a challenge that can be mastered, only if there is a concerted effort to protect

[61] https://www.techradar.com/news/how-the-5g-network-could-benefit-the-military, accessed September 2019.
[62] https://www.afcea.org/content/5g-warfighters, accessed September 2019.
[63] https://thehill.com/opinion/national-security/444251-5g-risk-is-about-more-than-simply-securing-competitive-advantage, accessed September 2019.
[64] https://www.mobileworldlive.com/featured-content/home-banner/uk-security-chief-warns-of-5g-terrorism-threat/, accessed September 2019.
[65] https://www.scmp.com/news/china/diplomacy/article/3020354/while-weighing-5g-security-risks-france-predicts-it-can-manage, accessed September 2019.

5G infrastructure and its importance goes beyond the threats posed by a single threat agent group.

Script kiddies: The emerging technology landscape has many components that are in the control of individual users. Examples are IoT devices, mobile phones, cloud and storage spaces, social media platforms, etc. These components are the perfect playground for technology-interested young individuals that have low motivation/low capabilities but are equipped with malicious tools. In the past, we have seen high impact attacks (e.g. DDoS) spreading from home devices and gadgets. With the availability of high-speed 5G networks and interconnected devices, activities of this threat agent group may cause significant impact though cascaded events affecting upstream components of 5G operators. Just as all other threat agent groups, script-kiddies may possess legitimate access to the network and be able to use network functions to manage their own devices, increasing thus the potential of misuse.

Table 3 - Involvement of threat agents in threats[66]

	Cyber-criminals	Insiders	Nation States	Cyber-warriors	Hacktivists	Corporations	Cyber-terrorists	Script-kiddies
Nefarious activity/Abuse	✓	✓	✓	✓	✓	✓	✓	✓
Eavesdropping/ Interception/ Hijacking	✓	✓	✓	✓	✓	✓	✓	✓
Disasters			✓	✓			✓	
Unintentional Damage	✓	✓	✓	✓				✓
Outages	✓	✓	✓	✓	✓		✓	
Failures/ malfunctions	✓	✓	✓	✓	✓	✓	✓	✓
Legal	✓	✓	✓	✓	✓	✓	✓	
Physical attacks	✓	✓	✓	✓	✓	✓	✓	

Legend:
Primary group for threat: ✓
Secondary group for threat: ✓

[66] It is worth mentioning that the involvement is indicative and at a high level of abstraction (i.e. threat categories). Interested stakeholders will be in the position to construct more precise threat agent profiles by assigning threats at lower level of abstraction from the threat taxonomy found in this document. A more detailed assignment has not been provided to increase readability of the table.

7. RECOMMENDATIONS/ CONCLUSIONS

7.1 RECOMMENDATIONS

Based on the assets, threats and the state-of-play of current developments, the following recommendations/courses of actions can be made for various stakeholders of the 5G ecosystem:

Recommended courses of action at EU level (e.g. Member States, European Commission, ENISA):

Share existing 5G knowledge to stakeholder communities: Current technical material should be disseminated at EU level. Consolidated results will enable evidence-based policy actions. The content produced needs to be widely disseminated and settled as a basis for guiding technical discussions and future iterations with all related stakeholder groups engaged in policy-making.

Promote bridges between all stakeholders: Within the coming years, it will be important to stimulate working relationships with all relevant 5G stakeholders with a focus on the material that serves as a basis for future knowledge capturing and knowledge dissemination in the area of 5G threat analysis. This needs to lead to an efficient network of experts in various domains that will be responsible for contributing to the creation of 5G Cyberthreat Intelligence (CTI). This material plays a central role in the production of future risk assessments, thus creating the conditions to compatible/coherent risk assessments.

Enable the necessary iterations to improve the current material on cyberthreats: Together with the engaged stakeholders, there is a need to create planning content for future iterations of threat/risk assessment work to be performed by various stakeholders at EU level. This plan will allow for better coordination of work; it will enable an efficient mobilisation of resources and will create a competitive advantage for EU 5G stakeholders. Coordination with the work of 5G standardisation bodies will be of particular importance. Coordination with EU 5G initiatives active in the security field will also be key to achieve since delivering.

Recommendations for 5G market stakeholders (e.g. vendors, MNOs, Operators of Serices, Standardisation Bodies, etc.):

Engage in EU-wide discussions on 5G matters: Organisations engaging in the 5G market (e.g. vendors, operators and verticals) hold a significant part of the knowledge on 5G, as they roll out initial pilots/versions of 5G infrastructures. Their experience in technical, organisational and business issues of a 5G deployment are of particular importance for the generation of practical security guidance.

Contribute to the knowledge collection/dissemination: A basis for injecting non-competitive information will need to be agreed and built up. For this purpose, trust models among the participating organisations need to be established. The provision of human resources to take care of this interaction will be necessary.

Bring in knowledge on economic/investment/market penetration dimensions: Currently, too less information on economic aspects and investment plans on 5G deployment are available. This information is necessary to assess the economic capacity of market players and understand/prioritise feasible steps for the implementation of security measures, perform gap analysis and understand the impact of security incidents. It is proposed to collect this kind of information that will help to create more targeted guidance on 5G cybersecurity implementation plans.

Recommendations for national competent bodies in the area of 5G cybersecurity (e.g. NRAs, NCSCs, National 5G Test Centres, etc.):

Disseminate existing 5G material: Competent bodies are an important link in the dissemination of 5G material from and to the EU stakeholders. This dissemination will need to be performed in a coordinated manner to achieve coherence with and the extension of the developed knowledge base. Such coordination will need to be performed within all national and EU groups engaging in 5G activities. It will be subject of plannable consolidation efforts to be taken into account within EU-wide plans.

Inform about 5G activities held in the scope of their responsibilities: Competent bodies will need to inform national and EU 5G stakeholders/partners about their activities. This will help to create national and EU-wide coordination and to leverage EU activities on national efforts. Produced information will be hooked-up to corresponding activities accordingly. This will contribute to an efficient mobilization and usage of existing 5G efforts/resources.

Provide available expertise and human resources: Available 5G resources are scarce/limited. The efficient use of those resources will be necessary to achieve maximum efficiency and reduce duplicated efforts. This will be a decisive factor for the achievement of the tasks on the 5G agenda and will increase the trust among participating experts.

While the above may be advisable future actions for various stakeholder groups, ENISA envisages an involvement in the following actions:

Disseminate current details of assets and threat landscape to all kinds of stakeholders: This action will enable the creation of a common terminology and a shared understanding of threat exposure of valuable 5G assets. This information will facilitate future interactions and will provide a solid basis for future – eventually more detailed – assessments, while enabling the expansion of the material on an on-demand basis. It will be essential to create feedback loops to keep this material updated so that it builds a comprehensive and solid EU-wide knowledge base (see also establishment of hooks below).

Refine/amend existing material according to the pace of 5G developments: While 5G specification and deployment activities progress within the related market, additional details are added to the current threat assessment to: cover emerging specifications, follow-up on further information from current market and policy developments.

Establish hooks to enrol and mobilise strategic stakeholders: The current level of 5G stakeholder engagement needs to be increased. Vendors, MNOs and NRAs need to be more actively integrated into the related work. Moreover, better coordination with EU bodies needs to be settled (e.g. NIS Cooperation Group, EU DGs and Units) to inject existing knowledge to Member States and EU-policy activities. This action will come to amplify the effects mentioned in the above points (disseminating knowledge and gradual amending existing material).

These proposals will need to be validated by Member States (NIS CG) and European Commission. In this respect, ENISA may be tasked with technical work reflected in these recommendations as deemed necessary.

7.2 CONCLUSIONS

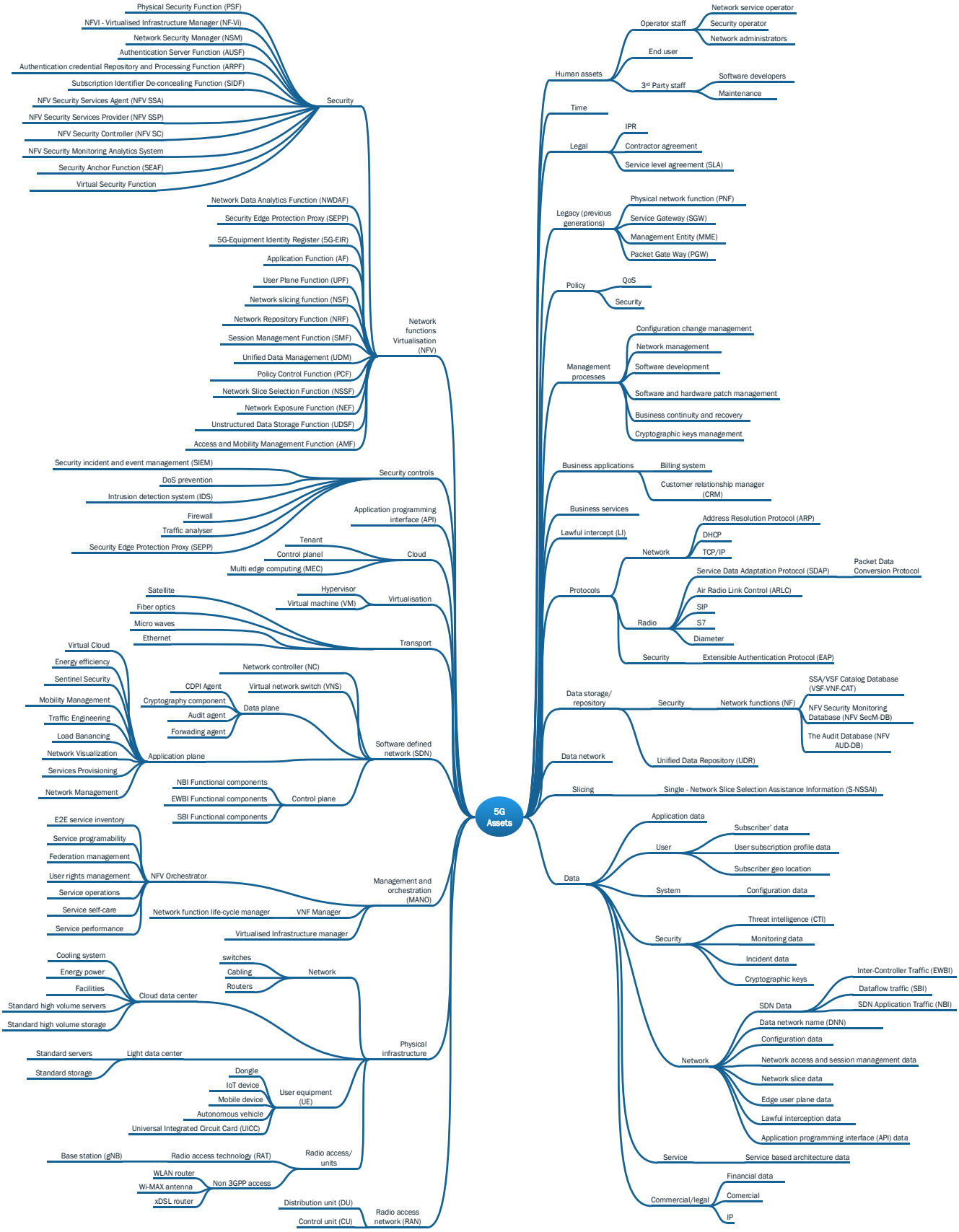
Concluding this first attempt towards the identification of 5G asset exposure to cyberthreats, ENISA draws the attention of all relevant stakeholders to the above-identified recommendations. It will be important to use this material in various stakeholder activities, identify current and future developments and try to accommodate those in future versions of the present report.

Such a development will speed up the adoption of security requirements and secure 5G practices and will create competitive advantages within the entire EU space.

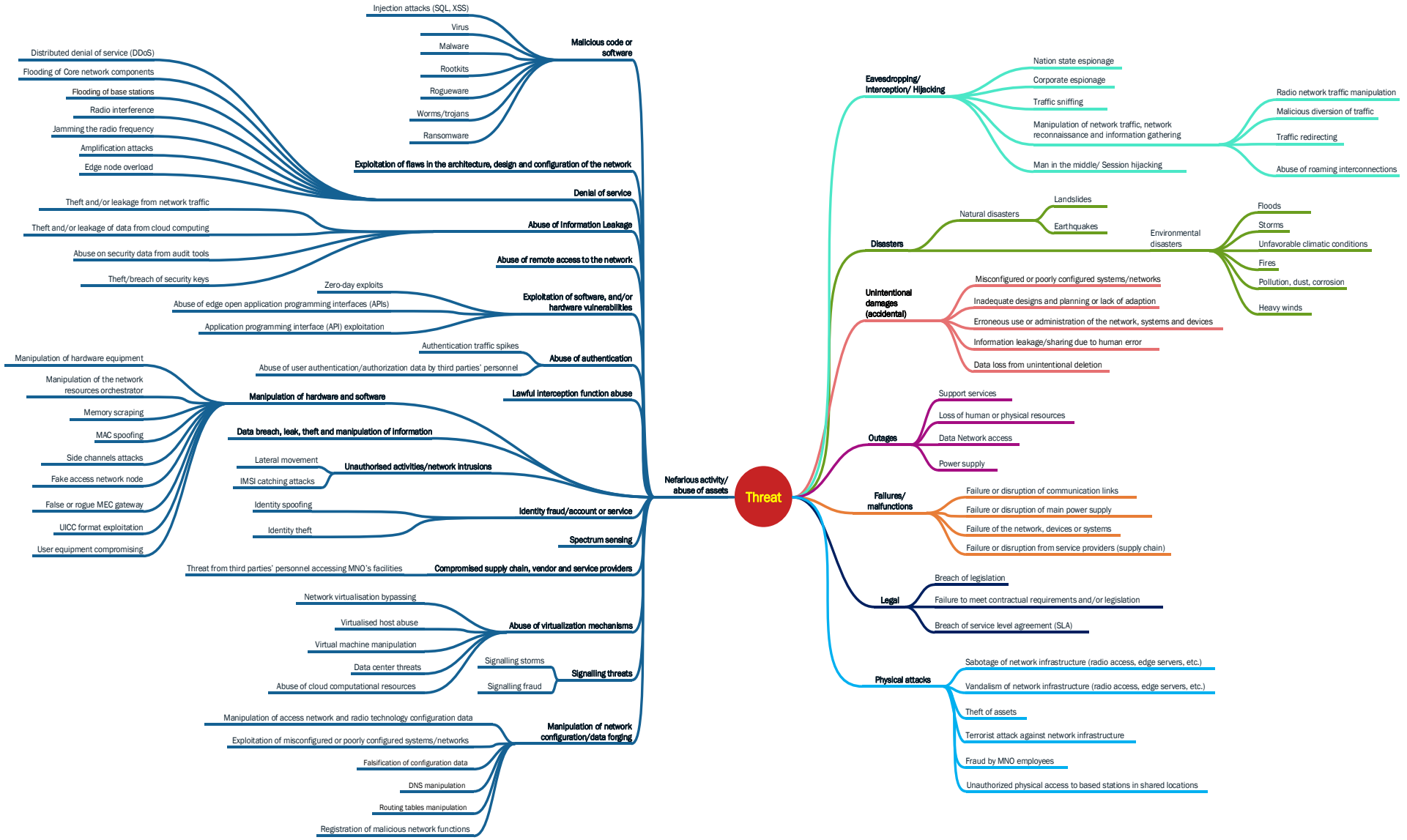
ENISA will continue engaging within cybersecurity activities of 5G. Coordination with EU-wide activities will be key to the success of this attempt.

Future ENISA actions on this matter will be agreed upon, mandated and coordinated with European Commission and Member States (NIS CG) as deemed necessary.

ANNEX A: ASSETS MAP (FULL)



ANNEX B: THREAT TAXONOMY MAP (FULL)



ANNEX C: MAPPING RISK SCENARIOS TO CYBERTHREATS

RISK SCENARIO Coordinated Risk Assessment	Relevant Threat Category	Comment
Misconfiguration of networks	Nefarious Activity Outages (of Data Networks) Legal (breach of service level) Unintentional Damages	
Lack of access controls	Outages Failures/Malfunctions Physical Attack Unintentional Damages Eavesdropping/Interception/Hijacking Disasters Nefarious Activity/Abuse of Assets	
Low product quality	Unintentional Damages Failures/Malfunctions Legal Nefarious Activities	Nefarious activities are mainly the ones that are concerned with the abuse of flaws in software due to low quality (i.e. vulnerabilities, leakages, architecture design)
Dependency	Outages Failures/Malfunctions Physical Attack Unintentional Damages Eavesdropping/Interception/Hijacking Disasters Nefarious Activity/Abuse of Assets	All cyberthreats affecting technical assets of a single strategic provider may lead to the materialization of this scenario
State interference through 5G supply chain	Nefarious Activity/Abuse of Assets Physical attack Eavesdropping/Interception/Hijacking	Nefarious activities concentrate on injection of malicious code and manipulation of hardware and software (see also corresponding threats in threat taxonomy)
Exploitation of 5G networks by organised crime	Nefarious Activity Physical Attack Eavesdropping/Interception/Hijacking Outages	Outages constitute a component of a more complex attack vector containing additional cyberthreats.
Injection of false messages to users through large scale phishing attack or online scam	Nefarious activity Eavesdropping/Interception/Hijacking	Relevant threats from this category are: Malicious code, abuse of authentication, information leakage, identity fraud, data forging, etc. (see also corresponding threats in threat taxonomy)

Significant disruption of critical infrastructures or services	Outages Failures/Malfunctions Physical Attack Unintentional Damages Eavesdropping/Interception/Hijacking Disasters Nefarious Activity/Abuse of Assets legal	
Massive failure of networks due to interruption of electricity supply or other support systems	Disasters Outages Failures/Malfunctions Physical Attack Unintentional Damages Nefarious Activity	
IoT exploitation	Nefarious Activity Eavesdropping/Interception/Hijacking Physical Attack Outages	Just as in other IT-assets, outages may cause exploitation opportunities for IoT devices

ANNEX D: MAPPING OF STAKEHOLDERS TO ASSETS

Stakeholder	Relevant Asset (Groups) (non-prioritized)	Degree of relevance (RACI Model[67])
Service customers (SC)	User Equipment Human Assets (end-user) Security Controls	Responsible Accountable Informed
Service providers (SP)	Business Services Business Applications Physical Infrastructure Security Controls Data Data Network Management Processes Policy Legal Human Assets Management and Orchestration Protocols	Responsible Accountable Consulted Informed
Mobile Network Operator (NOP or MNO)	Transport Security Controls Protocols Software Defined Network Business Services Business Applications Management Processes Policy Legal Human Assets Physical Infrastructure Data Data Storage Data Network Management and Orchestration	Responsible Accountable Consulted Informed
Virtualisation Infrastructure Service Providers (VISP)	Network Function Virtualisation Cloud Virtualisation Software Defined Network Management and Orchestration Management Processes Human Assets Protocols	Responsible Accountable Consulted Informed

[67] https://www.projectsmart.co.uk/raci-matrix.php, accessed November 2019.

Data Centre Providers (DCSP)	Network Function Virtualisation Cloud Virtualisation Software Defined Network Management and Orchestration Management Processes Physical Infrastructure Human Assets Protocols	Responsible Accountable Consulted Informed
Mobile Network Operator (NOP or MNO)	Transport Security Controls Protocols Software Defined Networks Business Services Business Applications Management Processes Policy Legal Human Assets Physical Infrastructure Data Data Storage Data Network	Responsible Accountable Consulted Informed
Internet Exchange Points (IXPs)	Data Network Physical Infrastructure	Responsible Accountable Consulted
National Regulators (NRAs)	Legal Data (Incident) Policy Radio access network (frequencies)	Consulted Informed
Information sharing and analysis centres (ISACs)	Data Management Processes Policy	Consulted Informed
National cybersecurity coordinators/agencies/centres (NCSCs)	Legal Data Policy Security Controls Human Assets Lawful Interception Management Processes Data Storage Business Applications Physical Infrastructure	Responsible Accountable Consulted Informed
National 5G Test Centres (NTCs)	Data Management Processes Security Controls	Responsible Accountable Consulted

	Physical Infrastructure **Human Assets**	**Informed**
National Certification Authorities (NCAs)	**All assets (as potential Targets of Certification – ToCs)**	**Accountable** **Consulted** **Informed** **Responsible (maintenance of assets accreditation, certification schemes)**
Competent EU institutions and European Commission Services	**All assets (as potential subject to preparation of policies)**	**Consulted** **Informed** **(regarding policy actions related to 5G assets)**

ABOUT ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its Member States, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU Member States in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU Member States by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-306-3
DOI:10.2824/49299